Int. J. Open Problems Compt. Math., Vol. 12, No. 3, September 2019
ISSN 1998-6262;
www.i-csrs.org

On the cubic root of polynomial in $\mathbb{F}_2[X]$

B. Ammous

Department of Mathematics, Faculty of Science, University of Sfax, Tunisia,
BP 1171, Sfax 3000
e-mail: ammous.basma@hotmail.fr

Received 03 June 2019; Accepted 29 July 2019

(Communicated by Tarek Sellami)

Abstract

The purpose of this paper is to exhibit a family of cubic formal power series with unbounded partial quotients. We are interested on the formal power series satisfying $f^3 = P$***, where*** $P \in \mathbb{F}_2[X]$***.***

Keywords: *Continued fractions, Formal power series, Finite fields.*
2010 Mathematics Subject Classification: 11A55, 11J81, 11R58.

1 Introduction

The study of continued fraction expansion of a real number offer an important means in number theory. In fact, continued fractions are very useful for solving problems related to the diophantine approximation. A well-known open question in diophantine approximation suggested by Khintchine in [4] asks whether x is an irrational algebraic number of degree > 2, then it has a continued fraction expansion whose sequence of partial quotients is unbounded. The answer to this conjecture remains a hard matter. Several works in the case of real gave a partial resolution to this question [1, 5, 6, 7].

However, for formal power series over a finite field, we have some examples of algebraic formal series of degree ≥ 3 whose sequence of partial quotients is bounded as well as examples whose partial quotients take an infinity of values.

In 1976, Baum and Sweet gave, in [2], the first example of algebraic formal series of degree 3 on $\mathbb{F}_2((X^{-1}))$ whose partial quotients have only a finite number of values. This work was pursued in [8] by Mills and Robbins who

gave an example of algebraic formal series over $\mathbb{F}_2((X^{-1}))$ whose sequence of partial quotients is unbounded and given explicitly. Moreover, Robbins gave in [10] a new family of cubic formal power series with bounded partial quotients in characteristic 2.

Motivated by the above researches, we establish in our work a family of cubic power series over $\mathbb{F}_2$ with unbounded partial quotients. The present paper is organized as follows: in Section 2, we define the field of formal series and the continued fraction expansions over this field. In Section 3, we state our main theorem and we give some lemmas that we will use to prove our result and we close this section by given the details of the proof of Theorem 3.1 and an example to illustrate our result.

2 Preliminaries

Let $q = p^n$ where p is a prime number and n is a non-zero integer.
Let $\mathbb{F}_q$ be a field with q elements of characteristic p, $\mathbb{F}_q[X]$ the ring of polynomials with coefficient in $\mathbb{F}_q$ and $\mathbb{F}_q(X)$ the field of rational functions. Let $\mathbb{F}_q((X^{-1}))$ be the field of formal power series

$$\mathbb{F}_q((X^{-1})) = \{f = \sum_{n \geq n_0} b_n X^{-n}; b_n \in \mathbb{F}_q; n_0 \in \mathbb{Z}\}.$$

Define the absolute value

$$|f| = \begin{cases} q^{degf} & \text{for } f \neq 0; \\ 0 & \text{for } f = 0. \end{cases}$$

Thus, $|\ .\ |$ is a not an archimedean absolute value over $\mathbb{F}_q((X^{-1}))$, that is :

$$\begin{array}{rcll} |f+g| & \leq & \max\,(|f|,|g|) & and \\ |f+g| & = & \max\,(|f|,|g|) & if\ |f| \neq |g|. \end{array}$$

Let f be an algebraic formal power series. We denote by $P(Y) = A_m Y^m + A_{m-1}Y^{m-1} + \ldots + A_0$, where $A_i \in \mathbb{F}_q[X]$, its minimal polynomial.

By analogy with the real case, we have a continued fraction algorithm in $\mathbb{F}_q((X^{-1}))$. A formal power series $f = \sum_{n \geq n_0} b_n X^{-n}$ has a unique decomposition as $f = [f] + \{f\}$ with $[f] \in \mathbb{F}_q[X]$ and $|\{f\}| < 1$.
The polynomial $[f]$ is called the polynomial part of f and $\{f\}$ is called the fractional part of f.

We can write for any $f \in \mathbb{F}_q((X^{-1}))$

$$f = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n + \cfrac{1}{\ddots}}}} = [a_0, a_1, a_2, \ldots],$$

where $a_0 = [f]$ and $a_i = [f_i] \in \mathbb{F}_q[X]$ with $\deg(a_i) \geq 1$ for any $i \geq 1$ and $f_i = \dfrac{1}{\{f_{i-1}\}}$.
The sequence $(a_i)_{i\geq 0}$ is called the partial quotients of f and we denote by $f_n = [a_n, a_{n+1}, \ldots]$ the n^{th} complete quotient of f.

