On the *p*-adic Skolem Problem

Piotr Bacik

Max Planck Institute for Software Systems, Germany

University of Oxford, UK

(Joint work with Joël Ouaknine, David Purser and James Worrell)

STACS 2026

Linear Recurrence Sequences (LRS)

Linear Recurrence Sequences (LRS)

Examples:

- The Fibonacci sequence $\langle F_n \rangle_{n=0}^{\infty} = \langle 0, 1, 1, 2, 3, 5, 8, \ldots \rangle$ satisfies $F_n = F_{n-1} + F_{n-2}$.

Linear Recurrence Sequences (LRS)

Examples:

- The Fibonacci sequence $\langle F_n \rangle_{n=0}^{\infty} = \langle 0, 1, 1, 2, 3, 5, 8, \ldots \rangle$ satisfies $F_n = F_{n-1} + F_{n-2}$.
- Reverse Tribonacci: $\langle T_n \rangle_{n=0}^{\infty} = \langle 1, 0, 0, 1, -1, 0, 2, -3, 1, 4, -8, \ldots \rangle$ satisfies $T_n = -T_{n-1} - T_{n-2} + T_{n-3}$.

Linear Recurrence Sequences (LRS)

Examples:

- The Fibonacci sequence $\langle F_n \rangle_{n=0}^{\infty} = \langle 0, 1, 1, 2, 3, 5, 8, \ldots \rangle$ satisfies $F_n = F_{n-1} + F_{n-2}$.
- Reverse Tribonacci: $\langle T_n \rangle_{n=0}^{\infty} = \langle 1, 0, 0, 1, -1, 0, 2, -3, 1, 4, -8, \ldots \rangle$ satisfies $T_n = -T_{n-1} - T_{n-2} + T_{n-3}$.
- An interleaving: $\langle u_n \rangle_{n=0}^{\infty} = \langle 0, 2, 0, 4, 0, 8, 0, 16, 0, \ldots \rangle$ satisfies $u_n = 2u_{n-2}$.

Linear Recurrence Sequences (LRS)

Examples:

- The Fibonacci sequence $\langle F_n \rangle_{n=0}^{\infty} = \langle 0, 1, 1, 2, 3, 5, 8, \ldots \rangle$ satisfies $F_n = F_{n-1} + F_{n-2}$.
- Reverse Tribonacci: $\langle T_n \rangle_{n=0}^{\infty} = \langle 1, 0, 0, 1, -1, 0, 2, -3, 1, 4, -8, \ldots \rangle$ satisfies $T_n = -T_{n-1} - T_{n-2} + T_{n-3}$.
- An interleaving: $\langle u_n \rangle_{n=0}^{\infty} = \langle 0, 2, 0, 4, 0, 8, 0, 16, 0, \ldots \rangle$ satisfies $u_n = 2u_{n-2}$.
- $\langle v_n \rangle_{n=0}^{\infty} = \langle n^2 - 2 \rangle_{n=0}^{\infty} = \langle -2, -1, 2, 7, 14, 23, \ldots \rangle$ satisfies $v_{n+3} = 3v_{n+2} - 3v_{n+1} + v_n$.

Linear Recurrence Sequences (LRS)

Examples:

- The Fibonacci sequence $\langle F_n \rangle_{n=0}^{\infty} = \langle 0, 1, 1, 2, 3, 5, 8, \ldots \rangle$ satisfies $F_n = F_{n-1} + F_{n-2}$.
- Reverse Tribonacci: $\langle T_n \rangle_{n=0}^{\infty} = \langle 1, 0, 0, 1, -1, 0, 2, -3, 1, 4, -8, \ldots \rangle$ satisfies $T_n = -T_{n-1} - T_{n-2} + T_{n-3}$.
- An interleaving: $\langle u_n \rangle_{n=0}^{\infty} = \langle 0, 2, 0, 4, 0, 8, 0, 16, 0, \ldots \rangle$ satisfies $u_n = 2u_{n-2}$.
- $\langle v_n \rangle_{n=0}^{\infty} = \langle n^2 - 2 \rangle_{n=0}^{\infty} = \langle -2, -1, 2, 7, 14, 23, \ldots \rangle$ satisfies $v_{n+3} = 3v_{n+2} - 3v_{n+1} + v_n$.

Definition

A *linear recurrence sequence* (LRS) is a sequence of integers $u = \langle u_n \rangle_{n=0}^{\infty}$ that satisfy a relation of the form

$$u_n = a_1 u_{n-1} + \cdots + a_d u_{n-d}$$

for $a_1, \ldots, a_d \in \mathbb{Z}$ and $a_d \neq 0$.

Linear Recurrence Sequences (LRS)

Examples:

- The Fibonacci sequence $\langle F_n \rangle_{n=0}^{\infty} = \langle 0, 1, 1, 2, 3, 5, 8, \ldots \rangle$ satisfies $F_n = F_{n-1} + F_{n-2}$.
- Reverse Tribonacci: $\langle T_n \rangle_{n=0}^{\infty} = \langle 1, 0, 0, 1, -1, 0, 2, -3, 1, 4, -8, \ldots \rangle$ satisfies $T_n = -T_{n-1} - T_{n-2} + T_{n-3}$.
- An interleaving: $\langle u_n \rangle_{n=0}^{\infty} = \langle 0, 2, 0, 4, 0, 8, 0, 16, 0, \ldots \rangle$ satisfies $u_n = 2u_{n-2}$.
- $\langle v_n \rangle_{n=0}^{\infty} = \langle n^2 - 2 \rangle_{n=0}^{\infty} = \langle -2, -1, 2, 7, 14, 23, \ldots \rangle$ satisfies $v_{n+3} = 3v_{n+2} - 3v_{n+1} + v_n$.

