On Mahler-Lech-Skolem Theorem

Aleksei Lopatin

June 2025

Abstract

This paper discusses the proof of the Mahler-Lech Skoll Theorem using Strassmann's theorem and its ties with p-adic analysis.

1 Introduction

The Mahler-Lech-Skolem theorem answers the question of how many roots a linear recurrence sequence can have. Skolem made the first step in the theorem and proved the theorem for a recurrence $a_n \in \mathbb{Z}$ for each n. Mahler and Lech later extended the proof to more general cases. Funnily so, Mahler later gave an independent proof apart from Lech's result and was embarrassed that Lech had already proven it.

The importance of the theorem is that it gives no mention to the p-adics while every known proof uses p-adic techniques in some way. It provides an example of how analytic methods can solve algebraic problems.

To tackle the theorem, we will introduce the technique of p-adic analysis. p-adic analysis is the study of functions and analysis in the context of the p-adics $\mathbb{Q}_p$ rather than the real or complex numbers.

The p-adics comes from another way of defining the distance between two rational numbers. The Euclidean absolute value $d(x, y) = |x - y|$ gives rise to the real numbers. The p-adics rely on the p-adic absolute value.

Contrary to the real numbers, p-adic numbers are "close together" if their difference is divisible by a high power of p. The p-adics have their notion of absolute value. In the realm of p-adic functions, we will largely be focused on p-adic analytic functions.

There are some interesting ways in which the p-adic numbers are distinct from the reals or complex numbers. While $\mathbb{Q}_p$ is a complete field, it is also totally disconnected (as the only connected subsets are one-point subsets). Additionally, while the algebraic closure of the real numbers (the complex numbers) is a complete field and finite-dimensional vector space over the real numbers, the algebraic closure of $\mathbb{Q}_p$ is an infinite dimensional vector space over $\mathbb{Q}_p$ and is not complete.

We will begin the preliminaries by introducing the p-adics and the connection between linear recurrence sequences and linear algebra. We will prove Strassmann's theorem, which is a key step in the proof. We will then give the first proof of the Mahler-Lech-Skolem theorem. Furthermore, we will explore p-adic logarithms and exponentials, alongside p-adic interpolation, to provide a second proof of the Mahler-Lech-Skolem theorem. We finish the paper with some open questions.

2 Acknowledgements

The author would like to thank Simon Rubinstein-Salzedo and Jacob Swenberg for their inputs, Serkan Salik for helping translate a useful paper, and the Euler Circle classmates who asked about the topic.

3 Preliminaries

Recall that we constructed the real numbers as equivalence classes of Cauchy sequences of rationals, using the usual absolute value $d(x,y) = |x-y|$. We construct the p-adics using the p-adic absolute value, which we will define in the following section. The following definitions are standard in p-adic textbooks, one can refer to [Gou97, Chapter 2].

3.1 Absolute Values and Valuations

We begin with the general notion of what an absolute value is.

Definition 3.1. An absolute value on a field $\Bbbk$ is a function $|| : \Bbbk \to \mathbb{R}_+$ that satisfies the following three conditions:

$$|x| = 0 \text{ if and only if } x = 0$$

$$|xy| = |x||y| \text{ for all } x, y \in \Bbbk$$

$$|x+y| \leq |x| + |y| \text{ for all } x, y \in \Bbbk$$

We will say that an absolute value on $\Bbbk$ is non-archimedean if it satisfies the following condition.

$$|x+y| \leq \max(|x|, |y|) \text{ for all } x, y \in \Bbbk$$

Notationally, we will consider $|x|_\infty$ to be the standard absolute value of x in $\mathbb{R}$ as in $|-3|_\infty = 3$. Notice that the fourth condition directly implies the third condition. We then define what a valuation is. Intuitively, a valuation tells us how ”large” elements in a field are. We introduce the p-adic valuation.

Definition 3.2. Fix a prime number $p \in \mathbb{Z}$. The p-adic valuation on $\mathbb{Q}$ is the function $v_p : \mathbb{R} - \{0\} \to \mathbb{Z}$ defined as follows: for each integer $n \in \mathbb{Z}$, let $v_p(n)$ be the unique positive integer satisfying

$$n = p^{v_p(n)} n'$$

with p not dividing n'. Moreover, we extend v_p to the field of rational numbers as follows: if $x = \frac{a}{b}$ in $\mathbb{Q}$, then

$$v_p(x) = v_p(a) - v_p(b)$$

We can play around with this definition.

Example. One can check the following.

$$v_5(3060) = 1$$

$$v_2(3) = 0$$

$$v_2(8) = 3$$

Naturally, we are curious as to what properties this valuation satisfies.

Theorem 3.3. *For all x and $y \in \mathbb{Q}$, we have*

$$v_p(xy) = v_p(x) + v_p(y)$$

$$v_p(x + y) \geq \min(v_p(x), v_p(y))$$

Proof. For the first part, let us denote $x = p^{x_1}x'$ and $y = p^{y_1}y'$.

$$xy = p^{x_1}x'p^{y_1}y' = p^{x_1+y_1}x'y'$$

$$v_p(xy) = x_1 + y_1 = v_p(x) + v_p(y)$$

For the second part, we just factor out the common power of p. Without loss of generalization we let $x \geq y$, so $p^{x_1} \geq p^{y_1}$.

$$x + y = p^{x_1}x' + p^{y_1}y' = p^{y_1}(p^{x_1-y_1}x' + y')$$

$$v_p(x + y) \geq y_1 = \min(v_p(x), v_p(y))$$

■

We now define the p-adic absolute value.

Definition 3.4. For any nonzero $x \in \mathbb{Q}$, we define the p-adic absolute value of x by

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

We extend this to all of $\mathbb{Q}$ by defining $|0|_p = 0$.

Using the p-adic absolute value, we can construct $\mathbb{Q}_p$ as equivalence classes of Cauchy sequences of rationals using the p-adic absolute value. We can also define $\mathbb{Z}_p$ and $p^m\mathbb{Z}_p$

Definition 3.5. $\mathbb{Z}_p$ (called the *ring of p-adic integer*) is the subring of $\mathbb{Q}_p$ comprised of p-adic numbers with p-adic absolute value less than or equal to 1.

Definition 3.6. For a non-negative integer m, the notation $p^m\mathbb{Z}$ refers to $\{p^m x | x \in \mathbb{Z}_p\}$.

This is the set of all p-adic integers divisible by p^m.

Example. One can check that the following infinite series converge in $\mathbb{Z}_5$:

$$1 = 1 + 0 \cdot 5 + 0 \cdot 5^2 + 0 \cdot 5^3 + \cdots \in \mathbb{Z}_5$$

$$x = 1 + 2 \cdot 5 + 3 \cdot 5^2 + \cdots \in \mathbb{Z}_5$$

$$-1 = 4 + 4 \cdot 5 + 4 \cdot 5^3 + \cdots \in \mathbb{Z}_5$$

The previous one is true by the fact that

$$-1 = (p-1) + (p-1)p + (p-1)p^2 + \cdots .$$

$$125 = 0 + 0 \cdot 5 + 0 \cdot 25 + 1 \cdot 125 + \cdots \in p^3\mathbb{Z}_p$$

$$x = 0 + 0 \cdot 5 + 0 \cdot 25 + 3 \cdot 125 + 4 \cdot 625 + \cdots \in p^3\mathbb{Z}_p$$

We define what a unit in $\mathbb{Q}_p$ is.

