The (inescapable) p-adics

Alex J. Best

10/10/22

VU Master Seminar - Algebra

Linear recurrence sequences

Definition: Linear recurrence sequence

A **linear recurrence sequence**, is a sequence whose nth term is a linear combination of the previous k terms (for all $n \geq k$).

We often consider sequences of integers, but we will consider these over fields like $\mathbb{Q}, \mathbb{C}$ also.

Linear recurrence sequences

Definition: Linear recurrence sequence

A **linear recurrence sequence**, is a sequence whose nth term is a linear combination of the previous k terms (for all $n \geq k$).

We often consider sequences of integers, but we will consider these over fields like $\mathbb{Q}, \mathbb{C}$ also.

Example: Fibonacci

Let $a_0 = 0, a_1 = 1$ and $a_n = a_{n-1} + a_{n-2}$ for $n \geq k = 2$:

$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 41$

Linear recurrence sequences

Definition: Linear recurrence sequence

A **linear recurrence sequence**, is a sequence whose nth term is a linear combination of the previous k terms (for all $n \geq k$).

We often consider sequences of integers, but we will consider these over fields like $\mathbb{Q}, \mathbb{C}$ also.

Example: Fibonacci

Let $a_0 = 0, a_1 = 1$ and $a_n = a_{n-1} + a_{n-2}$ for $n \geq k = 2$:

$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 41$

a_n grows exponentially.

Definition: Linear recurrence sequence

A **linear recurrence sequence**, is a sequence whose nth term is a linear combination of the previous k terms (for all $n \geq k$).

We often consider sequences of integers, but we will consider these over fields like $\mathbb{Q}, \mathbb{C}$ also.

Example: A periodic sequence

$a_0 = 1, a_1 = 0$ with $a_n = -a_{n-1} - a_{n-2}$

$1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1$

Linear recurrence sequences

Definition: Linear recurrence sequence

A **linear recurrence sequence**, is a sequence whose nth term is a linear combination of the previous k terms (for all $n \geq k$).

We often consider sequences of integers, but we will consider these over fields like $\mathbb{Q}, \mathbb{C}$ also.

Example: A periodic sequence

$a_0 = 1, a_1 = 0$ with $a_n = -a_{n-1} - a_{n-2}$

$1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1$

a_n is periodic now.

Linear recurrence sequences

Definition: Linear recurrence sequence

A **linear recurrence sequence**, is a sequence whose nth term is a linear combination of the previous k terms (for all $n \geq k$).

We often consider sequences of integers, but we will consider these over fields like $\mathbb{Q}, \mathbb{C}$ also.

Example: Natural numbers interlaced with zeroes

$a_0 = 1, a_1 = 0, a_2 = 2, a_3 = 0$ with $a_n = 2a_{n-2} - a_{n-4}$

$1, 0, 2, 0, 3, 0, 4, 0, 5, 0, 6, 0, 7, 0, 8, 0, 9, 0, 10, 0, 11, 0, 12, 0, 13, 0, 14, 0, 1$

Linear recurrence sequences

Definition: Linear recurrence sequence

A **linear recurrence sequence**, is a sequence whose nth term is a linear combination of the previous k terms (for all $n \geq k$).

We often consider sequences of integers, but we will consider these over fields like $\mathbb{Q}, \mathbb{C}$ also.

Example: Natural numbers interlaced with zeroes

$a_0 = 1, a_1 = 0, a_2 = 2, a_3 = 0$ with $a_n = 2a_{n-2} - a_{n-4}$

$1, 0, 2, 0, 3, 0, 4, 0, 5, 0, 6, 0, 7, 0, 8, 0, 9, 0, 10, 0, 11, 0, 12, 0, 13, 0, 14, 0, 1$

not periodic but the zeroes *do* have a regular repeating pattern, being zero half the time.

The ultimate question

Can we describe the set $\{n : a_n = 0\}$ for a general linear recurrence?

Is it ever finite?

The ultimate question

Can we describe the set $\{n : a_n = 0\}$ for a general linear recurrence?

Is it ever finite? Is it ever infinite?

The ultimate question

Can we describe the set $\{n : a_n = 0\}$ for a general linear recurrence?

Is it ever finite? Is it ever infinite? Could it ever be the set $\{n : \exists m, n = m^2\}$?

The ultimate question

Can we describe the set $\{n : a_n = 0\}$ for a general linear recurrence?

