Federico Accossato

Who's this person??

Recurrence, Transcendence, and Diophantine Approximation

Leiden, 14th July 2025

ME, BRIEFLY

- Federico Accossato
- Politecnico di Torino, Italy
- 3rd year PhD Student

(currently looking for a job :))

ME, BRIEFLY

- Federico Accossato
- Politecnico di Torino, Italy
- 3rd year PhD Student

  (currently looking for a job ☺)

- Interests:
  - Linear recurrences
  - Continued Fractions
  - Transcendence
  - Diophantine Approximation

RESEARCH INTERESTS AND COLLABORATIONS

- The arithmetic of linear recurrences

  ↳ "On the number of residues of certain second-order linear recurrences", 2024 (with Carlo SANNA)

RESEARCH INTERESTS AND COLLABORATIONS

- The arithmetic of linear recurrences

→ "On the number of residues of certain second-order linear recurrences", 2024 (with Carlo SANNA)

↓

- The distribution of sequences modulo 1

RESEARCH INTERESTS AND COLLABORATIONS

- Continued fractions & transcendence

↳ "Transcendence criteria for MULTIDIMENSIONAL continued fractions", 2025 (with Nadir MURRU and Giuliano ROMEO)

↓

Several open questions are still on our WISHLIST!

(Collaborations are welcome!)

RESEARCH INTERESTS AND COLLABORATIONS

- Diophantine Approximation

  ↳ Approximation of real numbers by algebraic INTEGERS

  (with Yann BUGEAUD)

RESEARCH INTERESTS AND COLLABORATIONS

- Diophantine Approximation

  ↪ Approximation of real numbers by algebraic INTEGERS

  (with Yann BUGEAUD)

WORK IN PROGRESS

Thank you! :)

federico.accossato@polito.it

https://sites.google.com/view/federico-accossato

A Brief Self–Introduction

Faustin ADICEAM

Recurrence, Transcendance and Diophantine Approximation
Leiden

14/07/2025

- Faustin ADICEAM;
- PhD in 2015 from Maynooth University (Ireland) in Number Theory;
- Junior Professor (tenure–track professorship);
- Université Paris-Est Créteil (France).
- Previous positions : University of York (UK), University of Waterloo (Canada) and University of Manchester (UK).

- Research Interests :
  - Metric, Analytic and Probabilistic Number Theory;
  - Discret and Convex Geometry (visibility problems);
  - Information Theory;
  - Mathematical Theory of Quasicrystals;
  - Combinatorics;
  - Transcendance Theory;
  - Probability Theory (recently).

Speed talk

Attila Bérczes

University of Debrecen

Leiden, 2025.

Attila Bérczes

1996: Degree in mathematics (BSc+MSc)

- Lajos Kossuth University (Debrecen)
- two semesters abroad (Paderborn, Trento)

2001: PhD in mathematics

- University of Debrecen
- **title:** "Some new diophantine results on decomposable polynomial equations and irreducible polynomials"
- **supervisor:** Kálmán Győry

2009: Habilitation

- University of Debrecen
- **title:** "New results in the theory of Diophantine equations" (in Hungarian)

2017: Doctor of the Hungarian Academy of Sciences

- **title:** "Effective results for Diophantine problems over finitely generated domains."

Research interest

Diophantine equations

- finiteness of the solutionset
- estimates for the number of solutions
- effective finiteness results
- complete solution of Diophantine equations

Recurrence sequences

- Diophantine properties of recurrence sequences
- Diophantine equations containing recurrence sequences
- application of recurrences in solution of Diophantine problems

Polynomials

- irreducibility of polynomials
- Diophantine properties of polynomials

Most important results

- Let A be an integral domain of characteristic 0 that is finitely generated over $\mathbb{Z}$.
- Let K denote the quotient field of A.
- Let $F \in A[X, Y]$ be a non-constant polynomial such that F **is not divisible by** any non-constant polynomial of the form

$$X^m Y^n - \alpha \quad \text{or} \quad X^m - \alpha Y^n, \text{where } m, n \in \mathbb{Z}_{\geq 0} \text{ and } \alpha \in \overline{K}^*.$$

- Let Γ be a finitely generated subgroup of K^*
- Denote by $\overline{\Gamma}$ the division group of Γ

Theorem – Effective version of the Lang and Liardet Theorems

All elements (x, y) of the set

$$\mathcal{C} := \{(x, y) \in (A^*)^2 \mid F(x, y) = 0\} \tag{1}$$

and

$$\mathcal{C} := \{(x, y) \in (\overline{\Gamma})^2 \mid F(x, y) = 0\}. \tag{2}$$

are effectively bounded.

Thank you for your attention!

INSTITUT DE RECHERCHE EN INFORMATIQUE FONDAMENTALE

Université Paris Cité

V. Berthé

Recurrence, transcendence, and Diophantine approximation

Funded by the European Union
European Research Council
Established by the European Commission

The project DynaMiCs Berthé-Luca-Ouaknine

Automata & Logic MSO $< \mathbb{N}; <, P_{u_n} >$

Products of matrices $M_{u_0} \cdots M_{u_n}$

Linear recurrences $u_{n+1} = u_n + u_{n-1}$

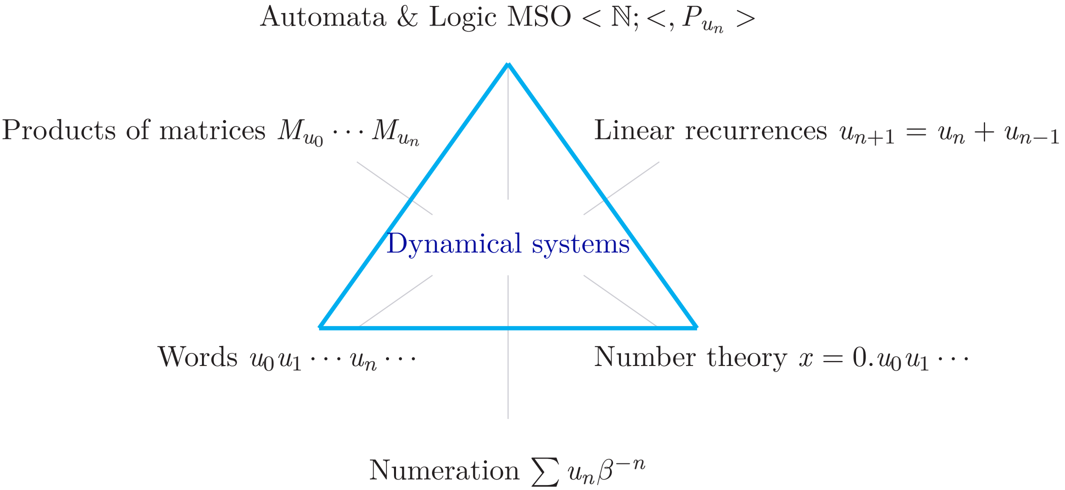
Dynamical systems & Codings of trajectories $(u_n)_n$

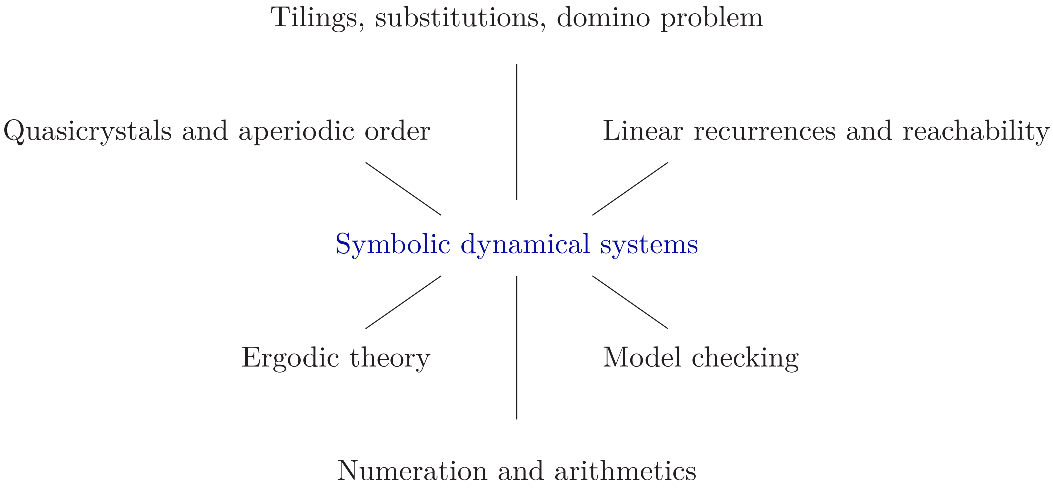
Words $u_0 u_1 \cdots u_n \cdots$

Number theory $x = 0.u_0 u_1 \cdots$

Numeration $\sum u_n \beta^{-n}$

The project DynaMiCs Berthé-Luca-Ouaknine





Tilings, substitutions, domino problem
Quasicrystals and aperiodic order
Linear recurrences and reachability
Symbolic dynamical systems
Ergodic theory
Model checking
Numeration and arithmetics

Name: Cristiana Bertolin

Citizenship: italian

Education:
M.Sc.: Università di Padova (with B. Dwork)
Ph.D.: Université Paris VI (with Y, André)
Habilitation: ETH Zürich

Current university affiliation: Math Department, University of Padua, Italy

objects I work with

I work with the following objects

- $\mathcal{E}/\mathbb{C}$ elliptic curves $\mathbb{C}$,
- products $\mathbb{G}_m \times \mathcal{E}$ over $\mathbb{C}$
- extensions $0 \to \mathbb{G}_m \to G \to \mathcal{E} \to 0$ over $\mathbb{C}$
- 1-motives $[u : \mathbb{Z} \to G], u(1) = R \in G(\mathbb{C})$

We can consider these objects over an arbitrary scheme S: abelian S-schemes, 1-motives over S,...

1-motives can be seen as length 1 complexes of abelian sheaves

1-motives define (mixed) motives in any tannakian category of motives (Voedodsky, Nori, Ayoub,...)

(1) Transcendance

Grothendieck-André Period Conjecture

If M is a motive defined over $K \subseteq \mathbb{C}$ then

$$\mathrm{transc.deg}_{\mathbb{Q}}\, K(\mathrm{periods}(M)) \geqslant \dim \mathrm{Gal}_{mot}(M)$$

For 1-motives, I make this conjecture explicit

I show that for adequate 1-motives it is equivalent to well-known conjectures as Schanuel Conjecture

(2) Cohomologies Groups

For 1-motives, I have studied and I still studying

- homomorphisms $\mathrm{Hom} = \mathrm{Ext}^0$
- extensions Ext^1
- biextensions Biext^1 (a biext. de (P, Q) par G is an ext. of Q_P by G_P and an ext. of P_Q by G_Q)
- line bundles $\mathrm{Pic} = \mathrm{H}^1(-, \mathbb{G}_m)$
- gerbes $\mathrm{H}^2(-, \mathbb{G}_m)$ (fibred categories loc. not empty and 2 objects in a fibre are loc. isomorphics.)

(3) Stack language

A Picard stack is a fibred category endowed with a group law (exemple: Extensions with Baer sum)

length 1 complexes $[K^{-1} \to K^0]$ define Picard stacks
In particular, 1-motives $M = [\mathbb{Z} \to G]$ define Picard stacks

A Picard 2-stack is a fibred 2-category endowed with a group law

length 2 complexes $[K^{-2} \to K^{-1} \to K^0]$ define Picard 2-stacks

For Picard (2)-stacks I have studied

- extensions Ext^1
- biextensions Biext^1
- torsors

Introduction

- Frits Beukers
- Emeritus professor
- University of Utrecht (NL)

Start

Let p be an odd prime and consider the polynomial

$$F_m(t) := \sum_{k=0}^{m-1} \binom{2k}{k} t^k,$$

the m-truncation of

$$\sum_{k=0}^{\infty} \binom{2k}{k} t^k = \frac{1}{\sqrt{1-4t}}.$$

Start

Let p be an odd prime and consider the polynomial

$$F_m(t) := \sum_{k=0}^{m-1} \binom{2k}{k} t^k,$$

the m-truncation of

$$\sum_{k=0}^{\infty} \binom{2k}{k} t^k = \frac{1}{\sqrt{1-4t}}.$$

A simple congruence

For any $a \in \mathbb{Q}$ we have

$$F_p(a) \equiv \left(\frac{1-4a}{p}\right) \pmod{p}.$$

Run

For special $a = 1, 1/2, 1/3$ the congruence holds mod p^2, e.g.

