Reprint from

ISSN 2220-5438

# Moscow Journal *of Combinatorics and Number Theory*

URSS

МФТИ

Volume 6 • Issue 2–3 2016

Moscow Journal of Combinatorics and Number Theory Volume 6 • Issue 2–3 2016

Moscow Journal
of Combinatorics
and Number Theory
2016, vol. 6, iss. 2–3,
pp. 14–37, [pp. 130–153]

# On a quartic equation and two families of hyperquadratic continued fractions in power series fields

Khalil Ayadi (Sfax), Alain Lasjaunias (Bordeaux)

Dedicated to David P. Robbins (1942–2003)

**Abstract:** Casually introduced thirty years ago, a simple algebraic equation of degree 4, with coefficients in $\mathbb{F}_p[T]$, has a solution in the field of power series in $1/T$, over the finite field $\mathbb{F}_p$. For each prime $p > 3$, the continued fraction expansion of this solution is remarkable and it has a different general pattern according to the remainder, 1 or 2, in the division of $p$ by 3. We describe two very large families of algebraic continued fractions, each containing these solutions, according to the class of $p$ modulo 3. We compute the irrationality measure for these algebraic continued fractions and, as a consequence, we obtain two different values for the solution of the quartic equation, only depending on the class of $p$ modulo 3.

**Keywords:** Continued fractions, Finite fields, Fields of power series

**AMS Subject Classification:** 11J70, 11T55

**Received:** 11.12.2014; **revised:** 20.05.2016

## 1. Introduction

Throughout this note $p$ is an odd prime number and $\mathbb{F}_p$ is the finite field with $p$ elements. We consider an indeterminate $T$ and $\mathbb{F}_p((T^{-1}))$, here simply denoted by $\mathbb{F}(p)$, the field of power series in $1/T$ over the finite field $\mathbb{F}_p$. A non-zero element of $\mathbb{F}(p)$ is

$$\alpha = \sum_{i \le i_0} u_i T^i \quad \text{where} \quad i \in \mathbb{Z}, u_i \in \mathbb{F}_p \quad \text{and} \quad u_{i_0} \neq 0.$$

An ultrametric absolute value is defined over this field by $| \alpha |=| T |^{i_0}$ where $| T |$ is a fixed real number greater than 1. We will also consider the subset $\mathbb{F}(p)^+ = \{\alpha \in \mathbb{F}(p) \quad s.t. \mid \alpha |> 1\}$. Note that $\mathbb{F}(p)$ is the completion of the field $\mathbb{F}_p(T)$ for this absolute value. The fields $\mathbb{F}(p)$ are analogues of the field of real numbers, consequently many questions in number theory in the context of real numbers, such as Diophantine approximation and continued fractions, can be transposed in the frame of formal power series which is considered here. We are concerned with continued fractions for elements of this field $\mathbb{F}(p)$ which are algebraic over the field $\mathbb{F}_p(T)$.

The starting point of our work is a particular quartic equation, with coefficients in $\mathbb{F}_p[T]$, where $p$ is an arbitrary prime greater than 3. This algebraic equation is the following:

$$(9/32)X^4 - TX^3 + X^2 - 8/27 = 0. \tag{$E$}$$

The origin of this equation is due to Mills and Robbins [13]. Mills and Robbins actually considered another equation: $(E_1)\quad X^4 + X^2 - TX + 1 = 0$. The very simple form of this last equation explains why it was considered by chance, while searching for promising algebraic continued fraction expansions. Using a computer, Mills and Robbins observed that $(E_1)$ has a root in $\mathbb{F}(13)$ presenting a remarkable continued fraction expansion. This continued fraction expansion could only be partially conjectured in [13] and only later, in a complicated form, fully conjectured in [3]. Finally, the conjecture concerning the continued fraction of the solution of $(E_1)$ in $\mathbb{F}(13)$ was proved in [6]. In [8], it has been remarked that Mills and Robbins equation $(E_1)$ could be considered for each characteristic $p > 3$, by reading $X^4 + X^2 - TX - 1/12 = 0$. After an adequate transformation, this led to the above equation $(E)$ (possibly, see [8, p. 30]).

For each prime $p > 3$, $(E)$ has a unique root in $\mathbb{F}(p)^+$, denoted by $\alpha(p)$. This root can be expanded as an infinite continued fraction. The continued fraction for $\alpha(p)$ varies according to the value of $p$ but, for all $p$, it appears to have a singular pattern. Moreover, observations by computer show that there are two different general patterns, according to the case considered: $p \equiv 1 \bmod 3$ or $p \equiv 2 \bmod 3$.

The first case, $p \equiv 1 \bmod 3$ (and particularly $p = 13$), has been extensively studied by the second author and this study has generated different works in the area of continued fractions in power series fields [5–8]. To show the differences and the similarities between both cases, we will recall several results already known for the first case. It will appear that the continued fraction expansion for the solution of $(E)$ belongs to two large families of expansion, according to the remainder of $p$ modulo 3. Hence, the great interest of our equation will be to give us the opportunity to introduce and to describe these families.

In order to illustrate our subject and to provoke the curiosity of the reader, we show, at the end of this introduction, what could be seen on a computer screen when considering the first few hundred of partial quotients of the solution $\alpha(p)$ of $(E)$, for the first two values of $p$. Note that the partial quotients, which are quickly very large, are only represented there by their degree in the indeterminate $T$. See Figure 1 and Figure 2.

If the solution of $(E)$ has a peculiar continued fraction expansion, for each $p > 3$, this is due to the fact that this element is hyperquadratic. Let $t \geq 0$ be an integer and $r = p^t$, an irrational element of $\mathbb{F}(p)$ will be called hyperquadratic of order $t$ if it satisfies a non-trivial algebraic equation of the following form

$$uX^{r+1} + vX^r + wX + z = 0 \quad \text{where} \quad (u, v, w, z) \in (\mathbb{F}_p[T])^4.$$

Note that a hyperquadratic element of order 0 is simply irrational quadratic. We shall see that the solution of $(E)$ is hyperquadratic of order 1 if $p \equiv 1 \bmod 3$ and hyperquadratic of order 2 if $p \equiv 2 \bmod 3$. The reader may consult the introduction of [2] for more precisions and references on hyperquadratic elements. Hyperquadratic power series in $\mathbb{F}(p)$ have long been considered by mathematicians studying Diophantine approximation in function fields of positive characteristic, such as Mahler [10], Osgood [12], Voloch [15] and de Mathan [11]. Simultaneously, other mathematicians, such as Baum and Sweet [1] or Mills and Robbins [13], have observed that the continued fraction expansion of certain hyperquadratic elements could be explicitly given. For a survey on the different contributions of these mathematicians in this area, the reader is refered to [4]. For a good account on continued fractions and Diophantine approximation in power series fields, as well as more references, see Schmidt's article [14].

We shall now describe briefly the continued fraction for the solution of $(E)$ in $\mathbb{F}(p)^+$. This root is expanded as an infinite continued fraction $\alpha(p) = [a_1, a_2, \ldots, a_n, \ldots]$, where the partial quotients $a_i$ are non-constant polynomials in $\mathbb{F}_p[T]$. From the equation, one can obtain the beginning of the power series expansion and we have $\alpha(p) = (32/9)T - 1/T + \dots$, which implies that $a_1 = (32/9)T$. To describe the sequence $(a_n)_{n\geq 1}$, in both cases, we need to introduce a particular polynomial in $\mathbb{F}_p[T]$ and two sequences of polynomials related to it.

