Infinity of Zeros of Recurrence Sequences

S. Kaouache (Corresponding author)

LMPA. Département de Mathématiques, Faculté des Sciences

Université de Jijel, BP 98, Ouled Aissa

Jijel 18000, Algerie

E-mail: smailkaouache@yahoo.fr

T. Zerzaihi

LMPA. Département de Mathématiques, Faculté des Sciences

Université de Jijel, BP 98, Ouled Aissa

Jijel 18000, Algerie

E-mail: zerzaihi@yahoo.com

Abstract

The purpose of this work is to study the zeros of linear recurrence sequence, with constant coefficients. We give a simple proof of well known Skolem-Mahler-Lech theorem. The advantage of this work is similar to the one done by V. Halava and collaborators, but in a simple way. We study the problem when the general term of the recurrent sequence is of exponential polynomial with some initial conditions that simplify the problem.

Keywords: Linear recurrent sequence, Skolem-Mahler-Lech theorem, p-adic numbers, Power series

1. Introduction

In this section, we give some basic concepts and well-known results about linear recurrence sequences which are needed in the later section.

Let $(u_n)_{n \in \mathbb{N}}$ be a $k - th$ order linear recurring sequence defined by

$$u_n = s_{k-1}u_{n-1} + \ldots\ldots\ldots + s_0 u_{n-k} \tag{1}$$

for all $n \geq k$ with fixed algebraic numbers s_i and u_j for $i = 0, ..., k - 1$ and $j = 0, ..., k - 1$. The k first elements $u_0, u_1 \ldots\ldots\ldots, u_{k-1}$ of the linear recurrent sequence $(u_n)_{n \in \mathbb{N}}$ in (1) are called the initial conditions. If the initial conditions are given, every element of the sequence is uniquely determined by the recurrence (1).

Every recurrent sequence satisfying (1) has a characteristic polynomial

$$p(x) = x^k - \sum_{i=0}^{k-1} s_i x^j \tag{2}$$

its zeros are called the characteristic roots. We assume that $s_0 \neq 0$, then each characteristic roots is different from zero. We let $\alpha_1, \alpha_1, ..., \alpha_r$, with multiplicity $m_i, 1 \leq i \leq r$, be the distinct characteristic roots of $(u_n)_{n \in \mathbb{N}}$, then there exist unique polynomials $h_i(x)$ for $i = 0, ..., r$ with $deg h_i \leq m_i - 1$, such that for each $n \in \mathbb{N}$, we have

$$u_n = \sum_{i=1}^{r} h_i(n)\alpha_i^n, \tag{3}$$

For a sequence $(u_n)_{n \in \mathbb{N}}$, we define its set of zeroes by

$$G(u_n) = \{n \in \mathbb{N} \text{ such that } u_n = 0\}. \tag{4}$$

Here, an infinite arithmetic progression is a set of the form $a + b\mathbb{Z}$ where $a \in \mathbb{Z}$ and b is a positive integer.
The following result is the well known Skolem-Mahler-Lech theorem.

Theorem 1. *(Skolem-Mahler-Lech): If (u_n) is a sequence given by a linear recurrence (1), then the set $G(u_n)$ defined by (4) is a union of finitely many arithmic progressions and a finite set.*

One of the most well known linear recurrence equation is that for which $u_n = 3u_{n-2} - u_{n-4}$ with the initial conditions ($u_0, u_1, u_2, u_3) = (0, 0, 1, 0)$. The sequence is given by

$$u_n = (1 + (-1)^n)\left(\left(\frac{1 + \sqrt{5}}{2}\right)^n - \left(\frac{1 - \sqrt{5}}{2}\right)^n\right). \tag{5}$$

And the set of n such that $u_n = 0$ is the union of the finite set $\{0\}$ and the the arithmitic progression $\{1, 3, 5, ...\}$.

To give a short history of the problem, it was first proved by T. Skolem in 1934 for a linear recurrence over the rational numbers. The result of Skolem was later proved for a linear recurrence over the algebraic numbers, also by Mahler in 1935 and by Lech in 1953 for arbitrary fields of characteristic 0. The result of Skolem-Mahler-Lech, also has been proved by Laxton [1968], Mignotte [1973], Van der poorten [1976], and Robba [1977]. Recently, V. Halava, T. Harju and J. Karhumaki [2005] presented the proof of a special case of Skolem-Mahler-Lech theorem in a form given by G.Hansel [1986]. The employed methods of proof of his different results are difficult.

