Survey of p-adic Numbers

Catherine Warner

December 14, 2018

1 Introduction

The p-adic numbers, denoted $\mathbb{Q}_p$ is a complete field that can be constructed from the rationals similarly to the construction of the reals using Cauchy sequences. In fact, the construction of the p-adics is a generalization of the construction of the reals. The p-adics are also an important example of a non-Archimedean field. Thus, many of the demonstrated properties of the p-adics can be applied to any non-Archimedian field.

This paper will show the completion of the rationals to the p-adics using the method of Cauchy sequences. The non-archimedean property of the p-adic numbers will then be used to prove the Skolem-Mahler-Lech theorem.

2 The Field of p-Adic Numbers

2.1 Construction of the Reals from the Rationals

The most familiar and intuitive field completion is that of the reals from the rationals. This process will be used first as an example as the algebraic completion of fields, and then it will be clear how the construction of the p-adics is the same process with the only difference being a change in the absolute value function.

The construction of the reals from the rationals is done in four basic steps. First, the ordinary absolute value function is taken over the rationals. Then a metric called the distance function is obtained on the rationals. Next, Cauchy sequences are taken in the rationals with respect to the metric. Finally, the reals are created by completing the Cauchy sequences over the rationals with respect to the ordinary absolute value metric.

To construct the p-adic numbers instead of the reals, the only difference in this method will be a change in the absolute value function. But first, let's understand in more detail the completion of the reals.

2.1.1 Absolute Value function

First, an absolute value function is taken on $\mathbb{Q}$ defined as

$$|\cdot| \quad : \quad \mathbb{Q} \to \mathbb{Q}_+.$$

For the construction of the reals, the ordinary absolute value is used, defined specifically as

$$|x| = \begin{cases} x & : \quad x \geq 0 \\ -x & : \quad x < 0 \end{cases}$$

It will eventually be shown that this map really goes from the rationals to the reals. Since the reals have not been defined yet, $\mathbb{Q}_+$ is used in their place. Recall that the ordinary absolute value function satisfies the following conditions for all x and y in $\mathbb{Q}$:

1. $|x| = 0$ if and only if $x = 0$.
2. $|xy| = |x||y|$

3. $|x + y| \leq |x| + |y|$

2.1.2 Metric

Next, a metric is induced by the absolute value function. The metric is called $'d'$ because it is a distance function. The ordinary absolute value combined with the rationals form a metric space. $\mathbb{Q}$ is the metric space, and the ordinary absolute value is the distance function.

This metric space is written as $(\mathbb{Q}, \quad |\cdot|)$ and defined as

$$d : \quad \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}_+$$

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

This is the same as the familiar definition of the distance between two points x and y as the absolute value of their distance. All metrics on $\mathbb{Q}$ satisfy the following conditions for all x and y in $\mathbb{Q}$:

1. $d(x, y) \geq 0$
2. $d(x, y) = d(y, x)$
3. $d(x, z) \leq d(x, y) + d(y, z)$ (The triangle inequality).

2.1.3 Cauchy sequences

Definition 1. A sequence of elements $x_n \in \mathbb{Q}$ is a Cauchy sequence if for every real $\epsilon > 0$, there is a positive integer bound M so that for all integers $m, \quad n \geq M$,

$$d(x_m, x_n) = |x_m - x_n| < \epsilon.$$

Thus, a Cauchy sequence is a sequence whose terms are crowded into smaller and smaller balls.

Note 1. The following condition is not equivalent to the Cauchy condition with the ordinary absolute value:

$$\lim_{x \to \infty} |x_{n+1} - x_n| = 0.$$

That is, a sequence whose terms get closer and closer together is not necessarily Cauchy under the ordinary absolute value function.

Here is a counterexample:

$$\{\sum_{n=1}^{m} \frac{1}{n} \quad : \quad m = 1, 2, 3, \ldots\}$$

In this sequence, the terms get closer together, but the sequence diverges, so it is not Cauchy.

Definition 2. A field is complete with respect to the absolute value function if every Cauchy sequence has a limit in the field.