Throughout this note $p$ is a prime with $p \geq 3$ (except when we consider $(E)$, where $p > 3$) and $k$ an integer with $1 \leq k < p/2$. Then we define

```
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 9, 41, 9, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 9, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 9, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 9, 41, 9, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 9, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 9, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 9,
41, 209, 1041, 209, 41, 9, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 9, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 9, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 9, 41, 9, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 9, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 9,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 9, 41, 9, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 9, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 9, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 9, 41,
209, 41, 9, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 9, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 9, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 9, 41, 9, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 9, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 9, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 9, 41, 9, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 9, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 9,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 9, 41, 209, 41, 9, 1, 1]
```

**Fig. 1.** Sequence of the degrees of p. q. for the solution $\alpha(5)$ of $(E)$ (450 p. q.)

```
[1, 1, 1, 3, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3, 1, 1, 1, 1, 17, 1, 1, 1, 1,
3, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3, 1, 1, 1, 1, 17, 1, 1, 1,
1, 3, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3, 1, 1, 1, 1, 17, 1, 1,
1, 1, 3, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3, 1, 1, 1, 1, 115,
1, 1, 1, 1, 3, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3, 1, 1, 1, 1,
17, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3, 1, 1, 1,
1, 17, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3, 1, 1,
1, 1, 17, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3, 1,
1, 1, 1, 17, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3,
1, 1, 1, 1, 115, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3, 1, 1, 1,
1, 3, 1, 1, 1, 1, 17, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3, 1, 1,
1, 1, 3, 1, 1, 1, 1, 17, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3, 1,
1, 1, 1, 3, 1, 1, 1, 1, 17, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3,
1, 1, 1, 1, 3, 1, 1, 1, 1, 17, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3, 1, 1, 1, 1,
3, 1, 1, 1, 1, 3, 1, 1, 1, 1, 115, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3, 1, 1,
1, 1, 3, 1, 1, 1, 1, 3, 1, 1, 1, 1, 17, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3, 1,
1, 1, 1, 3, 1, 1, 1, 1, 3, 1, 1, 1, 1, 17, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3,
1, 1, 1, 1, 3, 1, 1, 1, 1, 3, 1, 1, 1, 1, 17, 1, 1, 1, 1, 3, 1, 1, 1, 1]
```

**Fig. 2.** Sequence of the degrees of p. q. for the solution $\alpha(7)$ of $(E)$ (430 p. q.)

$P_k(T) = (T^2 - 1)^k \in \mathbb{F}_p[T]$. From $P_k$, we introduce in $\mathbb{F}_p[T]$ two sequences of polynomials $(A_n)_{n\geq 0}$ and $(B_n)_{n\geq 0}$ as follows. The first one is defined by

$$A_0 = T \quad \text{and recursively} \quad A_{n+1} = [A_n^p/P_k] \quad \text{for} \quad n \geq 0.$$

Here the brackets denote the integral (i. e. polynomial) part of the rational function. While the second one is defined by

$$B_0 = A_0 = T \quad \text{and} \quad B_1 = A_1 = [T^p/P_k]$$

and recursively

$$B_{n+1} = B_n^p P_k^{(-1)^{n+1}} \quad \text{for} \quad n \geq 1.$$

We are particularly interested in the degrees of these polynomials. We set $u_n = \deg(A_n)$ and $v_n = \deg(B_n)$. From the recursive definition of these polynomials, we get $u_0 = v_0 = 1$ and also

$$u_{n+1} = pu_n - 2k \quad \text{and} \quad v_{n+1} = pv_n + 2k(-1)^{n+1} \quad \text{for} \quad n \geq 0.$$

Note that the sequence $(u_n)_{n\geq 0}$ is constant if $2k = p-1$, then we have $A_n = A_0 = T$ for $n \geq 0$. Otherwise, both sequences $(u_n)_{n\geq 0}$ and $(v_n)_{n\geq 0}$ are strictly increasing. Note that, for $p = 5$ and $k = 2$, we get: $(v_n)_{n\geq 0} = 1, 1, 9, 41, 209, 1041, \ldots$ Whereas, for $p = 7$ and $k = 2$, we obtain $(u_n)_{n\geq 0} = 1, 3, 17, 115, 801, \ldots$
(See below and also Figure 1 and Figure 2.)

In the first case, $p \equiv 1 \bmod 3$, we set $k = (p-1)/3$ and we consider the sequence $(A_n)_{n\geq 1}$, introduced above. In [8], it has been proved (with a bound on the prime number $p$) that there exists a sequence $(\lambda_n)_{n\geq 1}$ in $\mathbb{F}_p^*$ and a sequence $(i(n))_{n\geq 1}$ in $\mathbb{N}$, such that

$$a_n = \lambda_n A_{i(n)} \quad \text{for} \quad n \geq 1. \qquad (I)$$

Both sequences $(\lambda_n)_{n\geq 1}$ and $(i(n))_{n\geq 1}$ have been given explicitly (see [7]).

In the second case, $p \equiv 2 \bmod 3$, we set $k = (p+1)/3$ and we consider the sequence $(B_n)_{n\geq 1}$ introduced above. Our observation, based on computer calculations giving a finite number of partial quotients, implies the following conjecture: there exists a sequence $(\lambda_n)_{n\geq 1}$ in $\mathbb{F}_p^*$ and a sequence $(i(n))_{n\geq 1}$ in $\mathbb{N}$, such that

$$a_n = \lambda_n B_{i(n)} \quad \text{for} \quad n \geq 1. \qquad (II)$$

In the first case, the formulas giving the sequence $(\lambda_n)_{n\geq 1}$ are quite sophisticated, as can be seen for instance for $p = 13$ in [3, 6]. Moreover, our proof and, consequently, the method to obtain this sequence are complicated (see [5, 7]). For these reasons, in the second case, we have not tried to describe the sequence $(\lambda_n)_{n\geq 1}$, even conjecturally. However, in this second case, we obtain the description of the sequence $(i(n))_{n\geq 1}$ as a consequence of a conjecture about more general continued fractions. The tools used to obtain a proof, in the first case, might well be applied in the second case, but we are aware that a different approach would be desirable. This note is complementary to [8], and hopefully it may shed new light on this mysterious quartic equation.

We sketch here the organization of this work. To obtain the proof in the first case, it has been necessary to consider hyperquadratic continued fractions more general than the one of the root of $(E)$. It happens that the same argument is true for the second case. In the next section we shall introduce these families, which we will call $P_k$-expansions of first kind and of second kind. In section 3, we will define and describe partially some $P_k$-expansions, which we call perfect. In section 4, we show that the solution of $(E)$ is a perfect $P_k$-expansion of first kind if $p \equiv 1 \bmod 3$ and of second kind if $p \equiv 2 \bmod 3$. In the last section, we give a measure of the growth of the degrees of the partial quotients (the irrationality measure of the continued fraction) for the perfect $P_k$-expansions in both cases. We apply it to the solution of $(E)$ and we get the irrationality measure for $\alpha(p)$, equal to $8/3$ in the first case and equal to 4 in the second one.

## 2. $P_k$-expansions

Concerning continued fractions in this area, we use classical notation, as they can be found for instance in the second section of [9]. Throughout the paper we are dealing with finite sequences (or words), consequently we recall the following notation on sequences in $\mathbb{F}_p[T]$. Let $W = w_1, w_2, \ldots, w_n$ be such a finite sequence, then we set $|W| = n$ for the length of the word $W$. If we have two words $W_1$ and $W_2$, then $W_1, W_2$ denotes the word obtained by concatenation. Moreover, if $y \in \mathbb{F}_p^*$, then we define $y \cdot W$ as the following sequence

$$y \cdot W = yw_1, y^{-1}w_2, \ldots, y^{(-1)^{n-1}}w_n.$$

As usual, we denote by $[W] \in \mathbb{F}_p(T)$ the finite continued fraction $w_1+1/(w_2+1/(\ldots))$. In this formula the $w_i$, called the partial quotients, are non-constant polynomials.

Still, we will also use the same notation if the $w_i$ are constant and the resulting quantity is in $\mathbb{F}_p$. However in this last case, by writing $[w_1, w_2, \ldots, w_n]$ we assume that this quantity is well defined in $\mathbb{F}_p$, i. e. $w_n \neq 0$, $[w_{n-1}, w_n] \neq 0, \ldots, [w_2, \ldots, w_n] \neq 0$. We use the notation $\langle W \rangle$ for the continuant built from $W$. We denote by $W'$ (resp. $W''$) the word obtained from $W$ by removing the first (resp. last) letter of $W$. Hence, we recall that we have $[W] = \langle W \rangle / \langle W' \rangle$. We let $W^* = w_n, w_{n-1}, \ldots, w_1$, be the word $W$ written in reverse order. We also have $[W^*] = \langle W \rangle / \langle W'' \rangle$. It is also known that $[y \cdot W] = y[W]$.