Definition

A *linear recurrence sequence* (LRS) is a sequence of integers $u = \langle u_n \rangle_{n=0}^{\infty}$ that satisfy a relation of the form

$$u_n = a_1 u_{n-1} + \cdots + a_d u_{n-d}$$

for $a_1, \ldots, a_d \in \mathbb{Z}$ and $a_d \neq 0$. We say u has order d.

Linear Recurrence Sequences (LRS)

Examples:

- The Fibonacci sequence $\langle F_n \rangle_{n=0}^{\infty} = \langle 0, 1, 1, 2, 3, 5, 8, \dots \rangle$ satisfies $F_n = F_{n-1} + F_{n-2}$. It is of order 2.
- Reverse Tribonacci: $\langle T_n \rangle_{n=0}^{\infty} = \langle 1, 0, 0, 1, -1, 0, 2, -3, 1, 4, -8, \dots \rangle$ satisfies $T_n = -T_{n-1} - T_{n-2} + T_{n-3}$.
- An interleaving: $\langle u_n \rangle_{n=0}^{\infty} = \langle 0, 2, 0, 4, 0, 8, 0, 16, 0, \dots \rangle$ satisfies $u_n = 2u_{n-2}$.
- $\langle v_n \rangle_{n=0}^{\infty} = \langle n^2 - 2 \rangle_{n=0}^{\infty} = \langle -2, -1, 2, 7, 14, 23, \dots \rangle$ satisfies $v_{n+3} = 3v_{n+2} - 3v_{n+1} + v_n$.

Definition

A *linear recurrence sequence* (LRS) is a sequence of integers $u = \langle u_n \rangle_{n=0}^{\infty}$ that satisfy a relation of the form

$$u_n = a_1 u_{n-1} + \cdots + a_d u_{n-d}$$

for $a_1, \dots, a_d \in \mathbb{Z}$ and $a_d \neq 0$. We say u has order d.

Linear Recurrence Sequences (LRS)

Examples:

- The Fibonacci sequence $\langle F_n \rangle_{n=0}^{\infty} = \langle 0, 1, 1, 2, 3, 5, 8, \ldots \rangle$ satisfies $F_n = F_{n-1} + F_{n-2}$. It is of order 2.
- Reverse Tribonacci: $\langle T_n \rangle_{n=0}^{\infty} = \langle 1, 0, 0, 1, -1, 0, 2, -3, 1, 4, -8, \ldots \rangle$ satisfies $T_n = -T_{n-1} - T_{n-2} + T_{n-3}$. It is of order 3.
- An interleaving: $\langle u_n \rangle_{n=0}^{\infty} = \langle 0, 2, 0, 4, 0, 8, 0, 16, 0, \ldots \rangle$ satisfies $u_n = 2u_{n-2}$.
- $\langle v_n \rangle_{n=0}^{\infty} = \langle n^2 - 2 \rangle_{n=0}^{\infty} = \langle -2, -1, 2, 7, 14, 23, \ldots \rangle$ satisfies $v_{n+3} = 3v_{n+2} - 3v_{n+1} + v_n$.

Definition

A *linear recurrence sequence* (LRS) is a sequence of integers $u = \langle u_n \rangle_{n=0}^{\infty}$ that satisfy a relation of the form

$$u_n = a_1 u_{n-1} + \cdots + a_d u_{n-d}$$

for $a_1, \ldots, a_d \in \mathbb{Z}$ and $a_d \neq 0$. We say u has order d.

Linear Recurrence Sequences (LRS)

Examples:

- The Fibonacci sequence $\langle F_n \rangle_{n=0}^{\infty} = \langle 0, 1, 1, 2, 3, 5, 8, \ldots \rangle$ satisfies $F_n = F_{n-1} + F_{n-2}$. It is of order 2.
- Reverse Tribonacci: $\langle T_n \rangle_{n=0}^{\infty} = \langle 1, 0, 0, 1, -1, 0, 2, -3, 1, 4, -8, \ldots \rangle$ satisfies $T_n = -T_{n-1} - T_{n-2} + T_{n-3}$. It is of order 3.
- An interleaving: $\langle u_n \rangle_{n=0}^{\infty} = \langle 0, 2, 0, 4, 0, 8, 0, 16, 0, \ldots \rangle$ satisfies $u_n = 2u_{n-2}$. It is of order 2.
- $\langle v_n \rangle_{n=0}^{\infty} = \langle n^2 - 2 \rangle_{n=0}^{\infty} = \langle -2, -1, 2, 7, 14, 23, \ldots \rangle$ satisfies $v_{n+3} = 3v_{n+2} - 3v_{n+1} + v_n$.

Definition

A *linear recurrence sequence* (LRS) is a sequence of integers $u = \langle u_n \rangle_{n=0}^{\infty}$ that satisfy a relation of the form

$$u_n = a_1 u_{n-1} + \cdots + a_d u_{n-d}$$

for $a_1, \ldots, a_d \in \mathbb{Z}$ and $a_d \neq 0$. We say u has order d.