It is easy to see that $\mathbb{Q}$ is not complete with respect to the ordinary absolute value metric. The sequence toward π, for instance, has no limit in $\mathbb{Q}$.

2.1.4 Complete $\mathbb{Q}$.

To complete $\mathbb{Q}$, all of the missing limits of Cauchy sequences must be added in. There are several ways to do this, but the most intuitive is probably the use of quotient groups. This is the method that will be described here.

To fill in the missing limits, replace the missing limit with the sequence itself. Define S as the set of all Cauchy sequences of rational numbers.

Definition 3. Two Cauchy sequences $s_1 = \{a_j\} \in S$ and $s_2 = \{b_j\} \in S$ are equivalent, $s_1 \sim s_2$ if $|a_j - b_j| \to 0$ as $j \to \infty$.

That is, two Cauchy sequences are equivalent if they converge to the same limit.

Definition 4. $\mathbb{R}$ is the set of equivalence classes of the Cauchy sequences of rational numbers.

This is a formal analytic completion of $\mathbb{Q}$ to $\mathbb{R}$, and the completion of $\mathbb{Q}$ to $\mathbb{Q}_p$ will be completed in the same manner, with more explanation of how a set of equivalences forms a complete field.

2.2 Construction of the p-adics from the rationals

As noted above, the creation of the p-adic numbers will be analogous to the above process, with a change in the absolute value function. The p-adic absolute value is defined for each fixed prime p. Note that all rational numbers can be written as $x = p^v \frac{a}{b}$ where $p, \quad a$, and b are all coprime.

2.2.1 Absolute value function

Definition 5. The p-adic absolute value of $x \in \mathbb{Q}$ is defined as,

$$|\cdot|_p \quad : \quad \mathbb{Q} \to \mathbb{Q}_+$$

$$|x|_p = |p^v \frac{a}{b}|_p = p^{-v}.$$

By convention, $|0|_p = 0$. The p-adic absolute value satisfies the normal three conditions of an absolute value from before, but its third condition is stronger, making it a non-archimedian absolute value.

Definition 6. An absolute value function is non-archimedian if it satisfies the following condition:

$$|x + y| \leq \max\{|x|, |y|\}$$

Lemma 1. *For a non-archimedian absolute value, if* $|x| \neq |y|$, *then* $|x + y| = \max\{|x|, |y|\}$.

Proof. Without loss of generality, assume $|x| > |y|$. Then

$$|x| = |(x + y) - y| = \max\{|(x + y)|, |y|\} = |x + y| \quad .$$

□

2.2.2 Metric

The metric induced by a non-archimedian absolute value has the same conditions as the ordinary absolute value function, but the triangle inequality is stronger. A non-archimedian absolute value induces an ultrametric space.

Definition 7. An ultrametric space is the metric spaced induced by a non-archimedian absolute value. It meets the three absolute value conditions, but its triangle inequality is stronger and states,

$$d(x, z) \leq \max\{d(x, y) + d(y, z)\}.$$

Lemma 2. *In an ultrametric space, all "triangles" are isosceles.*

Proof. Say x, y, and z are vertices of a triangle. If $|x-y| = |y-z|$, the lemma is proved. If not, $|x-z| = \max\{|x-y|, |y-z|\}$ by the third condition of a non-archimedian absolute value. □

Definition 8. The p-adic metric space $(\mathbb{Q}, \quad |\cdot|_p)$ is defined as

$$d : \quad \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}_+$$

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

As an aside, we may still think of this metric as the distance function, which reveals an interesting meaning of distance. For example, when $p = 3$, the number 2 is closer to 92 than it is to 3. Explicitly,

$$|92-2|_3 = |90|_3 = |3^2 \times 10|_3 = 3^{-2} = 1/9$$

$$|3-2|_3 = |1|_3 = |3^0|_3 = 3^{-0} = 1$$

Thus, 2 is 9 times closer to 92 than to 3 using the p-adic absolute value.