If $\alpha \in \mathbb{F}(p)$ is an infinite continued fraction, $\alpha = [a_1, a_2, \ldots, a_n, \ldots]$, we set $x_n = \langle a_1, a_2, \ldots, a_n \rangle$ and $y_n = \langle a_2, \ldots, a_n \rangle$. In this way, we have $x_n/y_n = [a_1, a_2, \ldots, a_n]$, with $x_1 = a_1$, $y_1 = 1$ and by convention $x_0 = 1$, $y_0 = 0$. Recall that, if $\alpha_{n+1} = [a_{n+1}, a_{n+2}, \ldots]$ is the tail of the expansion, we have $\alpha = (x_n\alpha_{n+1} + x_{n-1})/(y_n\alpha_{n+1} + y_{n-1})$, for $n \geq 1$.

As above $p$ is an odd prime and $k$ an integer with $1 \leq k < p/2$. Linked to the previous polynomial mentioned above: $P_k(T) = (T^2 - 1)^k$, we introduce a second polynomial $Q_k$ in $\mathbb{F}_p[T]$. We define

$$\omega_k = (-1)^k 2k \prod_{1 \leq i \leq k} (1 - 1/2i) \in \mathbb{F}_p^* \quad \text{and} \quad Q_k = \omega_k^{-1}(A_1P_k - T^p).$$

This pair $(P_k, Q_k)$ of polynomials was introduced in [5]. Note that $Q_k$ is simply, up to a constant factor, the remainder in the Euclidean division of $T^p$ by $P_k$. This second polynomial can also be defined by (see [5, p. 341])

$$Q_k(T) = \int_0^T (x^2 - 1)^{k-1}\,dx = \sum_{0 \leq i \leq k-1} (-1)^{k-1-i} \binom{k-1}{i} (2i+1)^{-1} T^{2i+1}.$$

Note that we also have $Q_k(1) = -\omega_k^{-1}$. We recall the following stated and proved in [5, p. 332].

Proposition 0. *Let* $l \geq 1$ *be an integer and* $(a_1, a_2, \ldots, a_l) \in (\mathbb{F}_p[T])^l$, *with* $\deg(a_i) > 0$ *for* $1 \leq i \leq l$. *Let* $r = p^t$ *with* $t > 0$ *and* $(P, Q) \in (\mathbb{F}_p[T])^2$ *with* $\deg(Q) < \deg(P) < r$. *Then there exists a unique infinite continued fraction* $\alpha = [a_1, a_2, \ldots, a_l, \alpha_{l+1}] \in \mathbb{F}(p)^+$ *satisfying*

$$\alpha^r = P\alpha_{l+1} + Q. \qquad (*)$$

*This element* $\alpha$ *is the unique root in* $\mathbb{F}(p)^+$ *of the following algebraic equation*:

$$y_l X^{r+1} - x_l X^r + (P y_{l-1} - Q y_l) X - P x_{l-1} + Q x_l = 0. \qquad (**)$$

As above, let $\alpha$ be defined by the $l$-tuple, $(a_1, a_2, \dots, a_l)$, and the equality $(*)$. Then we set the following definitions.

- $\alpha$ *is a* $P_k$*-expansion of first kind if* $r = p$ *and there exists* $(\epsilon_1, \epsilon_2) \in (\mathbb{F}_p^*)^2$ *such that* $(P, Q) = (\epsilon_1 P_k, \epsilon_2 Q_k)$.
- $\alpha$ *is a* $P_k$*-expansion of second kind if* $r = p^2$ *and there exists* $(\epsilon_1, \epsilon_2) \in (\mathbb{F}_p^*)^2$ *such that* $(P, Q) = (\epsilon_1 P_k^{p-1}, \epsilon_2 Q_k^p)$.

The importance of the pair $(P_k, Q_k)$ appears in the following proposition (see [5, p. 341], and note that $\omega_k$ was defined differently there than it is here).

PROPOSITION 1. *Let* $W_1$ *be the finite word such that* $P_k/Q_k = [W_1]$. *Then we have*

$$W_1 = v_1 T, \dots, v_i T, \dots, v_{2k} T,$$

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

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

*Furthermore we have* $W_1 = -\omega_k^2 \cdot W_1^*$.

From this proposition, using a technical lemma stated below, the sequence of partial quotients for certain $P_k$-expansion of first kind could be given explicitly, as we will see in the next section. This lemma is the following (see the origin in [5, p. 336 and p. 343] or [9, Section 2]).

LEMMA 1. *Let* $A \in \mathbb{F}_p[T]$, $\delta \in \mathbb{F}_p^*$ *and* $X \in \mathbb{F}(p)$. *Then we have*

$$A + \delta Q_k P_k^{-1} + X = [A, \delta^{-1} \cdot W_1, X'],$$

*where*

$$X' = X^{-1} P_k^{-2} + \omega_k^2 \delta^{-1} Q_k P_k^{-1}.$$

We shall use this lemma to establish the continued fraction for the rational $P_k^{p-1}/Q_k^p$. This continued fraction will be fundamental to study $P_k$-expansions of second kind. We have the following proposition.

Proposition 2. *Let $W_2$ be the finite word such that $P_k^{p-1}/Q_k^p = [W_2]$. Then $W_2$ is obtained from $W_1$ in the following way*:

$$W_2 = v_1A_1, w_1 \cdot W_1, v_2A_1, w_2 \cdot W_1, \dots, v_{2k-1}A_1, w_{2k-1} \cdot W_1, v_{2k}A_1,$$

*where the numbers $w_i \in \mathbb{F}_p^*$ are defined by*

$$w_i^{-1} = -\omega_k[v_i, v_{i-1}, \dots, v_1] \quad \textit{for} \quad 1 \leq i \leq 2k-1.$$

Proof. We have $P_k/Q_k = [v_1T, \dots, v_{2k}T]$. Since $P_k(1) = 0$ and $Q_k(1) \neq 0$, we obtain $[v_1, \dots, v_{2k}] = 0$ and $[v_i, \dots, v_1] \in \mathbb{F}_p^*$ for $1 \leq i \leq 2k-1$. We set $\alpha = [W_1]$ and $\beta = [W_2]$. Since $\alpha^p = [v_1T^p, \alpha_2^p]$, we have

$$\beta = (P_k/Q_k)^p P_k^{-1} = \alpha^p P_k^{-1} = [v_1T^p, \alpha_2^p]P_k^{-1} = [v_1T^pP_k^{-1}, P_k\alpha_2^p].$$

Since we have $T^p = A_1P_k - \omega_kQ_k$, the last equality becomes

$$\beta = v_1A_1 - \omega_kv_1Q_kP_k^{-1} + P_k^{-1}\alpha_2^{-p}.$$

Applying Lemma 1, with $\delta = -\omega_kv_1 = w_1^{-1}$ and $X = P_k^{-1}\alpha_2^{-p}$, we obtain

$$\beta = [v_1A_1, w_1 \cdot W_1, X'],$$

where

$$X' = P_k^{-1}\alpha_2^p + \omega_k^2w_1Q_kP_k^{-1}.$$

Since $|\alpha_2| = |T|$, we have $|X'| > 1$. Consequently, we get

$$b_1, \dots, b_{2k+1} = v_1A_1, w_1 \cdot W_1 \quad \text{and} \quad X' = \beta_{2k+2}.$$

Hence, with $\alpha_2^p = [v_2T^p, \alpha_3^p]$, this implies

$$\beta_{2k+2} = [v_2T^pP_k^{-1}, P_k\alpha_3^p] + \omega_k^2w_1Q_kP_k^{-1}.$$

Again, using $T^p = A_1P_k - \omega_kQ_k$ and applying the same lemma, with $\delta = -\omega_kv_2 + {}$ ${} + \omega_k^2w_1 = w_2^{-1}$ and $X = P_k^{-1}\alpha_3^{-p}$, we get

$$\beta_{2k+2} = [v_2A_1, w_2 \cdot W_1, X'],$$

where

$$X' = P_k^{-1}\alpha_3^p + \omega_k^2 w_2 Q_k P_k^{-1}.$$

As above, we get the desired partial quotients, from the rank $2k+2$ to the rank $4k+2$, and also $X' = \beta_{4k+3}$. The process carries on until we get

$$\beta_{4k^2-2k-1} = [v_{2k-1}A_1, w_{2k-1} \cdot W_1, X'],$$

where

$$\beta_{4k^2} = X' = P_k^{-1}\alpha_{2k}^p + \omega_k^2 w_{2k-1} Q_k P_k^{-1} = v_{2k} T^p P_k^{-1} + \omega_k^2 w_{2k-1} Q_k P_k^{-1}.$$

Again, using $T^p = A_1 P_k - \omega_k Q_k$, this becomes

$$\beta_{4k^2} = v_{2k}A_1 + \omega_k Q_k P_k^{-1}(\omega_k w_{2k-1} - v_{2k}).$$

But we have

$$\omega_k w_{2k-1} - v_{2k} = -[v_{2k-1}, \dots, v_1]^{-1} - v_{2k} = -[v_{2k}, v_{2k-1}, \dots, v_1] = 0.$$

Hence $\beta_{4k^2} = v_{2k}A_1$ and the proof of the proposition is complete.