Linear Recurrence Sequences (LRS)

Examples:

- The Fibonacci sequence $\langle F_n \rangle_{n=0}^{\infty} = \langle 0, 1, 1, 2, 3, 5, 8, \ldots \rangle$ satisfies $F_n = F_{n-1} + F_{n-2}$. It is of order 2.
- Reverse Tribonacci: $\langle T_n \rangle_{n=0}^{\infty} = \langle 1, 0, 0, 1, -1, 0, 2, -3, 1, 4, -8, \ldots \rangle$ satisfies $T_n = -T_{n-1} - T_{n-2} + T_{n-3}$. It is of order 3.
- An interleaving: $\langle u_n \rangle_{n=0}^{\infty} = \langle 0, 2, 0, 4, 0, 8, 0, 16, 0, \ldots \rangle$ satisfies $u_n = 2u_{n-2}$. It is of order 2.
- $\langle v_n \rangle_{n=0}^{\infty} = \langle n^2 - 2 \rangle_{n=0}^{\infty} = \langle -2, -1, 2, 7, 14, 23, \ldots \rangle$ satisfies $v_{n+3} = 3v_{n+2} - 3v_{n+1} + v_n$. It is of order 3.

Definition

A *linear recurrence sequence* (LRS) is a sequence of integers $u = \langle u_n \rangle_{n=0}^{\infty}$ that satisfy a relation of the form

$$u_n = a_1 u_{n-1} + \cdots + a_d u_{n-d}$$

for $a_1, \ldots, a_d \in \mathbb{Z}$ and $a_d \neq 0$. We say u has order d.

Skolem-Mahler-Lech

Theorem (Skolem-Mahler-Lech, 1935-1957)

The set $Z(u) = \{n \in \mathbb{N} : u_n = 0\}$ of zeros of an LRS u is a union of finitely many arithmetic progressions and a finite set.

Zeros of LRS

Examples:

- The Fibonacci sequence $\langle F_n \rangle_{n=0}^{\infty} = \langle 0, 1, 1, 2, 3, 5, 8, \dots \rangle$ satisfies $F_n = F_{n-1} + F_{n-2}$. It is of order 2.
- Reverse Tribonacci: $\langle T_n \rangle_{n=0}^{\infty} = \langle 1, 0, 0, 1, -1, 0, 2, -3, 1, 4, -8, \dots \rangle$ satisfies $T_n = -T_{n-1} - T_{n-2} + T_{n-3}$. It is of order 3.
- An interleaving: $\langle u_n \rangle_{n=0}^{\infty} = \langle 0, 2, 0, 4, 0, 8, 0, 16, 0, \dots \rangle$ satisfies $u_n = 2u_{n-2}$. It is of order 2.
- $\langle v_n \rangle_{n=0}^{\infty} = \langle n^2 - 2 \rangle_{n=0}^{\infty} = \langle -2, -1, 2, 7, 14, 23, \dots \rangle$ satisfies $v_{n+3} = 3v_{n+2} - 3v_{n+1} + v_n$. It is of order 3.

Zeros of LRS

Examples:

- The Fibonacci sequence $\langle F_n \rangle_{n=0}^{\infty} = \langle 0, 1, 1, 2, 3, 5, 8, \ldots \rangle$ satisfies $F_n = F_{n-1} + F_{n-2}$. It is of order 2. $Z(F) = \{0\}$
- Reverse Tribonacci: $\langle T_n \rangle_{n=0}^{\infty} = \langle 1, 0, 0, 1, -1, 0, 2, -3, 1, 4, -8, \ldots \rangle$ satisfies $T_n = -T_{n-1} - T_{n-2} + T_{n-3}$. It is of order 3.
- An interleaving: $\langle u_n \rangle_{n=0}^{\infty} = \langle 0, 2, 0, 4, 0, 8, 0, 16, 0, \ldots \rangle$ satisfies $u_n = 2u_{n-2}$. It is of order 2.
- $\langle v_n \rangle_{n=0}^{\infty} = \langle n^2 - 2 \rangle_{n=0}^{\infty} = \langle -2, -1, 2, 7, 14, 23, \ldots \rangle$ satisfies $v_{n+3} = 3v_{n+2} - 3v_{n+1} + v_n$. It is of order 3.

Zeros of LRS

Examples:

- The Fibonacci sequence $\langle F_n \rangle_{n=0}^{\infty} = \langle 0, 1, 1, 2, 3, 5, 8, \dots \rangle$ satisfies $F_n = F_{n-1} + F_{n-2}$. It is of order 2. $Z(F) = \{0\}$
- Reverse Tribonacci: $\langle T_n \rangle_{n=0}^{\infty} = \langle 1, 0, 0, 1, -1, 0, 2, -3, 1, 4, -8, \dots \rangle$ satisfies $T_n = -T_{n-1} - T_{n-2} + T_{n-3}$. It is of order 3. $Z(T) = \{1, 2, 5, 18\}$
- An interleaving: $\langle u_n \rangle_{n=0}^{\infty} = \langle 0, 2, 0, 4, 0, 8, 0, 16, 0, \dots \rangle$ satisfies $u_n = 2u_{n-2}$. It is of order 2.
- $\langle v_n \rangle_{n=0}^{\infty} = \langle n^2 - 2 \rangle_{n=0}^{\infty} = \langle -2, -1, 2, 7, 14, 23, \dots \rangle$ satisfies $v_{n+3} = 3v_{n+2} - 3v_{n+1} + v_n$. It is of order 3.