2.2.3 Cauchy sequences

Lemma 3. *A sequence (x_n) of rational numbers is a Cauchy sequence with respect to a non-archimedian absolute value if and only if*

$$\lim_{x\to\infty} |x_{n+1} - x_n| = 0.$$

Proof. Recall that an absolute value is non-archimedian if and only if $|x+y| \leq \max\{|x|, |y|\}$.

Then for $n + r > n$,

$$|x_{n+r} - x_n| = |x_{n+r} - x_{n+r-1} + x_{n+r-1} - x_{n+r-2} + x_{n+r-2} + \cdots + x_{n+1} - x_n|$$

$$|x_{n+r} - x_n| \leq \max\{|x_{n+r} - x_{n+r-1}|, |x_{n+r-1} - x_{n+r-2}|, \ldots, |x_{n+1} - x_n|\}$$

Without loss of generality, choose a maximum distance between elements.

Then, $\lim_{n\to\infty} |x_{n+r} - x_n| \leq \lim_{n\to\infty} |x_{n+1} - x_n|$, which is possible only if $\lim_{n\to\infty} |x_{n+1} - x_n| = 0$. □

Note that this condition was previously noted to *not* be equivalent to the Cauchy condition for the ordinary absolute value. It is also easy to see that $\mathbb{Q}$ is still not complete with respect to the p-adic absolute value function.

2.2.4 Complete $\mathbb{Q}$

Definition 9. The set of all Cauchy sequences of elements of $\mathbb{Q}$ is defined as

$$\mathscr{C}_p(\mathbb{Q}) = \{(x_n) \quad : \quad (x_n) \text{ is a cauchy sequence with respect to } ||_p\} \quad .$$

Proposition 1. *$\mathscr{C}$ is a commutative ring with unity with addition and multiplication defined as*

$$(x_n) + (y_n) = (x_n + y_n)$$

$$(x_n) \cdot (y_n) = (x_n y_n)$$

Note that $\mathscr{C}$ is not a field because $(x_n)\cdot(y_n) = (0)$ for $x_n, y_n \neq 0$. Still, $\mathscr{C}$ is technically a formal analytic completion of $\mathbb{Q}$ because all sequences in $\mathscr{C}$ converge to an element of $\mathscr{C}$.

As with the construction of the reals, the p-adics will be constructed by "modding out" equivalent sequences.

First, check that $\mathbb{Q}$ is at least included in $\mathscr{C}$, which is required for $\mathscr{C}$ to be a completion of $\mathbb{Q}$.

Lemma 4. $\mathbb{Q} \subset \mathscr{C}$

Proof. For $x \in \mathbb{Q}$, $x, x, x, \ldots = (x)$, which gives the following inclusion of $\mathbb{Q}$ into $\mathscr{C}$.

$$\mathbb{Q} \hookrightarrow \mathscr{C}$$

$$x \mapsto (x)$$

□

Next, equivalence classes must be constructed. These will become the elements of the final goal, which is $\mathbb{Q}_p$. Recall that Cauchy sequences are equivalent if their difference tends to zero. That is, their difference is a sequence whose final elements are a trail of zeros. Equivalently, their difference must be in the ideal $\mathcal{N}$.

Definition 10. The ideal, $\mathcal{N}$, of $\mathscr{C}$ is the set of sequences tending toward 0.

$$\mathcal{N} \subset \mathscr{C}$$

$$\mathcal{N} = \{(x_n) \quad : \quad x_n \to 0\} = \{(x_n) \quad : \quad \lim_{n\to\infty} |x_n|_p = 0\}.$$

This leads to the final construction of the p-adic numbers.

Definition 11. The field of p-adic numbers is defined as, $\mathbb{Q}_p = \mathscr{C}/\mathcal{N}$.

This definition states that elements of $\mathbb{Q}_p$ are equivalence classes of Cauchy sequences with respect to the p-adic absolute value. Now check that $\mathbb{Q}$ is still included in $\mathbb{Q}_p$.

Lemma 5. $\mathbb{Q} \subset \mathbb{Q}_p$.

Proof. The difference of constant sequences is another constant sequence, so they will never differ by an element of $\mathcal{N}$ and are therefore distinct elements of $\mathbb{Q}_p$.