We make a last remark on the continued fraction for $P_k^{p-1}/Q_k^p$. As for $W_1$, it can be seen that we also have $W_2 = -\omega_k^2 \cdot W_2^*$. It follows from this equality that the very same lemma as Lemma 1, holds in the second case when the pair $(P_k, Q_k)$ is replaced by the pair $(P_k^{p-1}, Q_k^p)$ and $W_1$ is replaced by $W_2$. In this way, $P_k$-expansions of second kind could possibly be studied following the same path as in the first case [5, 7]. However, as explained in the introduction, in the present work, we will leave this way aside. Instead, by intensive use of computer calculations, we have obtained a conjecture on $P_k$-expansions of second kind which is presented in the next section. □

## 3. Perfect $P_k$-expansions

If $p$ and $k$ are fixed, we recall that a $P_k$-expansion is defined by the $(l+2)$-tuple $(a_1, a_2, \dots, a_l, \epsilon_1, \epsilon_2) \in (\mathbb{F}_p[T])^l \times (\mathbb{F}_p^*)^2$. Once such a $(l+2)$-tuple is fixed, from the algebraic equation $(**)$, a computer can give the first partial quotients of the expansion, then it appears that some expansions are more "regular" than others. To be more precise, we use the following terminology. If $P \in \mathbb{F}_p[T]$, we say that $P$ is of type A (resp. of type B) if there exist $\lambda \in \mathbb{F}_p^*$ and $n \in \mathbb{N}$ such that $P = \lambda A_n$ (resp. $P = \lambda B_n$), where the polynomials $A_n$ (or $B_n$) belong to the sequences defined in the introduction. Then we say that a $P_k$-expansion of first kind (resp. of second kind) is perfect if every partial quotient is of type A (resp. of type B). It appears that a particular condition on the $(l+2)$-tuple $(a_1, a_2, \ldots, a_l, \epsilon_1, \epsilon_2)$ can be given, in order to have a perfect $P_k$-expansion and a description of the corresponding sequence of partial quotients is possible. This is what is discussed in this section, distinguishing each of both cases.

We will use the following notation. For $n \geq 0$, if we have the word $w, w, \ldots, w$ of length $n$, then we denote it shorly by $w^{[n]}$ with $w^{[0]} = \varnothing$. In the same way $W^{[n]}$ denotes the word $W, W, \ldots, W$ where the finite word $W$ is repeated $n$ times and $W^{[0]} = \varnothing$. If we have a finite sequence $W = w_1, w_2, \ldots, w_n$ of polynomials of type A (or of type B), we can associate it to a finite sequence $I = i_1, i_2, \ldots, i_n$ of positive integers, such that $w_m = \lambda_m A_{i_m}$ (or $w_m = \lambda_m B_{i_m}$), with $\lambda_m \in \mathbb{F}_p^*$ for $1 \leq m \leq n$. Let $I_1$ (resp. $I_2$) denote the sequence of integers attached to the word $W_1$ (resp. $W_2$) introduced in the previous section. Then, with this notation, we have

$$I_1 = 0^{[2k]} \quad \text{and} \quad I_2 = 1, (0^{[2k]}, 1)^{[2k-1]}.$$

Our aim is to describe the infinite sequence of integers associated to the infinite sequence of partial quotients for a perfect $P_k$-expansion. In each case, the sequences $I_1$ or $I_2$ are the stones from which this sequence is built.

### A) Perfect $P_k$-expansions of first kind

Let us consider a $P_k$-expansion of first kind. We have the following statement.

THEOREM A. *Let $p$ be an odd prime and $(k, l)$ as above. Let $\alpha \in \mathbb{F}(p)$ be a $P_k$-expansion of first kind, depending as above on the $(l+2)$-tuple $(a_1, a_2, \ldots, a_l, \epsilon_1, \epsilon_2) \in$ $\in (\mathbb{F}_p[T])^l \times (\mathbb{F}_p^*)^2$. We assume that this $(l+2)$-tuple satisfies the following hypothesis $\mathcal{H}(1)$: We have $(a_1, \ldots, a_l) = (\lambda_1 T, \ldots, \lambda_l T)$, where $\lambda_i \in \mathbb{F}_p^*$ for $1 \leq i \leq l$, together with the following condition*

$$[\lambda_l, \lambda_{l-1}, \ldots, \lambda_1 + \omega_k^{-1}\epsilon_2] = 2k\epsilon_1/\epsilon_2.$$

*Then there exists a sequence* $(\lambda_n)_{n\geq 1}$ *in* $\mathbb{F}_p^*$ *and a sequence* $(i(n))_{n\geq 1}$ *in* $\mathbb{N}$, *such that*

$$a_n = \lambda_n A_{i(n)} \quad \textit{for} \quad n \geq 1. \tag{1}$$

*Moreover, the sequence* $(i(n))_{n\geq 1}$, *with the above notation, is described as follows. Let* $(V_n)_{n\geq 0}$ *be the sequence of finite words of integers defined recursively by*

$$V_0 = 0 \quad \textit{and} \quad V_n = n, V_0^{[2k]}, V_1^{[2k]}, \dots, V_{n-1}^{[2k]}, \quad \textit{for } n \geq 1. \tag{2}$$

*Then the sequence* $(i(n))_{n\geq 1}$ *in* $\mathbb{N}$ *is given by the infinite word*:

$$V_0^{[l]}, V_1^{[l]}, V_2^{[l]}, \dots, V_n^{[l]}, \dots \tag{3}$$

Note, as indicated above, that the existence of the square bracket in $\mathcal{H}(1)$ implies a restricted choice of the $(l+2)$-tuple. Indeed one can check that there are exactly $(p-1)(p-2)^l$ such $(l+2)$-tuples in $(\mathbb{F}_p^*)^{l+2}$. The results stated in Theorem A have been proved in previous works (see [5, 7, 8]). Here, we have choosen the first $l$ partial quotients proportional to $A_0$, but it was remarked in [8] that a more general situation could have been considered. Moreover, the extremal case $k = (p-1)/2$ is interesting, since then $A_i = A_0$. It conduces to perfect expansions having all partial quotients proportional to $T$. In a joint work with J.-Y. Yao [9], the second author, following a similar method, could obtain $P_k$-expansions of first kind having all partial quotients of degree 1, starting from $l$ partial quotients of degree 1, not necessarily proportional to $T$. In a more general setting, particularly if the base field is not prime, the hypothesis $\mathcal{H}(1)$ is only a sufficient condition to have (1). In this larger context [7, p. 256], both sequences $(\lambda_n)_{n\geq 1}$ and $(i(n))_{n\geq 1}$ have been described. However, we do not give here indications on the sequence $(\lambda_n)_{n\geq 1}$ which is obtained by sophisticated recursive formulas from the initial $l$-tuple $(\lambda_1, \lambda_2, \dots, \lambda_l)$ and the pair $(\epsilon_1, \epsilon_2)$.

### B) Perfect $P_k$-expansions of second kind

Let us consider a $P_k$-expansion of second kind. We shall present here a conjecture in order to have all the partial quotients of type B. First, we make a comment on the origin of this conjecture. We started from the solution of $(E)$ for $p = 5, 11$ or $17$ and we obtained with a computer several thousands of partial quotients. This was not enough to guess the general pattern of this sequence of partial quotients. Inspired by the first case, we expected these particular expansions to belong to a much larger family. For small values of $p$, we knew that these expansions were generated in the way described above, i. e. were $P_k$-expansions of second kind (see [8, p. 33]). By observing the first $l$ partial quotients and the pair $(\epsilon_1, \epsilon_2)$ in these three cases, we could guess the right form of the $(l+2)$-tuple $(a_1, \ldots, a_l, \epsilon_1, \epsilon_2)$ in order to have a perfect expansion. It was only then, by considering a general $(l+2)$-tuple and letting the parameters $p, k$ and $l$ vary, that we could find the hypothesis $\mathcal{H}(2)$ and the description of the pattern for these continued fractions, given in the following conjecture.