Zeros of LRS

Examples:

- The Fibonacci sequence $\langle F_n \rangle_{n=0}^{\infty} = \langle 0, 1, 1, 2, 3, 5, 8, \dots \rangle$ satisfies $F_n = F_{n-1} + F_{n-2}$. It is of order 2. $Z(F) = \{0\}$
- Reverse Tribonacci: $\langle T_n \rangle_{n=0}^{\infty} = \langle 1, 0, 0, 1, -1, 0, 2, -3, 1, 4, -8, \dots \rangle$ satisfies $T_n = -T_{n-1} - T_{n-2} + T_{n-3}$. It is of order 3. $Z(T) = \{1, 2, 5, 18\}$
- An interleaving: $\langle u_n \rangle_{n=0}^{\infty} = \langle 0, 2, 0, 4, 0, 8, 0, 16, 0, \dots \rangle$ satisfies $u_n = 2u_{n-2}$. It is of order 2. $Z(u) = \{2n : n \in \mathbb{N}\}$
- $\langle v_n \rangle_{n=0}^{\infty} = \langle n^2 - 2 \rangle_{n=0}^{\infty} = \langle -2, -1, 2, 7, 14, 23, \dots \rangle$ satisfies $v_{n+3} = 3v_{n+2} - 3v_{n+1} + v_n$. It is of order 3.

Zeros of LRS

Examples:

- The Fibonacci sequence $\langle F_n \rangle_{n=0}^{\infty} = \langle 0, 1, 1, 2, 3, 5, 8, \ldots \rangle$ satisfies $F_n = F_{n-1} + F_{n-2}$. It is of order 2. $Z(F) = \{0\}$
- Reverse Tribonacci: $\langle T_n \rangle_{n=0}^{\infty} = \langle 1, 0, 0, 1, -1, 0, 2, -3, 1, 4, -8, \ldots \rangle$ satisfies $T_n = -T_{n-1} - T_{n-2} + T_{n-3}$. It is of order 3. $Z(T) = \{1, 2, 5, 18\}$
- An interleaving: $\langle u_n \rangle_{n=0}^{\infty} = \langle 0, 2, 0, 4, 0, 8, 0, 16, 0, \ldots \rangle$ satisfies $u_n = 2u_{n-2}$. It is of order 2. $Z(u) = \{2n : n \in \mathbb{N}\}$
- $\langle v_n \rangle_{n=0}^{\infty} = \langle n^2 - 2 \rangle_{n=0}^{\infty} = \langle -2, -1, 2, 7, 14, 23, \ldots \rangle$ satisfies $v_{n+3} = 3v_{n+2} - 3v_{n+1} + v_n$. It is of order 3. $Z(v) = \varnothing$

Skolem-Mahler-Lech

Theorem (Skolem-Mahler-Lech, 1935-1957)

The set $Z(u) = \{n \in \mathbb{N} : u_n = 0\}$ of zeros of an LRS u is a union of finitely many arithmetic progressions and a finite set.

Skolem-Mahler-Lech

Theorem (Skolem-Mahler-Lech, 1935-1957)

The set $Z(u) = \{n \in \mathbb{N} : u_n = 0\}$ of zeros of an LRS u is a union of finitely many arithmetic progressions and a finite set.

The proof is ineffective - though we can find the arithmetic progressions effectively, there is no known procedure to determine the exceptional finite set.

Skolem-Mahler-Lech

Theorem (Skolem-Mahler-Lech, 1935-1957)

The set $Z(u) = \{n \in \mathbb{N} : u_n = 0\}$ of zeros of an LRS u is a union of finitely many arithmetic progressions and a finite set.

The proof is ineffective - though we can find the arithmetic progressions effectively, there is no known procedure to determine the exceptional finite set.

The Skolem Problem

Instance: An LRS u.
Problem: Is there $n \in \mathbb{N}$ such that $u_n = 0$?

The Skolem Problem - State of the Art

- The Skolem Problem is not known to be decidable!

The Skolem Problem - State of the Art

- The Skolem Problem is not known to be decidable! Best known result:

Theorem (Mignotte, Shorey, Tijdeman 1984, Vereshchagin 1985, B. 2025)

The Skolem Problem is decidable for LRS of order at most 4.

The Skolem Problem - State of the Art

- The Skolem Problem is not known to be decidable! Best known result:

Theorem (Mignotte, Shorey, Tijdeman 1984, Vereshchagin 1985, B. 2025)

The Skolem Problem is decidable for LRS of order at most 4.

- Currently, the Skolem Problem is open for order-5 LRS.

The Skolem Problem - State of the Art

- The Skolem Problem is not known to be decidable! Best known result:

Theorem (Mignotte, Shorey, Tijdeman 1984, Vereshchagin 1985, B. 2025)

The Skolem Problem is decidable for LRS of order at most 4.

- Currently, the Skolem Problem is open for order-5 LRS.