Is it ever finite? Is it ever infinite? Could it ever be the set $\{n : \exists m, n = m^2\}$?

Question

What possible patterns are there for the zeroes of a linear recurrence sequence?

The ultimate question

Question

What possible patterns are there for the zeroes of a linear recurrence sequence?

To answer this we will use power series:

Observation

A linear recurrence sequence is the Taylor expansion around 0 of a rational function

$$\frac{a_0 + a_1 x + \cdots + a_\ell x^\ell}{b_0 + b_1 x + \cdots + b_k x^k}$$

with $b_0 \neq 0$ (so that the expansion makes sense).

Linear recurrence sequences

Example

$$\frac{x}{1 - x - x^2} \leftrightarrow \text{Fibonacci}$$

Linear recurrence sequences

Example

$$\frac{x}{1-x-x^2} \leftrightarrow \text{Fibonacci}$$

$$\frac{1}{1+x+x^2} \leftrightarrow 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0$$

Linear recurrence sequences

Example

$$\frac{x}{1-x-x^2} \leftrightarrow \text{Fibonacci}$$

$$\frac{1}{1+x+x^2} \leftrightarrow 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0$$

$$\frac{1}{(1-x^2)^2} \leftrightarrow 1, 0, 2, 0, 3, 0, 4, 0, 5, 0, 6, 0, 7, 0, 8, 0, 9, 0, 10, 0, 11, 0, 12, 0$$

Linear recurrence sequences

Example

$$\frac{x}{1-x-x^2} \leftrightarrow \text{Fibonacci}$$

$$\frac{1}{1+x+x^2} \leftrightarrow 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0$$

$$\frac{1}{(1-x^2)^2} \leftrightarrow 1, 0, 2, 0, 3, 0, 4, 0, 5, 0, 6, 0, 7, 0, 8, 0, 9, 0, 10, 0, 11, 0, 12, 0$$

$$\frac{(1+x)^3 - x^3}{(1+x)^5 - x^5} \leftrightarrow 1, -2, 3, -5, 10, -20, 35, -50, 50, 0, -175, 625,$$

$$-1625, 3625, -7250, 13125, -21250, 29375, -29375$$

$$0, 106250, -384375, 1006250, -2250000, 4500000,$$

$$-8140625, 13171875, -18203125, 18203125, 0, -658$$

Consequences

Observation

The set of all linear recurrence sequences over a field is a vector space! Hard to tell how the rule changes.

Consequences

Observation

The set of all linear recurrence sequences over a field is a vector space! Hard to tell how the rule changes.

As we can add any finite sequence can always mess up the behaviour of finitely many initial terms. So we want to know what is the structure of the zero set asymptotically?

Consequences

Observation

The set of all linear recurrence sequences over a field is a vector space! Hard to tell how the rule changes.

As we can add any finite sequence can always mess up the behaviour of finitely many initial terms. So we want to know what is the structure of the zero set asymptotically?We can also multiply rational functions, which convolutes the sequences!

Example

$$\frac{1}{(1-x^2)^2}-(1-x+2x^2+3x^4+4x^6) \leftrightarrow 0,1,0,0,0,0,0,0,5,0,6,0,7,0,8$$

Interlacing with 0 and *shifting* correspond to plugging in x^2 and multiplying by x respectively in the rational functions

$$\frac{1}{(1-x)^2} \leftrightarrow 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,$$

$$\frac{1}{(1-x^2)^2} \leftrightarrow 1,0,2,0,3,0,4,0,5,0,6,0,7,0,8,0,9,0,10,0,11,0,12,0,13$$

Linear recurrence sequences

Example

$$\frac{1}{(1-x^2)^2} - (1 - x + 2x^2 + 3x^4 + 4x^6) \leftrightarrow 0, 1, 0, 0, 0, 0, 0, 0, 5, 0, 6, 0, 7, 0, 8$$

Interlacing with 0 and *shifting* correspond to plugging in x^2 and multiplying by x respectively in the rational functions

Linear recurrence sequences

Example

$$\frac{1}{(1-x^2)^2} - (1 - x + 2x^2 + 3x^4 + 4x^6) \leftrightarrow 0, 1, 0, 0, 0, 0, 0, 0, 5, 0, 6, 0, 7, 0, 8$$

Interlacing with 0 and *shifting* correspond to plugging in x^2 and multiplying by x respectively in the rational functions

$$\frac{1}{(1-x)^2} \leftrightarrow 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21,$$

