Mahler-Lech-Skolem Theorem

Aleksei Lopatin
alex.lopatin01@gmail.com

Euler Circle

July 2025

What is it?

The Mahler-Lech-Skolem theorem answers the question of how many zeros a linear recurrence can have.

Theorem

Let $(a_n)_{n\in\mathbb{N}}$ be a linear recurrence. Then there exists some $r \in N$ and $j_1, \ldots, j_m \in \mathbb{N}$ with m possibly equal to 0 distinct elements and some finite subset $Z \in \mathbb{N}$ such that

$$S_a = Z \cup \bigcup_{i=1}^{m} \{j_i + rq | q \in \mathbb{N}\}$$

What is it?

The Mahler-Lech-Skolem theorem answers the question of how many zeros a linear recurrence can have.

Theorem

Let $(a_n)_{n \in \mathbb{N}}$ be a linear recurrence. Then there exists some $r \in N$ and $j_1, \ldots, j_m \in \mathbb{N}$ with m possibly equal to 0 distinct elements and some finite subset $Z \in \mathbb{N}$ such that

$$S_a = Z \cup \bigcup_{i=1}^{m} \{j_i + rq | q \in \mathbb{N}\}$$

In other words, the zero set of the sequence is a union of a finite set and a finite number of arithmetic progressions all with the same common difference.

Examples

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 $a_1 = 1$.

Examples

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 $a_1 = 1$.

In this case $S_a = \{0\}$. What if we have a linear recurrence $a_n = a_{n-1} + 2a_{n-2} + 3a_{n-3}$ with initial conditions $a_0 = a_1 = a_2 = 1$?

Examples

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 $a_1 = 1$.

In this case $S_a = \{0\}$. What if we have a linear recurrence $a_n = a_{n-1} + 2a_{n-2} + 3a_{n-3}$ with initial conditions $a_0 = a_1 = a_2 = 1$?

$S_a = \emptyset$
What if we have $a_n = a_{n-2}$ with $a_0 = 0$ and $a_1 = 1$?

Examples

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 $a_1 = 1$.

In this case $S_a = \{0\}$. What if we have a linear recurrence $a_n = a_{n-1} + 2a_{n-2} + 3a_{n-3}$ with initial conditions $a_0 = a_1 = a_2 = 1$?

$S_a = \emptyset$
What if we have $a_n = a_{n-2}$ with $a_0 = 0$ and $a_1 = 1$?

$S_a = \{n \in N | n \equiv 0 \pmod 2\}$
Curiously so, these are the only possibilities.

Importance

This result is fundamentally important in number theory and linear algebra as it categorizes the zeros of a general linear recurrence sequence.

Importance

This result is fundamentally important in number theory and linear algebra as it categorizes the zeros of a general linear recurrence sequence.

It is an especially fascinating result because it lays no relation to the p-adics, which are present in every known proof of the theorem.

Absolute Value

Recall that we constructed the real numbers as equivalence classes of Cauchy sequences of rationals, using the usual absolute value $d(x, y) = |x - y|$.

Absolute Value

Recall that we constructed the real numbers as equivalence classes of Cauchy sequences of rationals, using the usual absolute value $d(x, y) = |x - y|$.

Definition

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

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

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

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

Remark

This last inequality is referred to as the triangle inequality.

Ultrametric Inequality

We say that a non-archimedean absolute value is one in which it satisfies the following definition.

Definition

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

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

Ultrametric Inequality

We say that a non-archimedean absolute value is one in which it satisfies the following definition.

Definition

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

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

Definition

For a function d, we call it an ultrametric if and only if for any $x, y, z \in \mathbb{k}$, we have

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

Application

What are triangles in the ultrametric space?

Proposition

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:*

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

Application

What are triangles in the ultrametric space?

Proposition

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:*

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

Lemma

All "triangles" are isosceles in the ultrametric space.

Application

What are triangles in the ultrametric space?

Proposition

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:

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

Lemma

All "triangles" are isosceles in the ultrametric space.

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

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

P-adic Valuation

A valuation is a function on a field that provides a measure of the size of the field.

P-adic Valuation

A valuation is a function on a field that provides a measure of the size of the field.

Definition

Fix a prime number $p \in \mathbb{Z}$. The p-adic valuation on $\mathbb{Z}$ 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

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

P-adic Absolute Value

Definition

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 $|0|_p = 0$.

