p-adic Numbers and Linear Recurrence Relations

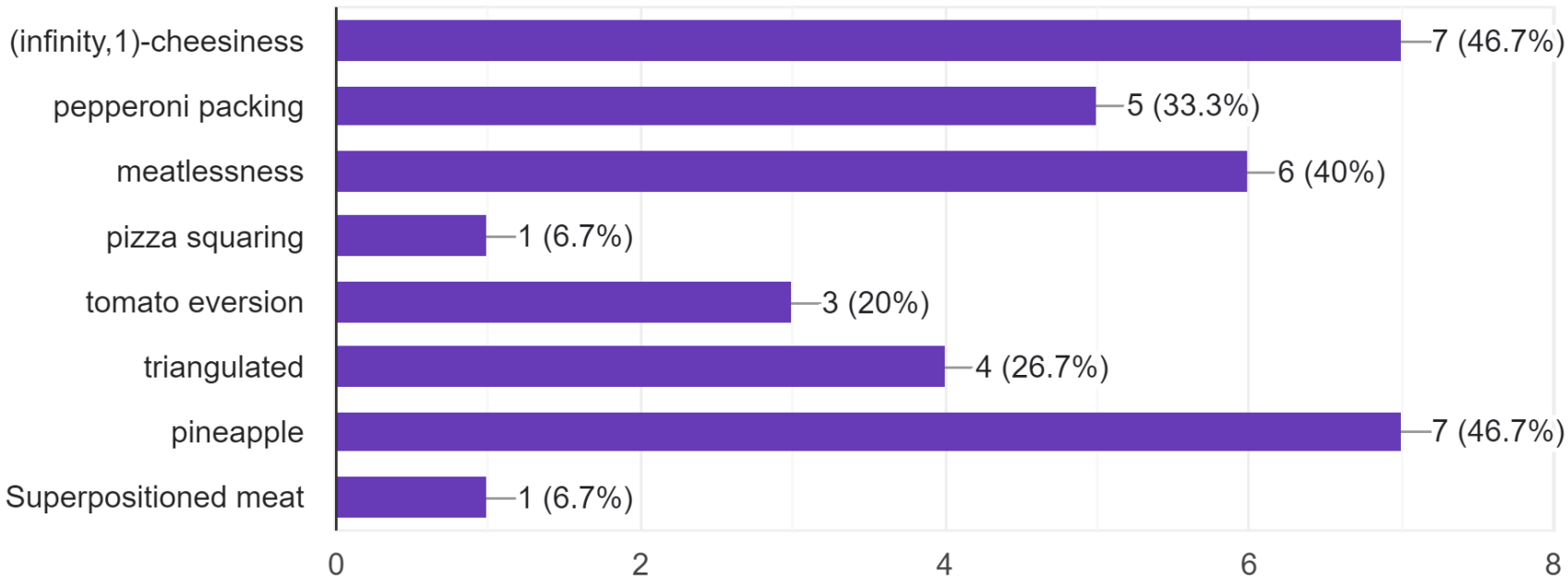
Pizza Seminar

Fanxin Wu

September 15, 2023

What are your favorite homotopy invariants of pizza?

15 responses



Pizza seminar is a place for:

- fun math
- cool math
- boring math
- math games
- math musicals
- discussing how to survive after grad school
- pizzas

etc.

Theorem (Skolem)

If $(x_n : n \in \mathbb{N})$ *is defined by* $x_n = a_1 x_{n-1} + \cdots + a_d x_{n-d}$ *where* $a_1, \ldots, a_d$ *and* $x_1, \ldots, x_d$ *are rational, then* $\{n \in \mathbb{N} : x_n = 0\}$ *can be written as* $F \sqcup P$*, where* F *is finite and* P *is periodic.*

Theorem (Skolem)

If $(x_n : n \in \mathbb{N})$ is defined by $x_n = a_1 x_{n-1} + \cdots + a_d x_{n-d}$ where $a_1, \ldots, a_d$ and $x_1, \ldots, x_d$ are rational, then $\{n \in \mathbb{N} : x_n = 0\}$ can be written as $F \sqcup P$, where F is finite and P is periodic.

This can be generalized to any field of characteristic zero.

All known proofs use p-adic numbers in some way, and all of them are *ineffective*, i.e., do not provide a bound on $\max F$; there do exist bounds on $|F|$.