Idea of the present paper:

The Skolem Problem - State of the Art

- The Skolem Problem is not known to be decidable! Best known result:

Theorem (Mignotte, Shorey, Tijdeman 1984, Vereshchagin 1985, B. 2025)

The Skolem Problem is decidable for LRS of order at most 4.

- Currently, the Skolem Problem is open for order-5 LRS.

Idea of the present paper:

- Searching for $n \in \mathbb{N}$ such that $u_n = 0$ is hard.

The Skolem Problem - State of the Art

- The Skolem Problem is not known to be decidable! Best known result:

Theorem (Mignotte, Shorey, Tijdeman 1984, Vereshchagin 1985, B. 2025)

The Skolem Problem is decidable for LRS of order at most 4.

- Currently, the Skolem Problem is open for order-5 LRS.

Idea of the present paper:

- Searching for $n \in \mathbb{N}$ such that $u_n = 0$ is hard.
- Expand the domain; search for zeros in $\mathbb{Z}_p \supseteq \mathbb{N}$ instead.

The Skolem Problem - State of the Art

- The Skolem Problem is not known to be decidable! Best known result:

Theorem (Mignotte, Shorey, Tijdeman 1984, Vereshchagin 1985, B. 2025)

The Skolem Problem is decidable for LRS of order at most 4.

- Currently, the Skolem Problem is open for order-5 LRS.

Idea of the present paper:

- Searching for $n \in \mathbb{N}$ such that $u_n = 0$ is hard.
- Expand the domain; search for zeros in $\mathbb{Z}_p \supseteq \mathbb{N}$ instead.

Next slides: what is $\mathbb{Z}_p$? What does it mean for $x \in \mathbb{Z}_p$ to be a zero of LRS u? Why do we care?

p-adic numbers – a very quick tour

Pick a prime number p.

p-adic numbers – a very quick tour

Pick a prime number p. Formally:

- Define the p-adic absolute value on $\mathbb{Z}$ by $|x|_p = p^{-v_p(x)}$, where $v_p(x)$ is "the number of times p divides x".

p-adic numbers – a very quick tour

Pick a prime number p. Formally:

- Define the p-adic absolute value on $\mathbb{Z}$ by $|x|_p = p^{-v_p(x)}$, where $v_p(x)$ is "the number of times p divides x".
- E.g. $|18|_3 = 3^{-2}$, $|2026|_5 = 5^0 = 1$.

p-adic numbers – a very quick tour

Pick a prime number p. Formally:

- Define the p-adic absolute value on $\mathbb{Z}$ by $|x|_p = p^{-v_p(x)}$, where $v_p(x)$ is "the number of times p divides x".
- E.g. $|18|_3 = 3^{-2}$, $|2026|_5 = 5^0 = 1$.
- The set of p-adic integers $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ with respect to the absolute value $|x|_p = p^{-v_p(x)}$.

p-adic numbers – a very quick tour

Pick a prime number p. Formally:

- Define the p-adic absolute value on $\mathbb{Z}$ by $|x|_p = p^{-v_p(x)}$, where $v_p(x)$ is "the number of times p divides x".
- E.g. $|18|_3 = 3^{-2}$, $|2026|_5 = 5^0 = 1$.
- The set of p-adic integers $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ with respect to the absolute value $|x|_p = p^{-v_p(x)}$.
- Analogue: complete $\mathbb{Q}$ wrt usual $|\cdot|$ to get $\mathbb{R}$.

p-adic numbers – a very quick tour

Pick a prime number p. Formally:

- Define the p-adic absolute value on $\mathbb{Z}$ by $|x|_p = p^{-v_p(x)}$, where $v_p(x)$ is "the number of times p divides x".
- E.g. $|18|_3 = 3^{-2}$, $|2026|_5 = 5^0 = 1$.
- The set of p-adic integers $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ with respect to the absolute value $|x|_p = p^{-v_p(x)}$.
- Analogue: complete $\mathbb{Q}$ wrt usual $|\cdot|$ to get $\mathbb{R}$.

Facts:

p-adic numbers – a very quick tour

Pick a prime number p. Formally:

- Define the p-adic absolute value on $\mathbb{Z}$ by $|x|_p = p^{-v_p(x)}$, where $v_p(x)$ is "the number of times p divides x".
- E.g. $|18|_3 = 3^{-2}$, $|2026|_5 = 5^0 = 1$.
- The set of p-adic integers $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ with respect to the absolute value $|x|_p = p^{-v_p(x)}$.
- Analogue: complete $\mathbb{Q}$ wrt usual $|\cdot|$ to get $\mathbb{R}$.

Facts:

- $\mathbb{Z}_p$ is a complete, compact ring – nice analytical properties!

p-adic numbers – a very quick tour

Pick a prime number p. Formally:

- Define the p-adic absolute value on $\mathbb{Z}$ by $|x|_p = p^{-v_p(x)}$, where $v_p(x)$ is "the number of times p divides x".
- E.g. $|18|_3 = 3^{-2}$, $|2026|_5 = 5^0 = 1$.
- The set of p-adic integers $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ with respect to the absolute value $|x|_p = p^{-v_p(x)}$.
- Analogue: complete $\mathbb{Q}$ wrt usual $|\cdot|$ to get $\mathbb{R}$.