Example

$$\frac{1}{(1-x^2)^2}-(1-x+2x^2+3x^4+4x^6) \leftrightarrow 0,1,0,0,0,0,0,0,5,0,6,0,7,0,8$$

Interlacing with 0 and *shifting* correspond to plugging in x^2 and multiplying by x respectively in the rational functions

$$\frac{1}{(1-x)^2} \leftrightarrow 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,$$

$$\frac{1}{(1-x^2)^2} \leftrightarrow 1,0,2,0,3,0,4,0,5,0,6,0,7,0,8,0,9,0,10,0,11,0,12,0,13$$

Linear recurrence sequences

$$\frac{1}{(1-x)^2} \leftrightarrow 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21,$$

$$\frac{1}{(1-x^2)^2} \leftrightarrow 1, 0, 2, 0, 3, 0, 4, 0, 5, 0, 6, 0, 7, 0, 8, 0, 9, 0, 10, 0, 11, 0, 12, 0, 13$$

$$\frac{1}{(1-x^4)^2} \leftrightarrow 1, 0, 0, 0, 2, 0, 0, 0, 3, 0, 0, 0, 4, 0, 0, 0, 5, 0, 0, 0, 6, 0, 0, 0, 7, 0, 0$$

Linear recurrence sequences

$$\frac{1}{(1-x)^2} \leftrightarrow 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21,$$

$$\frac{1}{(1-x^2)^2} \leftrightarrow 1, 0, 2, 0, 3, 0, 4, 0, 5, 0, 6, 0, 7, 0, 8, 0, 9, 0, 10, 0, 11, 0, 12, 0, 13$$

$$\frac{1}{(1-x^4)^2} \leftrightarrow 1, 0, 0, 0, 2, 0, 0, 0, 3, 0, 0, 0, 4, 0, 0, 0, 5, 0, 0, 0, 6, 0, 0, 0, 7, 0, 0$$

$$\frac{x}{(1-x^4)^2} \leftrightarrow 0, 1, 0, 0, 0, 2, 0, 0, 0, 3, 0, 0, 0, 4, 0, 0, 0, 5, 0, 0, 0, 6, 0, 0, 0, 7, 0$$

Linear recurrence sequences

$$\frac{1}{(1-x)^2} \leftrightarrow 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21,$$

$$\frac{1}{(1-x^2)^2} \leftrightarrow 1, 0, 2, 0, 3, 0, 4, 0, 5, 0, 6, 0, 7, 0, 8, 0, 9, 0, 10, 0, 11, 0, 12, 0, 13$$

$$\frac{1}{(1-x^4)^2} \leftrightarrow 1, 0, 0, 0, 2, 0, 0, 0, 3, 0, 0, 0, 4, 0, 0, 0, 5, 0, 0, 0, 6, 0, 0, 0, 7, 0, 0$$

$$\frac{x}{(1-x^4)^2} \leftrightarrow 0, 1, 0, 0, 0, 2, 0, 0, 0, 3, 0, 0, 0, 4, 0, 0, 0, 5, 0, 0, 0, 6, 0, 0, 0, 7, 0$$

$$\frac{1+2x}{(1-x^4)^2} \leftrightarrow 1, 2, 0, 0, 2, 4, 0, 0, 3, 6, 0, 0, 4, 8, 0, 0, 5, 10, 0, 0, 6, 12, 0, 0, 7, 1$$

Linear recurrence sequences

$$\frac{1}{(1-x)^2} \leftrightarrow 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21,$$

$$\frac{1}{(1-x^2)^2} \leftrightarrow 1, 0, 2, 0, 3, 0, 4, 0, 5, 0, 6, 0, 7, 0, 8, 0, 9, 0, 10, 0, 11, 0, 12, 0, 13$$

$$\frac{1}{(1-x^4)^2} \leftrightarrow 1, 0, 0, 0, 2, 0, 0, 0, 3, 0, 0, 0, 4, 0, 0, 0, 5, 0, 0, 0, 6, 0, 0, 0, 7, 0, 0$$

$$\frac{x}{(1-x^4)^2} \leftrightarrow 0, 1, 0, 0, 0, 2, 0, 0, 0, 3, 0, 0, 0, 4, 0, 0, 0, 5, 0, 0, 0, 6, 0, 0, 0, 7, 0$$

$$\frac{1+2x}{(1-x^4)^2} \leftrightarrow 1, 2, 0, 0, 2, 4, 0, 0, 3, 6, 0, 0, 4, 8, 0, 0, 5, 10, 0, 0, 6, 12, 0, 0, 7, 1$$

Still has periodic zero set, all n congruent to $2, 3$ modulo 4.