Given then that $\mathcal{N}$ is an ideal of $\mathscr{C}$, it can be shown that it is also the *maximal* ideal, which implies that $\mathcal{N}$ is a field. □

Lemma 6. *The ideal $\mathcal{N}$ is a maximal ideal of $\mathscr{C}$, and therefore a field.*

Proof. Let $(x_n) \in \mathscr{C}\backslash\mathcal{N}$ and let I be the ideal generated by (x_n) and $\mathcal{N}$. It must be shown that $I = \mathscr{C}$, which is equivalent to showing that the unit element $(1) = 1 + 1 + \ldots \in I$. Since $(x_n) \nrightarrow 0$, $|x_n|_p \geq c > 0$ for all $n \geq N$.

Define $(y_n) = \begin{cases} 0 & n < N \\ \frac{1}{x_n} & n \geq N \end{cases}$

$(y_n) \in \mathscr{C}$ because for $n \geq N$,

$$|y_{n+1} - y_n| = |\frac{1}{x_{n+1}} - \frac{1}{x_n}| = \frac{|x_{n+1} - x_n|}{|x_n x_{n+1}|}$$

And by the non-archimedean property, $\frac{|x_{n+1}-x_n|}{|x_n x_{n+1}|} \leq \frac{|x_{n+1}-x_n|}{c^2} \to 0$.

Notice that

$$x_n y_n = \begin{cases} 0 & n < N \\ 1 & n \geq N \end{cases}.$$

Thus, $(x_n)(y_n)$ is a series of $N-1$ zeros followed by ones.

Then $(1)-(x_n)(y_n)$ is a series of $N-1$ ones followed by zeros. It follows that $(1) = (x_n)(y_n)+(n \in \mathcal{N}) \in I$. Therefore, $I = \mathscr{C}$. □

Next, it must be verified that $\mathscr{C}$ is complete, that is, all Cauchy sequences converge to their limit. This verified by showing that all sequences eventually become stationary.

Lemma 7. *Let $(x_n) \in \mathscr{C}\backslash\mathcal{N}$. Then there exists an integer N such that $|x_n|_p = |x_m|_p$ for all $m, n \geq N$.*

Proof. As shown in the previous proof, since $(x_n) \nrightarrow 0$, it follows that $|x_n| \geq c > 0$ for all $n \geq N_1$. Also, $|x_n - x_m|_p < c$ for all $n, m \geq N_2$. Then combining these two equations, set $N = \max\{N_1, N_2\}$.Then,

$$|x_n - x_m|_p < \max\{|x_n|_p, |x_m|_p\} \text{ for all } m, n \geq N.$$

Then by non-archimedian "isosceles triangle" property, it follows that $|x_n|_p = |x_m|_p$. □

Then the p-adic numbers are defined as the limits of the Cauchy sequences that represent them.

Definition 12. If $\lambda \in \mathbb{Q}_p$ and (x_n) is any Cauchy sequence representing λ,

$$|\lambda|_p = \lim_{n\to\infty} |x_n|_p.$$

From this definition, it can be shown that $\mathbb{Q}_p$ is complete by a similar process that verified that $\mathscr{C}$ is complete. The completeness of $\mathbb{Q}_p$ implies that every Cauchy sequence in $\mathbb{Q}_p$ converges to an element of $\mathbb{Q}_p$. The calculations are somewhat tedious because it must be remembered that elements of $\mathbb{Q}_p$ are defined as Cauchy sequences of elements of $\mathbb{Q}$. Thus, to prove completion, it must be verified that every Cauchy sequence of Cauchy sequences of $\mathbb{Q}$ converges, which they do.

The following theorem gives a summary of what has been shown so far:

Theorem 1. *For every prime $p \in \mathbb{Z}$, there exists a field $\mathbb{Q}_p$with a non-archimedian absolute value $||_p$ such that*

i.) There exists an inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, and the absolute value induced by $||_p$ on $\mathbb{Q}$ via this inclusion is the p-adic absolute value.

ii.) $\mathbb{Q}$ is complete with respect to $||_p$.