Facts:

- $\mathbb{Z}_p$ is a complete, compact ring – nice analytical properties!
- Keeps nice number theory structure - e.g. $x \bmod p^r$ makes sense for all $x \in \mathbb{Z}_p$.

p-adic numbers - examples

Every $x \in \mathbb{Z}_p$ has a series expansion $x = \sum_{j=0}^{\infty} a_j p^j$ with $a_j \in \{0, 1, \ldots, p-1\}$.

p-adic numbers - examples

Every $x \in \mathbb{Z}_p$ has a series expansion $x = \sum_{j=0}^{\infty} a_j p^j$ with $a_j \in \{0, 1, \ldots, p-1\}$.

- $2026 = 3 + 2 \cdot 7 + 6 \cdot 7^2 + 5 \cdot 7^3 \in \mathbb{Z}_7$

p-adic numbers - examples

Every $x \in \mathbb{Z}_p$ has a series expansion $x = \sum_{j=0}^{\infty} a_j p^j$ with $a_j \in \{0, 1, \ldots, p-1\}$.

- $2026 = 3 + 2 \cdot 7 + 6 \cdot 7^2 + 5 \cdot 7^3 \in \mathbb{Z}_7$
- $-1 = 1 + 1 \cdot 2 + 1 \cdot 2^2 + 1 \cdot 2^3 + \cdots \in \mathbb{Z}_2$

p-adic numbers - examples

Every $x \in \mathbb{Z}_p$ has a series expansion $x = \sum_{j=0}^{\infty} a_j p^j$ with $a_j \in \{0, 1, \ldots, p-1\}$.

- $2026 = 3 + 2 \cdot 7 + 6 \cdot 7^2 + 5 \cdot 7^3 \in \mathbb{Z}_7$
- $-1 = 1 + 1 \cdot 2 + 1 \cdot 2^2 + 1 \cdot 2^3 + \cdots \in \mathbb{Z}_2$
- $\frac{1}{2} = 2 + 1 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^3 + \cdots \in \mathbb{Z}_3$

p-adic numbers - examples

Every $x \in \mathbb{Z}_p$ has a series expansion $x = \sum_{j=0}^{\infty} a_j p^j$ with $a_j \in \{0, 1, \ldots, p-1\}$.

- $2026 = 3 + 2 \cdot 7 + 6 \cdot 7^2 + 5 \cdot 7^3 \in \mathbb{Z}_7$
- $-1 = 1 + 1 \cdot 2 + 1 \cdot 2^2 + 1 \cdot 2^3 + \cdots \in \mathbb{Z}_2$
- $\frac{1}{2} = 2 + 1 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^3 + \cdots \in \mathbb{Z}_3$
- $\sqrt{2} = 3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + \cdots \in \mathbb{Z}_7$

p-adic numbers - examples

Every $x \in \mathbb{Z}_p$ has a series expansion $x = \sum_{j=0}^{\infty} a_j p^j$ with $a_j \in \{0, 1, \ldots, p-1\}$.

- $2026 = 3 + 2 \cdot 7 + 6 \cdot 7^2 + 5 \cdot 7^3 \in \mathbb{Z}_7$
- $-1 = 1 + 1 \cdot 2 + 1 \cdot 2^2 + 1 \cdot 2^3 + \cdots \in \mathbb{Z}_2$
- $\frac{1}{2} = 2 + 1 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^3 + \cdots \in \mathbb{Z}_3$
- $\sqrt{2} = 3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + \cdots \in \mathbb{Z}_7$
- $\sqrt{-1} = 2 + 5 + 2 \cdot 5^2 + 1 \cdot 5^3 + \cdots \in \mathbb{Z}_5$

Why $\mathbb{Z}_p$?

Theorem (Skolem-Mahler-Lech, 1935-1957)

The set $Z(u) = \{n \in \mathbb{N} : u_n = 0\}$ of zeros of an LRS is a union of finitely many arithmetic progressions and a finite set.

Why $\mathbb{Z}_p$?

Theorem (Skolem-Mahler-Lech, 1935-1957)

The set $Z(u) = \{n \in \mathbb{N} : u_n = 0\}$ of zeros of an LRS is a union of finitely many arithmetic progressions and a finite set.

Proven using p-adic analysis!

Why $\mathbb{Z}_p$?

Theorem (Skolem-Mahler-Lech, 1935-1957)

The set $Z(u) = \{n \in \mathbb{N} : u_n = 0\}$ of zeros of an LRS is a union of finitely many arithmetic progressions and a finite set.

Proven using p-adic analysis!
Main idea: given LRS u, pick prime number p. Split into subsequences $u_{Mn}, u_{Mn+1}, \ldots, u_{Mn+M-1}$.

Why $\mathbb{Z}_p$?

Theorem (Skolem-Mahler-Lech, 1935-1957)

The set $Z(u) = \{n \in \mathbb{N} : u_n = 0\}$ of zeros of an LRS is a union of finitely many arithmetic progressions and a finite set.

Proven using p-adic analysis!
Main idea: given LRS u, pick prime number p. Split into subsequences $u_{Mn}, u_{Mn+1}, \ldots, u_{Mn+M-1}$. Find p-adic analytic functions

$$f_\ell : \mathbb{Z}_p \to \mathbb{Z}_p, \quad x \mapsto \sum_{k=0}^{\infty} b_{k,\ell} x^k$$

such that $f_\ell(n) = u_{Mn+\ell}$ for all $n \in \mathbb{N}$, for each $0 \leq \ell \leq M-1$.