In this paper we shall give a simple proof of the well known Skolem-Mahler-Lech theorem. The advantage of this work is similar to [V. Halava, 2005] , but in a simple way. We study the problem where the general term of (u_n) defined in the field $\mathbb{Q}_p$ by

$$u_n = \sum_{i=1}^{r} h_i(n) exp(n \ln \alpha_i) \tag{6}$$

and we suppose that for each i ($i = 1, ...r$), the roots α_i satisfy $\alpha_i \equiv 1 (mod p)$, and we will apply the following theorem:

Theorem 2. *Let $p > 2$ be a prime number and d_i any sequence of integers, and define*

$$b_n = \sum_{i=0}^{n} c_n^i p^i d_i \tag{7}$$

If $b_n = 0$ for infinitely many n, then $b_n = 0$ for each n.

For a proof, see for example [V. Halava, 2005].

2. Valuations of algebraic numbers and $p-$adic power series

For convenience we review a few facts about valuations of number and some proprieties of power serie. For a more comprehension we refer to [A. M. Robert, 2000] and [S . Katok, 2000]. Let $p > 2$ be the prime number. The valuation of an integer x then can be defined as follows

$$v_p(x) = \begin{cases} 0, & \text{if } p \nmid x \\ r, & \text{if } p^r \backslash x \text{ but } p^{r+1} \nmid x \end{cases} \tag{8}$$

For any rational number $x = \frac{a}{b}$, we have $v_p(x) = v_p(a) - v_p(b)$ according to the previous definition. Valuation v_p is called the p-adic valuation.

We normalise these valuations as follows

$$|x|_p = \begin{cases} p^{-v_p(x)}, & \text{if } x \neq 0 \\ 0, & \text{if } x = 0 \end{cases} \tag{9}$$

$|.|_p$ is a non-Archimedian norm in $\mathbb{Q}$. The distance induced by a non-Archimedian norms is said to be an ultrametric. Instead of the triangle inequality for the usual distance function

$$d(a, c) \leq d(a, b) + d(b, c) \tag{10}$$

it satisfies the strong triangle inequality

$$d(a, c) \leq \max(d(a, b), d(b, c)). \tag{11}$$

Notice that if $a, b \in \mathbb{N}$, then $a \equiv b (mod p^n)$ if and only if $|a - b|_p \leq p^{-n}$.

We define the field $\mathbb{Q}_p$ to be the completion of $\mathbb{Q}$ with respect to the p-adic norm $|.|_p$. $\left(\mathbb{Q}_p, |.|_p\right)$ is a complete normed field. The set of the p-adic integers is denoted by $\mathbb{Z}_p$, so $\mathbb{Z}_p = \left\{\sum_{i=0}^{\infty} a_i p^i\right\}$. It is easy to see that

$$\mathbb{Z}_p = \left\{a \in \mathbb{Q}_p / |a|_p \leq 1\right\} \tag{12}$$

Lemma 3. *If the elements x, y of a non-Archemedian field satisfy the inequality $\|x - y\|_p < \|y\|_p$, then $\|x\|_p = \|y\|_p$.*

Proof. By the strong triangle inequality, we have

$$\|x\|_p = \|x - y + y\|_p \leq \max\left(\|x - y\|_p, \|y\|_p\right) = \|y\|_p.$$

On the other hand

$$\|y\|_p = \|y - x + x\|_p \leq \max\left(\|x - y\|_p, \|x\|_p\right)$$

Now $\|x - y\|_p > \|x\|_p$ would imply $\|y\|_p \leq \|x - y\|_p$, then a contradiction.
Therefore $\|x - y\|_p \leq \|x\|_p$, and $\|y\|_p \leq \|x\|_p$. So, $\|y\|_p = \|x\|_p$ □

Lemma 4. *if $p > 2$ is any prime number and for each $i \in \mathbb{N}$, then*

$$\left\|\frac{1}{i!}\right\|_p \leq p^{\frac{i}{p-1}} \tag{13}$$

Proof. For an integer $i \in \mathbb{N}$, we have

$$v_p(i!) = \frac{i - S_i}{p - 1},$$

where S_i is the sum of digits of i written in base p.
From the formula

$$\|x\|_p = p^{-v_p(x)},$$

we obtain

$$\left\|\frac{1}{i!}\right\|_p = p^{\frac{i-S_i}{p-1}}$$
$$\leq p^{\frac{i}{p-1}}$$