Definition 3.7. An element $x \in \mathbb{Q}_p$ is a unit if there exists an element $y \in \mathbb{Q}_p$ such that

$$xy = 1.$$

Moreover, we define the prime ideal. Intuitively, in the ring of integers $\mathbb{Z}$, the prime ideals are precisely 0 (the zero ideal) and p (the ideal generated by a prime number p). The condition $ab \in R \implies a \in R$ or $b \in R$ generalizes the fact that if p divides ab, then p divides one of a or b.

Definition 3.8. For a commutative ring R. An ideal $P \subset R$ is called a prime ideal if it satisfies the following properties

- It is a proper ideal $P \not\subset R$.
- For any two elements $a, b \in R$, if $ab \in R$, then either $a \in R$ or $b \in R$.

Notice that $||_p$ is a non-archimedean absolute value. Generally, absolute values capture information related to primes instead of what sign a number has, as in $|-5| = 5$. This brings us to the product formula as an example of how the absolute values work together.

Before we get into the proposition, note that we have written absolute values in the form $||_p$ where p is either a prime or infinity. It is convenient to think of the symbol ∞ as a prime number in $\mathbb{Z}$ and refer to it as the infinite prime. This will let us say "$||_p$ for all primes $p \leq \infty$." This is mainly for convenience.

Proposition 3.9. *For any $x \in \mathbb{Q}^\times$, we have*

$$\prod_{p \leq \infty} |x|_p = 1$$

where $p \leq \infty$ means that we take the product over all the primes of $\mathbb{Q}$, including the "prime at infinity."

Proof. We let $x = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$. Then, we have three cases:

$$|x|_q = 1 \text{ if } q \neq p_i$$

$$|x|_{p_i} = p_i^{-a_i} \text{ for } i = 1, 2, 3, \dots k$$

$$|x|_\infty = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

The result follows. ■

To conclude this section, the completion of $\mathbb{Q}$ with respect to the p-adic metric is denoted $\mathbb{Q}_p$. We think of the p-adics as equivalence classes of Cauchy sequences of rationals using the p-adic metric.

3.2 Metrics

Metrics are a notion of distance and lead to some unusual properties in the p-adic sense.

Definition 3.10. Let $\Bbbk$ be a field and $||$ an absolute value on $\Bbbk$. We define the distance $d(x, y)$ between two elements $x, y \in \Bbbk$ by

$$d(x, y) = |x - y|$$

The function $d(x, y)$ is called the metric induced by the absolute value.

A set on which a metric is defined is a metric space. We explore two simple properties of this metric.

Lemma 3.11. *For any $x, y \in \Bbbk$, $d(x, y) \geq 0$, and $d(x, y) = 0$ if and only if $x = y$.*

Proof. Notice that the absolute value function $|x - y|$ is greater than or equal to 0 because by definition it outputs a nonnegative value. Note that $|x - y| = 0$ if and only if $x - y = 0$, which implies the conclusion. ■

We notice that this metric is commutative.

Lemma 3.12. *For any $x, y \in \Bbbk$, $d(x, y) = d(y, x)$.*

Proof. Notice that $|x - y| = |y - x|$ by properties of the absolute value. This directly implies the conclusion. ■

We can also use the triangle inequality. Recall the following definition.

Lemma 3.13. *For a triangle with sides a,b, and c, we have $a + b > c$, $a + c > b$ and $b + c > a$*

Lemma 3.14. *For an $x, y, z \in \Bbbk$, $d(x, z) \leq d(x, y) + d(y, z)$.*

Proof. We plot x, y, z on a plane. Notice that they form a triangle. The absolute value distances are $|x-z|$, $|x-y|$, and $|y-z|$. By the triangle inequality, we have $|x-z| \leq |x-y| + |y-z|$.

To handle the edge cases, i.e. they are all on a line, we consider a line with x, y, z in that order. Permutations give the same result. Since they lie on a line $|x-y| + |y-z| = |x-z|$. This implies the conclusion. ■

There is an inequality which is stronger than the triangle inequality in a similar respect, and this is referred to as the ultrametric inequality. A set with a metric induced by a non-archimedean absolute value is called an ultrametric space. [Gou97][Chapter 2]

Lemma 3.15. *Let $||$ be an absolute value on a field $\Bbbk$, and defined a metric by $d(x, y) = |x-y|$. Then $||$ is non-archimedean if and only if for any $x, y, z \in \Bbbk$, we have*

$$d(x, y) \leq \max(d(x, z), d(z, y))$$

Curiously, the ultrametric inequality directly implies the triangle inequality. Alain Robert refers to the following as the "strongest wins principle" in page 429 of [vdP89].

Proposition 3.16. *Let $\Bbbk$ be a field and let $||$ be a non-archimedean absolute value on $\Bbbk$. If $x, y \in \Bbbk$ and $|x| \neq |y|$, then:*

$$|x+y| = \max(|x|, |y|)$$

Proof. Wlog $|x| > |y|$. Noting that we can apply the ultrametric inequality, we have:

$$|x+y| \leq |x| = \max(|x|, |y|).$$

Noting that $x = (x+y) - y$:

$$|x| \leq \max(|x+y|, |y|)$$

The only way for both of these inequalities to hold is if:

$$\max(|x+y|, |y|) = |x+y|$$

This implies $|x| \leq |x+y|$, which in turn lets us conclude $|x| = |x+y|$. ■

The following corollary proposes that triangles are isosceles.

Corollary 3.17. *In an ultrametric space, all "triangles" are isosceles.*

Proof. Let x, y, z be three elements of a vector space. Thus, we have $d(x, y) = |x-y|$, $d(y, z) = |y-z|$, and $d(x, z) = |x-z|$. Now, we make use of:

$$(x-y) + (y-z) = (x-z)$$

We then invoke the proposition to show that if $|x-y| \neq |y-z|$, then $|x-z|$ is equal to the bigger of the two. Either way, two "sides" are equal." ■

3.3 Recurrences relation with Matrices

Linear recurrence sequences can be analyzed using matrices. Our motivation for turning to matrices to study a general linear recurrence sequence is that it provides a concise expression for the recurrence sequence, as we will soon see.

We begin this subsection by proving the Binet formula with matrices.

Theorem 3.18. *Binet Formula*
If F_n is the nth Fibonacci number, then

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

We recall $x_{k+2} = x_{k+1} + x_k$ (this is the Fibonacci series), and we define v_k as:

$$v_k = \begin{bmatrix} x_k \\ x_{k+1} \end{bmatrix}$$

$$v_{k+1} = \begin{bmatrix} x_{k+1} \\ x_{k+2} \end{bmatrix} = \begin{bmatrix} x_{k+1} \\ x_{k+1} + x_k \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x_k \\ x_{k+1} \end{bmatrix} = Av_k$$

We let $A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$. Notice that A is diagonalizable, and particularly the characteristic polynomial is $P_A(x) = x(x-1) - 1 = x^2 - x - 1$. The roots are $\frac{1}{2}(1 \pm \sqrt{5})$. The eigenvalues are

$$\lambda_1 = \frac{1}{2}(1+\sqrt{5}) \text{ and } \lambda_2 = \frac{1}{2}(1-\sqrt{5})$$