Conjecture B. Let $p$ be an odd prime and $(k, l)$ as above. Let $\alpha \in \mathbb{F}(p)$ be a $P_k$-expansion of second kind, depending as above on the $(l+2)$-tuple $(a_1, a_2, \ldots, a_l, \epsilon_1, \epsilon_2) \in (\mathbb{F}_p[T])^l \times (\mathbb{F}_p^*)^2$. We assume that this $(l+2)$-tuple satisfies the following hypothesis $\mathcal{H}(2)$: Let $m \geq 1$ and $m$ integers $n_1, n_2 \ldots, n_m$ be such that

$$1 < n_1 < n_2 < \ldots < n_m \quad \text{with} \quad n_{i+1} - n_i \geq 3 \quad \text{for} \quad 1 \leq i < m.$$

We set $l = n_m$ and we consider a $l$-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_l) \in (\mathbb{F}_p^*)^l$ such that

$$[\lambda_1, \ldots, \lambda_{n_1-1}] \neq 0 \quad \text{and} \quad [\lambda_{n_i+1}, \ldots, \lambda_{n_{i+1}-1}] = 0 \quad \text{for} \quad 1 \leq i < m.$$

Then we assume that, for $1 \leq n \leq l$ and $i = 1 \ldots m$, we have

$$n \neq n_i \Rightarrow a_n = \lambda_n B_0 \quad \text{and} \quad n = n_i \Rightarrow a_n = \lambda_n B_1$$

and also

$$\epsilon_2 = -\omega_k[\lambda_1, \ldots, \lambda_{n_1-1}].$$

(Observe that the $m$-tuple $(\lambda_{n_1}, \lambda_{n_2} \ldots, \lambda_{n_m}) \in (\mathbb{F}_p^*)^m$ as well as $\epsilon_1 \in \mathbb{F}_p^*$ are chosen arbitrarily, while the existence of the square brackets in $\mathbb{F}_p$ implies restrictions on the choice of the remaining $\lambda_i$.)
Then there exists a sequence $(\lambda_n)_{n\geq 1}$ in $\mathbb{F}_p^*$ and a sequence $(i(n))_{n\geq 1}$ in $\mathbb{N}$, such that

$$a_n = \lambda_n B_{i(n)} \quad \text{for} \quad n \geq 1. \tag{4}$$

Moreover, the sequence $(i(n))_{n\geq 1}$ is described as follows. We define

$$l_1 = n_1 - 1 \quad \text{and} \quad l_{i+1} = n_{i+1} - n_i - 1 \quad \text{for} \quad 1 \leq i < m.$$

Let $V_0$ be the sequence of integers attached to the first $l$ partial quotients. According to the description made above, we can write

$$V_0 = 0^{[l_1]}, 1, 0^{[l_2]}, 1, \dots, 1, 0^{[l_m]}, 1. \tag{5}$$

We introduce the following sequence $(J_n)_{n\geq 1}$ of words, defined recursively by $J_1 = = 0^{[2k]}, 1$ and

$$J_{n+1} = (2n, 2n-1, J_n^{[2k-1]})^{[2k-1]}, 2n, 2n+1 \quad \text{for } n \geq 1. \tag{6}$$

Next, for $1 \leq i \leq m$ and $n \geq 1$, we define

$$V_{n,i} = (2n, 2n-1, J_n^{[2k-1]})^{[l_i-1]}, 2n, 2n+1. \tag{7}$$

Then the sequence $(i(n))_{n\geq 1}$ in $\mathbb{N}$ is given by the infinite word:

$$V_0, V_1, V_2, \dots, V_n, \dots \quad \text{where} \quad V_n = V_{n,1}, V_{n,2}, \dots, V_{n,m} \quad \text{for } n \geq 1. \tag{8}$$

Theorem A and Conjecture B, on perfect $P_k$-expansions, give each partial quotient up to a multiplicative constant in $\mathbb{F}_p^*$. Note that this gives the degree of each partial quotient. The growth of this sequence of degrees plays an important role in Diophantine approximation. We will see in the last section that Conjecture B is conforted by considerations of Diophantine approximation. Finally, let us repeat that we have not tried to describe, even conjecturally, the sequence of constants in (4), which depends on the $(l+1)$-tuple $(\lambda_1, \dots, \lambda_l, \epsilon_1)$.
In the sequel a perfect $P_k$-expansion is supposed to satisfy $\mathcal{H}(1)$ (first kind, Theorem A) or $\mathcal{H}(2)$ (second kind, Conjecture B). In the following section, we will show that the solution $\alpha(p)$ of $(E)$ belongs to one of these families, according to the remainder of $p$ modulo 3.

## 4. Link between $P_k$-expansions and the solution of $(E)$

In this section $p > 3$ is a prime. For $i = 1$ or $i = 2$, we define

$$k = (p + (-1)^i)/3 \quad \text{if} \quad p \equiv i \bmod 3.$$

Note that we have $k < p/2$ and $k$ is even. Hence we set $k = 2j$. We consider the finite words $W_1$ and $W_2$ defined in Section 2. We have $|W_1| = 2k$ and also

$|W_2| = 2k + (2k-1)|W_1| = 4k^2$. Hence, we can write

$$W_1 = v_1T, v_2T, \dots, v_{2k}T \quad \text{and} \quad W_2 = b_1, b_2, \dots, b_{4k^2}.$$

We introduce the following words:

$$\widehat{W_1} = v_{j+1}T, v_{j+2}T, \dots, v_{2k}T \quad \text{with} \quad \widehat{W_2} = b_{k^2+1}, b_{k^2+2}, \dots, b_{4k^2}.$$

We define $\epsilon(p) \in \mathbb{F}_p^*$ as follows:

$$\epsilon(p) = 32/(9v_{j+1}) \quad \text{if} \quad p \equiv 1 \bmod 3 \tag{9}$$

and

$$\epsilon(p) = 32/(9w_j^{(-1)^j} v_{3j+1}) \quad \text{if} \quad p \equiv 2 \bmod 3. \tag{10}$$

Then we define $\Lambda(p) \in (\mathbb{F}_p[T])^l$ in the following way:

$$\Lambda(p) = \epsilon(p) \cdot \widehat{W_1} \quad \text{if} \quad p \equiv 1 \bmod 3 \tag{11}$$

and

$$\Lambda(p) = \epsilon(p) \cdot \widehat{W_2} \quad \text{if} \quad p \equiv 2 \bmod 3. \tag{12}$$

Hence $l = |\Lambda(p)|$ and we have $l = 3j = (p-1)/2$, if $p \equiv 1 \bmod 3$, and $l = 3k^2 = (p+1)^2/3$, if $p \equiv 2 \bmod 3$. We define $\epsilon_2(p) \in \mathbb{F}_p^*$ as follows:

$$\epsilon_2(p) = -\epsilon(p)\omega_k[v_{j+1}, v_{j+2}, \dots, v_{2k-1}, 3v_{2k}/5] \quad \text{if} \quad p \equiv 1 \bmod 3 \tag{13}$$

and

$$\epsilon_2(p) = -\epsilon(p)\omega_k w_j^{(-1)^j}[v_{3j+1}, v_{3j+2}, \dots, v_{2k}] \quad \text{if} \quad p \equiv 2 \bmod 3. \tag{14}$$

Finally, we define $\epsilon_1(p) \in \mathbb{F}_p^*$, for $p \equiv 1 \quad \text{or} \quad 2 \bmod 3$, as follows:

$$\epsilon_1(p) = -\epsilon_2(p)\omega_k^{-2}\epsilon(p)^{(-1)^{l+1}}. \tag{15}$$

We have the following theorem.