P-adic Absolute Value

Definition

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 $|0|_p = 0$.

Example

$$v_5(3060) = 1 \rightarrow |3060|_5 = 5^{-1} = \frac{1}{5}$$

$$v_2(3) = 0 \rightarrow |3|_2 = 2^0 = 1$$

P-adic Analytic Function

Definition

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

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

P-adic Analytic Function

Definition

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

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

Definition

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 $z \in B$.

Strassman's Theorem

A key tool that we will need is understanding what the zeros of a p-adic analytic function are.

Theorem

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

Strassman's Theorem

A key tool that we will need is understanding what the zeros of a p-adic analytic function are.

Theorem

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

Definition

$\mathbb{Z}_p$ is the ring of p-adic integers with p-adic absolute value less than or equal to 1.

Lemma

$\mathbb{Z}_p$ is compact.

Recurrence to Matrix

We are motivated to work with matrices for their niceness.

Definition

The polynomial $P_A(x)$ is the characteristic polynomial of a matrix x relative to a matrix A, specifically as

$$P_A(x) = \det(xI - A).$$

Recurrence to Matrix

We are motivated to work with matrices for their niceness.

Definition

The polynomial $P_A(x)$ is the characteristic polynomial of a matrix x relative to a matrix A, specifically as

$$P_A(x) = \det(xI - A).$$

Theorem

$$P_A(A) = 0$$

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

Example

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

$$P_A(x) = \det(\begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix} - \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}) = \det(\begin{bmatrix} x-1 & -2 \\ -3 & x-4 \end{bmatrix})$$

Example

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

$$P_A(x) = \det(\begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix} - \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}) = \det(\begin{bmatrix} x-1 & -2 \\ -3 & x-4 \end{bmatrix})$$

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

Upon substituting $x = A$:

Example

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

$$P_A(x) = \det(\begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix} - \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}) = \det(\begin{bmatrix} x-1 & -2 \\ -3 & x-4 \end{bmatrix})$$

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

Upon substituting $x = A$:

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

Idea

- Closed form for linear recurrence as a matrix
- Pick an appropriate prime p
- Write out our set of p-adic analytic functions
- Use the binomial expansion theorem
- Apply Strassman's theorem

Tying things together

Let us imagine that from a linear recurrence sequence a_k, we could find a set of p-adic analytic functions f_i with $0 \leq i \leq m-1$ such that

$$f_i(n) = mn + i$$

for large n.

Tying things together

Let us imagine that from a linear recurrence sequence a_k, we could find a set of p-adic analytic functions f_i with $0 \leq i \leq m-1$ such that

$$f_i(n) = mn + i$$

for large n.

Then, each f_i would either be identically zero, or would have only finitely many zeros. Our goal is to find such a function.

Starting Out

An integer linear recurrence a_n may be written as

$$a_n = [A^n v, w]$$

Starting Out

An integer linear recurrence a_n may be written as

$$a_n = [A^n v, w]$$

Recall the Fibonacci recurrence $F_n = F_{n-1} + F_{n-2}$ with initial conditions $F_0 = 0$ and $F_1 = 1$.

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

Starting Out

An integer linear recurrence a_n may be written as

$$a_n = [A^n v, w]$$

Recall the Fibonacci recurrence $F_n = F_{n-1} + F_{n-2}$ with initial conditions $F_0 = 0$ and $F_1 = 1$.

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

Let $A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$, and the initial vector is $v = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$.

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

Proving it

We choose a prime p such that A is invertible modulo p. We define m as such for $A^m \equiv 1 \pmod{p}$, which will be the period of the arithmetic progression.

Proving it

We choose a prime p such that A is invertible modulo p. We define m as such for $A^m \equiv 1 \pmod{p}$, which will be the period of the arithmetic progression.

$A^m \pmod{p}$ over $\mathbb{F}_p$ 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.

Finale

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.

Finale

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.

$$f_i(n) = \sum_k p^k P_k(n)$$

for some polynomials P_k, which follow from the binomial coefficients. This power series makes sense as a p-adic analytic function convergent on all of Z_p.

Thank you

Thanks for listening, make sure to read my paper for more.

- alex.lopatin01@gmail.com
- Alex-131 on discord