The eigenvectors are respectively $e_1 = \begin{bmatrix} 1 \\ \lambda_1 \end{bmatrix}$ and $e_2 = \begin{bmatrix} 1 \\ \lambda_2 \end{bmatrix}$. Moreover, the diagonalizing matrix for A is $P = \begin{bmatrix} e_1 & e_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ \lambda_1 & \lambda_2 \end{bmatrix}$ Given the simple matrix, it is implied that the solutions are of the form $v_k = b_1\lambda_1^k e_1 + b_2\lambda_2^k e_2$. We find the coefficients b_1 and b_2 as they are

$$\begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = P^{-1}v_0 = \frac{-1}{\sqrt{5}} \begin{bmatrix} \lambda_2 & -1 \\ -\lambda_1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{5}} \begin{bmatrix} \lambda_1 \\ -\lambda_2 \end{bmatrix}$$

The last line follows from the formula for an inverse 2x2 matrix. We now substitute this:

$$v_k = \frac{\lambda_1}{\sqrt{5}}\lambda_1^k \begin{bmatrix} 1 \\ \lambda_1 \end{bmatrix} - \frac{\lambda_2}{\sqrt{5}}\lambda_2^k \begin{bmatrix} 1 \\ \lambda_2 \end{bmatrix}$$

By comparing top entries, we receive

$$x_k = \frac{1}{\sqrt{5}}(\lambda_1^{k+1} - \lambda_2^{k+1})$$

It appears that any linear recurrence can be translated to a matrix, and we show that this is true. We first recall what a characteristic polynomial is.

Definition 3.19. The *characteristic polynomial* of A is defined as

$$P_A(x) = \det(Ix - A)$$

where A is a $n \times n$ matrix with integer entries and x is a chosen matrix. I refers to the identity matrix.

Theorem 3.20. *Cayley-Hamilton Theorem*

$$P_A(A) = 0$$

In words, this means that every square matrix has a distinct equation called a characteristic polynomial.

This seems a bit confusing, so let's do an example to make it clearer. Let $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$.

$$P_A(x) = (x-1)(x-4) - 2 \cdot 3 = x^2 - 5x - 2$$

Upon substituting $x = A$:

$$P_A(A) = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}^2 - 5\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} - 2\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

We give an idea of how one can prove this. Readers who want to pursue this particular part further should consult [HK71, Chapter 6]. We first specify that all matrices in this proof have coefficients over the complex numbers, and that the space of such matrices of a fixed size has a natural topology coming from identifying $n \times n$ matrices with vectors with n^2 entries. We are essentially proving the Cayley-Hamilton theorem for matrices with integer entries in $\mathbb{Z}$ (and in an algebraically-closed field). Let us assume that A is diagonalizable to get a glimpse of the general idea.

We assume A is diagonalizable. Therefore, we can write $A = SDS^{-1}$ for an invertible matrix S, and a matrix D of the form:

$$D = \begin{bmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & \lambda_n \end{bmatrix}$$

We consider $P_A(D)$:

$$P_A(D) = \begin{bmatrix} p(\lambda_1) & 0 & \dots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & p(\lambda_n) \end{bmatrix}$$

Notice that λ_i for $i \in [0, n]$ are the eigenvalues of A, so $P_A(\lambda_i) = 0$. Thus, $P_A(D)$ is the zero matrix.

Let's apply $P_A(x)$ to $A = SDS^{-1}$:

$$P_A(A) = SP_A(D)S^{-1}$$

Because $P_A(D) = 0$, $P_A(A) = 0$. This covers the simpler case, which brings us to the general proof.

Proof. We use the fact that any matrix A can be approximated by diagonalizable matrices. Specifically, we can find a sequence of matrices $(A_k : k \in N)$ that converge to A such that $A_k \to A$ as $k \to \infty$, and each matrix A_k has n distinct eigenvalues. Therefore, the matrix A_k is diagonalizable for each $k \in N$. We apply the results of the previous discussion, so $P_{A_k}(A_k) = 0$ where $P_{A_k} = \det(\lambda I - A_k)$ is the characteristic polynomial of A_k.

Note that each entry of the matrix $P_A(A)$ can be written as a polynomial in the entries of A. Because $\lim_{k\to\infty} A_k = A$, we have $\lim_{k\to\infty} P_{A_k}(A_k) = P_A(A)$. As $P_{A_k} = 0$, $P_A(A) = 0$. We are done. ■

The first step in the proof of the Mahler-Lech-Skolem theorem involves writing a linear recurrence as $a_n = [A^n v, w]$ for an $n \times n$ integer matrix and v and w are integer vectors. We give one example to show how this is possible.

Recall the Fibonacci recurrence $F_n = F_{n-1} + F_{n-2}$ with initial conditions $F_0 = 0$ and $F_1 = 1$. Let us write vectors in the form $\begin{bmatrix} F_1 \\ F_0 \end{bmatrix}$. Notice that this is equal to $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$.

$$\begin{bmatrix} F_{n+1} \\ F_n \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} F_n \\ F_{n-1} \end{bmatrix} = \begin{bmatrix} F_n + F_{n-1} \\ F_n \end{bmatrix}$$

Let $A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$, and the initial vector is $v = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$. To generate F_2, we just calculate $A^2 v$ and take the integer part at the top.

$$A^2 v = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^2 v = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \end{bmatrix}$$

Furthermore, for higher values, we can use $F_n = A^n v$.

However, we do not use w here. We have another way. [Blo17] Given a linear recurrence (a_n) of dimension k (this means we recursively call k functions of a_i for $0 \le i < n$), we can form a $k \times k$ matrix A such that $A_{i,1} = c_i$ for all i (where c_i are the coefficients of the a_i), $A_{i,i-1} = 1$ for $2 \le i \le k$ and everything else is 0.

$$A = \begin{bmatrix} c_1 & c_2 & \cdots & c_{k-1} & c_k \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}$$

Let

$$v = \begin{bmatrix} a_{k-1} \\ a_{k-2} \\ \vdots \\ a_0 \end{bmatrix}$$

$$w = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

For $n \geq k$, $a_n = vA^{n+1-k}w$, which gives the general form $a_n = [a^n v, w]$. Note that we do not make mention of the dimension in the proof of the Mahler-Lech-Skolem theorem as we cover all possible dimensions.

4 Strassmann's Theorem

Now that we have the appropriate preliminaries, we turn to the theorem that will do most of the heavy lifting in our proof: Strassmann's Theorem.

4.1 Interlude

In the proof of Strassmann's theorem, we will make use of the fact that we can re-order a double sum. Thus, we show the following lemma.

Lemma 4.1. *Let $\Bbbk$ be a field which is complete with respect to the non-archimedean valuation $|\cdot|$. Let $a_{ij} \in \Bbbk$ for $i, j = 0, 1, 2, \ldots$. Suppose that for every $\epsilon > 0$ there is a $f(\epsilon)$ such that $|a_{ij}| < \epsilon$ whenever $\max(i,j) \geq f(\epsilon)$. Then the series*

$$\sum_i (\sum_j a_{ij}) \text{ and } \sum_j (\sum_i a_{ij})$$

both converge, and are equal.

Proof. Recall that in the non-archimedean case a series converges if and only if the terms that are summed tend to zero as in [Gou97, Chapter 5]. We know that $a_{ij} \to 0$ as $j \to \infty$ for every i and vice versa, so

$$\sum_j a_{ij} \text{ and } \sum_i a_{ij}$$

both converge. Using the ultrametric inequality, we have

$$|\sum_j a_{ij}| \leq \max_j |a_{ij}| \to 0$$

so that the first double sum converges, and similarly for the second one. Note that the notation $\max_j |a_{ij}|$ refers to the max of the set of a_{ij} as $i \to \infty$.