THEOREM C. *Let $p > 3$ be a prime number. Let $\alpha(p)$ be the root of $(E)$ in $\mathbb{F}(p)$. If $p \equiv 1 \bmod 3$ (resp. $p \equiv 2 \bmod 3$) then $k = (p-1)/3$ (resp. $k = (p+1)/3$). Let $\beta(p) \in \mathbb{F}(p)$ be the $P_k$-expansion, of first kind if $p \equiv 1 \bmod 3$ and of second kind if $p \equiv 2 \bmod 3$, defined by the $(l+2)$-tuple $(\Lambda(p), \epsilon_1(p), \epsilon_2(p))$ described above. If $p \equiv 1 \bmod 3$ (resp. $p \equiv 2 \bmod 3$), then the hypothesis, on $\beta(p)$, $\mathcal{H}(1)$ of Theorem A (resp. $\mathcal{H}(2)$ of Conjecture B) is satisfied.*

*With a limitation on the size of p, we have $\alpha(p) = \beta(p)$ and consequently:*

*If $p \equiv 1 \bmod 3$, then the partial quotients of $\alpha(p)$ are of type A and the distribution of these partial quotients is the one described in Theorem A.*

*If $p \equiv 2 \bmod 3$, then, conjecturally, the partial quotients of $\alpha(p)$ are of type B and the distribution of these partial quotients is the one described in Conjecture B.*

PROOF. For $p > 3$, let $A \in \mathbb{F}_p[T][X]$ be the polynomial defined by $A(X) = (9/32)X^4 - TX^3 + X^2 - 8/27$. We set $(r, P, Q) = (p, P_k, Q_k)$ if $p \equiv 1 \bmod 3$, and otherwise $(r, P, Q) = (p^2, P_k^{p-1}, Q_k^p)$. From the $l$-tuple $\Lambda(p) = (a_1, a_2, \dots, a_l)$, we build the four continuants $x_l, y_l, x_{l-1}$ and $y_{l-1}$ in $\mathbb{F}_p[T]$. We introduce two polynomials $U$ and $V$ in $\mathbb{F}_p[T]$

$$U = \epsilon_1(p)Py_{l-1} - \epsilon_2(p)Qy_l \quad \text{and} \quad V = \epsilon_2(p)Qx_l - \epsilon_1(p)Px_{l-1},$$

and also $H$ in $\mathbb{F}_p[T][X]$, depending on $(\Lambda(p), \epsilon_1(p), \epsilon_2(p), P, Q)$, such that

$$H(\Lambda(p), \epsilon_1(p), \epsilon_2(p), P, Q; X) = y_l X^{r+1} - x_l X^r + UX + V.$$

Hence, $\alpha(p)$ is the unique root in $\mathbb{F}(p)^+$ of $A$ while, according to Proposition 0 stated in Section 2, $\beta(p)$ is the unique root in $\mathbb{F}(p)^+$ of $H$. Consequently, we will obtain $\alpha(p) = \beta(p)$ if we can prove that the polynomial $A$ divides the polynomial $H$ in the ring $\mathbb{F}_p[T][X]$. This division is established by straightforward computations with the help of a computer. It follows that, in both cases, the result holds with a bound on the prime number $p$, even though there is no reason to doubt that the same is true for all primes $p$. To complete the proof of the theorem, it is enough to check that the $(l+2)$-tuple $(\Lambda(p), \epsilon_1(p), \epsilon_2(p))$ satisfies $\mathcal{H}(1)$ (resp. $\mathcal{H}(2)$) if $p \equiv 1 \bmod 3$ (resp. if $p \equiv 2 \bmod 3$).

Let us consider the first case: $p \equiv 1 \bmod 3$. According to the form of $\widehat{W_1}$, from (11), we get

$$a_i = \lambda_i T = \epsilon(p)^{(-1)^{i+1}} v_{j+i} T \quad \text{for} \quad 1 \leq i \leq l. \tag{16}$$

Thus, to have $\mathcal{H}(1)$ satisfied, we need have

$$[\lambda_l, \lambda_{l-1}, \dots, \lambda_1 + \omega_k^{-1}\epsilon_2(p)] = 2k\epsilon_1(p)/\epsilon_2(p).$$

This formula can be inversed and it is equivalent to

$$[\lambda_1, \lambda_2, \dots, \lambda_l - 2k\epsilon_1(p)/\epsilon_2(p)] = -\omega_k^{-1}\epsilon_2(p). \tag{17}$$

Using (15) and (16), recalling that $[\epsilon \cdot W] = \epsilon[W]$, for $\epsilon$ in $\mathbb{F}_p^*$, (17) becomes

$$\epsilon(p)[v_{j+1}, v_{j+2}, \dots, v_{2k-1}, v_{2k} + 2k\omega_k^{-2}] = -\omega_k^{-1}\epsilon_2(p). \tag{18}$$

From Proposition 1, we have $v_1 = 2k - 1 = -\omega_k^2 v_{2k}$. Since $k = -1/3$ in $\mathbb{F}_p^*$, we can write

$$v_{2k} + 2k\omega_k^{-2} = -v_{2k}/(2k-1) = 3v_{2k}/5. \tag{19}$$

Combining (18) and (19), we see that (17), and therefore $\mathcal{H}(1)$, are satisfied if

$$\epsilon_2(p) = -\epsilon(p)\omega_k[v_{j+1}, v_{j+2}, \dots, v_{2k-1}, 3v_{2k}/5].$$

which is the value that we assumed, in (13), for $\epsilon_2(p)$.
Let us now consider the second case: $p \equiv 2 \bmod 3$. We first check that $\Lambda(p)$ has the form required in $\mathcal{H}(2)$. For $1 \leq m \leq 2k$, we set $u_m = 2(m-1)k+m$. Proposition 2, giving the form of $W_2 = b_1, \dots, b_i, \dots, b_{4k^2}$, implies

$$b_i = \lambda B_1 \quad (\text{resp.} \quad \lambda B_0) \quad \text{if} \quad i = u_m \quad (\text{resp.} \quad i \neq u_m), \tag{20}$$

where $\lambda \in \mathbb{F}_p^*$. Moreover $i = u_m$ implies $\lambda = v_m$. We observe that we have $u_j < k^2 + 1 < u_{j+1}$. Consequently, the definition of $\widehat{W_2}$ implies

$$\widehat{W_2} = W_3, v_{j+1}B_1, w_{j+1} \cdot W_1, v_{j+2}B_1, \dots, v_{2k-1}B_1, w_{2k-1} \cdot W_1, v_{2k}B_1, \tag{21}$$

where $W_3$ is formed by the last $j$ letters of $w_j \cdot W_1$. Hence, we have

$$W_3 = w_j^{(-1)^j} v_{3j+1}T, w_j^{(-1)^{j+1}} v_{3j+2}T, \dots, w_j^{-1} v_{2k}T. \tag{22}$$

Since $\Lambda(p) = \epsilon(p) \cdot \widehat{W_2}$, with the notation introduced in Conjecture B, setting $n_i = j + u_i$ for $1 < i \leq 3j$, from (20), (21) and (22), we observe that $m = 3j$

and $\Lambda(p)$ has the form required in $\mathcal{H}(2)$. Also $n_i = i(2k+1) - 3j$ for $1 < i \leq 3j$, $l_1 = |W_3| = j$ and $l_i = 2k$ for $1 < i \leq 3j$. Moreover, from (21) and (22), the following equalities hold

$$[\lambda_1 T, \ldots, \lambda_{n_1-1} T] = [\epsilon(p) \cdot W_3] = \epsilon(p)[W_3] \tag{23}$$

and, for $1 \leq i < m$,

$$[\lambda_{n_i+1} T, \ldots, \lambda_{n_{i+1}-1} T] = [\epsilon(p)^{\pm 1} \cdot (w_{j+i} \cdot W_1)] = \epsilon(p)^{\pm 1} w_{j+i}[W_1]. \tag{24}$$

Since $[W_1]_{T=1} = (P_k/Q_k)_{T=1} = 0$, for $1 \leq i < m$, we observe that (24) implies the required condition

$$[\lambda_{n_i+1}, \ldots, \lambda_{n_{i+1}-1}] = \epsilon(p)^{\pm 1} w_{j+i}[W_1]_{T=1} = 0.$$

Moreover, by (22) and (23), we have

$$[\lambda_1, \ldots, \lambda_{n_1-1}] = \epsilon(p)[W_3]_{T=1} = \epsilon(p) w_j^{(-1)^j}[v_{3j+1}, \ldots, v_{2k}]. \tag{25}$$

Finally $\mathcal{H}(2)$ is fully satisfied if we have

$$\epsilon_2(p) = -\omega_k[\lambda_1, \ldots, \lambda_{n_1-1}]. \tag{26}$$

According to the value given to $\epsilon_2(p)$ in (14), we see that (25) implies (26). So the proof of the theorem is complete. □

## 5. Irrationality measure

Mahler [10], by an adaptation of an old and famous theorem on algebraic real numbers, due to Liouville, could prove the following theorem.
*Let $\alpha \in \mathbb{F}(p)$ be algebraic of degree $n > 1$ over $\mathbb{F}_p(T)$. Then there exists a positive real constant $C$ such that*

$$|\alpha - P/Q| \geq C|Q|^{-n} \quad \textit{for all} \quad P/Q \in \mathbb{F}_p(T).$$

The irrationality measure of an irrational power series $\alpha$ is defined by

$$\nu(\alpha) = -\limsup_{|Q|\to\infty} \log(|\alpha - P/Q|)/\log(|Q|).$$

by Roth's theorem, the irrationality measure of an irrational algebraic real number is 2. For power series over a finite field there is no analogue of Roth's theorem. However, according to Mahler's theorem, we have $\nu(\alpha) \in [2, n]$ if $\alpha$ is algebraic of degree $n > 1$ over $\mathbb{F}_p(T)$.