The next theorem is noteworthy because it illuminates the significance of the field of p-adic numbers.

Theorem 2. *(Ostrowski's Theorem). Every non-trivial absolute value on $\mathbb{Q}$ is equivalent to one of the absolute values $||_p$, where p is a prime or $p = \infty$.*

Proof. A thorough proof can be found in Gouvea, 43. □

This theorem reveals that the real completion of $\mathbb{Q} \hookrightarrow \mathbb{R}$ and the p-adic completion of $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ are the *only* possible Cauchy completions of $\mathbb{Q}$. Note that the ordinary absolute value is defined as $||_p$, where $p = \infty$. Thus, the p-adic completion of the rationals is really its only possible Cauchy completion.

3 The Skolem-Mahler-Lech Theorem

This section gives an example of a concrete theorem that can be proved using p-adic numbers. The p-adic version of this proof is due to Georges Hansal in 1985, and is significantly shorter than the original proof over $\mathbb{Q}$ created by Thoralf Skolem in 1933.

3.1 Linear Recurrence

Definition 13. A sequence of complex numbers $(u)_n = u_0, u_1, ...$ is a linear recurrence of order m if there exist complex $\alpha_1, \alpha_2, ..., \alpha_m$ where $\alpha_0, \alpha_m \neq 0$ such that for all n,

$$\alpha_0 u_n + a_1 u_{n+1} + \cdots + \alpha_m u_{n+m} = 0 \quad .$$

Definition 14. An integer linear recurrence is a linear recurrence where all of the u_n's and $\alpha_i's$ are integers. A familiar example of an integer linear recurrence is the Fibonnaci sequence.

Definition 15. The zero set of a linear recurrence sequence is the set,

$$\{n \in \mathbb{Z} | u_n = 0\}$$

Then the zero set tells when the linear recurrence takes on the value of zero. Note that the period of the zero set may be zero, specifically when the zero set is the empty set, as is the case for the Fibonnaci sequence. The Skolem-Mahler-Lech theorem will then show that the zero set is eventually periodic.

Example 1. Consider the integer linear recurrence $u_n = u_{n-1} + 2u_{n-2} + 3u_{n-3}$ with $u_0 = u_1 = u_2 = 1$. It is clear that u_n is never zero, since it is always positive. So the zero set is the empty set.

Example 2. Now consider $u_n = -2u_{n-1} + u_{n-2}$ with $u_0 = 2, u_1 = 1$. Here, the zero set is only $\{3\}$, which can be seen by considering the general formula for this sequence,

$$u_n = (1 - \frac{3}{2\sqrt{2}})(-1 - \sqrt{2})^n + \frac{1}{4}(4 + 3\sqrt{2})(\sqrt{2} - 1)^n$$

and noting that the left term dominates for large n.

Example 3. Finally consider $u_n = u_{n-2}$ with $u_0 = 0, u_1 = 1$. Then u_n is zero when n is even. Thus, the zero set is $2\mathbb{Z}$. Note also that it is possible to have a zero set equal to $a + N\mathbb{Z}$. for $a \in \mathbb{Z}, N \in \mathbb{N}$.

The Skolem-Mahler-Lech theorem says that these three types of zero sets are the only ones that can occur. It is impossible to have a zero set of the primes, the squares, or some other non-periodic set. Specifically:

Theorem. *(Skolem-Mahler-Lech 1). Let (u_n) be a linear recurrence. Then there exists $N \in \mathbb{Z}_{\geq 1}$, a possibly empty set $S \subseteq \{0, 1, ..., N-1\}$, and a finite set $T \subset \mathbb{Z}$ such that*

$$u_n = 0 \text{ if and only if } n \in T \cup (S + N\mathbb{Z}) \quad .$$

To prove this theorem, there remain several necessary characteristics of linear recurrences.

Remark 1. If (u_n) and (v_n) are linear recurrences, then $(u_n v_n)$ and $(u_n + v_n)$ are, too. And if A is the solution of (u_n) and B of (v_n), then $A \cup B$ is the solution of $(u_n v_n)$.