For the second part, we note that for finite sums, the rearrangement of i and j do not matter, specifically we have

$$\sum_{i=0}^{f(\epsilon)}(\sum_{j=0}^{f(\epsilon)} a_{ij}) = \sum_{j=0}^{f(\epsilon)}(\sum_{i=0}^{f(\epsilon)} a_{ij})$$

We apply the ultrametric inequality again:

$$|\sum_{i=0}^{f(\epsilon)}(\sum_{j=0}^{f(\epsilon)} a_{ij}) - \sum_{i=0}^{\infty}(\sum_{j=0}^{\infty} a_{ij})| = |\sum_{i} \sum_{j \text{ with } \max(i,j)>f(\epsilon)} a_{ij}| \leq \max_{i,j \text{ s.t. } \max(i,j)>f(\epsilon)} |a_{ij} < \epsilon$$

And similarly with the i and j exchanged. Hence

$$|\sum_{i}(\sum_{j} a_{ij}) - \sum_{i}(\sum_{j} a_{ij})| = |\sum_{i}(\sum_{j} a_{ij}) - \sum_{i=0}^{f(\epsilon)}(\sum_{j=0}^{f(\epsilon)} a_{ij}) + \sum_{j=0}^{f(\epsilon)}(\sum_{i=0}^{f(\epsilon)} a_{ij}) - \sum_{j}(\sum_{i} a_{ij})|$$

$$\leq \max\{|\sum_{i=0}^{f(\epsilon)}(\sum_{j=0}^{f(\epsilon)} a_{ij}) - \sum_{i=0}^{\infty}(\sum_{j=0}^{\infty} a_{ij})|, |\sum_{j=0}^{f(\epsilon)}(\sum_{i=0}^{f(\epsilon)} a_{ij}) - \sum_{j=0}^{\infty}(\sum_{i=0}^{\infty} a_{ij})|\} < \epsilon.$$

Thus, the two series are equal. ■

We are ready to prove Strassmann's theorem.

Theorem 4.2. *Strassmann's Theorem*

Let

$$f(x) = \sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + \dots$$

be a non-zero power series with coefficients in $\mathbb{Q}_p$*, and suppose that we have* $\lim_{n\to\infty} a_n = 0$ *so that* $f(x)$ *converges for all* $x \in \mathbb{Z}_p$*. Let* N *be the integer defined by the two conditions*

$$|a_N| = \max(|a_n|) \text{ and } |a_n| < |a_N| \text{ for } n > N$$

Then the function $f : \mathbb{Z}_p \to \mathbb{Q}_p$ *defined by* $x \to f(x)$ *has at most* N *zeros.*

Proof. The core of this proof is induction on N. If $N = 0$, we must have that $|a_0| > |a_n|$ for all $n \geq 1$. In this case, we show there are no zeros for $f(x)$. To show this, we proceed by contradiction. Assume that we have $f(x) = 0$, then:

$$f(x) = a_0 + a_1 x + a_2 x^2 + \dots = 0$$

We bound $|a_0|$.

$$|a_0| = |a_1 x + a_2 x^2 + \dots| \leq \max |a_n x^n| \leq \max |a_n|$$

Thus $|a_0| \leq |a_n|$, but this in direct contradiction with the assumption. Therefore, $f(x)$ has no zeros.

As for the inductive step, we suppose that

$$|a_N| = \max(|a_n|) \text{ and } |a_n| < |a_N| \text{ for } n > N$$

We look to factor $f(x)$, so we assume that it has a root $\alpha \in Z_p$. For any $x \in Z_p$, we have

$$f(x) = f(x) - f(\alpha) = \sum_{n\geq 1} a_n(x^n - \alpha^n) =$$

$$= (x-\alpha)\sum_{n\geq 1}\sum_{j=0}^{n-1} a_n x^j \alpha^{n-1-j}$$

We re-order the series as a power series in x (applying the previous lemma), which gives

$$f(x) = (x-\alpha)\sum_{j=0}^{\infty} b_j x^j = (x-\alpha)g(x)$$

with defining the coefficients b_j as

$$b_j = \sum_{k=0}^{\infty} a_{j+1+k}\alpha^k.$$

Because $\lim_{n\to\infty} a_n = 0$, $\lim_{j\to\infty} b_j = 0$. However, we cannot have all the coefficients be 0 as then $f(x)$ would be the 0 power series, contradicting our assumptions. Thus, $g(x)$ satisfies the assumptions of the theorem.

We proceed with the induction hypothesis. We describe the last $|b_j|$ with maximum absolute value. Notice that

$$|b_j| \leq \max_{k\geq 0} |a_{j+1+k}| \leq |a_N|$$

for every j, so the $|b_j|$ are bounded by $|a_N|$. However, since $|\alpha| \leq 1$, for any $i \geq 1$, we have $|a_{N+i}\alpha^i| \leq |a_{N+i}| < |a_N|$. Now, we make use of the ultrametric inequality:

$$|b_{N-1}| = |a_N + a_{N+1}\alpha + a_{N+2}\alpha^2 + \ldots| = |a_N|$$

For $j \geq N$:

$$|b_j| \leq \max_{k\geq 0} |a_{j+k+1}| \leq \max_{j\geq N+1} |a_j| < |a_N|$$

Therefore $g(x)$ has $N-1$ roots. By the induction argument, $g(x)$ has at most $N-1$ roots, so $f(x)$ has at most N roots. We are done.

■

This is an important theorem about the zeros of functions on $\mathbb{Q}_p$ defined by power series. We give several consequences using the notation of Strassmann's Theorem.

Corollary 4.3. *Let $f(x) = \sum a_n x^n$ be a non-zero power series which converges on $\mathbb{Z}_p$, and let $\alpha_1, \ldots, \alpha_m$ be the roots of $f(x)$ in $\mathbb{Z}_p$ (multiplicity allowed). Then, we can find a power series $g(x)$ which converges on $\mathbb{Z}_p$ but has no zeros in Z_p, specifically:*

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_m) g(x)$$

Proof. This corollary comes from the factoring idea in the inductive step in the proof of Strassman's Theorem. Note that since α_1 is a root of f, standard facts about topological fields tells us that f must be off the form

$$f(x) = (x - \alpha_1) g_1(x)$$

where $g_1(x)$ is a function with at most $m - 1$ zeros. We repeat this process indefinitely

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_m) g_m(x)$$

until $g_m(x)$ has no zeros. Then, we let $g(x) = g_m(x)$. ■

Corollary 4.4. *Let $f(x) = \sum a_n x^n$ be a non-zero power series which converges on $p^m \mathbb{Z}_p$, for some $m \in \mathbb{Z}_p$. Then $f(x)$ has a finite number of zeros in $p^m Z_p$.*

Proof. Let $g(x) = f(p^m x) = \sum a_n p^{mn} x^n$. Because $f(x)$ is known to converge on $p^m \mathbb{Z}_p$, $g(x)$ converges for $x \in \mathbb{Z}_p$. We now apply Strassmann's theorem to $g(x)$ which gives the desired conclusion. ■

Finally, we end off this section with a bound for the number of roots in $p^m \mathbb{Z}_p$.