Theorem (Skolem)

If $(x_n : n \in \mathbb{N})$ is defined by $x_n = a_1 x_{n-1} + \cdots + a_d x_{n-d}$ where $a_1, \ldots, a_d$ and $x_1, \ldots, x_d$ are rational, then $\{n \in \mathbb{N} : x_n = 0\}$ can be written as $F \sqcup P$, where F is finite and P is periodic.

This can be generalized to any field of characteristic zero.

All known proofs use p-adic numbers in some way, and all of them are *ineffective*, i.e., do not provide a bound on $\max F$; there do exist bounds on $|F|$.

Question

Is there an algorithm that decides whether a given linear recurrence sequence has any zero?

Thoralf Albert Skolem (23 May 1887 – 23 March 1963) was a Norwegian mathematician. He was both an early contributor to and critic of set theory. He also published papers on Diophantine equations, group theory and lattice theory.

He is known for the discovery of "Skolem's paradox", that the notion of countability is not absolute: a set which is uncountable from the viewpoint of a universe V may well be countable in a larger universe W.

p-adic number

p-adic numbers arise naturally in solving Diophantine equations.

Does $x^3 - 8y^3 = 12$ have integer solution?

p-adic number

p-adic numbers arise naturally in solving Diophantine equations.

Does $x^3 - 8y^3 = 12$ have integer solution?

No: if (x, y) is a solution then x must be even, but $8 \nmid 12$. This shows the equation doesn't even have a solution in $\mathbb{Z}/8\mathbb{Z}$.

p-adic number

p-adic numbers arise naturally in solving Diophantine equations.

Does $x^3 - 8y^3 = 12$ have integer solution?

No: if (x, y) is a solution then x must be even, but $8 \nmid 12$. This shows the equation doesn't even have a solution in $\mathbb{Z}/8\mathbb{Z}$.

What if mod 8 doesn't settle it? We may try $16, 32, 64 \ldots$

p-adic number

p-adic numbers arise naturally in solving Diophantine equations.

Does $x^3 - 8y^3 = 12$ have integer solution?

No: if (x, y) is a solution then x must be even, but $8 \nmid 12$. This shows the equation doesn't even have a solution in $\mathbb{Z}/8\mathbb{Z}$.

What if mod 8 doesn't settle it? We may try $16, 32, 64 \ldots$ If an equation has a solution modulo *every* 2^n, then turns out it has a solution in 2-adic numbers.

p-adic number

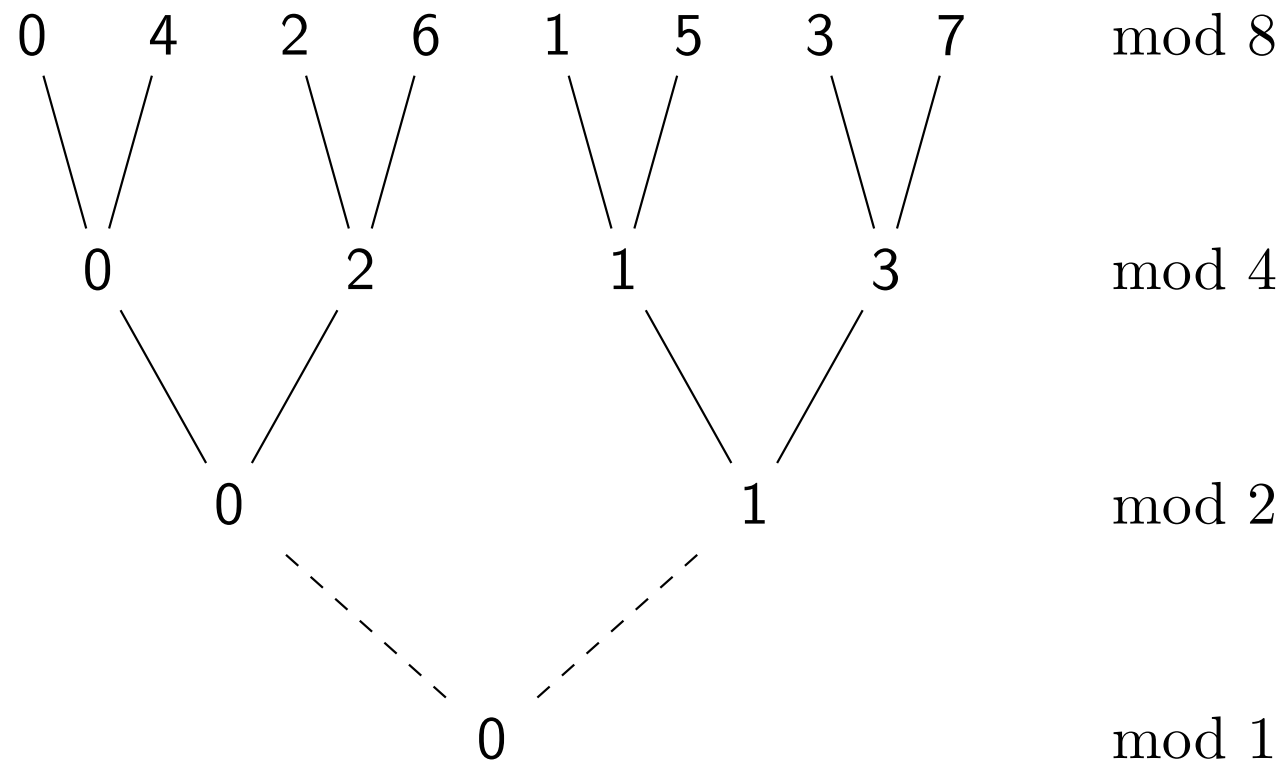
Abbreviate $\mathbb{Z}/n\mathbb{Z}$ as $\mathbb{Z}/n$. For a prime p, the ring $\mathbb{Z}_p$ of *p-adic integers* is the inverse limit of the following sequence:

$$\cdots \to \mathbb{Z}/p^4 \to \mathbb{Z}/p^3 \to \mathbb{Z}/p^2 \to \mathbb{Z}/p \dashrightarrow 0$$

Where $\mathbb{Z}/p^{n+1} \to \mathbb{Z}/p^n$ is the natural quotient map.

In other words, $\mathbb{Z}_p$ is a subring of $\prod_{n=1}^{\infty} \mathbb{Z}/p^n$; it consists of all sequences $(\ldots, a_3, a_2, a_1)$ such that $a_n \in \{0, 1, \ldots, p^n - 1\}$ and $a_{n+1} = a_n \mod p^n$.

p-adic number



A 2-adic integer is a branch through this tree, such as $(\ldots, 3, 3, 1)$.

Basic properties of $\mathbb{Z}_p$

The multiplicative unit of $\mathbb{Z}_p$ is $\bar{1} = (\ldots, 1, 1, 1)$. Clearly any multiple of it is nonzero, so $\operatorname{char} \mathbb{Z}_p = 0$.

If $x = (\ldots, a_3, a_2, a_1)$ where $a_1 \neq 0 \mod p$ then x is a unit, because $a \in \mathbb{Z}/p^n$ is a unit iff $p \nmid a$, so inductively a_n is a unit in $\mathbb{Z}/p^n$ with inverse b_n; can check that $(\ldots, b_3, b_2, b_1) \in \mathbb{Z}_p$.

In particular, $\bar{n} = \underbrace{(\ldots, 1, 1, 1) + \cdots + (\ldots, 1, 1, 1)}_{n \text{ times}}$ is a unit whenever $p \nmid n$.

$\mathbb{Z}_p \simeq \{0, 1, \ldots, p-1\}^{\mathbb{N}}$ is a compact metric space.

Basic properties of $\mathbb{Z}_p$

Let $\mathfrak{m}$ be the set of sequences with $a_1 = 0 \mod p$. This is the unique maximal ideal of $\mathbb{Z}_p$; it is generated by $\bar{p} = (\ldots, p, p, 0)$.

If $x = (\ldots, a_3, a_2, a_1)$, then $x \in \mathfrak{m}^n$ iff $a_1, \ldots, a_n$ are zero.

Every nonzero $x \in \mathbb{Z}_p$ can be expressed as $\bar{p}^n u$ for some n and some unit u. Say $x = (\ldots, 44, 12, 12, 4, 0, 0) \in \mathbb{Z}_2$, then

$$x = (\ldots, 4, 4, 4, 4, 0, 0) \cdot (\ldots, 11, 3, 3, 1) = \bar{2}^2 \cdot (\ldots, 11, 3, 3, 1)$$

It follows that $\mathbb{Z}_p$ is an integral domain.