Remark 2. The sequence (u_n) is a linear recurrence if and only if $u_n = \sum_{1 \leq i \leq s} p_i(n)\lambda_i^n$ for some $\lambda_i \in \mathbb{C}$ and polynomials $p_i \in \mathbb{C}[X]$.

Lemma 8. *Take any linear recurrence characterized by the formula*

$$U := \{(u_n) | \alpha_0 u_n + a_1 u_{n+1} + \cdots + \alpha_m u_{n+m} = 0\}$$

for fixed $\alpha_0, ..., \alpha_m \in \mathbb{C}$. Then there is a basis of U in terms of λ where λ is the root of the polynomial

$$g(T) = \alpha_m T^m + \cdots + \alpha_1 T + \alpha_0.$$

Proof. First note that U is a $\mathbb{C}$-vector space of dimension m, since each sequence is determined by $u_0, ..., u_{m-1}$. Thus, it will have a basis.

Then if λ is a root of $g(T)$, it follows that $(\lambda^n) \in U$ since

$$\alpha_m \lambda^{n+m} + \alpha_{m-1}\lambda^{n+m-1} + \cdots + \alpha_0 = \lambda^n g(\lambda) = 0.$$

Case 1. The m roots $\lambda_1, ..., \lambda_m$ of $g(T)$ are distinct. Then $\{(\lambda_i^n)\}_{1 \leq i \leq m}$ will form a basis of U.

Case 2. λ is a multiple root of $g(T)$. That is, $g(\lambda) = g'(\lambda) = 0$. Then the polynomial $T^n g(T)$ will also have λ as a multiple root, giving $(T^n g(T))'_{T=\lambda} = 0$.

$$\alpha_m(n+m)\lambda^{n+m-1} + \alpha_{m-1}(n+m-1)\lambda^{n+m-2} + \cdots + \alpha_0 n\lambda^{n-1} = 0 \quad .$$

Thus, $(n\lambda^{n-1}) \in U$ and $(n\lambda^n) \in U$. Take for instance, $\lambda$is a root of order at least 3. Then $(n^2\lambda^n) \in U$. In general, if λ is a root of order μ, then

$$(n^k \lambda^n) \in U \text{ for } k = 0, 1, ..., \mu - 1.$$

Therefore, when $g(T)$ has roots $\lambda_1, ..., \lambda_s$ of order $\mu_1, ..., \mu_s$ with $\sum_{\mu=1}^{s} \mu_i = m$, the basis of U is

$$(n^k \lambda_i^n)_{0 \leq k \leq \mu_i - 1}^{1 \leq i \leq s} \quad .$$

□

This then gives a more convenient form of linear recurrences for proving the main theorem.

Corollary 1. *Let (u_n) be a linear recurrence of order m. Then there exist $\lambda_1, ..., \lambda_s$ and polynomials $p_1(T), ..., p_s(T)$ with $\sum_{1 \leq i \leq s}(\deg p_i + 1) \leq m$ such that*

$$u_n = p_1(n)\lambda_1^n + \cdots + p_s(n)\lambda_s^n.$$

This then gives an equivalent form of the main theorem.

Theorem. *(Skolem-Mahler-Lech 2). Let $p_1(T), ..., p_s(T) \in \mathbb{C}[T]$ be some polynomials and $\lambda_1, ..., \lambda_s \in \mathbb{C}^\times$ be pairwise disjoint. Then there exists $N \in \mathbb{N}$, a possibly empty set $S \subset \{0, 1, ..., N-1\}$, and a finite set $T \subset \mathbb{Z}$ such that*

$$p_1(n)\lambda_1^n + \cdots + p_s(n)\lambda_s^n = 0 \text{ if and only if } n \in T \cup (S + N\mathbb{Z}) \quad .$$

There remains one main theorem that will be used to prove Skolem-Mahler-Lech.

3.2 Strassmann's Theorem

Theorem 3. *(Strassmann). Let*

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

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

$$|a_N| = \max_n |a_n| \text{ and } |a_n| < |a_N| \text{ for } n > N.$$

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

Proof. Consider the two cases.