Why $\mathbb{Z}_p$?

Theorem (Skolem-Mahler-Lech, 1935-1957)

The set $Z(u) = \{n \in \mathbb{N} : u_n = 0\}$ of zeros of an LRS is a union of finitely many arithmetic progressions and a finite set.

Proven using p-adic analysis!
Main idea: given LRS u, pick prime number p. Split into subsequences $u_{Mn}, u_{Mn+1}, \ldots, u_{Mn+M-1}$. Find p-adic analytic functions

$$f_\ell : \mathbb{Z}_p \to \mathbb{Z}_p, \quad x \mapsto \sum_{k=0}^{\infty} b_{k,\ell} x^k$$

such that $f_\ell(n) = u_{Mn+\ell}$ for all $n \in \mathbb{N}$, for each $0 \leq \ell \leq M-1$.

Each f_ℓ is analytic on compact domain $\rightarrow$ either identically zero or has finitely many zeros.

p-adic zeros of LRS

Key point: each subsequence $u_{Mn+\ell}$ is a function

$$\mathbb{N} \to \mathbb{Z}, \quad n \mapsto u_{Mn+\ell}$$

p-adic zeros of LRS

Key point: each subsequence $u_{Mn+\ell}$ is a function

$$\mathbb{N} \to \mathbb{Z}, \quad n \mapsto u_{Mn+\ell}$$

and they uniquely extend to analytic functions

$$f_\ell : \mathbb{Z}_p \to \mathbb{Z}_p, \quad x \mapsto f_\ell(x)\,.$$

p-adic zeros of LRS

Key point: each subsequence $u_{Mn+\ell}$ is a function

$$\mathbb{N} \to \mathbb{Z}, \quad n \mapsto u_{Mn+\ell}$$

and they uniquely extend to analytic functions

$$f_\ell : \mathbb{Z}_p \to \mathbb{Z}_p, \quad x \mapsto f_\ell(x)\,.$$

Definition (p-adic zero)

Call $x \in \mathbb{Z}_p$ a p-adic zero of LRS u if $f_\ell(x) = 0$ for some $0 \leq \ell \leq M - 1$.

The p-adic Skolem Problem

Theorem (Skolem-Mahler-Lech, 1935-1957)

The set of zeros of an LRS is a union of finitely many arithmetic progressions and a finite set.

The p-adic Skolem Problem

Theorem (Skolem-Mahler-Lech, 1935-1957) (true version)

The set of p-adic zeros of an LRS is a union of finitely many arithmetic progressions and a finite set.

The p-adic Skolem Problem

Theorem (Skolem-Mahler-Lech, 1935-1957) (true version)

The set of p-adic zeros of an LRS is a union of finitely many arithmetic progressions and a finite set.

The proof is ineffective, we can find the arithmetic progressions, but unclear how to find the finite set.

The p-adic Skolem Problem

Theorem (Skolem-Mahler-Lech, 1935-1957) (true version)

The set of p-adic zeros of an LRS is a union of finitely many arithmetic progressions and a finite set.

The proof is ineffective, we can find the arithmetic progressions, but unclear how to find the finite set.

The p-adic Skolem Problem

Instance: An LRS u.
Problem: Does u have a p-adic zero?

The p-adic Skolem Problem

Theorem (Skolem-Mahler-Lech, 1935-1957) (true version)

The set of p-adic zeros of an LRS is a union of finitely many arithmetic progressions and a finite set.

The proof is ineffective, we can find the arithmetic progressions, but unclear how to find the finite set.

The p-adic Skolem Problem

Instance: An LRS u.
Problem: Does u have a p-adic zero?

Theorem

Assuming the p-adic Schanuel Conjecture, the p-adic Skolem Problem is decidable. Moreover, all p-adic zeros are computable.

The p-adic Skolem Problem

Theorem (Skolem-Mahler-Lech, 1935-1957) (true version)

The set of p-adic zeros of an LRS is a union of finitely many arithmetic progressions and a finite set.

The proof is ineffective, we can find the arithmetic progressions, but unclear how to find the finite set.

The p-adic Skolem Problem

Instance: An LRS u.
Problem: Does u have a p-adic zero?

Theorem

Assuming the p-adic Schanuel Conjecture, the p-adic Skolem Problem is decidable. Moreover, all p-adic zeros are computable.
SKOLEM tool: `https://skolem.mpi-sws.org/`

The p-adic Skolem Problem

Theorem (Skolem-Mahler-Lech, 1935-1957) (true version)

The set of p-adic zeros of an LRS is a union of finitely many arithmetic progressions and a finite set.

The proof is ineffective, we can find the arithmetic progressions, but unclear how to find the finite set.

The p-adic Skolem Problem

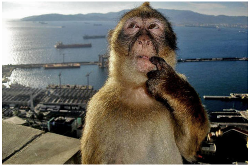
Instance: An LRS u.
Problem: Does u have a p-adic zero?

Theorem

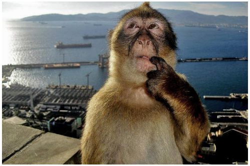
Assuming the p-adic Schanuel Conjecture, the p-adic Skolem Problem is decidable. Moreover, all p-adic zeros are computable.
SKOLEM tool: `https://skolem.mpi-sws.org/`

Correctness is unconditional!