Definition 2.1 *If* $(\deg(a_i))_{i\geq 0}$ *is bounded, then* f *is said to have a bounded continued fraction expansion.*

Note that similarly to the real case, we have the continued fraction expansion is finite if and only if $f \in \mathbb{F}_q(X)$. Moreover, the theorem of Lagrange [3] remains true in $\mathbb{F}_q((X^{-1}))$:

Theorem 2.2 *The sequence of partial quotients of* f *is ultimately periodic if and only if* f *is quadratic over* $\mathbb{F}_q(X)$.

Now, we define two sequences of polynomials $(P_n)_{n\geq 0}$ and $(Q_n)_{n\geq 0}$ as follows:

$$P_0 = a_0, \quad Q_0 = 1, \quad P_1 = a_0a_1 + 1, \quad Q_1 = a_1$$

and

$$P_n = a_nP_{n-1} + P_{n-2}, \quad Q_n = a_nQ_{n-1} + Q_{n-2}, \text{ for any } n \geq 2.$$

We easily check that

$$P_nQ_{n-1} - P_{n-1}Q_n = (-1)^{n-1}, \text{ for any } n \geq 1$$

and

$$\frac{P_n}{Q_n} = [a_0, a_1, a_2 \ldots\ldots, a_n], \text{ for any } n \geq 0.$$

$\dfrac{P_n}{Q_n}$ is called the n^{th}convergent of f and it satisfies the following :

$$\lim_{n\to\infty} \frac{P_n}{Q_n} = f = [a_0, a_1, \ldots, a_n, \ldots].$$

With the non archimedean absolute value, we find the following important equality

$$\left| f - \frac{P_n}{Q_n} \right| = \left| \frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n} \right| = |Q_nQ_{n+1}|^{-1} = |a_{n+1}|^{-1}|Q_n|^{-2}. \tag{1}$$

In 1976, Baum and Sweet proved in [2] the following results:

Theorem 2.3 *Let $f \in \mathbb{F}_2((X^{-1}))$ and $P, Q \in \mathbb{F}_2[X]$; $\gcd(P,Q) = 1$. Then*

a- *If* $|Qf - P| < \dfrac{1}{|Q|}$, *then for some* $n \geq 0$, $\begin{cases} P = P_n \\ Q = Q_n. \end{cases}$

b- *If* $|Qf - P| = \dfrac{1}{|Q|}$, *then for some* $n \geq 0$, $\begin{cases} P = P_n + P_{n-1} \\ Q = Q_n + Q_{n-1}. \end{cases}$

From these results, Baum and Sweet showed in [2] that the unique solution in $\mathbb{F}_2((X^{-1}))$ of the cubic equation

$$f^3 + x^{-1}f + 1 = 0, \tag{2}$$

has a continued fraction expansion with partial quotients of degree ≤ 2 and consequently, they proved that the conjecture of Khintchine [4] is false in $\mathbb{F}_q((X^{-1}))$. Furthermore, they showed in [2] that this result is not true if we replace the cubic power of the equation (2) by 2^n+1 where $n > 1$ and they also gave some examples of formal series whose the sequence of partial quotients is unbounded in higher characteristic.

3 Main results

Theorem 3.1 *Let $f \in \mathbb{F}_2((X^{-1}))$ such that $f^3 = P$ where P is irreducible in $\mathbb{F}_2[X]$ such that the degree of P is a multiple of 3. If there exist $n \geq 0$ such that*

$$\deg(a_{n+1}) > \deg(P),$$

then f admits unbounded partial quotients.

Before giving the proof of this theorem, we will introduce these lemmas that we will need.

Lemma 3.2 *Let $f \in \mathbb{F}_q((X^{-1}))$. If $f = [a_0, a_1, a_2, \ldots]$, then $f^p = [a_0^p, a_1^p, a_2^p, \ldots]$.*

Proof : This is due to the morphism of Frobenius : In fact, we have $[f^p] = [f]^p$ and $\{f^p\} = \{f\}^p$.

Lemma 3.3 *Let $P \in \mathbb{F}_2[X]$ such that the degree of P is a multiple of 3, then there is a unique $f \in \mathbb{F}_2((X^{-1}))$ such that $f^3 = P$.*

Proof : The uniqueness of f is obvious. Let $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ in which n is a multiple of 3. We seek $f = \sum_{i \geq n_0} f_i X^{-i}$ in $\mathbb{F}_2((X^{-1}))$ such that $f^3 = P$ and $f_{n_0} \neq 0$. It is sufficient to determine the f_i step by step.
The equality $f^3 = P$ yields that $n = -3n_0$ and $f_{n_0}^3 = a_n$, thus $f_{n_0} = 1$.