Approach

Expand into partial fractions

$$\frac{p(x)}{q(x)} = \sum_{i=1}^{m} \sum_{j=1}^{n_j} \frac{r_{ij}}{(1 - \alpha_i x)^j}$$

Approach

Expand into partial fractions

$$\frac{p(x)}{q(x)} = \sum_{i=1}^{m} \sum_{j=1}^{n_j} \frac{r_{ij}}{(1-\alpha_i x)^j}$$

do some rearranging:

$$\sum a_n x^n = \sum_{n=0}^{\infty} \left(\sum_{i=1}^{m} \sum_{j=1}^{n_j} r_{ij} \binom{n+j-1}{j-1} \alpha_i^n \right) x^n$$

Approach

Expand into partial fractions

$$\frac{p(x)}{q(x)} = \sum_{i=1}^{m} \sum_{j=1}^{n_j} \frac{r_{ij}}{(1-\alpha_i x)^j}$$

do some rearranging:

$$\sum a_n x^n = \sum_{n=0}^{\infty} \left(\sum_{i=1}^{m} \sum_{j=1}^{n_j} r_{ij} \binom{n+j-1}{j-1} \alpha_i^n \right) x^n$$

Upshot: there are polynomials $A_i(n)$ over $\mathbb{C}$ such that

$$a_n = \sum_{i=1}^{m} A_i(n) \alpha_i^n.$$

Example: Binet's formula for Fibonacci

$F_n = \frac{1}{\sqrt{5}} \phi^n - \frac{1}{\sqrt{5}} (-\phi^{-1})^n$

Approach

So a_n is an analytic function of n which has zeroes for infinitely many integer values.

Approach

So a_n is an analytic function of n which has zeroes for infinitely many integer values.

Like

$$\sin(\pi x)!$$

Approach

So a_n is an analytic function of n which has zeroes for infinitely many integer values.

Like

$$\sin(\pi x)!$$

What can we say about the zeros of this function?

Approach

So a_n is an analytic function of n which has zeroes for infinitely many integer values.

Like

$$\sin(\pi x)!$$

What can we say about the zeros of this function?

For one: There are finitely many in any compact region (unless the function is zero)

Approach

So a_n is an analytic function of n which has zeroes for infinitely many integer values.

Like

$$\sin(\pi x)!$$

What can we say about the zeros of this function?

For one: There are finitely many in any compact region (unless the function is zero)

Ridiculous suggestion
What if the integers were bounded? If that was true, infinitely many zeroes $\implies$ the function is zero!

What is bounded?

What if the integers were bounded?

How do we define boundedness?

Definition: Absolute Values

Let C be a commutative ring, an **absolute value** on C, is a function $|\cdot|\colon R \to \mathbb{R}_{\geq 0}$ satisfying for all $x, y \in C$

$$|x| = 0 \iff x = 0$$

$$|xy| = |x||y|$$

$$|x + y| \leq |x| + |y|$$

Are there other absolute values for the integers?

$$|x| = 0 \iff x = 0$$

$$|xy| = |x||y|$$

$$|x + y| \leq |x| + |y|$$

Property 2 implies that $|1| = 1$ and $|-1|^2 = 1$ so $|-1| = 1$ also. So it remains to decide what happens for all primes $p \in \mathbb{Z}$.

We could set $|x| = 1$ for all $x \neq 0$, this is the **trivial absolute value**.

Or $|x| = x$ for all positive x, this gives the usual absolute value.

A strange absolute value

We can in fact define another absolute value $|\cdot|_p$ for each prime p.

Pick a value $\alpha = |p|_p < 1$, and let $|q|_p = 1$ for all other primes q.

Now we have that

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

Theorem: Ostrowski

The only nontrivial absolute values on $\mathbb{Q}$ are

$$x \mapsto \operatorname{sgn}(x)x \;\; \textit{and} \;\; |\cdot|_p \textit{ for some prime } p$$

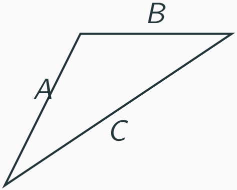
Why is it strange?