□

Definition 5. A formal power series $f(x) \in \mathbb{Q}_p[[x]]$ is an expression of the form

$$f(x) = \sum_{n=1}^{\infty} a_n x^n$$

It is clear that it converges if and only if $|a_n x^n|_p \to 0$. In particular, every $f(x) \in \mathbb{Z}_p[[x]]$ converges in the disc $\{x \in \mathbb{Q}_p \ / \ |x|_p < 1\}$.
Now, let us consider the formal power series $f(x) \in \mathbb{Q}_p[[x]]$ Such that

$$f(x) = \ln_p(x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(x-1)^n}{n} \tag{14}$$

wich is called the logarithm in base p. It is clear that $f(x)$ converges in

$$D_p = \left\{x \in \mathbb{Q}_p \ / \ |x-1|_p < 1\right\} = 1 + p\mathbb{Z}_p. \tag{15}$$

and diverges otherwise.

Similary, we define the $p - adic$ exponential and denoted by

$$\exp_p(x) = \sum_{n=1}^{\infty} \frac{x^n}{n!} \tag{16}$$

wich converges in the disc

$$B_p = \left\{x \in \mathbb{Q}_p \ / \ |x|_p < p^{\frac{-1}{p-1}}\right\} = p\mathbb{Z}_p \tag{17}$$

and diverges otherwise.

3. Main Result

In this section, we present the simple proof of Skolem-Mahler-Lech theorem. The content of the simple proof of our main result is the following:

Theorem 6. *Let $p > 2$ be a prime number. If $\alpha \in \mathbb{Q}_p$ with $\alpha \equiv 1(mod\,p)$, then for all $x \in \mathbb{Z}_p$, there exist a formal power series $V_\alpha(x) = \sum_{j=0}^\infty v_{\alpha,j} x^j$, wich converge in $\mathbb{Z}_p$ and $V_\alpha(n) = \alpha^n$, $\forall n \in \mathbb{N}$.*

Remark 7. *We see that if $\alpha \equiv 1(mod\,p)$, we obtain $\alpha^{p-1} \equiv 1(mod\,p)$, then the previous theorem is still true if we change the role of α by α^{p-1}.*
The following auxiliary result is necessary for the proof of the theorem (6).

Lemma 8. *Let $p > 2$ be a prime number. If $\alpha \in \mathbb{Q}_p$ with $\alpha \equiv 1(mod\,p)$, we have*

$$\left| \ln_p(1 + \alpha) \right|_p = |\alpha|_p \tag{18}$$

Proof. Since $\alpha \equiv 1(mod\,p)$ and $\left| \frac{1}{n!} \right|_p \leq p^{\frac{n-1}{p-1}}$, for each $n \geq 2$, we have

$$\left| \frac{\alpha^n}{n} \right|_p \leq \left| \frac{\alpha^n}{n!} \right|_p \leq \left(|\alpha|_p \cdot p^{\frac{1}{p-1}} \right)^{n-1} \cdot |\alpha|_p < |\alpha|_p \tag{19}$$

Then

$$\max_{n \geq 2} \left| \frac{\alpha^n}{n} \right|_p < |\alpha|_p \tag{20}$$

Moreover, by the strong triangle inequality, we have

$$\left| \alpha + \sum_{n=2}^\infty (-1)^{n+1} \frac{\alpha^n}{n} \right|_p \leq \max \left(|\alpha|_p, \max_{n \geq 2} \left| \frac{\alpha^n}{n} \right|_p \right) = |\alpha|_p \tag{21}$$

and by isosceles triangle property, we obtain

$$\left| \alpha + \sum_{n=2}^\infty (-1)^{n+1} \frac{\alpha^n}{n} \right| = |\alpha|_p, \tag{22}$$

and hence

$$\left| \ln_p(1 + \alpha) \right|_p = |\alpha|_p \tag{23}$$

$\square$

Proof of theorem (6) Let $n \in \mathbb{N}$ and $\alpha \in \mathbb{Q}_p$, with $\alpha \equiv 1(mod\,p)$, then

$$\begin{aligned}
\alpha^n &= \exp_p(n \ln_p \alpha) = \sum_{j=0}^\infty \frac{(\ln_p \alpha)^j}{j!} n^j \\
&= \sum_{j=0}^\infty v_{\alpha,j} n^j, \text{ where } v_{\alpha,j} = \frac{(\ln_p \alpha)^j}{j!}
\end{aligned}$$