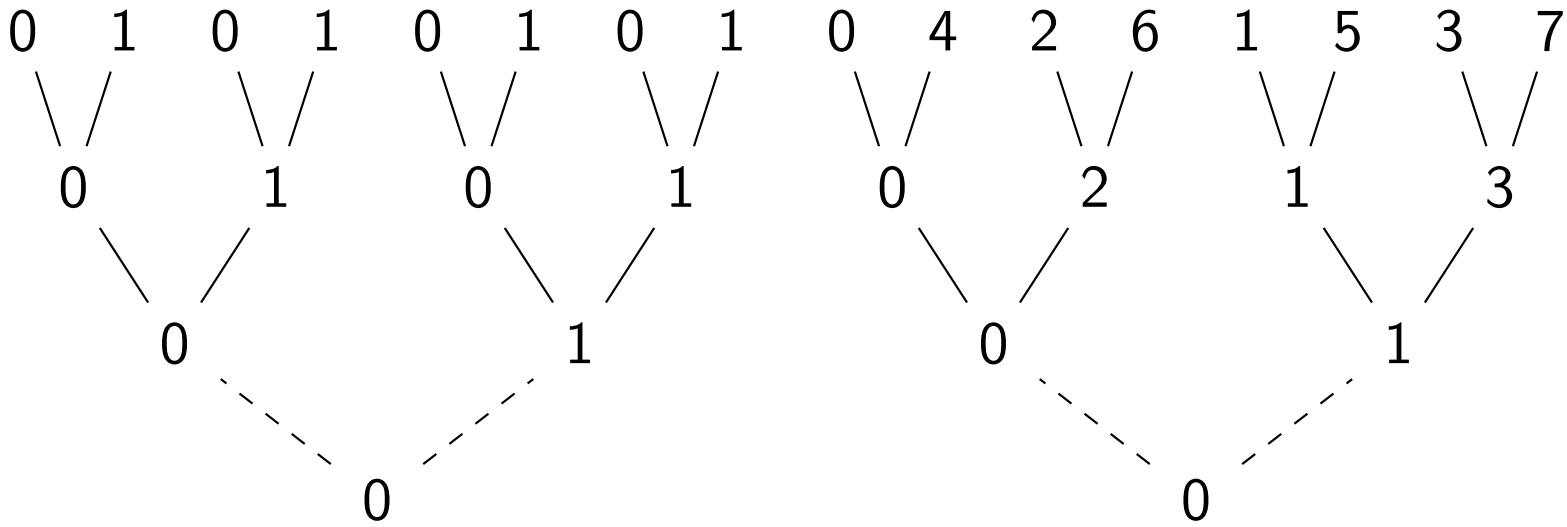
Basic properties of $\mathbb{Z}_p$

$\sum_{n=0}^{\infty} p^n x_n$ is well-defined for any sequence $(x_n)_n \subseteq \mathbb{Z}_p$.

$$
\begin{array}{cccccc}
 & (\ldots & a_4 & a_3 & a_2 & a_1) \\
 & (\ldots & b_4 & b_3 & b_2 & 0) \\
 & (\ldots & c_4 & c_3 & 0 & 0) \\
+ & (\ldots & \vdots & \vdots & \vdots & \vdots \\
\hline
 & (\ldots & \ldots & a_3+b_3+c_3 & a_2+b_2 & a_1)
\end{array}
$$

Slightly more generally, $\sum_{n=0}^{\infty} p^{s(n)} x_n$ is well-defined if $s(n) \to \infty$.

Another representation of p-adic number



The sequence $(\ldots, 0, 1, 1)$ corresponds to $(\ldots, 3, 3, 1)$ in the inverse limit notation. It is also written as

$1 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + \cdots$

In this representation, addition is as in base 2 except that we can "carry forever". E.g., $(\ldots, 1, 1, 1) + (\ldots, 0, 0, 1) = (\ldots, 1, 1, 2) = (\ldots, 1, 2, 0) = (\ldots, 2, 0, 0) = \cdots = 0$.

Step one: linear algebra

We begin the proof of Skolem's theorem. Suppose we have the linear recurrence relation

$$x_n = a_1 x_{n-1} + \cdots + a_d x_{n-d},$$

where $a_1, \ldots, a_d, x_1 \ldots, x_d \in \mathbb{Q}$. WLOG $a_d \neq 0$. We may actually assume these to be integers:

$$\begin{aligned} x_n M^n &= a_1 x_{n-1} M^n + \cdots + a_d x_{n-d} M^n \\ x_n M^n &= a_1 M(x_{n-1} M^{n-1}) + \cdots + a_d M^d (x_{n-d} M^{n-d}) \\ y_n &= b_1 y_{n-1} + \cdots + b_d y_{n-d} \end{aligned}$$

Step one: linear algebra

$$\begin{pmatrix} x_n \\ x_{n-1} \\ \vdots \\ x_{n-d+2} \\ x_{n-d+1} \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \cdots & a_{d-1} & a_d \\ 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \end{pmatrix} \begin{pmatrix} x_{n-1} \\ x_{n-2} \\ \vdots \\ x_{n-d+1} \\ x_{n-d} \end{pmatrix}$$

If we let $\mathbf{x}_n = (x_{n+d-1}, \ldots, x_n)^T$ and A be the integer matrix, then $\mathbf{x}_{n+1} = A\mathbf{x}_n$ and $\mathbf{x}_n = A^{n-1}\mathbf{x}_1$. Consequently x_n is the last entry of $A^{n-1}\mathbf{x}_1$.