The inequality

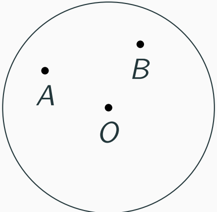
$$|x + y| \leq \max(|x|, |y|)$$

is called **ultrametric** and has some unusual properties:

Every triangle is isosceles.



Every point of a ball is its center



Completion

We can define the real numbers as equivalence classes of Cauchy sequences of rationals, (with respect to the normal absolute value).

We can do the same thing with $|\cdot|_p$ to get the *p*-adics, a topologically complete ring $\mathbb{Q}_p$, which is analogous to $\mathbb{R}$ but very different.

$$\{(x_n)_n : x_n \in \mathbb{Q}, \forall \epsilon > 0, \exists N, n, m > N \implies |x_n - x_m| < \epsilon\}/\sim$$

The absolute value $|\cdot|_p$ extends to give one on $\mathbb{Q}_p$ which is still ultrametric.

How to think about p-adic numbers

For real numbers we use a decimal expansion, to write a number with the most significant digits first. This works as $\frac{1}{10^n}$ gets smaller ($|\cdot| \to 0$) as $n \to \infty$.

How to think about p-adic numbers

For real numbers we use a decimal expansion, to write a number with the most significant digits first. This works as $\frac{1}{10^n}$ gets smaller $(|\cdot| \to 0)$ as $n \to \infty$.

For $\mathbb{Q}_p$ we have $|p^n|_p = \frac{1}{p^n} \to 0$ as $n \to \infty$. Because of this we can take the analogue of a decimal expansion: For example for the 5-adics:

$$15 = 3 \cdot 5$$

How to think about p-adic numbers

For real numbers we use a decimal expansion, to write a number with the most significant digits first. This works as $\frac{1}{10^n}$ gets smaller ($|\cdot| \to 0$) as $n \to \infty$.

For $\mathbb{Q}_p$ we have $|p^n|_p = \frac{1}{p^n} \to 0$ as $n \to \infty$. Because of this we can take the analogue of a decimal expansion: For example for the 5-adics:

$$15 = 3 \cdot 5$$

$$16 = 1 + 3 \cdot 5$$

How to think about p-adic numbers

For real numbers we use a decimal expansion, to write a number with the most significant digits first. This works as $\frac{1}{10^n}$ gets smaller ($|\cdot| \to 0$) as $n \to \infty$.

For $\mathbb{Q}_p$ we have $|p^n|_p = \frac{1}{p^n} \to 0$ as $n \to \infty$. Because of this we can take the analogue of a decimal expansion: For example for the 5-adics:

$$15 = 3 \cdot 5$$

$$16 = 1 + 3 \cdot 5$$

$$16 + 1/5 = 1 \cdot 5^{-1} + 1 + 2 \cdot 5$$

How to think about p-adic numbers

For real numbers we use a decimal expansion, to write a number with the most significant digits first. This works as $\frac{1}{10^n}$ gets smaller $(|\cdot| \to 0)$ as $n \to \infty$.

For $\mathbb{Q}_p$ we have $|p^n|_p = \frac{1}{p^n} \to 0$ as $n \to \infty$. Because of this we can take the analogue of a decimal expansion: For example for the 5-adics:

$$15 = 3 \cdot 5$$

$$16 = 1 + 3 \cdot 5$$

$$16 + 1/5 = 1 \cdot 5^{-1} + 1 + 2 \cdot 5$$

$$-\frac{1}{} = \frac{1}{} = 1 + 5 + 5^2 + 5^3 + \cdots$$

With $|\cdot|_p$ the integers are bounded!

Back to recurrences

With $|\cdot|_p$ the integers are bounded! Going back to the problem of finding the zero's of

$$a_n = \sum_{i=1}^{m} A_i(n)\alpha_i^n$$

as a function of n. We can think of this as a function $\mathbb{N} \to \overline{\mathrm{Q}}_p$. And ask, are the α_i^n p-adic analytic functions of n?

Do they have an expression as a p-adic power series?

Back to recurrences

With $|\cdot|_p$ the integers are bounded! Going back to the problem of finding the zero's of

$$a_n = \sum_{i=1}^{m} A_i(n)\alpha_i^n$$

as a function of n. We can think of this as a function $\mathbb{N} \to \overline{\mathbb{Q}}_p$. And ask, are the α_i^n p-adic analytic functions of n?

Do they have an expression as a p-adic power series?

Problem
The p-adic exponential function has finite radius of convergence.