Corollary 4.5. *The bound for the number of roots of a function in $p^m \mathbb{Z}_p$ is N.*

Proof. Note that N is defined in the same way as in the statement of Strassmann's theorem. We use a similar form to the previous corollary. We want to put $f(x) = \sum a_n x^n$. In order to do that, we have to look at the series $\sum a_n p^{mn} x^n$. We find N such that the conditions for Strassmann's theorem are met.

$$|p^{mN} a_N| = \max |p^{nm} a_n| \text{ and } |p^{mn} a_n| < |p^{mN} a_N| \text{ for } n > N$$

Therefore $f(x)$ has at most N zeros on $p^m Z_p$. ■

For more information on the theorem and applications, one can consult [CONb] and [Che18].

4.2 Alternative proof

Alternatively, we can prove this theorem using the definition of a p-adic analytic function, which we will use in the proof of the Mahler-Lech-Skolem Theorem. To define what a p-adic analytic function is, we introduce the idea of an open ball.

Definition 4.6. Let $\Bbbk$ be a field with absolute value $||$. Let $a \in \Bbbk$ be an element and $r \in R_+$ be a real number. The open ball of radius r and center a is the set

$$B(a, r) = \{x \in \Bbbk : d(x, a) < r\} = \{x \in \Bbbk : |x - a| < r\}.$$

The closed ball of radius r and center a is the set

$$\overline{B}(a, r) = \{x \in \Bbbk : d(x, a) \leq r\} = \{x \in \Bbbk : |x - a| \leq r\}.$$

This allows us to define what a p-adic analytic function is.

Definition 4.7. Let B be an open ball in $\mathbb{Z}_p$. A function $f : B \to \mathbb{Z}_p$ is p-adic analytic if it is defined by a power series

$$f(z) = \sum_{k \geq 0} a_k (z - b_0)^k$$

for some $b_0 \in B$, with the power series convergent for all $z \in B$.

This definition implies that an analytic function on a ball is defined by a single power series. At every point b in the domain, there is some smaller ball around B such that the function is computed using a power series in that smaller ball. We emphasize that p-adic analytic functions which are locally power series on a ball are actually globally so. The reader can consult [Kob77, Chapter 4] for more information on this specifically.

We then rewrite Strassmann's theorem to incorporate the concept of p-adic analytic function.

Theorem 4.8. *Let $f : B \to \mathbb{Z}_p$ be a p-adic analytic function. Then either f is identically zero, or it has only finitely many zeros in B.*

We make use of following theorem, which is further discussed in [Gou97, Chapter 5].

Theorem 4.9. *$\mathbb{Z}_p$ is compact.*

We are now ready to prove Strassmann's theorem.

Proof. We start by contradiction, assuming f has infinitely many zeros, say $f(b_k) = 0$. By applying the lemma in the previous slide, the b_k have a limit point b.

We expand f about b using $f(z) = \sum a_k (z - b)^k$. If f is not identically zero, some $a_k \neq 0$; let a_N be the first coefficient.

$$f(z) = (z - b)^n (a_N + (z - b) g(z))$$

Moreover, for $|z - b|_p$ being very small, we see that

$$|(z - b) g(z)|_p < |a_N|_p$$

Specifically, f is non-zero in some small punctured disk about b. This is a direct contradiction. ■

5 First Proof

We might ask, how exactly does this p-adic approach help with arithmetic progressions? Let us imagine that given a linear recurrence a_k we could find some p-adic analytic functions f_i with $i \in [0, m-1]$ such that $f_i(n) = mn+i$ for large n. Then, each f_i would be 0 or it would have finitely many zeros. Moreover, this would complete the proof, and the main point of the proof is to find such a function f_i.

Theorem 5.1. *Let a_i determine a linear recurrence. The set of zeros of this linear recurrence form a finitely set or an arithmetic sequence.*

Let us work through some examples. We consider the traditional Fibonacci sequence $a_n = a_{n-1} + a_{n-2}$ with initial conditions $a_0 = 0$ and $a_1 = 1$. Let S_a denote the zero set.

In this case $S_a = \{0\}$ because the only zero is at a_0, and the recurrence keeps increasing.

Suppose we have a linear recurrence $a_n = a_{n-1} + 2a_{n-2} + 3a_{n-3}$ with initial conditions $a_0 = a_1 = a_2 = 1$.

$S_a = \emptyset$ because we start out at a positive integer, and keep increasing.

Finally, what if we have $a_n = a_{n-2}$ with $a_0 = 0$ and $a_1 = 1$?

$S_a = \{n \in N | n \equiv 0 \pmod 2\}$. This is because the sequence alternates between 0 and 1, and only indices that are zero are $n \equiv 0 \pmod 2$ are 0.

Proof. This proof is due to Hansel [Han86]. Notice that a linear recurrence can be expressed as a matrix $a_k = [A^k v, w]$ for A an $n \times n$ integer matrix and v, w being integer vectors (here v is the initial conditions; A is the transition matrix; and w picks out the top entry of a vector). We choose a prime p such that A is invertible modulo p, meaning that p does not divide the determinant of A.

The group of invertible matrices $\pmod p$ is finite, so we define m as such for $A^m \equiv 1 \pmod p$, which will be the period of the arithmetic progression. To understand why we there is such a m, notice that $A^m \pmod p$ over $\mathbb{F}_p$ (this is a finite field with p elements) takes on finitely many values. Thus, by pigeonhole principle, there exists such an m.

Let us write $A^m = I + pB$ for some matrix B. We now construct our f_i. For $i \in [0, m-1]$:

$$f_i(n) = a_{mn+i} = [A^{mn} A^i v, w] = [(I + pB)^n A^i v, w].$$

We now expand the $(I + pB)^n$ part with the binomial expansion theorem.

$$f_i(n) = \sum_j p^j P_j(n)$$

for some polynomials P_j with coefficients in the p-adic integers, which follow from the binomial coefficients. Indeed, the binomial expansion of $(I + pB)^n$

contains terms involving a polynomial in n times $\frac{p^k}{k!}$ for natural number k (in the binomial expansion). The number of times that p divides k is

$$\lfloor\frac{k}{p}\rfloor + \lfloor\frac{k}{p^2}\rfloor + \cdots \leq \frac{k}{p} + \frac{k}{p^2} + \cdots = \frac{k}{p-1}$$

which grows slower than k since $p \geq 2$. Thus, each of the P_j can be built using only finitely many of the terms in the binomial expansion. Note that we use the index j because we have p^n in the binomial expansion, so we cannot use i.

This power series makes sense as a p-adic analytic function convergent on all of $\mathbb{Z}_p$. We are done, since each f_i has only finitely many zeros or is identically zero by Strassmann's theorem.

■

6 Exponentials and Logarithmns

We have investigated the use of p-adics in Strassmann's theorem and linear algebra. We combined both methods to give the first proof. We now look at exponential and logarithmnic functions in the p-adic sense to construct another proof of the Mahler-Lech-Skolem theorem.

Our goal is to use power series to define p-adic functions that are analogous to the trivial exponential and logarithm functions we regularly use. Take log to mean the formal power series, not the function.

The power series for a logarithm is:

$$f(x) = \log(x+1) = \sum_{n=1}^{\infty}(-1)^{n+1}\frac{x^n}{n} = x - \frac{x^2}{2} + \frac{x^3}{3} - \infty$$

Since the coefficients of the power series are rational, it is not a far leap to think of the series as a power series in $\mathbb{Q}_p$ (for any prime p). We begin by finding the radius of convergence.