Supercongruence

$$F_p(1) = \sum_{k=0}^{p-1} \binom{2k}{k} \equiv \left(\frac{-3}{p}\right) \pmod{p^2}.$$

Finish

Dwork congruences

For any $a \in \mathbb{Q}$ and $r \geq 1$,

$$F_{p^r}(a) \equiv \left(\frac{1-4a}{p}\right) F_{p^{r-1}}(a) \pmod{p^r}.$$

Finish

Dwork congruences

For any $a \in \mathbb{Q}$ and $r \geq 1$,

$$F_{p^r}(a) \equiv \left(\frac{1-4a}{p}\right) F_{p^{r-1}}(a) (\mathrm{mod}\ p^r).$$

For the special a we expect congruences mod p^{2r}, e.g.

Conjecture

For any $r \geq 1$,

$$F_{p^r}(1) \equiv \left(\frac{-3}{p}\right) F_{p^{r-1}}(1) (\mathrm{mod}\ p^{2r}).$$

Finish

Dwork congruences

For any $a \in \mathbb{Q}$ and $r \geq 1$,

$$F_{p^r}(a) \equiv \left(\frac{1-4a}{p}\right) F_{p^{r-1}}(a) \pmod{p^r}.$$

For the special a we expect congruences mod p^{2r}, e.g.

Conjecture

For any $r \geq 1$,

$$F_{p^r}(1) \equiv \left(\frac{-3}{p}\right) F_{p^{r-1}}(1) \pmod{p^{2r}}.$$

Thank you

Alin Bostan

Recurrence, transcendence & Diophantine approximation

Lorentz Center, Leiden, Netherlands

Introduction

Research areas:

- Computer algebra and experimental mathematics
- Applications to combinatorics and number theory

Keywords:

- Algebraic algorithms and their complexity
- Computational mathematics
- Functional equations
- D-finite functions
- Algebraicity/transcendence

Computational paradigms:

- Guess-and-Prove (via Hermite-Padé approximants)
- Creative Telescoping

Two questions of interest

How to *decide*, both in theory and (especially!) in practice:

1. if one (or several) univariate (or multivariate) power series are *transcendental* / *algebraically (in)dependent*?
   $\longrightarrow$ more on Wednesday morning

2. if a given (P-)recursive sequence has (almost) *integral terms*?
   $\longrightarrow$ open problem

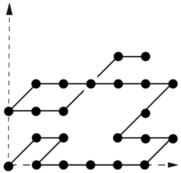
   (Related question: compute the *Eisenstein constant* of a given algebraic function.)

Example: Guess-and-Prove for Gessel walks

- $g(i,j,n)$ = number of n-steps $\{\nearrow, \swarrow, \leftarrow, \rightarrow\}$-walks in $\mathbb{N}^2$ from $(0,0)$ to (i,j)

▷ **Question**: What is the nature of the generating function

$$G(x,y,t) = \sum_{i,j,n=0}^{\infty} g(i,j,n)\, x^i y^j t^n \ ?$$

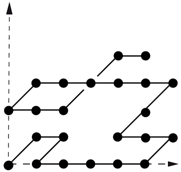


Example: Guess-and-Prove for Gessel walks

- $g(i,j,n)$ = number of n-steps $\{\nearrow, \swarrow, \leftarrow, \rightarrow\}$-walks in $\mathbb{N}^2$ from $(0,0)$ to (i,j)

▷ **Question**: What is the nature of the generating function

$$G(x,y,t) = \sum_{i,j,n=0}^{\infty} g(i,j,n)\, x^i y^j t^n \text{ ?}$$



▷ **Algebraic reformulation**: Solve the functional equation

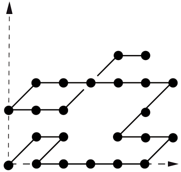
$$\begin{aligned} G(x,y,t) = {} & 1 + t\left(xy + x + \frac{1}{xy} + \frac{1}{x}\right) G(x,y,t) \\ & - t\left(\frac{1}{x} + \frac{1}{x}\frac{1}{y}\right) G(0,y,t) - t\,\frac{1}{xy}\Big(G(x,0,t) - G(0,0,t)\Big) \end{aligned}$$

Example: Guess-and-Prove for Gessel walks

- $g(i,j,n)$ = number of n-steps $\{\nearrow, \swarrow, \leftarrow, \rightarrow\}$-walks in $\mathbb{N}^2$ from $(0,0)$ to (i,j)

▷ **Question**: What is the nature of the generating function

$$G(x,y,t) = \sum_{i,j,n=0}^{\infty} g(i,j,n)\, x^i y^j t^n \ ?$$



Answer: [B., Kauers, 2010] $G(x,y,t)$ is an algebraic function†.

▷ **Approach**: ⟶ very general and robust!

1. Generate data: compute $G(x,y,t)$ to precision t^{1200} (≈ 1.5 billion coeffs!)
2. Guess: conjecture polynomial equations for $G(x,0,t)$ and $G(0,y,t)$ (degree 24 each, coeffs. of degree $(46,56)$, with 80-bit digits coeffs.)
3. Prove: multivariate resultants of (very big) polynomials (30 pages each)

† Minimal polynomial $P(G(x,y,t); x,y,t) = 0$ has $> 10^{11}$ terms; $\approx 30\,$Gb (6 DVDs!)

Speed Talks

- Sander Dahmen
- VU (Vrije Universiteit) Amsterdam

Effectively solve Diophantine problems, like

- Generalized Fermat equations

$$x^p + y^q = z^r \qquad x, y, z \in \mathbb{Z},\ \gcd(x, y, z) = 1$$

- Finding perfect powers in recurrence sequences, e.g. elliptic divisibility sequences

Developing/using

- Modular methods: Frey (hyper)elliptic curves, (classical/Hilbert/..) modular forms, Galois representations
- Rational points on curves: e.g. Chabauty methods
- More 'classical'methods: e.g. number field enumerations

Formalization: (mostly) proof assistant *Lean*

Name: Robin de Jong

Name: Robin de Jong

Affiliation: Leiden University

Name: Robin de Jong

Affiliation: Leiden University

Research interests: arithmetic and analytic aspects of curves, abelian varieties and their moduli spaces

Name: Robin de Jong

Affiliation: Leiden University

Research interests: arithmetic and analytic aspects of curves, abelian varieties and their moduli spaces

Keywords: local and global heights; arithmetic intersection theory

My **favorite theorem proven** is an effective version of the Bogomolov conjecture about the existence of “small points” on curves in their Jacobians (J. Alg. Geom 2018).

My **favorite theorem proven** is an effective version of the Bogomolov conjecture about the existence of “small points” on curves in their Jacobians (J. Alg. Geom 2018).

The idea of the proof was recently used by Xinyi Yuan to show a uniform version of the Bogomolov conjecture (Ann. of Math. 2025).

My **favorite theorem proven** is an effective version of the Bogomolov conjecture about the existence of "small points" on curves in their Jacobians (J. Alg. Geom 2018).

The idea of the proof was recently used by Xinyi Yuan to show a uniform version of the Bogomolov conjecture (Ann. of Math. 2025).

Theorem:

My **favorite theorem proven** is an effective version of the Bogomolov conjecture about the existence of “small points” on curves in their Jacobians (J. Alg. Geom 2018).

The idea of the proof was recently used by Xinyi Yuan to show a uniform version of the Bogomolov conjecture (Ann. of Math. 2025).

Theorem: *Let X be a smooth projective geometrically connected curve of genus $g \geq 2$ with semistable reduction over a number field K.*

My **favorite theorem proven** is an effective version of the Bogomolov conjecture about the existence of "small points" on curves in their Jacobians (J. Alg. Geom 2018).

The idea of the proof was recently used by Xinyi Yuan to show a uniform version of the Bogomolov conjecture (Ann. of Math. 2025).

Theorem: *Let X be a smooth projective geometrically connected curve of genus $g \geq 2$ with semistable reduction over a number field K. Let Z be the image of X in its Jacobian J under an Abel–Jacobi map.*

My **favorite theorem proven** is an effective version of the Bogomolov conjecture about the existence of "small points" on curves in their Jacobians (J. Alg. Geom 2018).

The idea of the proof was recently used by Xinyi Yuan to show a uniform version of the Bogomolov conjecture (Ann. of Math. 2025).

Theorem: *Let X be a smooth projective geometrically connected curve of genus $g \geq 2$ with semistable reduction over a number field K. Let Z be the image of X in its Jacobian J under an Abel–Jacobi map. Then the inequalities*

$$\liminf_{z \in Z(\overline{K})} \mathrm{h}_J(z) \geq \frac{1}{[K:\mathbb{Q}]} \frac{1}{4(g-1)(3g-1)} \sum_{v \in M(K)} \varphi(X_v) \log Nv > 0$$

hold.

Now, to connect with the secret main theme of this workshop,

Now, to connect with the secret main theme of this workshop,

my **first theorem proven** was very kindly referred to by Jan-Hendrik in his paper "On the norm form inequality $|F(\mathsf{x})| \leq h$" (Publ. Math. Debrecen 2000).

Now, to connect with the secret main theme of this workshop,

my **first theorem proven** was very kindly referred to by Jan-Hendrik in his paper "On the norm form inequality $|F(x)| \leq h$" (Publ. Math. Debrecen 2000).

It was obtained in my master thesis written under his supervision.

Speed talk

Jan-Hendrik Evertse
Universiteit Leiden

Recurrence, Transcendence, and Diophantine Approximation,
Lorentz Center, Leiden, July 15, 2025

Number of solutions

Much of my research deals with deriving uniform upper bounds for the number of solutions of Diophantine equations from certain infinite classes, using techniques from Diophantine approximation.

Number of solutions

Much of my research deals with deriving uniform upper bounds for the number of solutions of Diophantine equations from certain infinite classes, using techniques from Diophantine approximation.

To give an example, let $q \in \mathbb{C}^*$ and let Γ be a finitely generated multiplicative subgroup of $\mathbb{C}^*$ of rank r, i.e.,

$$\Gamma = \{\zeta \cdot \gamma_1^{z_1} \cdots \gamma_r^{z_r} : z_1, \dots, z_r \in \mathbb{Z}, \zeta \text{ root of unity}\}$$

where $\gamma_1, \dots, \gamma_r \in \mathbb{C}^*$ are multiplicatively independent, and consider

$$x_1 + \cdots + x_n = q \quad \text{in } x_1, \dots, x_n \in \Gamma. \tag{1}$$

Denote by $N_{n,\Gamma}(q)$ the number of *non-degenerate* solutions to (1), these are the solutions with $\sum_{i \in I} x_i \neq 0$ for each subset I of $\{1, \dots, n\}$.

Theorem (Schlickewei, Schmidt, E., 2002)

$N_{\Gamma,n}(q) \leq c(n)^{r+1}$.

Proof.

A.o. Quantitative Subspace Theorem □

Asymptotic results

Let $S = \{p_1, \ldots, p_r\}$ be a finite set of prime numbers and $\Gamma = U_S$ the *group of S-units*, i.e., $U_S = \{\pm p_1^{z_1} \cdots p_r^{z_r} : z_1, \ldots, z_r \in \mathbb{Z}\}$.
Define the height of $q = a/b \in \mathbb{Q}$, with $a, b \in \mathbb{Z},\ \gcd(a,b) = 1$ by $H(q) := \max(|a|, |b|)$.