The irrationality measure is directly related to the growth of the sequence of the degrees of the partial quotients $a_n$ in the continued fraction expansion of $\alpha$. Indeed we have (see [4, p. 214])

$$\nu(\alpha) = 2 + \nu_0(\alpha) = 2 + \limsup_n (\deg(a_{n+1}) / \sum_{1 \le i \le n} \deg(a_i)). \tag{27}$$

This formula allows to compute $\nu(\alpha)$ if the continued fraction is explicitly known. Note that if $\alpha$ is a $P_k$-expansion then we have $\nu(\alpha) \in [2, r+1]$ and moreover if $\alpha(p)$ is the solution of $(E)$ we have $\nu(\alpha(p)) \in [2, 4]$. We shall compute the irrationality measure for perfect $P_k$-expansions and for the solution of $(E)$ in $\mathbb{F}(p)$. We have the following.

THEOREM D. *Let $p$ be an odd prime. Let $\alpha \in \mathbb{F}(p)$ be a perfect $P_k$-expansion. If $\alpha$ is of first kind then we have*

$$\nu(\alpha) = 2 + (p - 2k - 1)/l.$$

*According to Conjecture B, if $\alpha$ is of second kind then we have*

$$\nu(\alpha) = 2 + (p-1)(p-2k+1)\max(1/\nu_1, p/\nu_2),$$

*where $\nu_1 = m(p - 2k - 1) + l$ and $\nu_2 = \nu_1 + l_1(p^2 - 1) - 2k(p - 1)$.*
*Let $p > 3$ be a prime and $\alpha(p)$ be the root in $\mathbb{F}(p)$ of $(E)$. According to Theorem C, with a limitation on the size of the prime $p$, we have*

$$\nu(\alpha(p)) = 8/3 \quad \text{if} \quad p \equiv 1 \bmod 3$$

*and, conjecturally,*

$$\nu(\alpha(p)) = 4 \quad \text{if} \quad p \equiv 2 \bmod 3.$$

PROOF. We need the following notation. Let $W$ be a finite sequence $W = w_1, w_2, \ldots, w_n$ of polynomials of type A (or of type B), associated as above to the finite sequence

$I = i_1, i_2, \ldots, i_n$ of positive integers, such that $w_m = \lambda_m A_{i_m}$ (or $w_m = \lambda_m B_{i_m}$), where $\lambda_m \in \mathbb{F}_p^*$ for $1 \leq m \leq n$. We let $D(W)$ be the sum $\sum_{1\leq i\leq n} \deg(w_i)$ and, by extension, we define $D(I) = D(W)$.

We start with the first kind. Here, for $n \geq 1$, we have $a_n = \lambda_n A_{i(n)}$ and consequently $\deg(a_n) = u_{i(n)}$. From the recurrent definition of $A_n$, we have $u_n = (p^n(p-2k-1)+2k)/(p-1)$ for $n \geq 0$. To compute the limit in (27), we need to observe the first occurence of $u_n$ in the sequence of the degrees of the partial quotients, then compute the sum of all the degrees appearing before this term in this sequence. According to the description of $(i(n))_{n\geq 1}$ given by (2) and (3) in Theorem A, we see that $n$ appears for the first time at the begining of $V_n$. Hence, by (27), we have

$$\nu_0(\alpha) = \lim_n (u_n / D(V_0^{[l]}, V_1^{[l]}, V_2^{[l]}, \ldots, V_{n-1}^{[l]})). \tag{28}$$

Let us compute $D(V_n)$. We have $D(V_0) = u_0 = 1$ and also by (2)

$$D(V_n) = D(n, V_0^{[2k]}, V_1^{[2k]}, \ldots, V_{n-1}^{[2k]}) = u_n + 2k \sum_{1\leq i\leq n-1} D(V_i). \tag{29}$$

By induction, from (29), it is elementary to verify that $D(V_n) = p^n$ holds, for $n \geq 0$. Consequently (28) implies

$$\nu_0(\alpha) = \lim_n (u_n / l \sum_{1\leq i\leq n-1} p^i) = \lim_n (p^n(p-2k-1)+2k)/(l(p^n-1)).$$

Finally, we obtain

$$\nu_0(\alpha) = (p-2k-1)/l. \tag{30}$$

Note that $\nu_0(\alpha) = 0$ if $2k = p-1$. In this case, we have $a_n = \lambda_n T$, for $n \geq 1$. However the sequence $(\lambda_n)_{n\geq 1}$ is generally not ultimately periodic and therefore $\alpha$ is not quadratic.

We consider now the second kind. Here, for $n \geq 1$, we have $a_n = \lambda_n B_{i(n)}$ and consequently $\deg(a_n) = v_{i(n)}$. We have $v_n = (p^n(p-2k+1)+2k(-1)^n)/(p+1)$ for $n \geq 0$, again from the recurrent definition of $B_n$. The description of the sequence $(i(n))_{n\geq 1}$ is given by the formulas (5) – (8) in Conjecture B. We observe that $2n$ appears for the first time at the beginning of $V_n$, whereas $2n+1$ apears for the first time at the end of $V_{n,1}$. As above, to use (27), we need to compute the sum of the degrees before these occurences. We set $V_{n,1} = W_{n,1}, 2n+1$ and we have $D(W_{n,1}) = D(V_{n,1}) - v_{2n+1}$. We set $r_n = D(V_0, V_1, \dots, V_{n-1})$. We have $D(V_0, V_1, \dots, V_{n-1}, W_{n,1}) = r_n + D(V_{n,1}) - v_{2n+1}$. Then we define

$$s_n = v_{2n}/r_n \quad \text{and} \quad t_n = v_{2n+1}/(r_n + D(V_{n,1}) - v_{2n+1}). \tag{31}$$

Hence, by (27), we have

$$\nu_0(\alpha) = \max(\lim_n s_n, \lim_n t_n). \tag{32}$$

We need to compute $D(V_{n,i})$ and $D(V_n)$. First, let us compute $D(J_n)$. We have $D(J_1) = D(0^{[2k]}, 1) = 2kv_0 + v_1 = 2k + p - 2k = p$. For $n \geq 1$, by (6), we get

$$D(J_{n+1}) = (2k-1)(v_{2n} + v_{2n-1} + (2k-1)D(J_n)) + v_{2n} + v_{2n+1}. \tag{33}$$

For $n \geq 1$, we observe that $v_n + v_{n-1} = p^{n-1}(p - 2k + 1)$. Hence (33) can be written as

$$D(J_{n+1}) = (2k-1)(p^{2n-1}(p-2k+1) + (2k-1)D(J_n)) + p^{2n}(p-2k+1).$$

By induction, it is elementary to check that this formula implies

$$D(J_n) = p^{2n-1} \quad \text{for} \quad n \geq 1. \tag{34}$$

Now we use (7) to compute $D(V_{n,i})$ for $n \geq 1$ and $1 \leq i \leq m$. We have

$$D(V_{n,i}) = (l_i - 1)(v_{2n} + v_{2n-1} + (2k-1)D(J_n)) + v_{2n} + v_{2n+1}.$$