Let $f(x) = \sum_{n=1}^{\infty}(-1)^{n+1}\frac{x^n}{n}$, so $a_n = \frac{(-1)^n}{n}$. Then,

$$|a_n| = |\frac{1}{n}| = p^{v_p(n)}$$

From this we have:

$$\sqrt[n]{|a_n|} = p^{\frac{v_p(n)}{n}} \to 1$$

This last part follows as $v_p(n)$ is the largest m such that p^m divides n, so $v_p(n) \leq \frac{\log(n)}{\log(p)}$. Moreover, $\frac{v_p(n)}{n} \leq \frac{\log(n)}{n\log(p)}$, which tends to 0 as $n \to \infty$.

Hence, the radius is 1. But, we have to check whether convergence happens on the open or closed ball of radius 1. We investigate $|x| = 1$. In this case $|a_n x^n| = |a_n| = |\frac{1}{n}|$ does not tend to 0 (in fact it is 1 when p does not divide n).

Lemma 6.1. *The series*

$$f(x) = \sum_{n=1}^{\infty}(-1)^{n+1}\frac{x^n}{n} = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \dots$$

converges for $|x| < 1$ (and diverges otherwise).

We conclude that $f(x)$ defines a function on the open ball $B(0, 1)$ of radius 1 and center 0. This suggests that we define the logarithm as $f(x) = \log(x+1)$.

Definition 6.2. Let $U_1 = B(1, 1) = (x \in \mathbb{Z}_p : |x - 1| < 1) = 1 + p\mathbb{Z}_p$. We define the p-adic logarithm of $x \in U_1$ as

$$\log_p(x) = \log(1 + (x - 1)) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(x-1)^n}{n}$$

We note that this function satisfies the simplest proposition of the logarithm.

Proposition 6.3. *Suppose $a, b \in 1 + p\mathbb{Z}_p$. Then,*

$$\log_p(ab) = \log_p(a) + \log_p(b)$$

Proof. This proof dives into some deeper results, which we leave the reader a reference [Gou97, Chapter 5]. ■

Curiously so, notice that if $p = 2$, then $-1 \in B$, so $\log_p(-1)$ makes sense. To evaluate it, all we have to notice is that $2\log_2(-1) = \log_2(-1)^2 = \log_2(1) = 0$, so $\log_p(-1) = 0$.

Now that we have understood logarithmns, let us examine exponentials. Classically, the series

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!} = 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \cdots$$

converges for all $x \in \mathbb{R}$ as the coefficients $\frac{1}{n!}$ tend to 0. However, in the p-adic context, this is not true, because as $\frac{1}{n!}$ tends to 0, $\frac{1}{n!}$ becomes very large as n gets larger. Our first business is to determine the radius, i.e. how divisible $n!$ is by p.

Lemma 6.4. *Let p be a prime. Then*

$$v_p(n!) = \sum_{i=1}^{\infty} \lfloor \frac{n}{p_i} \rfloor < \frac{n}{p-1}$$

Proof. A proof can be found in [Gou97, Chapter 5]. ■

With these estimates, we work out the radius of convergence for the exponential. This will become a key part in the latter proof.

Lemma 6.5. *Let*

$$g(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots$$

Then $g(x)$ converges if and only if $|x| < p^{\frac{-1}{p-1}}$.

Proof. Since

$$|a_n| = |\frac{1}{n!}| = p^{v_p(n!)} < p^{\frac{n}{p-1}}$$

by our work in the previous part, we have

$$p \geq p^{\frac{-1}{p-1}}$$

Therefore, the series converges for $|x| < p^{\frac{-1}{p-1}}$.

On the other hand, suppose that we have $|x| = p^{\frac{-1}{p-1}}$ and let $n = p^m$ be a power of p. Thus:

$$v_p(n!) = v_p(p^m!) = 1 + p + \cdots + p^{m-1} = \frac{p^{m-1}}{p-1}$$

Because $v_p(x) = \frac{1}{p-1}$:

$$v_p(\frac{x^n}{n!}) = v_p(\frac{x^{p^m}}{p^m!}) = \frac{p^m}{p-1} - \frac{p^m - 1}{p-1} = \frac{1}{p-1}$$

This does not depend on m, hence $\frac{x^n}{n!}$ cannot tend to 0, and the series does not converge. The region of convergence is a disk, which proves our lemma. ■

The astute reader can see something strange about the inequality. If $p \neq 2$ and $x \in \mathbb{Z}_p$, then the absolute value of x is either 1 (bigger than $p^{\frac{-1}{p-1}}$) or less than or equal to $\frac{1}{p}$ (which is smaller): there are no values in the middle. Thus, if $p \neq 2$:

$$|x| < p^{\frac{-1}{p-1}} \iff |x| \leq p^{-1} \iff x \in p\mathbb{Z}_p \iff |x| < 1,$$

so that the disk in the lemma is just the open disk of radius 1.

As long as we stay in $\mathbb{Q}_p$, things are not too troublesome. If $p \neq 2$, $g(x) = \exp(x)$ converges for $x \in p\mathbb{Z}_p$. If $p = 2$, $\frac{-1}{2-1} = -1$, so the lemma tells us that $g(x) = \exp(x)$ converges when $|x| < \frac{1}{2}$, which occurs when $x \in 4\mathbb{Z}_2$. We can now define the p-adic exponential function.

Definition 6.6. Let $D = B(0, p^{\frac{-1}{p-1}}) = (x \in \mathbb{Z}_p : |x| < p^{\frac{-1}{p-1}})$. The p-adic exponential is the function $\exp_p : D \to \mathbb{Q}_p$ defined by

$$\exp_p(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

Notice that $\exp_p(1)$ is not defined, so there is no natural p-adic analogue of e in $\mathbb{Q}_p$. Let us make sure that this satisfies most of the formal properties of the classical exponential.

Proposition 6.7. *If $x, y \in D$, we have $x + y \in D$ and*

$$\exp_p(x + y) = \exp_p(x)\exp_p(y).$$

Proof. We essentially just manipulate power series.

$$\exp_p(x+y) = \sum_{n=0}^{\infty} \frac{(x+y)^n}{n!} = \sum_{n=0}^{\infty} \frac{1}{n!} \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k =$$

$$= \sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{1}{n!} \frac{n!}{(n-k)!k!} x^{n-k} y^k = \sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{x^{n-k}}{(n-k)!} \frac{y^k}{k!} =$$

$$= (\sum_{m=0}^{\infty} \frac{x^m}{m!})(\sum_{k=0}^{\infty} \frac{y^k}{k!}) = \exp_p(x)\exp_p(y)$$

as we want. ■

We dive into an interesting lemma that gives a formula for $v_p(n!)$.