From work of G.R. Everest (1990), which is the hard core, and recent refinements by Frei, Tichy and Ziegler, and Győry, Hajdu, Luca, Remete, and E., which is ongoing work, it follows that as $Q \to \infty$,

$$\sum_{q \in \mathbb{Q}^*,\, H(q) \leq Q} N_{n,U_S}(q) = c_{n,r}(\log Q)^{nr} + O((\log Q)^{nr-1}),$$

$$\#\{q \in \mathbb{Q}^* :\ H(q) \leq Q,\ N_{n,U_S}(q) > 0\} = \frac{c_{n,r}}{n!}(\log Q)^{nr} + O((\log Q)^{nr-1}).$$

Recall that $N_{n,\Gamma}(q)$ is the number of non-degenerate solutions to $x_1 + \cdots + x_n = q$ in $x_1, \ldots, x_n \in \Gamma$.

Asymptotic results

Let $S = \{p_1, \ldots, p_r\}$ be a finite set of prime numbers and $\Gamma = U_S$ the *group of S-units*, i.e., $U_S = \{\pm p_1^{z_1} \cdots p_r^{z_r} : z_1, \ldots, z_r \in \mathbb{Z}\}$.

Define the height of $q = a/b \in \mathbb{Q}$, with $a, b \in \mathbb{Z}$, $\gcd(a, b) = 1$ by $H(q) := \max(|a|, |b|)$.

From work of G.R. Everest (1990), which is the hard core, and recent refinements by Frei, Tichy and Ziegler, and Győry, Hajdu, Luca, Remete, and E., which is ongoing work, it follows that as $Q \to \infty$,

$$\sum_{q \in \mathbb{Q}^*,\, H(q) \leq Q} N_{n,U_S}(q) = c_{n,r} (\log Q)^{nr} + O((\log Q)^{nr-1}),$$

$$\#\{q \in \mathbb{Q}^* : H(q) \leq Q,\, N_{n,U_S}(q) > 0\} = \frac{c_{n,r}}{n!} (\log Q)^{nr} + O((\log Q)^{nr-1}).$$

Future perspectives:

- Generalization to arbitrary finitely generated subgroups Γ of $\mathbb{Q}^*$ or $\overline{\mathbb{Q}}^*$.

- Further extensions, e.g., to exponential polynomial equations $\sum_{i=1}^{n} p_i(z_1, \ldots, z_m) \alpha_{i,1}^{z_1} \cdots \alpha_{i,m}^{z_m} = q$, p_i polynomial.

Integer solutions of the generalised polynomial Pell equations

Akanksha Gupta
(joint work with Dr. Ekata Saha)

Department of Mathematics
Indian Institute of Technology Delhi, India

Recurrence, Transcendence and Diophantine Approximation (14th July, 2025)

Let R be an integral domain of characteristic 0. For non-constant, non-square $D(x) \in R[x]$, does the polynomial Pell equation

$$P(x)^2 - D(x)Q(x)^2 = n \tag{1}$$

have solutions $P, Q \in R[x]$ with Q non-zero, where $n \in \mathbb{Z} \setminus \{0\}$? If yes, we say D is Pellian over R with norm n. (If $n = 1$, we say D is Pellian over R)

How to decide if a given D is Pellian over R with norm n?

Open problem: Determine the set of polynomials D such that D is Pellian over $\mathbb{Z}$ with norm n.

Let $D = x^2 + ax + b$ be a non-square polynomial in $\mathbb{Z}[x]$ and $\Delta = a^2 - 4b$ be the discriminant of D.

Theorem (AG, E. Saha)

For $n \in \mathbb{N}$, we have:

- *If D is reducible in $\mathbb{Z}[x]$, then D is Pellian over $\mathbb{Z}$ with norm n^2 if and only if $\Delta | 4n^2$.*
- *If D is irreducible in $\mathbb{Z}[x]$, then D is Pellian over $\mathbb{Z}$ with norm n^2 if and only if $\Delta | 8n$.*

Theorem (AG, E. Saha)

Let n be a non-square integer, then D is Pellian over $\mathbb{Z}$ (resp. over $\mathbb{Q}$) with norm n if and only if $4n/\Delta$ is a square in $\mathbb{Z}$ (resp. in $\mathbb{Q}$).

Corollary

For a monic non-square quadratic polynomial $D \in \mathbb{Z}[x]$, the negative polynomial Pell equation

$$P^2 - DQ^2 = -1 \qquad (2)$$

has a non-trivial solution in $\mathbb{Z}[x]$ if and only if $D = (x+k)^2 + 1$ for some $k \in \mathbb{Z}$. Furthermore, this equation has non-trivial solutions in $\mathbb{Q}[x]$, if and only if $D = (x+k)^2 + r^2$ for $k \in \mathbb{Z}$ and $r \in \mathbb{N}$.

Characterisation for non-monic quadratic polynomials Pellian over $\mathbb{Z}$

- Goal: Classify all non monic quadratic polynomials that are Pellian over $\mathbb{Z}$.
- Difficulty: Solutions over $\mathbb{Z}$ are hard to find, let alone the minimal solutions. [By minimal solution, we mean the solution (P, Q) in $\mathbb{Z}[x]$, where $\deg P$ is the least.]

Theorem (AG, E. Saha)

For non-square $D = a^2x^2 + bx + c \in \mathbb{Z}[x]$ and $\Delta = b^2 - 4a^2c$, we have D is Pellian over $\mathbb{Z}$ if and only if

- $\Delta \mid \gcd(8a^4, 4b^2)$,
- *the p-adic valuation $v_p(a^4/\Delta) > 0$ for every odd prime p dividing a.*

Ongoing studies (AG, E. Saha):

- Other integral norms
- D of higher degrees

Speed Talk in Recurrence, Transcendence, and Diophantine Approximation

Sarthak Gupta

Supervisor: **Dr. Nora Györkös-Varga**

Number Theory Research Group

Department of Algebra and Number Theory

University of Debrecen

Research Interests

Erdős - Selfridge theorem states that the product of consecutive positive integers is never a perfect power i.e., the equation

$$x(x+1)(x+2)\cdots(x+k-1) = y^l$$

has no solutions in positive integers x, k, y, l with $k \geq 2$ and $l \geq 2$.

Research Interests

Erdős - Selfridge theorem states that the product of consecutive positive integers is never a perfect power i.e., the equation

$$x(x+1)(x+2)\cdots(x+k-1) = y^l$$

has no solutions in positive integers x, k, y, l with $k \geq 2$ and $l \geq 2$.

- Various generalizations of the above theorem.

Research Interests

Erdős - Selfridge theorem states that the product of consecutive positive integers is never a perfect power i.e., the equation

$$x(x+1)(x+2)\cdots(x+k-1) = y^l$$

has no solutions in positive integers x, k, y, l with $k \geq 2$ and $l \geq 2$.

- Various generalizations of the above theorem.
- Power values of various polynomials (e.g., Newman polynomials).

Research Interests

Erdős - Selfridge theorem states that the product of consecutive positive integers is never a perfect power i.e., the equation

$$x(x+1)(x+2)\cdots(x+k-1) = y^l$$

has no solutions in positive integers x, k, y, l with $k \geq 2$ and $l \geq 2$.

- Various generalizations of the above theorem.
- Power values of various polynomials (e.g., Newman polynomials).
- Number of solutions of Thue Equations.

Speed talk

L. Hajdu

University of Debrecen

Recurrence, Transcendence, and Diophantine Approximation

Lorentz Center, Leiden

14 July 2025

Main interest

• Discrete tomography (mostly algebraic aspects, many results with **Rob Tijdeman**)

• Polynomials

- problems of Turán and Szegedy (with **Bérczes**)
- Schur-type problems (with **Győry, Tijdeman**)
- relations between roots, heights, coefficients (with **Tijdeman, Varga)**

• Diophantine number theory (**sorry, too many coauthors to be mentioned**)

- powers in arithmetic progressions
- polynomial Diophantine equations
- exponential Diophantine equations
- recurrence sequences
- ...

Skolem's conjecture (a general variant)

Think of say $3 \cdot 5^{\alpha_{11}} \cdot 7^{\alpha_{12}} + 13 \cdot 11^{\alpha_{21}} \cdot 23^{\alpha_{22}} - 19 \cdot 41^{\alpha_{31}} \cdot 53^{\alpha_{32}} = 101$.

Conjecture

Let $a_1, \dots, a_k$, $b_{11}, \dots, b_{1\ell}, \dots, b_{k1}, \dots, b_{k\ell}$ be non-zero integers, c be an integer, and consider the exponential diophantine equation

$$a_1 b_{11}^{\alpha_{11}} \dots b_{1\ell}^{\alpha_{1\ell}} + \dots + a_k b_{k1}^{\alpha_{k1}} \dots b_{k\ell}^{\alpha_{k\ell}} = c \qquad (1)$$

in non-negative integers $\alpha_{11}, \dots, \alpha_{1\ell}, \dots, \alpha_{k1}, \dots, \alpha_{k\ell}$.

Suppose that equation (1) *has no solutions. Then there exists an integer m with $m \geq 2$ such that the congruence*

$$a_1 b_{11}^{\alpha_{11}} \dots b_{1\ell}^{\alpha_{1\ell}} + \dots + a_k b_{k1}^{\alpha_{k1}} \dots b_{k\ell}^{\alpha_{k\ell}} \equiv c \pmod{m} \qquad (2)$$

has no solutions in non-negative integers $\alpha_{11}, \dots, \alpha_{1\ell}, \dots, \alpha_{k1}, \dots, \alpha_{k\ell}$.

Skolem's conjecture (a general variant)

Some special cases (up to three terms or rank one) are handled by **Schinzel; Bartolome, Bilu, Luca; Bérczes, Tijdeman, H; Luca, Tijdeman, H.**

Bertók and H (2016, 2018): The conjecture is true for any fixed a_i, b_{ij}, for 'almost all' c on the right hand side.

Bertók and H (2016, 2018): A heuristic, efficient algorithm and several numerical examples. For example, the Conjecture is valid for

$$2^{\alpha_1} + 3^{\alpha_2} + 5^{\alpha_3} + 7^{\alpha_4} + 11^{\alpha_5} + 13^{\alpha_6} + 17^{\alpha_7} + 19^{\alpha_8} - 23^{\alpha_9} = 55191.$$

This equation has no solutions, but it has solutions if 55191 is replaced by any c with $0 \le c < 55191$.

Skolem's conjecture (a general variant)

Bertók and H (2016, 2018): Based upon the Conjecture, a heuristic, efficient algorithm to **completely solve exponential Diophantine equations in several unknowns**. Some examples:

- $10^{\alpha_1} + 11^{\alpha_2} + 12^{\alpha_3} = 13^{\alpha_4} + 14^{\alpha_5}$ has only the solutions $(0,0,1,1,0),\ (2,2,2,2,2)$;
- $2^{\alpha_1}3^{\alpha_2} + 5^{\alpha_3}7^{\alpha_4} - 11^{\alpha_5}13^{\alpha_6} = 1$ has only the solutions $(0,0,0,0,0,0),\ (0,2,1,0,0,1)$;
- $2^{\alpha_1} + 3^{\alpha_2} + 5^{\alpha_3} = U_n \qquad (U_n \in \{F_n, L_n, P_n, Q_n\})$ has solutions only with $n \leq 12$.

I do not know of any other method to solve such equations completely.

There are various related open problems (not fitting this speed talk).

I would be happy to discuss about them with interested Colleagues!