By (34) and the formula for $v_n + v_{n-1}$, this last formula gives

$$D(V_{n,i}) = (l_i - 1)p^{2n} + p^{2n}(p-2k+1) = p^{2n}(p-2k+l_i). \tag{35}$$

Therefore, by (8) and (35), by sommation, with $\sum_{i=1}^{m} l_i = l - m$, we get

$$D(V_n) = p^{2n} \sum_{1 \leq i \leq m} (p - 2k + l_i) = p^{2n}(m(p-2k-1) + l). \tag{36}$$

We set $\nu_1 = m(p-2k-1)+l$. By (5), $D(V_0) = \sum_{i=1}^{m} l_i + m(p-2k)$ and consequently we have $D(V_0) = \nu_1$. Again by sommation, (36) implies

$$r_n = \sum_{0\leq i\leq n-1} D(V_i) = \nu_1(p^{2n} - 1)/(p^2 - 1). \tag{37}$$

Thus we have $s_n = v_{2n}/r_n = (p-1)(p^{2n}(p-2k+1)+2k)/(\nu_1(p^{2n}-1))$, which implies

$$\lim_n s_n = (p-1)(p-2k+1)/\nu_1. \tag{38}$$

We have $1/t_n = (1/s_n)(v_{2n}/v_{2n+1}) + D(V_{n,1})/v_{2n+1} - 1$. From (35), we get

$$\lim_n (D(V_{n,1})/v_{2n+1}) = (p-2k+l_1)(p+1)/(p(p-2k+1)). \tag{39}$$

From (38), since $\lim_n (v_{2n}/v_{2n+1}) = 1/p$, we also get

$$\lim_n ((1/s_n)(v_{2n}/v_{2n+1})) = \nu_1/(p(p-1)(p-2k+1)). \tag{40}$$

Combining (39) and (40), we obtain

$$\lim_n (1/t_n) = (\nu_1 + (p-2k+l_1)(p^2-1))/(p(p-1)(p-2k+1)) - 1.$$

Finally, this implies

$$\lim_n t_n = p(p-1)(p-2k+1)/\nu_2, \tag{41}$$

where

$$\nu_2 = \nu_1 + (p-2k+l_1)(p^2-1) - p(p-1)(p-2k+1) = \nu_1 + l_1(p^2-1) - 2k(p-1).$$

Combining (32), (38) and (41), we obtain

$$\nu_0(\alpha) = (p-1)(p-2k+1)\max(1/\nu_1, p/\nu_2). \tag{42}$$

A simple calculation shows that $p-2k+1 \leq \nu_1$ and $p(p-2k+1) \leq \nu_2$. Moreover we have $\nu_1 = \nu_2/p = p-2k+1$ if and only if $m = 1$ and $l = 2$. Consequently, we obtain $\nu_0(\alpha) = p-1$ if $m = 1$ and $l = 2$ and $\nu_0(\alpha) < p-1$ otherwise. Note that

$\nu_0(\alpha)$ is far from the admitted upper bound $p^2 - 1$.
This extremal case, corresponding to $m = 1$ and $l = 2$, is noteworthy. In this case, we have $l_1 = 1$, $V_0 = 0, 1$ and $V_n = V_{n,1} = 2n, 2n + 1$, this shows that the infinite word describing the sequence $(i(n))_{n\geq 1}$ is simply $\mathbb{N}$. We have $\epsilon_2 = -\omega_k\lambda_1$, and the continued fraction is defined by the triple $(\lambda_1, \lambda_2, \epsilon_1)$ in $(\mathbb{F}_p^*)^3$. There exists a sequence $(\lambda_n)_{n\geq 1}$ in $\mathbb{F}_p^*$ such that $a_n = \lambda_n B_{n-1}$, for $n \geq 1$. Amazingly enough, we observed that this sequence is simply defined by $\lambda_{2n+1} = \epsilon_1^{-n}\lambda_1$ and $\lambda_{2n+2} = \epsilon_1^n\lambda_2$, for $n \geq 0$.
We turn now to the solution of $(E)$. Applying Theorem C, with a limitation on $p$, we know that $\alpha(p)$ is a perfect $P_k$-expansion in both cases.
First case: $p \equiv 1 \bmod 3$. Here $\alpha(p)$ is a perfect $P_k$-expansion of first kind, where $k = (p-1)/3$ and $l = (p-1)/2$. Applying (30), we get $\nu(\alpha(p)) = 2+\nu_0(\alpha(p)) = 8/3$.
Second case $p \equiv 2 \bmod 3$. Here $\alpha(p)$ is a perfect $P_k$-expansion of second kind, where $k = (p + 1)/3$, $l = (p + 1)^2/3$, $m = (p + 1)/2$ and $l_1 = k/2$. A direct computation shows that $(p - 1)(p - 2k + 1) = 2\nu_1/3$, whereas $p(p - 1)(p - 2k + 1) = 2\nu_2$. Consequently, applying (42), we have $\nu(\alpha(p)) = 2 + \nu_0(\alpha(p)) = 4$. So the proof is complete. □

Note that, according to Mahler's theorem, $\alpha(p)$ being algebraic of degree 4, we have $\nu(\alpha(p)) \in [2, 4]$ in both cases as expected. Moreover, in the second case, $\nu(\alpha(p))$ has the maximal possible theoretical value.

## Acknowledgment

We warmly thank Bill Allombert for his advice in programming and for his help in inserting the figures in this note.

## Bibliography

1. ***L. Baum, M. Sweet,*** *Continued fraction of algebraic power series in characteristic* 2, Annals of Mathematics **103** (1976), 593–610.
2. ***A. Bluher, A. Lasjaunias,*** *Hyperquadratic power series of degree four*, Acta Arithmetica, **124** (2006), 257–268.
3. ***W. Buck, D. Robbins,*** *The continued fraction of an algebraic power series satisfying a quartic equation*, Journal of Number Theory, **50** (1995), 335–344.
4. ***A. Lasjaunias,*** *A survey of Diophantine approximation in fields of power series*, Monatshefte für Mathematik, **130** (2000), 211–229.

5. ***A. Lasjaunias,*** *Continued fractions for hyperquadratic power series over a finite field*, Finite Fields and their Applications, **14** (2008), 329–350.
6. ***A. Lasjaunias,*** *On Robbins example of a continued fraction for a quartic power series over* $\mathbb{F}_{13}$, Journal of Number Theory, **128** (2008), 1109–1115.
7. ***A. Lasjaunias,*** *Algebraic continued fractions in* $\mathbb{F}_q((T^{-1}))$ *and recurrent sequences in* $\mathbb{F}_q$ , Acta Arithmetica, **133** (2008), 251–265.
8. ***A. Lasjaunias,*** *On the continued fraction of the unique root in* $\mathbb{F}(p)$ *of the equation* $x^4 + x^2 - Tx - 1/12 = 0$ *and other related hyperquadratic expansions*, Finite Fields and their Applications, **18** (2012), 26–34.
9. ***A. Lasjaunias, J.-Y. Yao,*** *Hyperquadratic continued fractions in odd characteristic with partial quotients of degree one*, Journal of Number Theory , **149** (2015), 259–284.
10. ***K. Mahler,*** *On a Theorem of Liouville in fields of positive characteristic*, Canadian Journal of Mathematics, **1** (1949), 397–400.
11. ***B. de Mathan,*** *Approximation exponents for algebraic functions*, Acta Arithmetica, **60** (1992), 359–370.
12. ***C. Osgood,*** *Effective bounds on the "diophantine approximation" of algebraic functions over fields of arbitrary characteristic and applications to differential equations*, Indagationes Mathematicae, **37** (1975), 105–119.
13. ***W. Mills, D. Robbins,*** *Continued fractions for certain algebraic power series*, Journal of Number Theory, **23** (1986), 388–404.
14. ***W. Schmidt,*** *On continued fractions and Diophantine approximation in power series fields*, Acta Arithmetica, **95** (2000), 139–166.
15. ***J.-F. Voloch,*** *Diophantine approximation in positive characteristic*, Periodica Mathematica Hungarica, **19** (1988), 217–225.

KHALIL AYADI

Département de Mathématiques
Faculté des Sciences de Sfax
Sfax 3018, Tunisie
ayedikhalil@yahoo.fr

ALAIN LASJAUNIAS

Institut de Mathématiques de Bordeaux
CNRS-UMR 5251
Université de Bordeaux
Talence 33405, France
Alain.Lasjaunias@math.u-bordeaux.fr