Case 1. $N = 0$. Then $|a_0| > |a_n|$ for all $n \geq 1$. Assume that some $f(x) = 0$. Then,

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

So it follows that

$$|a_0| = |a_1 x + a_2 x^2 + \cdots| \leq \max_{n\geq 1} |a_n x^n| \leq \max_{n \geq 1} |a_n| \quad ,$$

which contradicts the assumption that $|a_0| > |a_n|$ for all $n \geq 1$. Therefore, $f(x) \neq 0$ for all $x \in \mathbb{Z}_p$. That is, there are no zeros when $N = 0$.

Case 2. $N \neq 0$. Assume $f(\alpha) = 0$ for some $\alpha \in \mathbb{Z}_p$. Taking $x \in \mathbb{Z}_p$ gives,

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

$$= (x - \alpha) \sum_{n \geq 1} \sum_{j < n} a_n x^j a^{n-1-j} \quad .$$

Note that this series can be re-ordered to an equivalent power series in x:

$$f(x) = (x - \alpha) \sum_{n=0}^{\infty} b_j x^j \text{ where } b_j = \sum_{k \geq 0} a_{j+1+k} \alpha^k \quad .$$

Then,

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

and

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

If $j \geq N$, it follows that

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

By induction on N, it can be assumed that $\sum_{n=0}^{\infty} b_j x^j$ has at most $N-1$ zeros in $\mathbb{Z}_p$. This implies that $f(X)$ has at most N zeros since it has the additional zero at $x = \alpha$.

□

Corollary. *For an analytic function f that is not identically zero, the set of zeros of f is discrete.*

Definition 16. For a complete nonarchimedian field K, a function $f : D(a,r) \to K$ on some disk of radius r with center in a is analytic if

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

where the series converges for all $z \in D(a,r)$.

This then allows $u(n)$ to be treated as an analytic function on $\mathbb{Z}_p$. This will require the use of nonarchimedian exponents and logarithms. Here, it will only be noted that the nonarchimedian exponent is well-defined as $exp(z)$ for $z \in \mathbb{Z}_p$. Then it simply follows that $\exp(n \log \lambda_i) = \lambda_i^n$. More importantly, the nonarchimedian logarithm is only defined on the disk $D(1, \rho_p)$. Thus, it must be shown that all z lie in the disk $D(1, \rho_p)$ for $log(z)$ to be well defined. This will be shown in the beginning of the proof of the Skolem-Mahler-Lech theorem.

3.3 The Skolem-Mahler-Lech Theorem

Now to prove the main result.

Theorem. *(Skolem-Mahler-Lech 1). Let (u_n) be a linear recurrence. Then there exists $N \in \mathbb{Z}_{\geq 1}$, a possibly empty set $S \subseteq \{0, 1, ..., N-1\}$, and a finite set $T \subset \mathbb{Z}$ such that*

$$u_n = 0 \text{ if and only if } n \in T \cup (S + N\mathbb{Z}) \quad .$$

and equivalently,

Theorem. *(Skolem-Mahler-Lech 2). Let $p_1(T), ..., p_s(T) \in \mathbb{C}[T]$ be some polynomials and $\lambda_1, ..., \lambda_s \in \mathbb{C}^\times$ be pairwise disjoint. Then there exists $N \in \mathbb{N}$, a possibly empty set $S \subset \{0, 1, ..., N-1\}$, and a finite set $T \subset \mathbb{Z}$ such that*

$$p_1(n)\lambda_1^n + \cdots + p_s(n)\lambda_s^n = 0 \text{ if and only if } n \in T \cup (S + N\mathbb{Z}) \quad .$$

Proof. Define $u(n) := p_1(n)\lambda_1^n + \cdots + p_s(n)\lambda_s^n$ for $\lambda_1, ...k\lambda_s \in K^\times$ and $p_1(T), ..., p_s(T) \in K[T]$. Then there exists a nonarchimedian absolute value $|\cdot|_v$ on K such that

$$|\lambda_1|_v = \cdots = |\lambda_s|_v = 1 \quad .$$

Then this v allows for a finite extension of $\mathbb{Q}_p$ into K_v, which is the completion with respect to $|\cdot|_v$.