Lemma 6.8. *Let n be a positive integer, and let $n = a_0 + a_1 p + a_2 p^2 + \cdots + a_k p^k$ be its expansion in base p. Let $s = a_0 + a_1 + \cdots + a_k$ be the sum of the digits in the expansion. Show that*

$$v_p(n!) = \frac{n-s}{p-1}$$

Proof. Notice that $v_p(n!) = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \cdots + \lfloor \frac{n}{p^k} \rfloor$. We consider each component.

$$\lfloor \frac{n}{p} \rfloor = \lfloor \frac{a_0 + a_1 p + a_2 p^2 + \cdots + a_k p^k}{p} \rfloor = a_1 + a_2 p + a^3 p^2 + \cdots + a_k p^{k-1}$$

Notice that since $a_0 < p$, $\lfloor \frac{a_0}{p} \rfloor = 0$. Similarly, we have

$$\lfloor \frac{n}{p^2} \rfloor = a_2 + a_3 p + \cdots + a_k p^{k-2}$$

$$\vdots$$

$$\lfloor \frac{n}{p^k} \rfloor = a_k$$

If we sum everything up, we have:

$$v_p(n!) = a_1 + a_2(p+1) + a_3(p^2+p+1) + \cdots + a_k(p^{k-1} + p^{k-2} + \cdots + 1)$$

We now consider $\frac{n-s}{p-1}$:

$$\frac{n-s}{p-1} = \frac{(a_0 + a_1 p + \cdots + a_k p^k) - (a_0 + a_1 + \cdots + a_k)}{p-1} =$$

$$= \frac{a_1(p-1) + a_2(p^2-1) + a_3(p^3-1) + \cdots + a_k(p^k-1)}{p-1} =$$

$$= a_1 + a_2(p+1) + a_3(p^2+p+1) + \cdots + a_k(p^{k-1} + p^{k-2} + \cdots + 1)$$

This matches our expression for $v_p(n!)$, so we are done. ■

We end this section with a proposition that shows that wrapping $\log_p$ over $\exp_p(x)$ and vice versa leaves x.

Proposition 6.9. *Let $x \in \mathbb{Z}_p, |x| < p^{\frac{-1}{p-1}}$. Then we have*

$$|\exp_p(x) - 1| < 1$$

so that $\exp_p(x)$ *is in the domain of* $\log_p$*, and*

$$\log_p(\exp_p(x)) = x.$$

Conversely, if $|x| < p^{\frac{-1}{(p-1)}}$ *we have*

$$|\log_p(1+x)| < p^{\frac{-1}{(p-1)}}$$

so that $\log_p(x+1)$ *is in the domain of* $\exp_p$*, and*

$$\exp_p(\log_p(x+1)) = x + 1.$$

Proof. Consult [Gou97, Chapter 5] for a proof. ■

7 P-adic Interpolation

[CONa] Interpolation is the idea of finding a function given a data set. We give the standard example of p-adic interpolation. Suppose $n \in \mathbb{Z}_p$ is any p-adic integer, and α is an integer. Then it make sense to compute n^α. Thus, we consider the function $f(\alpha) = n^\alpha$, which is well defined for $\alpha \in \mathbb{Z}$.

Essentially we want to extend this function to the widest possible range of p-adic values of α. Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$ (we showed this in the alternative proof for Strassmann's theorem).

The problem of finding such an extension is called the problem of finding a p-adic interpolation of the function $f(\alpha) = n^\alpha$. We leave the well-known theorem in preparation for the next proposition.

Theorem 7.1. *Any continuous function defined on a compact set is automatically uniformly continuous and bounded*

Proof. [Gou97][Chapter 5] has more information ■

Suppose that $f(\alpha)$ can be extended to $\mathbb{Z}_p$, then since $\mathbb{Z}_p$ is compact, the extension has to be founded and uniformly continuous. Hence, so would $f(\alpha)$. Curiously, these two conditions are sufficient.

Proposition 7.2. *Let S be a dense subset of $\mathbb{Z}_p$, and let $f : S \to \mathbb{Q}_p$ be a function. Then there exists a continuous extension $f' : \mathbb{Z}_p \to \mathbb{Q}_p$ of f to $\mathbb{Z}_p$ if and only if f is bounded and uniformly continuous. If it exists, this extension is unique.*

Proof. By our discussion above, we know that the condition is necessary, and that the extension is unique if it exists. Notice that if $x \in \mathbb{Z}_p$, there exists a sequence

$$\alpha_1, \alpha_2, \dots \alpha_k, \dots$$

of elements of S which tend to x (because S is dense). If f' exists, then we will have

$$f'(x) = \lim_{k \to \infty} f'(\alpha_k) = \lim_{k \to \infty} f(\alpha_k).$$

Note that (α_k) is a Cauchy sequence, so

$$\lim_{k \to \infty} |\alpha_{k+1} - \alpha_k| = 0.$$

Hence, it follows that since f is uniformly continuous and bounded,

$$\lim_{k \to \infty} |f(\alpha_{k+1}) - f(\alpha_k)| = 0$$

so that $f(\alpha_k)$ is indeed a Cauchy sequence. Moreover, it has a limit in $\mathbb{Q}_p$. We define f' by the condition it has to satisfy:

$$f'(x) := \lim_{k to \infty} f(\alpha_k)$$

for any sequence (α_k) converging to x. This gives the extension.

■

We know that f' exists, but we do not know anything else about it. Can it be written as a power series? Can we extend it to a set larger than $\mathbb{Z}_p$?

Recall the definition of uniform continuity. We take $f(\alpha)$ to be a function defined on a dense subset S of $\mathbb{Z}_p$, with values in $\mathbb{Q}_p$. Being "close" in S implies being congruent modulo a high power of p, and being "close" in $\mathbb{Q}_p$. Hence f is uniformly continuous if it satisfies the following condition:

$$\alpha \equiv \beta \pmod{p^N} \implies f(\alpha) = f(\beta) \pmod{p^m}$$

for $m \in \mathbb{Z}$ there exists an $N in \mathbb{Z}$ such that the above is true. Therefore, uniform continuity has a translation in terms of congruity. We return to the exponential $\alpha \to n^\alpha$ for $\alpha \in \mathbb{Z}$ and $n \in \mathbb{Z}_p$, and we want to extend it to all of $\alpha \in \mathbb{Z}_p$. However this depends on the n.

Let us work with the assumption that n is a $1-$unit (this just means that $n \in 1 + p\mathbb{Z}_p$. We make use of the binomial series to get the interpolation.

Corollary 7.3. *For any $n \in 1 + \mathbb{Z}_p$, there exists a continuous function $f_n : \mathbb{Z}_p \to \mathbb{Q}_p$ such that for any $\alpha \in \mathbb{Z}$ we have $f_n(\alpha) = n^\alpha$*

We outline some possible approaches. We introduce a simple piece of notation.

Definition 7.4. For any $\alpha \in \mathbb{Z}_p$ and any $x \in p\mathbb{Z}_p$, we define

$$(1+x)^\alpha := \boldsymbol{B}(\alpha, x)$$

Proof. We can merely give $f_n(\alpha) = \boldsymbol{B}(\alpha, n-1)$, which converges because we assumed $n \in 1 + p\mathbb{Z}_p$. However checking continuity is not so easy. Note that we want continuity in α, not n, so it is not valid to merely say that power series are continuous functions. This is outside the scope of the paper, so we omit the proof. Interested readers can consult [Gou97, Chapter 5] for more discussion. ■

We can also show this corollary in a more direct approach by showing that if $n \in 1+p\mathbb{Z}_p$ then $\alpha \to n^\alpha$ is bounded and uniformly continuous. Boundedness is trivial as any integer power of n will be in $\mathbb{Z}_p$ because n is a 1-unit. Uniform continuity is not too bad either. We notice that

$$(1+pk)^{p^m} \equiv 1 \pmod{p^{m+1}}$$

so if $\beta = \alpha + ip^m$ we have

$$n^\beta = n^\alpha \cdot (n^{p^m})^i \equiv n^\alpha \pmod{p^{m+1}}$$

which is what we want. Thus, we know that f_n exists. Proving that $f_n(\alpha) = B(\alpha, n-1)$ requires showing continuity, as mentioned before.