Now, let us consider $V_\alpha(x) = \sum_{j=0}^\infty v_{\alpha,j} x^j$, so for every integer $p - adic$ $x \in \mathbb{Z}_p$, we have

$$\left\| v_{\alpha,j} x^j \right\|_p \leq \left\| v_{\alpha,j} \right\|_p \leq \left\| \ln_p(1 + (\alpha - 1)) \right\|_p^j \cdot \left\| \frac{1}{j!} \right\|_p \tag{24}$$

Using the lemma (4) and lemma (8), we have

$$\left\| v_{\alpha,j} x^j \right\|_p \leq \|\alpha - 1\|_p^j \cdot \left\| \frac{1}{j!} \right\|_p \leq p^{-j} \cdot p^{\frac{j}{p-1}} = p^{-j\frac{p-2}{p-1}}$$

and hence $p^{-j\frac{p-2}{p-1}} \to 0$, when $j \to \infty$, for each $p > 2$.

Proof of theorem (1). (Skolem-Mahler-Lech Theorem)
Let us consider u_n in $\mathbb{Q}_p$, be given as

$$u_n = \sum_{i=1}^r h_i(n) \exp(n \ln \alpha_i), \tag{25}$$

where $\alpha_i \equiv 1 (mod\, p)$.

For any number n, we can write $n = m + (p-1)N$, where $0 \le m \le p-2$ and $n \in \mathbb{N}$. Then we have

$$u_{m+(p-1)N} = \sum_{i=1}^{r} h_i(m + (p-1)N)\alpha_i{}^m (\alpha_i{}^{p-1})^N \qquad (26)$$

And by theorem (2) and remark (7), every sequence

$$
\begin{aligned}
u_{(p-1)N} &= \sum_{i=1}^{r} h_i((p-1)N)(\alpha_i{}^{p-1})^N \\
u_{1+(p-1)N} &= \sum_{i=1}^{r} h_i(1 + (p-1)N)\alpha_i(\alpha_i{}^{p-1})^N \\
&\qquad\qquad \vdots \\
u_{(p-2+(p-1)N)} &= \sum_{i=1}^{r} h_i(p-2) + (p-1)N)\alpha_i{}^{p-2}(\alpha_i{}^{p-1})^N
\end{aligned}
$$

is equal to formal power series which converge in $\mathbb{Z}_p$.

which shows that either sequence $(u_{m+(p-1)N})$, for all $0 \le m \le p-2$, vanishes identically or contains only finitely many zeros. This completes the proof.

References

A. J. Van der Poorten. (1976). Zeros of p-adic exponenttial polynomials, Nedert. Akad. Wetensch. porc. Ser. A 79; *Indag. Math.*, 38, 46-49.

A. M. Robert. (2000). A Course in p-adic Analysis, Springer-Verlag Berlin Heidelbery New York.

C. Lech. (1953). A note on recurring series. *Ark. Mat.,* 2, 417–421.

G. Hansel. (1986). Une\ d emonstration simple du théorème de Skolem-Mahler-Lech. *Theoret. Comput. Sci.,* 43, no. 1, 91–98.

H. P. Schlickewei. Multiplicities of algebraic linear recurrences (to appear).

K. Mahler. (1935). Eine arithmetische Eigenschaft der Taylor Koeffizienten rationaler Funktionen. *Proc. Akad. Wet. Amsterdam*, 38, 51–60.

M. Mignotte. (1973). Suites récurrents linéaires, Sém. Delange-Pisot-Poitou 15e années, l74 n14, 9pp.

P. Robba. (1977). Zéros de suites récurrentes linéaires, Groupe d'étude d'analyse ultramétrique 5e année, l 78, n 13, 5pp.

R. R. Laxton. (1968). linear p-adic recurrences, *Quart. J. Math. Oxford*, (2), 19, 305-311.

S . Katok. (2001). real and p-adic analysis, course notes for Math 497C, Mass Program, Fall 2000.

T. Skolem. (1935). Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen. In: Comptes rendus du congrés des mathèmaticiens scandinaves, *Stockholm*, 1934, pp. 163–188.

V. Halava, T. Harju, M. Hirvensalo and J. Karhumaki. (2005). Skolem's Problem– On the Border Between Decidability and Undecidability. *TUCS Technical Report*, No 683, pp.19, 21-22. (April 2005).