Introducing myself

Albert-Ludwigs-Universität Freiburg

Annette Huber

Mathematisches Institut
Albert-Ludwigs-Universität Freiburg
July 2025

Academic CV

- 1986–1991 Undergrad. degree Frankfurt, Cambridge, Münster
- 1994 Doctorate Münster
  Motives and their realization in derived categories
- 1995/96 Postdoc UC Berkeley
- 1994/95, 1996-2000 Postdoc Münster
- 1999 Habilitation
- 2000-2008 Professor Universität Leipzig
- 2008- now Professor Universität Freiburg

Research Area

- **arithmetic geometry**
  (algebraic geometry, number theory, K-theory)
- motives, special values of L-functions
- differential forms in algebraic geometry
- periods
- currently:
  - o-minimal geometry and the period conjecture
    jt. with Commelin, Habegger, Oswal, Kaiser
  - structure theory of finite dim. algebras and period spaces
    jt. with Kalck, Memlouk

Key publications

UNI FREIBURG

1. —, G. Kings. **Degeneration of l-adic Eisenstein classes and of the elliptic polylog.** Inventiones Mathematicae 135(3): 545–594, 1999.
2. —, G. Kings. **Equivariant Bloch-Kato conjecture and non-abelian Iwasawa Main Conjecture.** Proceedings of the ICM, Beijing 2002, vol. II, pp. 149–162. Higher Education Press, Beijing, 2002.
3. —, S. Müller-Stach, with contributions of Benjamin Friedrich and Jonas von Wangenheim, **Periods and Nori Motives**, Ergebnisse der Mathematik und ihrer Grenzgebiete 65, Springer Verlag 2017.
4. —, G. Wüstholz, **Transcendence and linear relations of 1-periods**, Cambridge Tracts in Mathematics 227, Cambridge University Press 2022

Automatic Positivity Proofs for Linear Recurrences

Alaa Ibrahim

Third year PhD student

Supervisors: Bruno SALVY, Alin Bostan, Mohab Safey El Din

ENS DE LYON

Positivity Problem

Input: $\begin{cases} p_d(n)u_{n+d} = p_{d-1}(n)u_{n+d-1} + \cdots + p_0(n)u_n, \; p_i \in \mathbb{Q}[n] \\ u_0, u_1, \ldots, u_{d-1} \in \mathbb{Q} \end{cases}$

Order d

Output: **True** if $\forall n \in \mathbb{N}, u_n > 0$

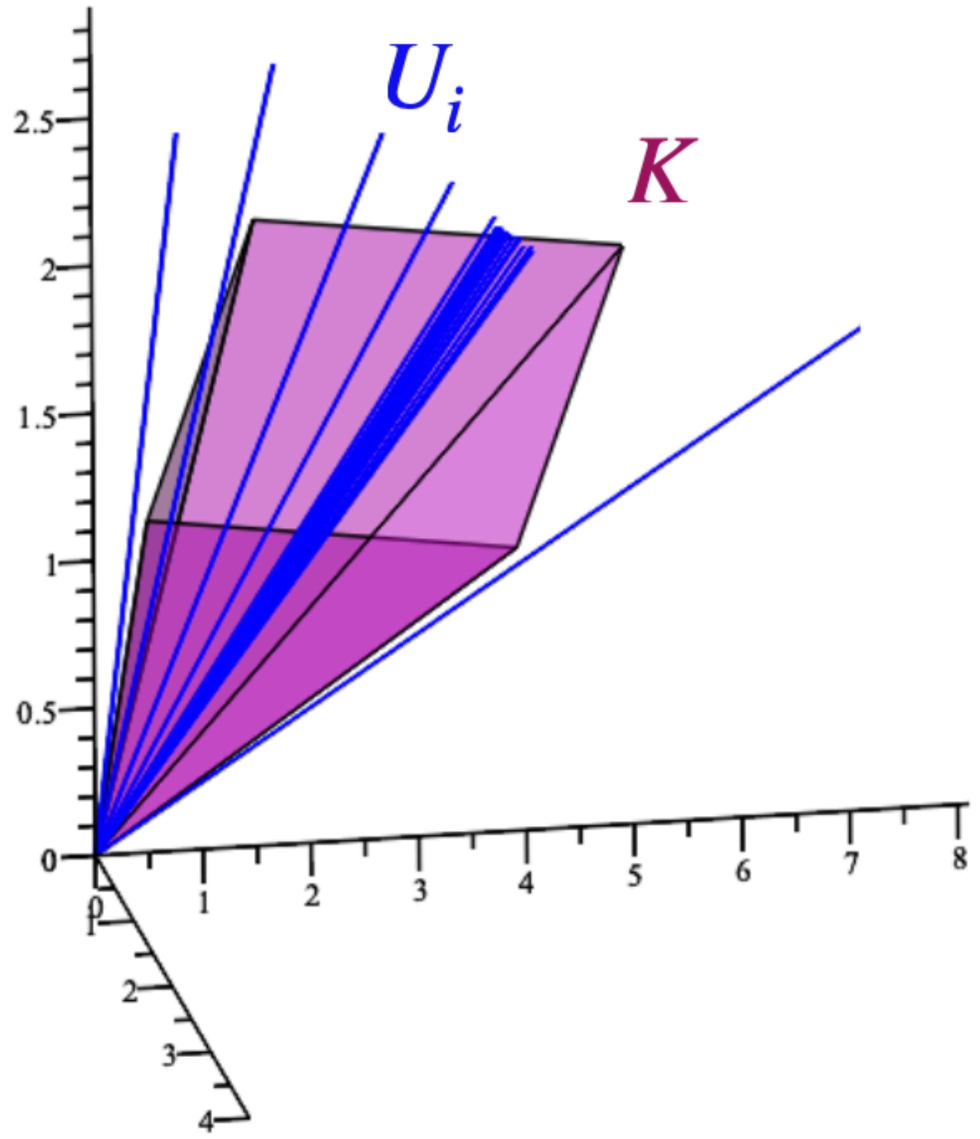
$$s_n = \sum_{k=0}^{n} (-27)^{n-k} 2^{2k-n} \frac{(3k)!}{k!^3} \binom{k}{n-k} \geq 0, n \in \mathbb{N}$$

[Straub-Zudilin 2015]

Cone-Based approach

Let $U_n = (u_n, u_{n+1}, \ldots, u_{n+d-1})^t$, then

$$U_{n+1} = \underbrace{\begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ \frac{p_0(n)}{p_d(n)} & \frac{p_1(n)}{p_d(n)} & \frac{p_2(n)}{p_d(n)} & \ldots & \frac{p_{d-1}(n)}{p_d(n)} \end{pmatrix}}_{A(n)} U_n$$



$$A = \lim_{n\to\infty} A(n) \in \mathbb{Q}^{d\times d}, \lambda_i \text{ eigenvalues of } A$$

Theorem [I.-Salvy 2024]

Positivity is decidable for $d \in \mathbb{N}$ with $\lambda_1 > \lvert\lambda_2\rvert \geq \lvert\lambda_3\rvert \geq \ldots$ + Generic initial conditions + λ_1 simple

Cube sum problem, p-Selmer groups, ideal class group and p-converse theorem

Recurrence, transcendence, and Diophantine approximation
Lorentz Center, Leiden

Somnath Jha

IIT Kanpur

14 July 2025

Research interests:

1. Selmer group of elliptic curves, relation with the ideal class groups, cube sum problem

Research interests:

1. Selmer group of elliptic curves, relation with the ideal class groups, cube sum problem
2. Selmer groups of modular forms, Hida family, Iwasawa theory, p-converse to Gross-Zagier & Kolyvagin theorem.

Research interests:

1. Selmer group of elliptic curves, relation with the ideal class groups, cube sum problem
2. Selmer groups of modular forms, Hida family, Iwasawa theory, p-converse to Gross-Zagier & Kolyvagin theorem.

Theorem (J.-Majumdar-Shingavekar 2024)

$E_a := Y^2 = X^3 + a, K = \mathbb{Q}(\zeta_3)$. Assume $a \notin K^{*2}$ and a be sixth-power free in K. $\phi : E_a \longrightarrow E_{-27a}$, degree 3-isogeny. Put $L = \mathbb{Q}(\zeta_3, \sqrt{a})$ and $h^3_L = \dim_{\mathbb{F}_3} \mathrm{Cl}_L[3]$.

Research interests:

1. Selmer group of elliptic curves, relation with the ideal class groups, cube sum problem
2. Selmer groups of modular forms, Hida family, Iwasawa theory, p-converse to Gross-Zagier & Kolyvagin theorem.

Theorem (J.-Majumdar-Shingavekar 2024)

$E_a := Y^2 = X^3 + a, K = \mathbb{Q}(\zeta_3)$. Assume $a \notin K^{*2}$ and a be sixth-power free in K. $\phi : E_a \longrightarrow E_{-27a}$, degree 3-isogeny. Put $L = \mathbb{Q}(\zeta_3, \sqrt{a})$ and $h_L^3 = \dim_{\mathbb{F}_3} \mathrm{Cl}_L[3]$. Assume some technical conditions.

Research interests:

1. Selmer group of elliptic curves, relation with the ideal class groups, cube sum problem
2. Selmer groups of modular forms, Hida family, Iwasawa theory, p-converse to Gross-Zagier & Kolyvagin theorem.

Theorem (J.-Majumdar-Shingavekar 2024)

$E_a := Y^2 = X^3 + a, K = \mathbb{Q}(\zeta_3)$. Assume $a \notin K^{*2}$ and a be sixth-power free in K. $\phi : E_a \longrightarrow E_{-27a}$, degree 3-isogeny. Put $L = \mathbb{Q}(\zeta_3, \sqrt{a})$ and $h_L^3 = \dim_{\mathbb{F}_3} \mathrm{Cl}_L[3]$. Assume some technical conditions.
Then $\dim_{\mathbb{F}_3} S_\phi(E_a/K) \in \{h_L^3, h_L^3 + 1\}$ and it is uniquely determined by the root number of $E_a/\mathbb{Q}$.

Research interests:

1. Selmer group of elliptic curves, relation with the ideal class groups, cube sum problem
2. Selmer groups of modular forms, Hida family, Iwasawa theory, p-converse to Gross-Zagier & Kolyvagin theorem.

Theorem (J.-Majumdar-Shingavekar 2024)

$E_a := Y^2 = X^3 + a, K = \mathbb{Q}(\zeta_3)$. Assume $a \notin K^{*2}$ and a be sixth-power free in K. $\phi : E_a \longrightarrow E_{-27a}$, degree 3-isogeny. Put $L = \mathbb{Q}(\zeta_3, \sqrt{a})$ and $h_L^3 = \dim_{\mathbb{F}_3} \mathrm{Cl}_L[3]$. Assume some technical conditions. Then $\dim_{\mathbb{F}_3} S_\phi(E_a/K) \in \{h_L^3, h_L^3 + 1\}$ and it is uniquely determined by the root number of $E_a/\mathbb{Q}$.

Question

Which integers n are rational cube sums (i.e. $n = a^3 + b^3$ with $a, b \in \mathbb{Q}$)?

Research interests:

1. Selmer group of elliptic curves, relation with the ideal class groups, cube sum problem
2. Selmer groups of modular forms, Hida family, Iwasawa theory, *p*-converse to Gross-Zagier & Kolyvagin theorem.

Theorem (J.-Majumdar-Shingavekar 2024)

$E_a := Y^2 = X^3 + a, K = \mathbb{Q}(\zeta_3)$. Assume $a \notin K^{*2}$ and a be sixth-power free in K. $\phi : E_a \longrightarrow E_{-27a}$, degree 3-isogeny. Put $L = \mathbb{Q}(\zeta_3, \sqrt{a})$ and $h_L^3 = \dim_{\mathbb{F}_3} \mathrm{Cl}_L[3]$. Assume some technical conditions. Then $\dim_{\mathbb{F}_3} S_\phi(E_a/K) \in \{h_L^3, h_L^3 + 1\}$ and it is uniquely determined by the root number of $E_a/\mathbb{Q}$.

Question

Which integers n are rational cube sums (i.e. $n = a^3 + b^3$ with $a, b \in \mathbb{Q}$)?

Important work of Alpöge-Bhargava-Shnidman-Burungale-Skinner and now improvement due to Peter Koymans-Alexander Smith.