Step one: linear algebra

Fix a prime $p > \max\{2, |A|\}$, so $A \mod p$ is invertible. Thus A is a unit in the ring $M_k(\mathbb{F}_p)$. There exists m s.t. $A^m = I + pB$ for some integer matrix B. This m will be the period.

It suffices to show that for every $1 \leq r \leq m$, if $\{n \in \mathbb{N} : x_{r+nm} = 0\}$ is infinite then it is equal to $\mathbb{N}$.

$x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, \ldots$

x_{r+nm} is the last entry of $A^{r+nm-1}\mathbf{x}_1$. If we let $u = (0, \ldots, 0, 1)^T$ and $v = A^{r-1}\mathbf{x}_1$ then $x_{r+nm} = \langle u, A^{nm}v \rangle = \langle u, (I + pB)^n v \rangle$.

It suffices to show that for any map of the below form, if it has infinitely many zeros then it is identically zero:

$f : \mathbb{N} \to \mathbb{N},\ n \mapsto \langle u, (I + pB)^n v \rangle$

Step two: analytic extension

$f : \mathbb{N} \to \mathbb{N},\ n \mapsto \langle u, (I + pB)^n v \rangle$

Turns out this extends to an *analytic function* $f : \mathbb{Z}_p \to \mathbb{Z}_p$.

If a (p-adic) analytic function on a compact set ($\mathbb{Z}_p$) has infinitely many zeros then it is identically zero, so we are done.

Step two: analytic extension

$f : \mathbb{N} \to \mathbb{N},\ n \mapsto \langle u, (I + pB)^n v \rangle$

Turns out this extends to an *analytic function* $f : \mathbb{Z}_p \to \mathbb{Z}_p$.

If a (p-adic) analytic function on a compact set ($\mathbb{Z}_p$) has infinitely many zeros then it is identically zero, so we are done. We will prove this from scratch.

Step two: analytic extension

By binomial formula,

$$(I + pB)^n = \sum_{k=0}^{n} \binom{n}{k} p^k B^k = \sum_{k=0}^{\infty} \binom{n}{k} p^k B^k$$

where $\binom{n}{k} = \dfrac{n(n-1)\cdots(n-k+1)}{k!} = \dfrac{(n)_k}{k!}$ is zero if $k > n$.

We can certainly extend $(n)_k$ to a polynomial on $\mathbb{Z}_p$:

$$(x)_k = x(x-1)\cdots(x-k+1)$$

The main point is to show $p^k/k!$ is in $\mathbb{Z}_p$, and it's "small" so that the sum converges.

Step two: analytic extension

The number of times that p divides $k!$ is

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

Recall that any (rational) integer not divisible by p is a unit in $\mathbb{Z}_p$.

Since $p \geq 3$, we can write $\dfrac{p^k}{k!} = p^{s(k)} u_k$ where u_k is a unit and $s(k) \to \infty$.

Step two: analytic extension

$(I+pB)^n = \sum_{k=0}^{\infty} \frac{p^k}{k!}(n)_k B^k = \sum_{k=0}^{\infty} p^{s(k)} u_k \cdot (n)_k \cdot B^k$; the last expression extends to $\mathbb{Z}_p$. Therefore,

$$f : \mathbb{N} \to \mathbb{N},\ n \mapsto \langle u, (I+pB)^n v\rangle = \sum_{k=0}^{\infty} p^{s(k)} u_k \cdot \langle u, B^k v\rangle \cdot (n)_k$$

can be extended to

$$f : \mathbb{Z}_p \to \mathbb{Z}_p,\ x \mapsto \sum_{k=0}^{\infty} p^{s(k)} u_k \cdot \langle u, B^k v\rangle \cdot (x)_k.$$

Step two: analytic extension

$$f : \mathbb{Z}_p \to \mathbb{Z}_p,\ x \mapsto \sum_{k=0}^{\infty} p^{s(k)} u_k \cdot \langle u, B^k v \rangle \cdot (x)_k.$$

f is of the form $\sum_{k=0}^{\infty} p^k f_k$ where each $f_k : \mathbb{Z}_p \to \mathbb{Z}_p$ is a polynomial. Let's call such a function f *analytic*.