The term in $X^{n-1} = X^{-(3n_0+1)}$, on the one hand, is equal to a_{n-1} and on the other hand is equal to $f_{n_0}^2 f_{n_0+1}$, then we get $f_{n_0+1} = a_{n-1}$.
By identification of the term in X^{n-2}, we find that $a_{n-2} = f_{n_0+2}f_{n_0}^2 + f_{n_0+1}^2 f_{n_0}$ which gives $f_{n_0+2} = a_{n-2} - a_{n-1}^2$.
By identification of the term in X^{n-3}, we find that $a_{n-3} = f_{n_0+3}f_{n_0}^2 + f_{n_0+1}^3$ which gives $f_{n_0+3} = a_{n-3} - a_{n-1}^3$.
And we finish until we find all the f_i.

Proof of Theorem 3.1

Let $f = [a_0, a_1, \ldots, a_n, \ldots]$ such that $\dfrac{p_n}{q_n}$ its convergent, by Lemma 3.2, we have $f^2 = [a_0^2, a_1^2, \ldots, a_n^2, \ldots]$ where $\dfrac{p_n^2}{q_n^2}$ is a convergent to f^2.
From the equality (1), we have

$$|q_n f - p_n| = \frac{1}{|a_{n+1}||q_n|}$$

this implies that

$$|q_n^2 f^2 - p_n^2| = \frac{1}{|a_{n+1}|^2|q_n|^2}$$

Since $f^3 = P$, thus

$$\left|q_n^2 \frac{P}{f} - p_n^2\right| = \frac{1}{|a_{n+1}|^2|q_n|^2}$$

We get

$$|q_n^2 P - f p_n^2| = \frac{|f|}{|a_{n+1}|^2|q_n|^2}$$

We take $U = p_n^2$ and $V = q_n^2 P$. Since P is irreducible, this yields that

$$gcd(U, V) = 1. \tag{3}$$

On the other hand,

$$|Uf - V| = \frac{|f|^3}{|a_{n+1}|^2|U|} < \frac{1}{|U|}, \tag{4}$$

because, by assumption and by Lemma 3.3, we get

$$\deg(a_{n+1}) > \deg(P) = 3\ \deg(f) > \frac{3}{2}\deg(f).$$

It follows from (3), (4) and Theorem 2.3 that there exists $s \geq 0$ such that $U = q_s$ and $V = p_s$ satisfies

$$|q_s f - p_s| = \frac{1}{|a_{s+1}||q_s|}.$$

We thus obtain that

$$\deg(a_{s+1}) = 2\ \deg(a_{n+1}) - 3\ \deg(f) > \deg(a_{n+1}).$$

Therefore, the sequence of partial quotients of f is unbounded.

4 Application

Example 4.1 *Let $P \in \mathbb{F}_2[X]$ such that $P = X^3 + X^2 + 1$. The continued fraction expansion for the solution of the following equation*

$$f^3 = X^3 + X^2 + 1,$$

has unbounded partial quotients.

Proof : In computation of the first partial quotients of f, we obtain that:

$$f = [X + 1, X, X^2 + X, X + 1, X, X^2 + 1, X, X^2, X^5 + X^4, X^3 + X + 1, \ldots].$$

We check that $\deg(a_8) > \deg(P)$, then according to Theorem 3.1, f admits unbounded partial quotients.

5 Open Problems

On the theory of continued fractions in $\mathbb{F}_q((X^{-1}))$, there are several open problems. Among these problems, we propose the following :

Open problem 5.1

Conjecture 5.2 *(Niederreiter)[9] The formal power series $f \in \mathbb{F}_2((X^{-1}))$ which verifies the equation $f^3 = P$, with $P \in \mathbb{F}_2[X]$, admits unbounded partial quotients.*

In this paper, we gave a partial answer to this conjecture in the case $\deg(a_{n+1}) > \deg(P)$. The question here is that this result remains true if $\deg(a_{n+1}) \leq \deg(P)$ or not?

Open problem 5.3 *The main result is it still true if we replace the characteristic 2 by $p > 2$?*

References

[1] A. Baker, *Continued fractions of transcendental numbers*, Mathematika, 9, (1962), 1–8.

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

[3] G. H. Hardy et E. M. Wright, *An Introduction to the Theory of Numbers*, Clarendon, Oxford, (1975).

[4] A. Khintchine, *Continued fractions*, (In Russian), Gosudarstv. Izdat. Tech.-Teor. Lit. Moscow-Leningrad, 2nd edition, (1949).

[5] S. Lang, *Introduction to Diophantine Approximations*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1966.

[6] J. Liouville, *Sur des classes trés étendues de quantités dont la valeur n'est ni algébrique, ni même réductibles à des irrationnelles algébriques*, J. Math. Pures Appl, 16, (1851), 133–142.

[7] E. Maillet, *Introduction à la théorie des nombres transcendants et des propriétés arithmétiques des fonctions*, Gauthier-Villars, Paris, (1906), Chap VII, 274.

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

[9] H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge Univ. Press, 1986.

[10] D. P. Robbins, *Cubic Laurent Series in Characteristic 2 with Bounded Partial Quotients*, arXiv:math \ 9903092$v1$[math.NT]16 Mar.1999.