Theorem (J.-Majumdar-Sury 2023)

Let q be a prime. Each residue class $a \pmod{q}$, for $0 < a < q$, contains infinitely many primes which are cube sums.

Theorem (J.-Majumdar-Sury 2023)

Let q be a prime. Each residue class $a \pmod{q}$, for $0 < a < q$, contains infinitely many primes which are cube sums. There are infinitely many primes in each of the residue classes $\pm 1 \pmod{9}$ which are cube sums.

Theorem (J.-Majumdar-Sury 2023)

Let q be a prime. Each residue class $a \pmod{q}$, for $0 < a < q$, contains infinitely many primes which are cube sums. There are infinitely many primes in each of the residue classes $\pm 1 \pmod{9}$ which are cube sums.

Theorem (Gross-Zagier & Kolyvagin)

Let E be an elliptic curve defined over $\mathbb{Q}$. Then, for $r \in \{0, 1\}$ we have:
$\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) = r \implies \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) = r$ *and* $\text{Ш}(E/\mathbb{Q})$ *is finite.*

Theorem (J.-Majumdar-Sury 2023)

Let q be a prime. Each residue class $a \pmod{q}$, for $0 < a < q$, contains infinitely many primes which are cube sums. There are infinitely many primes in each of the residue classes $\pm 1 \pmod{9}$ which are cube sums.

Theorem (Gross-Zagier & Kolyvagin)

Let E be an elliptic curve defined over $\mathbb{Q}$. Then, for $r \in \{0, 1\}$ we have:
$ord_{s=1} L(E/\mathbb{Q}, s) = r \implies rank_{\mathbb{Z}} E(\mathbb{Q}) = r$ and $Ш(E/\mathbb{Q})$ is finite.

Theorem (Bansal-J.-Pal-Venkat $\geq$ 2025)

Let $p > 5$ be a rational prime. Let $E/\mathbb{Q}$ be an elliptic curve and assume that E has split multiplicative reduction at p, $E[p]$ is irreducible $G_{\mathbb{Q}}$ module.
Then $rank_{\mathbb{Z}} E(\mathbb{Q}) = 1$ and $\#Ш(E/\mathbb{Q})_{p^\infty} < \infty \implies \mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) = 1$.

Theorem (J.-Majumdar-Sury 2023)

Let q be a prime. Each residue class $a \pmod q$, for $0 < a < q$, contains infinitely many primes which are cube sums. There are infinitely many primes in each of the residue classes $\pm 1 \pmod 9$ which are cube sums.

Theorem (Gross-Zagier & Kolyvagin)

Let E be an elliptic curve defined over $\mathbb{Q}$. Then, for $r \in \{0, 1\}$ we have:
$ord_{s=1} L(E/\mathbb{Q}, s) = r \implies rank_{\mathbb{Z}} E(\mathbb{Q}) = r$ *and* $Ш(E/\mathbb{Q})$ *is finite.*

Theorem (Bansal-J.-Pal-Venkat $\geq$ 2025)

Let $p > 5$ be a rational prime. Let $E/\mathbb{Q}$ be an elliptic curve and assume that E has split multiplicative reduction at p, $E[p]$ is irreducible $G_{\mathbb{Q}}$ module.
Then $rank_{\mathbb{Z}} E(\mathbb{Q}) = 1$ *and* $\#Ш(E/\mathbb{Q})_{p^\infty} < \infty \implies \mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) = 1.$

Thank You

Toghrul Karimov, MPI-SWS, Saarbrücken, Germany

Work with: V. Berthé, J. Ouaknine, J. Worrell, F. Luca, ...

Work on: decision problems in computer science connected to number theory and ergodic theory

[K., Luca, Nieuwveld, Ouaknine, Worrell]

Given a linear system $Ax = 0 \wedge Bx > 0$ with $x \in \mathbb{Z}^m, A \in \mathbb{Z}^{k \times m}$, $B \in \mathbb{Z}^{l \times m}$ and $T_1, \ldots, T_m \in \{\mathbb{Z}, 2^{\mathbb{N}}, 3^{\mathbb{N}}\}$, it is decidable whether a solution satisfying $x_i \in T_i$ exists

[K., Nieuwveld, Ouaknine]

Let $(u_n)_n$ be a non-degenerate $\mathbb{Z}$-LRS with two simple dominant roots. The first-order theory of $(\mathbb{N}; +, \{u_n\})$ is undecidable.

Speed talk

Peter Koymans
Utrecht University

Recurrence, transcendence, and Diophantine approximation

14 July 2025

Hilbert's tenth problem

My main research is in number theory, specifically arithmetic statistics.

Hilbert's tenth problem

My main research is in number theory, specifically arithmetic statistics. In particular, statistical problems that have applications to other fields and connect to classical Diophantine equations.

Hilbert's tenth problem

My main research is in number theory, specifically arithmetic statistics. In particular, statistical problems that have applications to other fields and connect to classical Diophantine equations.

At the 1900 mathematical conference in Paris, Hilbert introduced his famous list of 23 problems.

Hilbert's tenth problem

My main research is in number theory, specifically arithmetic statistics. In particular, statistical problems that have applications to other fields and connect to classical Diophantine equations.

At the 1900 mathematical conference in Paris, Hilbert introduced his famous list of 23 problems.

Theorem (MRDP, 1970)

Hilbert's tenth problem is undecidable, i.e. there is no algorithm that can decide whether a polynomial $p \in \mathbb{Z}[x_1, \ldots, x_n]$ *has a zero or not.*

Hilbert's tenth problem

My main research is in number theory, specifically arithmetic statistics. In particular, statistical problems that have applications to other fields and connect to classical Diophantine equations.

At the 1900 mathematical conference in Paris, Hilbert introduced his famous list of 23 problems.

Theorem (MRDP, 1970)

Hilbert's tenth problem is undecidable, i.e. there is no algorithm that can decide whether a polynomial $p \in \mathbb{Z}[x_1, \ldots, x_n]$ has a zero or not.

Theorem (K.–Pagano, 2024)

Let R be a finitely generated ring with $|R| = \infty$. Then Hilbert's tenth problem is undecidable over R.

Hilbert's tenth problem

My main research is in number theory, specifically arithmetic statistics. In particular, statistical problems that have applications to other fields and connect to classical Diophantine equations.

At the 1900 mathematical conference in Paris, Hilbert introduced his famous list of 23 problems.

Theorem (MRDP, 1970)

Hilbert's tenth problem is undecidable, i.e. there is no algorithm that can decide whether a polynomial $p \in \mathbb{Z}[x_1, \ldots, x_n]$ has a zero or not.

Theorem (K.–Pagano, 2024)

Let R be a finitely generated ring with $|R| = \infty$. Then Hilbert's tenth problem is undecidable over R.

This is related to constructing elliptic curves of a given rank.

Solubility of Diophantine equations

Another question that I am interested in is solubility of Diophantine equations in families.

Solubility of Diophantine equations

Another question that I am interested in is solubility of Diophantine equations in families.

Theorem (K.–Pagano, 2022)

There exists a constant $C > 0$ such that

$$\#\{d \in \mathbb{Z}_{>0} : d \text{ sqf. and } x^2 - dy^2 = -1 \text{ is soluble in } x, y \in \mathbb{Z}\} \sim \frac{CX}{\sqrt{\log X}}.$$

Solubility of Diophantine equations

Another question that I am interested in is solubility of Diophantine equations in families.

Theorem (K.–Pagano, 2022)

There exists a constant $C > 0$ *such that*

$$\#\{d \in \mathbb{Z}_{>0} : d \text{ sqf. and } x^2 - dy^2 = -1 \text{ is soluble in } x, y \in \mathbb{Z}\} \sim \frac{CX}{\sqrt{\log X}}.$$

The next result improves on work of Alpöge–Bhargava–Shnidman.

Solubility of Diophantine equations

Another question that I am interested in is solubility of Diophantine equations in families.

Theorem (K.–Pagano, 2022)

There exists a constant $C > 0$ such that

$$\#\{d \in \mathbb{Z}_{>0} : d \text{ sqf. and } x^2 - dy^2 = -1 \text{ is soluble in } x, y \in \mathbb{Z}\} \sim \frac{CX}{\sqrt{\log X}}.$$

The next result improves on work of Alpöge–Bhargava–Shnidman.

Theorem (K.–Smith, 2024)

We have

$$\liminf_{H \to \infty} \frac{\#\{1 \leq n \leq H : x^3 + y^3 = n \text{ is soluble with } x, y \in \mathbb{Q}\}}{H} \geq 0.3195.$$

Brief overview of my current research

Veekesh Kumar
Indian Institute of Technology Dharwad, India

14th July, 2025

- Applications of Schmidt subspace theorem, S-unit equation theorem
- Algebraic approximations to powers sums
- Irrationality of odd zeta values and related problems
- Problems on measure of algebraic independence
- Transcendence nature of lacunary type series

Theorem (with J. Sprang and V. Singh, work in progress)

Let $(A_n)_{n\in\mathbb{Z}}$ be a non-degenerate linear recurrence sequence in a real quadratic field. Then the sequence $(\ell(A_n))_n$ of period lengths is unbounded except one of the following three cases hold:

1. *$A_n \in \mathbb{Q}$ for all $n \in \mathbb{Z}$,*
2. *$A_n = (\pm 1)^n \beta + B_n$ for all $n \in \mathbb{Z}$ with β quadratic irrational and $(B_n)_n$ a linear recurrence in with bounded denominators,*
3. *A_n is the sum of a unital Pisot sequence and a rational linear recurrence sequence.*

We define the S-height of a non-zero element $\alpha \in K^\times$ to be

$$H_S(\alpha) := \prod_{v\notin S} \max\{1, |\alpha|_v\}.$$

Theorem (with G. Prasad Sena, 2025)

Let K be a number field of degree d over $\mathbb{Q}$ and $M_K^\infty \subset S \subset M_K$ be a finite set. Let $0 \neq \lambda \in \overline{\mathbb{Q}}$ and ε, δ be positive real numbers with $0 < \delta < 1/d(d+1)$. Then there exists only finitely many pairs $(u, q) \in K^* \times \mathbb{Z}$ with $H_S(u)H_S(u^{-1}) \leq H^\delta(u)$ and $d = [\mathbb{Q}(u) : \mathbb{Q}]$ such that $|\lambda q u| > 1$, $\lambda q u$ is not a pseudo-Pisot number and the following inequality holds:

$$0 < ||\lambda q u|| < \frac{1}{H(u)^\varepsilon q^{d+\varepsilon} \hat{H}_S(u)^{d(d+1)}}.$$

- If $\theta \in (0, 1/4)$, then for any odd integer b, there exists $k_0 > 1$ such that for any integer $k \geq k_0$, the inequality

$$||2^{kn}/(2^n + b)|| < \theta^n$$

has only finitely many solutions in $n \in \mathbb{N}$.

My research: All about L-functions

Matilde Lalín

Université de Montréal & Centre de recherches mathématiques

matilde.lalin@umontreal.ca
http://www.dms.umontreal.ca/~mlalin/

Recurrence, Transcendence, and Diophantine Approximation
Lorentz Center, Universiteit Leiden
July 14, 2025

Statistics of L-functions over $\mathbb{F}_q[t]$

- David, Florea, & L. (2025+) Let $q \equiv 1 \pmod{2\ell}$ and c $\square$-free. Let $\chi = \left(\frac{c}{\cdot}\right)_\ell$.

$$\text{Proportion of } L(\tfrac{1}{2}, \chi) \neq 0 \geq \begin{cases} \frac{1}{6} & \ell = 3, \\ \frac{3}{26} & \ell = 4, \\ \frac{2(\ell-2)}{2\ell^2+\ell-2} & 5 \leq \ell \leq 8, \\ \frac{2(\ell-2)}{3\ell^2-7\ell-2} & \ell = 9, 10, \\ \frac{6(\ell-2)}{9\ell^2-25\ell-6} & 11 \leq \ell. \end{cases}$$

Statistics of L-functions over $\mathbb{F}_q[t]$

- David, Florea, & L. (2025+) Let $q \equiv 1 \pmod{2\ell}$ and c $\square$-free. Let $\chi = \left(\frac{c}{\cdot}\right)_\ell$.

$$\text{Proportion of } L(\tfrac{1}{2}, \chi) \neq 0 \geq \begin{cases} \frac{1}{6} & \ell = 3, \\ \frac{3}{26} & \ell = 4, \\ \frac{2(\ell-2)}{2\ell^2+\ell-2} & 5 \leq \ell \leq 8, \\ \frac{2(\ell-2)}{3\ell^2-7\ell-2} & \ell = 9, 10, \\ \frac{6(\ell-2)}{9\ell^2-25\ell-6} & 11 \leq \ell. \end{cases}$$

ℓ	proportion
3	0.16666...
4	0.1153...
5	0.1132...
6	0.1052...
7	0.0970 ...
8	0.0895...
9	0.0786...
10	0.0701...
11	0.0668...
12	0.0606...
13	0.0554...
14	0.0511...
15	0.0474...