The remaining necessary condition is a field in which $\log \lambda_i$ is defined, it will be necessary to obtain $|\lambda_i - 1|_v < \rho_p = p^{-\frac{1}{p-1}}$. So let q_v be the prime ideal of O_{K_v}. Then the image of λ in the quotient ring O_{K_v}/q_v^m is 1. That is, $|\lambda - 1|_v < \rho_p$ is equivalent to $\lambda \equiv 1 \pmod{q_v^m}$ for some $m \in \mathbb{Z}_{\geq 1}$. Then it follows that $\lambda \in O_{K_v}^\times$, since $|\lambda|_v = 1$.

Now recall Fermat's little theorem, which states that for prime p and integer a, $a^p \equiv a \pmod{p}$. Letting N be the order of the ring O_{K_v}/q_v^m, it follows that

$$\lambda^N \equiv 1 \pmod{q_v^m} \quad .$$

Thus the λ_i^N's lie in the disk $D(1, \rho_p)$, and $\log\lambda_i^N$ is well-defined.
Then for each $r \in \{0, 1, ..., N-1\}$, define

$$u_r(z) := \sum_{1 \le i \le s} p_i(r + Nz)\lambda_i^r \exp(z \log \lambda_i^N)$$

If $n \equiv r \pmod{N}$, then $n = r + Nk$ with $u(n) = u_r(k)$. Thus,

$$\begin{aligned} u_r(k) &= \sum_{1 \le i \le s} p_i(r + Nk)\lambda_i^r \exp(k \log \lambda_i^N) \\ &= \sum_{1 \le i \le s} p_i(n)\lambda_i^r \exp(k \log \lambda_i^N) \\ &= \sum_{1 \le i \le s} p_i(n)\lambda_i^r \lambda_i^{Nk} \\ &= \sum_{1 \le i \le s} p_i(n)\lambda_i^n = u(n). \end{aligned}$$

Then for a fixed r, consider the two cases.

Case 1. $u_r(z)$ is identically zero. Then $u(n) = 0$ for $n \equiv r \pmod{N}$. These r's form a set $S \subseteq \{0, 1, ..., N-1\}$.

Case 2. $u_r(z)$ is not identically zero. Then by Strassman's theorem, $u(n) = 0$ for finitely many $n \equiv r \pmod{N}$. Then these zeros form a finite set $T \subset \mathbb{Z}$.

□

As a final note, the Skolem-Mahler-Lech Theorem gives neither the zero set nor its size. The question of the number of zeros remains open. Similar conjectures are also unproven for various other fields, particularly fields of negative characteristic. There exists a generalization of this theorem to all fields of positive characteristic due to Harm Derkson in 2005.

3. Bibliography

[1] Bilu, Yuri. *p-Adic Numbers and Diophantine Equations*. Bordeaux: Universie de Bordeaux, 2013. https://www.math.u-bordeaux.fr/ abesheno/bilu.pdf (accessed November 16, 2018)

[2] Block, Adam. *The Skolem-Mahler-Lech Theorem*. New York: Columbia, 2017.

[3] Chartrand, Gary, Albert D. Polimeni, and Ping Zhang. *Mathematical Proofs: A Transition to Advanced Mathematics*. 3rd ed. New Jersey: Pearson, 2013.

[4] Derkson, Harm. *A Skolem-Mahler-Lech Theorem in Positive Characteristic and Finite Automata*. 3rd ed. ArXiv Mathematics e-prints, 2005.

[5] Gouvea, Fernando. *p-Adic Numbers: An Introduction*. Waterville: Springer, 1997.

[6] Hansel, Georges. *A Simple Proof of the Skolem-Mahler-Lech Theorem*. Automata, Languages and Programming. Lecture Notes in Computer Science, vol 194. Berlin: Springer, 1985.

[7] Litt, Daniel. *Zeros of Integer Linear Recurrences*. New York: Columbia, 2011.