Back to recurrences

With $|\cdot|_p$ the integers are bounded! Going back to the problem of finding the zero's of

$$a_n = \sum_{i=1}^{m} A_i(n)\alpha_i^n$$

as a function of n. We can think of this as a function $\mathbb{N} \to \overline{\mathbb{Q}}_p$. And ask, are the α_i^n p-adic analytic functions of n?

Do they have an expression as a p-adic power series?

Problem

The p-adic exponential function has finite radius of convergence.

The fix

Choose p so that $|\alpha_i|_p = 1$ for all i, then $\alpha_i^{p-1} = 1 + \lambda_i$ with $|\lambda_i|_p \leq \frac{1}{p}$. Now $(\alpha_i^{p-1})^n$ is analytic!

Write n as $r + (p-1)n'$ with $0 \leq r < p-1$

Write n as $r + (p-1)n'$ with $0 \leq r < p-1$, then

$$a_n = \sum_{i=1}^{m} A_i(n)\alpha_i^n = \sum_{i=1}^{m} A_i(r + (p-1)n')\alpha_i^{r+(p-1)n'}$$

$$= \sum_{i=1}^{m} A_i(r + (p-1)n')\alpha_i^r(\alpha_i^{(p-1)})^{n'}$$

for each fixed r this function of n' is analytic.

Write n as $r + (p-1)n'$ with $0 \leq r < p-1$, then

$$a_n = \sum_{i=1}^{m} A_i(n)\alpha_i^n = \sum_{i=1}^{m} A_i(r + (p-1)n')\alpha_i^{r+(p-1)n'}$$

$$= \sum_{i=1}^{m} A_i(r + (p-1)n')\alpha_i^r(\alpha_i^{(p-1)})^{n'}$$

for each fixed r this function of n' is analytic. Infinitely many zeroes for integer n means $\exists r$ with infinitely many zeroes of the form $r + (p-1)n'$. So the function

$$\sum_{i=1}^{m} A_i(r + (p-1)n')\alpha_i^r(\alpha_i^{(p-1)})^{n'}$$

is identically zero, and all these $a_n = 0$ when $n \equiv r \pmod{p-1}$.

Finale

Theorem: Skolem $\rightsquigarrow$ Mahler $\rightsquigarrow$ Lech

Let x_n be a linear recurrence sequence in a field of characteristic 0 (i.e. containing $\mathbb{Q}$). Then the n for which $a_n = 0$ lie in a union of finitely many arithmetic progressions, i.e. they are all of the form $tM + b$ for some fixed M and $b \in B \subset \{0, \ldots, M-1\}$, as $t \in \mathbb{N}$ varies.

Finale

Theorem: Skolem $\rightsquigarrow$ Mahler $\rightsquigarrow$ Lech

Let x_n be a linear recurrence sequence in a field of characteristic 0 (i.e. containing $\mathbb{Q}$). Then the n for which $a_n = 0$ lie in a union of finitely many arithmetic progressions, i.e. they are all of the form $tM + b$ for some fixed M and $b \in B \subset \{0, \ldots, M-1\}$, as $t \in \mathbb{N}$ varies.

Aside, positive

What about for fields of positive characteristic?

Aside, positive

What about for fields of positive characteristic? For finite fields everything is periodic by default.

Aside, positive

What about for fields of positive characteristic? For finite fields everything is periodic by default. But for fields like $\mathbb{F}_p(x)$ the theorem is false!

Aside, positive

What about for fields of positive characteristic? For finite fields everything is periodic by default. But for fields like $\mathbb{F}_p(x)$ the theorem is false!

(Example from Harm Derksen) Consider the sequence $a_n \in \mathbb{F}_4(x)$ defined by

$$a(n) = x^n + (x+1)^n + (x+\alpha)^n + (x+1+\alpha)^n,$$

where $\alpha \in \mathbb{F}_4 \backslash \mathbb{F}_2$. We can compute $a(0) = a(1) = a(2) = 0$ and $a(3) = 1$. This sequence satisfies a recurrence relation of order 4

$$a(n+4) = a(n+1) + \left(x^4 + x\right) a(n).$$

the set of n for which $a_n = 0$ is

$$\left\{4^a + 4^b | a, b \in \mathbb{N}\right\} \cup \left\{2 \cdot \left(4^a + 4^b\right) | a, b \in \mathbb{N}\right\} \cup \{0, 1\}$$