Wait a minute...

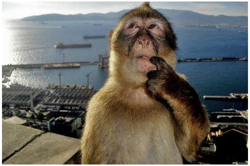


Wait a minute...



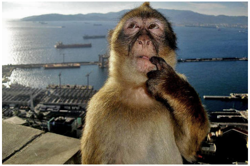
- All natural number zeros are p-adic zeros

Wait a minute...



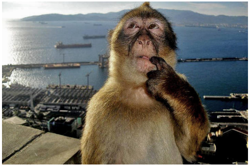
- All natural number zeros are p-adic zeros
- We can find all p-adic zeros

Wait a minute...



- All natural number zeros are p-adic zeros
- We can find all p-adic zeros
- The Skolem Problem asks for natural number zeros of LRS...

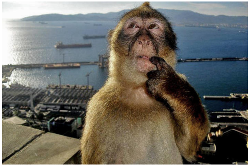
Wait a minute...



- All natural number zeros are p-adic zeros
- We can find all p-adic zeros
- The Skolem Problem asks for natural number zeros of LRS...

Did we just solve the Skolem Problem?

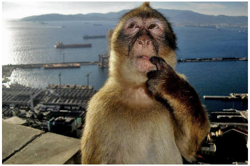
Wait a minute...



- All natural number zeros are p-adic zeros
- We can find all p-adic zeros
- The Skolem Problem asks for natural number zeros of LRS...

Did we just solve the Skolem Problem? Not quite.

Wait a minute...

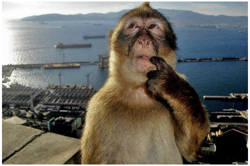


- All natural number zeros are p-adic zeros
- We can find all p-adic zeros
- The Skolem Problem asks for natural number zeros of LRS...

Did we just solve the Skolem Problem? Not quite.

Given a p-adic zero $x = \sum_{k=0}^{\infty} a_k p^k$, not clear how to determine whether $x \in \mathbb{N}$.

Wait a minute...



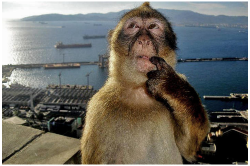
- All natural number zeros are p-adic zeros
- We can find all p-adic zeros
- The Skolem Problem asks for natural number zeros of LRS...

Did we just solve the Skolem Problem? Not quite.

Given a p-adic zero $x = \sum_{k=0}^{\infty} a_k p^k$, not clear how to determine whether $x \in \mathbb{N}$.

Can compute arbitrarily many a_k, but to know whether $x \in \mathbb{N}$, need to know whether or not $a_k = 0$ for all sufficiently large k.

Wait a minute...



- All natural number zeros are p-adic zeros
- We can find all p-adic zeros
- The Skolem Problem asks for natural number zeros of LRS...

Did we just solve the Skolem Problem? Not quite.

Given a p-adic zero $x = \sum_{k=0}^{\infty} a_k p^k$, not clear how to determine whether $x \in \mathbb{N}$.

Can compute arbitrarily many a_k, but to know whether $x \in \mathbb{N}$, need to know whether or not $a_k = 0$ for all sufficiently large k.

But sometimes this is possible...

Simultaneous Skolem Problem

The Simultaneous Skolem Problem

Instance: Two LRS u, v.
Problem: Is there $n \in \mathbb{N}$ such that $u_n = v_n = 0$?

Simultaneous Skolem Problem

The Simultaneous Skolem Problem

Instance: Two LRS u, v.
Problem: Is there $n \in \mathbb{N}$ such that $u_n = v_n = 0$?

Theorem

Assuming the p-adic Schanuel Conjecture, the Simultaneous Skolem Problem is decidable for coprime LRS.

Simultaneous Skolem Problem

The Simultaneous Skolem Problem

Instance: Two LRS u, v.

Problem: Is there $n \in \mathbb{N}$ such that $u_n = v_n = 0$?

Theorem

Assuming the p-adic Schanuel Conjecture, the Simultaneous Skolem Problem is decidable for coprime LRS.

It turns out that simultaneous p-adic zeros are special.

Simultaneous Skolem Problem

The Simultaneous Skolem Problem

Instance: Two LRS u, v.
Problem: Is there $n \in \mathbb{N}$ such that $u_n = v_n = 0$?

Theorem

Assuming the p-adic Schanuel Conjecture, the Simultaneous Skolem Problem is decidable for coprime LRS.

It turns out that simultaneous p-adic zeros are special.

The p-adic Schanuel Conjecture implies simultaneous p-adic zeros are rational.

Simultaneous Skolem Problem

The Simultaneous Skolem Problem

Instance: Two LRS u, v.
Problem: Is there $n \in \mathbb{N}$ such that $u_n = v_n = 0$?

Theorem

Assuming the p-adic Schanuel Conjecture, the Simultaneous Skolem Problem is decidable for coprime LRS.

It turns out that simultaneous p-adic zeros are special.

The p-adic Schanuel Conjecture implies simultaneous p-adic zeros are rational.

$\rightarrow$ Use p-adic Skolem algorithm to find simultaneous p-adic zeros, then natural number zeros can be identified.