Statistics of L-functions over $\mathbb{F}_q[t]$

- David, Florea, & L. (2025+) Let $q \equiv 1 \pmod{2\ell}$ and c $\square$-free. Let $\chi = \left(\frac{c}{\cdot}\right)_\ell$.

$$\text{Proportion of } L(\tfrac{1}{2},\chi) \neq 0 \geq \begin{cases} \frac{1}{6} & \ell = 3, \\ \frac{3}{26} & \ell = 4, \\ \frac{2(\ell-2)}{2\ell^2+\ell-2} & 5 \leq \ell \leq 8, \\ \frac{2(\ell-2)}{3\ell^2-7\ell-2} & \ell = 9, 10, \\ \frac{6(\ell-2)}{9\ell^2-25\ell-6} & 11 \leq \ell. \end{cases}$$

ℓ	proportion
3	0.16666...
4	0.1153...
5	0.1132...
6	0.1052...
7	0.0970 ...
8	0.0895...
9	0.0786...
10	0.0701...
11	0.0668...
12	0.0606...
13	0.0554...
14	0.0511...
15	0.0474...

- Florea, L., Malik, & Sahay (2025+) When $\deg(h) \leq [n/2]$,

$$\sum_{f \in \mathcal{M}_n} d(f)d(f+h) = q^n \sum_{g|h} \frac{1}{|g|}\left[\Big(n-2\deg(g)+1\Big)^2 - \frac{1}{q}\Big(n-2\deg(g)-1\Big)^2\right]$$

Special values of L-functions as Mahler measures

$P \in \mathbb{C}(x_1, \dots, x_n)^\times$, the (logarithmic) Mahler measure is :

$$\mathrm{m}(P) = \frac{1}{(2\pi i)^n} \int_{\mathbb{T}^n} \log |P(x_1, \dots, x_n)| \frac{dx_1}{x_1} \cdots \frac{dx_n}{x_n},$$

where $\mathbb{T}^n = \{(x_1, \dots, x_n) \in \mathbb{C}^n : |x_i| = 1\}$.

- L. (2003, 2006)

$$\mathrm{m}\left(1 + x + \left(\frac{1 - x_1}{1 + x_1}\right)(1 + y)z\right) = \frac{24}{\pi^3} L(\chi_{-4}, 4)$$

- L., Nair, & Roy (2024)

$$\mathrm{m}\left(1 + x + \left(\frac{1 - x_1}{1 + x_1}\right)^2 (1 + y)z\right) = \frac{21}{2\pi^2} \zeta(3)$$

Special values of L-functions as Mahler measures

$P \in \mathbb{C}(x_1, \dots, x_n)^\times$, the (logarithmic) Mahler measure is :

$$\mathrm{m}(P) = \frac{1}{(2\pi i)^n} \int_{\mathbb{T}^n} \log |P(x_1, \dots, x_n)| \frac{dx_1}{x_1} \cdots \frac{dx_n}{x_n},$$

where $\mathbb{T}^n = \{(x_1, \dots, x_n) \in \mathbb{C}^n : |x_i| = 1\}$.

- L. (2003, 2006)

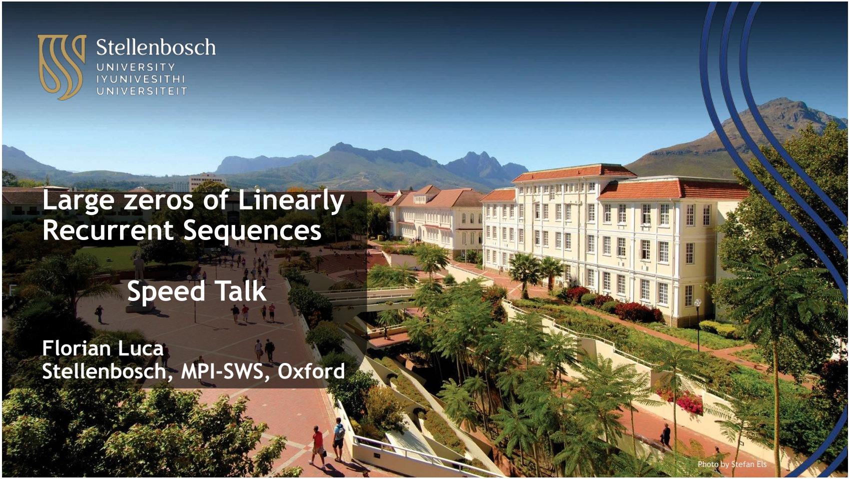
$$\mathrm{m}\left(1 + x + \left(\frac{1 - x_1}{1 + x_1}\right)(1 + y)z\right) = \frac{24}{\pi^3} L(\chi_{-4}, 4)$$

- L., Nair, & Roy (2024)

$$\mathrm{m}\left(1 + x + \left(\frac{1 - x_1}{1 + x_1}\right)^2 (1 + y)z\right) = \frac{21}{2\pi^2} \zeta(3)$$

- Boyd (2005), L. (2015), Brunault (2023+)

$$\mathrm{m}(z + (x + 1)(y + 1)) = 2L'(E_{15}, -1) \left(= \frac{225}{4\pi^4} L(E_{15}, 3)\right)$$



Stellenbosch
UNIVERSITY
IYUNIVESITHI
UNIVERSITEIT

Large zeros of Linearly Recurrent Sequences

Speed Talk

Florian Luca
Stellenbosch, MPI-SWS, Oxford

A **linear recurrent sequence (LRS)** is a sequence in $\mathbb{Z}$ (or $\mathbb{Q}$) $\langle u_0, u_1, u_2, \ldots \rangle$ such that there are constants $a_1, \ldots, a_k$ and,

$$\forall n \geq 0 : \quad u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \ldots + a_k u_n.$$

Linearly recurrent sequences

A **linear recurrent sequence (LRS)** is a sequence in $\mathbb{Z}$ (or $\mathbb{Q}$) $\langle u_0, u_1, u_2, \ldots \rangle$ such that there are constants $a_1, \ldots, a_k$ and, $\forall n \geq 0 : \quad u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \ldots + a_k u_n.$

One can write

$$u_n = \sum_{j=1}^{k} P_j(n) \lambda_j^n \qquad \forall n \geq 0, \qquad P_j(x) \in \mathbb{C}[x].$$

The above data can be read from the recurrence and initial values.

Linearly recurrent sequences

A **linear recurrent sequence (LRS)** is a sequence in $\mathbb{Z}$ (or $\mathbb{Q}$) $\langle u_0, u_1, u_2, \ldots \rangle$ such that there are constants $a_1, \ldots, a_k$ and,
$\forall n \geq 0 : \quad u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \ldots + a_k u_n.$

One can write

$$u_n = \sum_{j=1}^{k} P_j(n)\lambda_j^n \qquad \forall n \geq 0, \qquad P_j(x) \in \mathbb{C}[x].$$

The above data can be read from the recurrence and initial values.

The sequence is nondegenerate if $(\lambda_j/\lambda_j)^m \neq 1$ for $i \neq j$, $m \in \mathbb{N}$.

Linearly recurrent sequences

A **linear recurrent sequence (LRS)** is a sequence in $\mathbb{Z}$ (or $\mathbb{Q}$) $\langle u_0, u_1, u_2, \ldots \rangle$ such that there are constants $a_1, \ldots, a_k$ and,
$\forall n \geq 0 : \quad u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \ldots + a_k u_n.$

One can write

$$u_n = \sum_{j=1}^{k} P_j(n)\lambda_j^n \qquad \forall n \geq 0, \qquad P_j(x) \in \mathbb{C}[x].$$

The above data can be read from the recurrence and initial values.

The sequence is nondegenerate if $(\lambda_j/\lambda_j)^m \neq 1$ for $i \neq j$, $m \in \mathbb{N}$.

Problem SKOLEM

Instance: A linear recurrence sequence $\langle u_0, u_1, u_2, \ldots \rangle$

Question: Does $\exists n \geq 0$ such that $u_n = 0$?

Linearly recurrent sequences

A **linear recurrent sequence (LRS)** is a sequence in $\mathbb{Z}$ (or $\mathbb{Q}$) $\langle u_0, u_1, u_2, \ldots \rangle$ such that there are constants $a_1, \ldots, a_k$ and,
$\forall n \geq 0 : \quad u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \ldots + a_k u_n.$

One can write

$$u_n = \sum_{j=1}^{k} P_j(n)\lambda_j^n \qquad \forall n \geq 0, \qquad P_j(x) \in \mathbb{C}[x].$$

The above data can be read from the recurrence and initial values.

The sequence is nondegenerate if $(\lambda_j/\lambda_j)^m \neq 1$ for $i \neq j$, $m \in \mathbb{N}$.

Problem SKOLEM

Instance: A linear recurrence sequence $\langle u_0, u_1, u_2, \ldots \rangle$
Question: Does $\exists n \geq 0$ such that $u_n = 0$?

This problem has been open for about 90 years. It suffices to solve it for nondegenerate LRS's.

Classical approaches versus our approach

Classical approaches versus our approach

- Classical approaches: concentrated in explicitly bounding the zeros of a nondegenerate LRS for certain classes of sequences (for example, at most 3 roots of maximal absolute values).

Classical approaches versus our approach

- Classical approaches: concentrated in explicitly bounding the zeros of a nondegenerate LRS for certain classes of sequences (for example, at most 3 roots of maximal absolute values).
- Our approach (joint mainly with J. Ouaknine and J. Worrell) concentrates in subsets of the positive integers on which one can explicitly solve the Skolem problem for any LRS. We call them **universal Skolem sets**.

Classical approaches versus our approach

- Classical approaches: concentrated in explicitly bounding the zeros of a nondegenerate LRS for certain classes of sequences (for example, at most 3 roots of maximal absolute values).
- Our approach (joint mainly with J. Ouaknine and J. Worrell) concentrates in subsets of the positive integers on which one can explicitly solve the Skolem problem for any LRS. We call them **universal Skolem sets**.
- In the talk, we give three examples of universal Skolem sets.

Classical approaches versus our approach

- Classical approaches: concentrated in explicitly bounding the zeros of a nondegenerate LRS for certain classes of sequences (for example, at most 3 roots of maximal absolute values).
- Our approach (joint mainly with J. Ouaknine and J. Worrell) concentrates in subsets of the positive integers on which one can explicitly solve the Skolem problem for any LRS. We call them **universal Skolem sets**.
- In the talk, we give three examples of universal Skolem sets.
  - (i) The first one is very sparse.

Classical approaches versus our approach

- Classical approaches: concentrated in explicitly bounding the zeros of a nondegenerate LRS for certain classes of sequences (for example, at most 3 roots of maximal absolute values).
- Our approach (joint mainly with J. Ouaknine and J. Worrell) concentrates in subsets of the positive integers on which one can explicitly solve the Skolem problem for any LRS. We call them **universal Skolem sets**.
- In the talk, we give three examples of universal Skolem sets.
  - (i) The first one is very sparse.
  - (ii) The second one contains a positive proportion of positive integers. The proportion is 1 under the Bateman-Horn conjecture. However, we conjecture that this set misses infinitely many positive integers.