It remains to show that if an analytic function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ has infinitely many zeros $x_1, x_2, x_3, \ldots$ then it is identically zero.

Step three: zeros of analytic functions

It remains to show that if an analytic function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ has infinitely many zeros $x_1, x_2, x_3, \ldots$ then it is identically zero.

First note that little Bézout holds for analytic functions: if $f = \sum_{k=0}^{\infty} p^k f_k$ and $f(x_1) = 0$, then there exists an analytic function g such that $f = (x - x_1)g$. Write $f_k = (x - x_1)g_k + c_k$ where $c_k \in \mathbb{Z}_p$; let $g = \sum_{k=0}^{\infty} p^k g_k$ and $c = \sum_{k=0}^{\infty} p^k c_k$; then $f = (x - x_1)g + c$, so $c = 0$.

Step three: zeros of analytic functions

It remains to show that if an analytic function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ has infinitely many zeros $x_1, x_2, x_3, \ldots$ then it is identically zero.

There are two cases:

(i) $\deg f_0 > 0$, then applying little Bézout we get $f = (x - x_1)g$, where g must satisfy $\deg g_0 < \deg f_0$.

(ii) $\deg f_0 = 0$, then $p \mid f_0$, otherwise $f = f_0 + p \cdot \sum_{k=1}^{\infty} p^{k-1} f_k$ cannot have zero; it follows that $f = p \cdot f'$ for some f'.

Step three: zeros of analytic functions

It remains to show that if an analytic function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ has infinitely many zeros $x_1, x_2, x_3, \ldots$ then it is identically zero.

There are two cases:

(i) $\deg f_0 > 0$, then applying little Bézout we get $f = (x - x_1)g$, where g must satisfy $\deg g_0 < \deg f_0$.

(ii) $\deg f_0 = 0$, then $p \mid f_0$, otherwise $f = f_0 + p \cdot \sum_{k=1}^{\infty} p^{k-1} f_k$ cannot have zero; it follows that $f = p \cdot f'$ for some f'.

In case (i), write $g = (x - x_2)h$, so that either $\deg g_0 = 0$ or $\deg h_0 < \deg g_0 < \deg f_0$, etc. After finitely many steps we must run into case (ii), i.e., $f = (x - x_1) \cdots (x - x_s) \cdot p \cdot f'$ for some f'.

Step three: zeros of analytic functions

What we have proved: if an analytic function f has infinitely many zeros, then $f = p \cdot f'$ for some analytic f'.

Step three: zeros of analytic functions

What we have proved: if an analytic function f has infinitely many zeros, then $f = p \cdot f'$ for some analytic f'.

f' still has infinitely many zeros. By induction we can factor out arbitrarily many p, so $p^n \mid f(x)$ for any $x \in \mathbb{Z}_p$ and $n \in \mathbb{N}$. Then $f(x)$ must be zero, since $p^n \mid f(x)$ iff $f(x) \in \mathfrak{m}^n$ iff the last n digits of $f(x)$ are all zero.

This finishes the proof of Skolem's Theorem.

Theorem (Skolem-Mahler-Lech)

Let k be a field of characteristic zero. If $(x_n : n \in \mathbb{N})$ is defined by $x_n = a_1 x_{n-1} + \cdots + a_d x_{n-d}$ where $a_1, \ldots, a_d, x_1, \ldots, x_d \in k$, then $\{n \in \mathbb{N} : x_n = 0\}$ can be written as $F \sqcup P$, where F is finite and P is periodic.

Mahler proved the case of algebraic numbers, and Lech proved the general case.

We found an (explicit) m such that if we partition $\mathbb{N}$ into m arithmetic progressions, each of them either (i) has finitely many zeros, or (ii) is identically zero.

By some more difficult argument, there is a bound on the number of zeros in case (i), but currently there is no bound on the maximal size of those zeros. There's not even known algorithm to decide whether the zero set is nonempty. It is known that this is NP-hard.

SML is generalized by Chabauty theorem, which in turn is a special case of Falting's theorem (Mordell conjecture). Both of then, like SML, give effective bounds on number of zeros, but not their sizes.

Reference


Blog post by Terence Tao,
https://terrytao.wordpress.com/2007/05/25/
open-question-effective-skolem-mahler-lech-theorem/