We can also do this an entirely different way, making use of exponentials and logarithmns that we just went over. We define $n^\alpha = \exp_p(\alpha \log_p(n))$. This works because there are no convergence issues to check (and gives the same result by continuity).

The mishap is that we require $|\alpha \log_p(n)| < p^{\frac{-1}{p-1}}$ to be able to compute the exponential, and $|n-1| < 1$ to compute the logarithm. The second condition is already assumed as $n \in 1+p\mathbb{Z}_p$. We have shown that it implies $|\log_p(n)| < 1$, so if $\alpha \in \mathbb{Z}_p$ and $p \neq 2$, that in $\mathbb{Z}_p$ having more absolute value less than 1 implies having absolute value $\leq \frac{1}{p}$. Generally, this idea does not work as well, but here it is fine.

8 Second Proof

[vdP89, Chapter 3] We are now ready to present the second proof of the Mahler-Lech-Skolem theorem. The general case requires a technique that we have not talked about, which is quite complex, so we present the case of sequences defined over the rationals. For a detailed proof in the general case, consult [vdP89, Chapter 3]. The main idea of p-adic interpolation is altogether the same as below.

Definition 8.1. The characteristic of a field is the smallest positive integer p such that adding 1 p times yields 0. If no such p exists, then the field is said to have characteristic 0.

Theorem 8.2. *The set of zeros of a linear recurrence sequence over a field of characteristic zero comprises a finite set together with a finite number of arithmetic progressions.*

Proof. [EvdPSW03, Chapter 2] Let $\mathbb{L}$ denote the splitting field of the characteristic polynomial of the given linear recurrence a.

A splitting field is the smallest field extension in which the polynomial factors completely into linear factors.

We choose a prime p with the property that all characteristic roots are units in $\mathbb{Q}_p$ and the prime ideal generated by p splits completely in $\mathbb{L}$.

Then, for each i, $\alpha_i^{p-1} \equiv 1 \pmod{p}$, so the p-adic logarithms

$$\log_p(\alpha_i^{p-1}) = \log_p(1 - (1 - \alpha_i^{p-1}))$$

are defined, and satisfy $v_p(\log_p(\alpha_i^{p-1})) \geq 1$. We recall that the p-adic exponential $\exp_p(t)$ converges for $t \in \mathbb{C}_p$ with $v_p(t) > \frac{1}{p-1}$.

This allows us to p-adically interpolate the $(p-1)$ sequences $(a(r+(p-1)x)), 0 \leq r \leq p-2$, yielding p-adic analytic functions

$$a_{p,r}(t) = \sum_{i=1}^{m} A_i(r+(p-1)t)\alpha_i^r \exp(t \log \alpha_i^{p-1}), r = 0, 1, 2, \ldots, p-2$$

converging for $v_p(t) > -1 + \frac{1}{p-1}$, and in particular on $\mathbb{Z}_p$.

Since $\mathbb{Z}$ is a dense subset of the compact set $\mathbb{Z}_p$, if any of these functions has infinitely many integer zeros it must vanish identically. It follows by the pigeonhole principle that, if the original linear recurrence sequence a has infinitely many zeros, then at least one of those $p-1$ functions vanishes. In particular, it follows that for some r, $a(r+(p-1)x) = 0, x = 1, 2, \ldots$.

■

9 Open Questions

Lech proved in 1953 that the set of zeros of a linear recurrence sequence in a field of characteristic 0 is the union of a finite set and finitely many infinite arithmetic progressions.

In 2005, Harm Derksen proved an analog of the Mahler-Lech-Skolem theorem in positive characteristic. Interested readers are recommended to read [Der07]. We now present some open questions.

- Can the size of the common difference of the arithmetic progressions in the degenerate case be estimated?
- Can the theorem be used to decided whether a given linear recurrence sequence has infinitely many zeros?
- Can the number of zeros of a non-degenerate linear recurrence sequence be estimated?
- Can the set of zeros be found effectively?

- Can the general bounds for special interesting families of linear recurrence sequences be improved?
- For what other interesting classes of sequences does a similar result hold?

There is much to say about these questions, and most have a satisfactory partial solution. The lone exception is the fourth question: no effective method is known to find the set of all zeros for an arbitrary non-degenerate linear recurrence sequence.

The simplest question is the first. For a linear recurrence sequence of order n over an algebraic number field $\mathbb{K}$ with degree d over $\mathbb{Q}$, the least common multiple of the differences of the corresponding zero progressions does not exceed $M(d,n)$ where $M(d,n)$ is given as following:

Theorem 9.1. *Let a denote a linear recurrence sequence of order n over an algebraic number field $\mathbb{K}$ of degree d over $\mathbb{Q}$. Then there is a constant*

$$M(d,n) \leq \begin{cases} \exp(2n(3\log n)^{\frac{1}{2}}) & \text{if } d = 1 \\ 2^{nd+1} & \text{if } d \geq 2 \end{cases}$$

such that for some $M \leq M(d,n)$ each subsequence $(a(Mx+\ell))$ is either identically zero, or is non-degenerate.

Interested readers can consult [BM76] and [Rob78] for more information.

References

[Blo17] Adam B Block. The skolem-mahler-lech theorem. *New York: Columbia*, 2017.

[BM76] Jean Berstel and Maurice Mignotte. Deux propriétés décidables des suites récurrentes linéaires. *Bull. Soc. Math. Fr.*, 104:175–184, 1976.

[Che18] Yuchen Chen. p-adics, hensel's lemma and strassman's theorem. *University of Chicago*, 2018.

[CONa] Keith CONRAD. p-adic interpolation. *URL http://www. math. uconn. edu/kconrad/math5020f11/padicinterpolation. pdf.*

[CONb] KEITH CONRAD. Strassmann's theorem and an application.

[Der07] Harm Derksen. A Skolem-Mahler-Lech theorem in positive characteristic and finite automata. *Invent. Math.*, 168(1):175–224, 2007.

[EvdPSW03] Graham Everest, Alf van der Poorten, Igor Shparlinski, and Thomas Ward. *Recurrence sequences*, volume 104 of *Math. Surv. Monogr.* Providence, RI: American Mathematical Society (AMS), 2003.

[Gou97] Fernando Q. Gouvêa. *p-adic numbers: An introduction.* Universitext. Berlin: Springer, 2nd ed. edition, 1997.

[Han86] G. Hansel. A simple proof of the Skolem-Mahler-Lech theorem. *Theor. Comput. Sci.*, 43:91–98, 1986.

[HK71] K. Hoffman and R. Kunze. Linear algebra. Englewood Cliffs, N. J.: Prentice-Hall, Inc. VIII, 407 p. (1971)., 1971.

[Kob77] Neal Koblitz. *P-adic numbers, p-adic analysis, and zeta-functions*, volume 58 of *Grad. Texts Math.* Springer, Cham, 1977.

[Rob78] Philippe Robba. Zeros de suites recurrentes linéaires. In *Groupe d'étude d'analyse ultramétrique. 5ème année: 1977/78.* Paris: Secrétariat Mathématique, 1978.

[vdP89] A. J. van der Poorten. Some facts that should be better known, especially about rational functions. Number theory and applications, Proc. NATO ASI, Banff/Can. 1988, NATO ASI Ser., Ser. C 265, 497-528 (1989)., 1989.