Classical approaches versus our approach

- Classical approaches: concentrated in explicitly bounding the zeros of a nondegenerate LRS for certain classes of sequences (for example, at most 3 roots of maximal absolute values).
- Our approach (joint mainly with J. Ouaknine and J. Worrell) concentrates in subsets of the positive integers on which one can explicitly solve the Skolem problem for any LRS. We call them **universal Skolem sets**.
- In the talk, we give three examples of universal Skolem sets.
  - (i) The first one is very sparse.
  - (ii) The second one contains a positive proportion of positive integers. The proportion is 1 under the Bateman-Horn conjecture. However, we conjecture that this set misses infinitely many positive integers.
  - (iii) The third one is of density 1 and under a modified version of the Cramér conjecture on distances between consecutive primes it contains all the positive integers except for a finite set.


Thank you very much
Hartelijk dank
Stellenbosch
UNIVERSITY
IYUNIVESITHI
UNIVERSITEIT
Photo by Stefan Els

Solving Diophantine equations using fundamental groups

Martin Lüdtke

Leiden, 14 July 2025

Non-abelian Chabauty

Research interest: solving Diophantine equations via (non-abelian) Chabauty

Diophantine equations:

- rational points on curves X of genus $g \geq 2$
- S-integral points of affine curves, e.g., $X = \mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$ ($\to$ S-unit equation)

Non-abelian Chabauty:

- for an auxiliary prime p, construct p-adic analytic functions $f : X(\mathbb{Q}_p) \to \mathbb{Q}_p$ with $X(\mathbb{Q}) \subseteq V(f) \subseteq X(\mathbb{Q}_p)$
- compute $X(\mathbb{Q})$ explicitly or obtain bounds on $\#X(\mathbb{Q})$
- classical Chabauty–Coleman works when $r := \operatorname{rk} \operatorname{Jac}_X(\mathbb{Q}) < g$, non-abelian generalisation by Kim (2005) aims to remove this condition
- sequence of Chabauty–Kim loci $X(\mathbb{Q}_p)_1 \supseteq X(\mathbb{Q}_p)_2 \supseteq \ldots$ containing $X(\mathbb{Q})$
- Kim's Conjecture: $X(\mathbb{Q}_p)_n = X(\mathbb{Q})$ for $n \gg 0$

Non-abelian Chabauty

Research interest: solving Diophantine equations via (non-abelian) Chabauty

Diophantine equations:

- rational points on curves X of genus $g \geq 2$
- S-integral points of affine curves, e.g., $X = \mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$ ($\to$ S-unit equation)

Non-abelian Chabauty:

- for an auxiliary prime p, construct p-adic analytic functions $f : X(\mathbb{Q}_p) \to \mathbb{Q}_p$ with $X(\mathbb{Q}) \subseteq V(f) \subseteq X(\mathbb{Q}_p)$
- compute $X(\mathbb{Q})$ explicitly or obtain bounds on $\#X(\mathbb{Q})$
- classical Chabauty–Coleman works when $r := \operatorname{rk} \operatorname{Jac}_X(\mathbb{Q}) < g$, non-abelian generalisation by Kim (2005) aims to remove this condition
- sequence of Chabauty–Kim loci $X(\mathbb{Q}_p)_1 \supseteq X(\mathbb{Q}_p)_2 \supseteq \ldots$ containing $X(\mathbb{Q})$
- Kim's Conjecture: $X(\mathbb{Q}_p)_n = X(\mathbb{Q})$ for $n \gg 0$

Non-abelian Chabauty

Research interest: solving Diophantine equations via (non-abelian) Chabauty

Diophantine equations:

- rational points on curves X of genus $g \geq 2$
- S-integral points of affine curves, e.g., $X = \mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$ ($\rightarrow$ S-unit equation)

Non-abelian Chabauty:

- for an auxiliary prime p, construct p-adic analytic functions $f\colon X(\mathbb{Q}_p) \rightarrow \mathbb{Q}_p$ with $X(\mathbb{Q}) \subseteq V(f) \subseteq X(\mathbb{Q}_p)$
- compute $X(\mathbb{Q})$ explicitly or obtain bounds on $\#X(\mathbb{Q})$
- classical Chabauty–Coleman works when $r := \mathrm{rk}\,\mathrm{Jac}_X(\mathbb{Q}) < g$, non-abelian generalisation by Kim (2005) aims to remove this condition
- sequence of Chabauty–Kim loci $X(\mathbb{Q}_p)_1 \supseteq X(\mathbb{Q}_p)_2 \supseteq \ldots$ containing $X(\mathbb{Q})$
- Kim's Conjecture: $X(\mathbb{Q}_p)_n = X(\mathbb{Q})$ for $n \gg 0$

Research interest: solving Diophantine equations via (non-abelian) Chabauty

Diophantine equations:

- rational points on curves X of genus $g \geq 2$
- S-integral points of affine curves, e.g., $X = \mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$ ($\rightarrow$ S-unit equation)

Non-abelian Chabauty:

- for an auxiliary prime p, construct p-adic analytic functions $f : X(\mathbb{Q}_p) \rightarrow \mathbb{Q}_p$ with $X(\mathbb{Q}) \subseteq V(f) \subseteq X(\mathbb{Q}_p)$
- compute $X(\mathbb{Q})$ explicitly or obtain bounds on $\#X(\mathbb{Q})$
- classical Chabauty–Coleman works when $r := \operatorname{rk} \operatorname{Jac}_X(\mathbb{Q}) < g$, non-abelian generalisation by Kim (2005) aims to remove this condition
- sequence of Chabauty–Kim loci $X(\mathbb{Q}_p)_1 \supseteq X(\mathbb{Q}_p)_2 \supseteq \ldots$ containing $X(\mathbb{Q})$
- Kim's Conjecture: $X(\mathbb{Q}_p)_n = X(\mathbb{Q})$ for $n \gg 0$

Non-abelian Chabauty

Research interest: solving Diophantine equations via (non-abelian) Chabauty

Diophantine equations:

- rational points on curves X of genus $g \geq 2$
- S-integral points of affine curves, e.g., $X = \mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$ ($\rightarrow$ S-unit equation)

Non-abelian Chabauty:

- for an auxiliary prime p, construct p-adic analytic functions $f\colon X(\mathbb{Q}_p) \rightarrow \mathbb{Q}_p$ with $X(\mathbb{Q}) \subseteq V(f) \subseteq X(\mathbb{Q}_p)$
- compute $X(\mathbb{Q})$ explicitly or obtain bounds on $\#X(\mathbb{Q})$
- classical Chabauty–Coleman works when $r := \operatorname{rk} \mathrm{Jac}_X(\mathbb{Q}) < g$, non-abelian generalisation by Kim (2005) aims to remove this condition
- sequence of Chabauty–Kim loci $X(\mathbb{Q}_p)_1 \supseteq X(\mathbb{Q}_p)_2 \supseteq \ldots$ containing $X(\mathbb{Q})$
- Kim's Conjecture: $X(\mathbb{Q}_p)_n = X(\mathbb{Q})$ for $n \gg 0$

Research interest: solving Diophantine equations via (non-abelian) Chabauty

Diophantine equations:

- rational points on curves X of genus $g \geq 2$
- S-integral points of affine curves, e.g., $X = \mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$ ($\rightarrow$ S-unit equation)

Non-abelian Chabauty:

- for an auxiliary prime p, construct p-adic analytic functions $f\colon X(\mathbb{Q}_p) \to \mathbb{Q}_p$ with $X(\mathbb{Q}) \subseteq V(f) \subseteq X(\mathbb{Q}_p)$
- compute $X(\mathbb{Q})$ explicitly or obtain bounds on $\#X(\mathbb{Q})$
- classical Chabauty–Coleman works when $r := \operatorname{rk} \operatorname{Jac}_X(\mathbb{Q}) < g$, non-abelian generalisation by Kim (2005) aims to remove this condition
- sequence of Chabauty–Kim loci $X(\mathbb{Q}_p)_1 \supseteq X(\mathbb{Q}_p)_2 \supseteq \ldots$ containing $X(\mathbb{Q})$
- Kim's Conjecture: $X(\mathbb{Q}_p)_n = X(\mathbb{Q})$ for $n \gg 0$

Non-abelian Chabauty

Research interest: solving Diophantine equations via (non-abelian) Chabauty

Diophantine equations:

- rational points on curves X of genus $g \geq 2$
- S-integral points of affine curves, e.g., $X = \mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$ ($\rightarrow$ S-unit equation)

Non-abelian Chabauty:

- for an auxiliary prime p, construct p-adic analytic functions $f \colon X(\mathbb{Q}_p) \to \mathbb{Q}_p$ with $X(\mathbb{Q}) \subseteq V(f) \subseteq X(\mathbb{Q}_p)$
- compute $X(\mathbb{Q})$ explicitly or obtain bounds on $\#X(\mathbb{Q})$
- classical Chabauty–Coleman works when $r := \operatorname{rk} \operatorname{Jac}_X(\mathbb{Q}) < g$, non-abelian generalisation by Kim (2005) aims to remove this condition
- sequence of Chabauty–Kim loci $X(\mathbb{Q}_p)_1 \supseteq X(\mathbb{Q}_p)_2 \supseteq \dots$ containing $X(\mathbb{Q})$
- Kim's Conjecture: $X(\mathbb{Q}_p)_n = X(\mathbb{Q})$ for $n \gg 0$

Some past and ongoing work

Refined Chabauty–Kim for S-integral points on $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$:

- proof of Kim's Conjecture for $S = \{2\}$, arbitrary p
- construction of Kim functions in depth ≤ 4 for $S = \{2, q\}$
- upper bounds for $\#X(\mathbb{Z}_S)$ via bounding zeros of Coleman functions
- depth 4 over cyclotomic fields (in progress)

Linear, quadratic, and cubic Chabauty for affine curves:

- derived a (quadratic) Chabauty condition for $Y = X \setminus D$ affine:

$$r + \#S < g + \#|D| + \frac{1}{2}\#(D(\mathbb{C}) \setminus D(\mathbb{R})) - 1 \;\; (+\rho)$$

- develop an explicit Chabauty–Coleman method for affine curves using the generalised Jacobian (in progress)
- depth 3 Chabauty–Kim for punctured elliptic curves (in progress)

Some past and ongoing work

Refined Chabauty–Kim for S-integral points on $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$:

- proof of Kim's Conjecture for $S = \{2\}$, arbitrary p
- construction of Kim functions in depth ≤ 4 for $S = \{2, q\}$
- upper bounds for $\#X(\mathbb{Z}_S)$ via bounding zeros of Coleman functions
- depth 4 over cyclotomic fields (in progress)

Linear, quadratic, and cubic Chabauty for affine curves:

- derived a (quadratic) Chabauty condition for $Y = X \setminus D$ affine:

$$r + \#S < g + \#|D| + \frac{1}{2}\#(D(\mathbb{C}) \setminus D(\mathbb{R})) - 1 \ \ (+\rho)$$

- develop an explicit Chabauty–Coleman method for affine curves using the generalised Jacobian (in progress)
- depth 3 Chabauty–Kim for punctured elliptic curves (in progress)

Some past and ongoing work

Refined Chabauty–Kim for S-integral points on $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$:

- proof of Kim's Conjecture for $S = \{2\}$, arbitrary p
- construction of Kim functions in depth ≤ 4 for $S = \{2, q\}$
- upper bounds for $\#X(\mathbb{Z}_S)$ via bounding zeros of Coleman functions
- depth 4 over cyclotomic fields (in progress)

Linear, quadratic, and cubic Chabauty for affine curves:

- derived a (quadratic) Chabauty condition for $Y = X \setminus D$ affine:

$$r + \#S < g + \#|D| + \frac{1}{2}\#(D(\mathbb{C}) \setminus D(\mathbb{R})) - 1 \ \ (+\rho)$$

- develop an explicit Chabauty–Coleman method for affine curves using the generalised Jacobian (in progress)
- depth 3 Chabauty–Kim for punctured elliptic curves (in progress)

Some past and ongoing work

Refined Chabauty–Kim for S-integral points on $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$:

- proof of Kim's Conjecture for $S = \{2\}$, arbitrary p
- construction of Kim functions in depth ≤ 4 for $S = \{2, q\}$
- upper bounds for $\#X(\mathbb{Z}_S)$ via bounding zeros of Coleman functions
- depth 4 over cyclotomic fields (in progress)

Linear, quadratic, and cubic Chabauty for affine curves:

- derived a (quadratic) Chabauty condition for $Y = X \setminus D$ affine:

$$r + \#S < g + \#|D| + \frac{1}{2}\#(D(\mathbb{C}) \setminus D(\mathbb{R})) - 1 \ \ (+\rho)$$

- develop an explicit Chabauty–Coleman method for affine curves using the generalised Jacobian (in progress)
- depth 3 Chabauty–Kim for punctured elliptic curves (in progress)

Some past and ongoing work

Refined Chabauty–Kim for S-integral points on $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$:

- proof of Kim's Conjecture for $S = \{2\}$, arbitrary p
- construction of Kim functions in depth ≤ 4 for $S = \{2, q\}$
- upper bounds for $\#X(\mathbb{Z}_S)$ via bounding zeros of Coleman functions
- depth 4 over cyclotomic fields (in progress)

Linear, quadratic, and cubic Chabauty for affine curves:

- derived a (quadratic) Chabauty condition for $Y = X \setminus D$ affine:

$$r + \#S < g + \#|D| + \frac{1}{2}\#(D(\mathbb{C}) \setminus D(\mathbb{R})) - 1 \ \ (+\rho)$$

- develop an explicit Chabauty–Coleman method for affine curves using the generalised Jacobian (in progress)
- depth 3 Chabauty–Kim for punctured elliptic curves (in progress)

Some past and ongoing work

Refined Chabauty–Kim for S-integral points on $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$:

- proof of Kim's Conjecture for $S = \{2\}$, arbitrary p
- construction of Kim functions in depth ≤ 4 for $S = \{2, q\}$
- upper bounds for $\#X(\mathbb{Z}_S)$ via bounding zeros of Coleman functions
- depth 4 over cyclotomic fields (in progress)

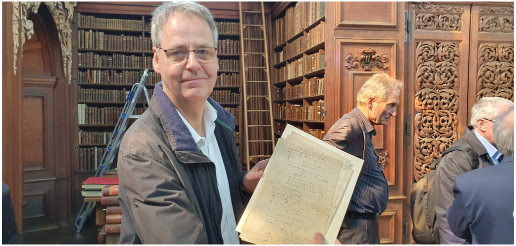
Linear, quadratic, and cubic Chabauty for affine curves:

- derived a (quadratic) Chabauty condition for $Y = X \setminus D$ affine:

$$r + \#S < g + \#|D| + \frac{1}{2}\#(D(\mathbb{C}) \setminus D(\mathbb{R})) - 1 \ \ (+\rho)$$

- develop an explicit Chabauty–Coleman method for affine curves using the generalised Jacobian (in progress)
- depth 3 Chabauty–Kim for punctured elliptic curves (in progress)

PIETER MOREE



- PhD 1993 in Leiden with Robert Tijdeman (topic: smooth ideal distribution)
- Scientific Coordinator, Max Planck Institute for Mathematics in Bonn (since 2004)
- Around 130 publications, 1000 MathSciNet citations by 650 different authors
- Editor in Chief of Indagationes Mathematicae (since 2025), editor of Research in Number Th. and Ramanujan J.

Frequent themes

- Ramanujan-Nagell equations with many solutions (with Evertse, Stewart, Tijdeman)
- Artin primitive root conjecture
- Counting divisors of sequences
- Euler-Kronecker constants and their distribution

Frequent themes

- Ramanujan-Nagell equations with many solutions (with Evertse, Stewart, Tijdeman)
- Artin primitive root conjecture
- Counting divisors of sequences
- Euler-Kronecker constants and their distribution
- (Kellner)-Erdős-Moser equation
- Prime number distribution, L-functions
- Ramanujan type-congruences for modular form coefficients
- Applications of Selberg-Delange method (on summation of multiplicative functions)

Frequent themes

- Ramanujan-Nagell equations with many solutions (with Evertse, Stewart, Tijdeman)
- Artin primitive root conjecture
- Counting divisors of sequences
- Euler-Kronecker constants and their distribution
- (Kellner)-Erdős-Moser equation
- Prime number distribution, L-functions
- Ramanujan type-congruences for modular form coefficients
- Applications of Selberg-Delange method (on summation of multiplicative functions)

Last two themes covered by:

- B. Berndt and P. Moree, Sums of two squares and the tau-function: Ramanujan's trail, *Expositiones Mathematicae*, to appear.

Kellner-Erdős-Moser Conjecture

Define $S_k(m) := 1^k + 2^k + \cdots + (m-1)^k$.

Kellner-Erdős-Moser Conjecture

For positive integers a, k, m with $m \geq 3$,

$$aS_k(m) = m^k \iff (a, k, m) \in \{(1,1,3), (3,3,3)\}$$

(That is $1 + 2 = 3$ and $3 \cdot (1 + 2^3) = 27$.)

Define $S_k(m) := 1^k + 2^k + \cdots + (m-1)^k$.

Kellner-Erdős-Moser Conjecture

For positive integers a, k, m with $m \geq 3$,

$$aS_k(m) = m^k \iff (a, k, m) \in \{(1,1,3), (3,3,3)\}$$

(That is $1 + 2 = 3$ and $3 \cdot (1 + 2^3) = 27$.)

Theorem (combination of several theorems)

General a:

- $a = 1$ *or* $a > 1500$
- *both a and m have no regular prime divisor*

Kellner-Erdős-Moser Conjecture

Define $S_k(m) := 1^k + 2^k + \cdots + (m-1)^k$.

Kellner-Erdős-Moser Conjecture

For positive integers a, k, m with $m \geq 3$,

$$aS_k(m) = m^k \iff (a,k,m) \in \{(1,1,3),(3,3,3)\}$$

(That is $1 + 2 = 3$ and $3 \cdot (1 + 2^3) = 27$.)

Theorem (combination of several theorems)

General a:

- $a = 1$ *or* $a > 1500$
- *both a and m have no regular prime divisor*

The case $a = 1$ *(Erdős-Moser equation)*

- $k, m > 10^{10^{10}}$, *new*!
- $lcm(1, 2, \ldots, 200)$ *divides k*

Definition

Let p, q be two primes with $p < q$. We let $(n_i)_{i\geq 0}$ be the sequence of consecutive integers of the form $n = p^a \cdot q^b$ with $a, b \geq 0$.

Definition

Let p, q be two primes with $p < q$. We let $(n_i)_{i\geq 0}$ be the sequence of consecutive integers of the form $n = p^a \cdot q^b$ with $a, b \geq 0$.

Tijdeman, 1975

There exist effective constants C_1 and C_2 such that

$$\frac{n_i}{(\log n_i)^{C_1}} \ll_{p,q} n_{i+1} - n_i \ll_{p,q} \frac{n_i}{(\log n_i)^{C_2}}.$$

The constants C_1, C_2 and the two implicit constants all may depend on p and q.

Effective gaps between S-units

Definition

Let p, q be two primes with $p < q$. We let $(n_i)_{i \geq 0}$ be the sequence of consecutive integers of the form $n = p^a \cdot q^b$ with $a, b \geq 0$.

Tijdeman, 1975

There exist effective constants C_1 and C_2 such that

$$\frac{n_i}{(\log n_i)^{C_1}} \ll_{p,q} n_{i+1} - n_i \ll_{p,q} \frac{n_i}{(\log n_i)^{C_2}}.$$

The constants C_1, C_2 and the two implicit constants all may depend on p and q.

Languasco, Luca, M., Togbé made this result effective ($\leq$2026), improving on earlier work in this direction by Langevin (1975).

p being a prime of ...

$$\prod_{\mathfrak{B}} = \prod_{p} \frac{1-p^{-4s}}{(1-p^{-s})(1-p^{-5s})}$$

p being a prime of the form $5k+1$.

It is easy to prove from (2.5) that

(2.6) $$t_1 + t_2 + t_3 + \dots + t_n = \underline{o}(n).$$

It can be shown by transcendental methods that

(2.7) $$t_1 + t_2 + t_3 + \dots + t_n \sim \frac{Cn}{(\log n)^{\frac{1}{4}}},$$

and

(2.8) $$t_1 + t_2 + t_3 + \dots + t_n = C\int_1^n \frac{dx}{(\log x)^{\frac{1}{4}}} + \underline{O}\,\frac{n}{(\log n)^r},$$

where C is a constant and r is any positive number.

Wim Nijgh

Position: PhD student
- Leiden University
- Supervisor: Ronald van Luijk

Research: Arithmetic of surfaces
- Rational points;
- Computing Picard groups;
- Automorphisms of K3 surfaces.

Wim Nijgh

Position: PhD student
- Leiden University
- Supervisor: Ronald van Luijk

Research: Arithmetic of surfaces
- Rational points;
- Computing Picard groups;
- Automorphisms of K3 surfaces.

Example:
Let $S \subseteq \mathbb{A}^3(x, y, z)$ be the surface defined by the equation

$$y^2 = x^3 + z^6 + 1.$$

Then the set $S(\mathbb{Q})$ of rational points is Zariski dense in S.

Speeding through my work

Alina Ostafe

The University of New South Wales

Over the last 5 years I have been working mostly on the following directions:

- Diophantine specialisation problems:
    - Multiplicative dependence of points on algebraic curves;
    - Skolem problem for parametric linear recurrences (tomorrow's talk).
- Arithmetic dynamics:
    - Special structures in (forward and backward) orbits (eg, roots of unity, higher order multiplicative relations, perfect powers, abelian points);
    - Dynamical irreducibility.
- Arithmetic statistics:
    - Matrices: counting matrices over $\mathbb{Z}$ or $\mathbb{Q}$ of bounded height, or over finitely generated groups, with various restrictions: with given characteristic polynomial, rank or determinant, with a square-free determinant, non-diagonalisable, multiplicatively dependent;
    - Linear recurrences or S-unit equations: counting integer linear recurrences satisfying a multiplicative relation, counting solvable S-unit equations.

Here is one result in arithmetic statistics for integer matrices:

Habegger, A.O. & Shparlinski (2024)

Uniformly over monic $f \in \mathbb{Z}[X]$ *with* $\deg f = n$ *we have*

$$\#\{A \in \mathcal{M}_n(\mathbb{Z}) : |a_{ij}| \le H, \det(X \cdot I_n - A) = f\}$$
$$\le \begin{cases} H^{1+o(1)}, & n = 2 \\ H^{4+o(1)}, & n = 3 \\ H^{n^2-n-1+o(1)}, & n \ge 4. \end{cases}$$

Note that the upper bound $H^{n^2-n+o(1)}$ is trivial (modulo what is known about matrices with a given determinant).

The expected upper bound $H^{n(n-1)/2+o(1)}$ seems to be out of reach even for $n = 3$.

Among all my coauthors, quite a few are attending this workshop:

Attila Bérczes, Yann Bugeaud, Kalman Györy, Lajos Hajdu, Florian Luca, Joseph Silverman.

Thank you to all my coauthors, from whom I have learned and keep learning a lot!!

Dynamical Systems meets Computation

Joël Ouaknine

Max Planck Institute for Software Systems, Germany

Workshop on recurrence, transcendence, and Diophantine approximation
Lorentz Center, Netherlands, 14–18 July 2025

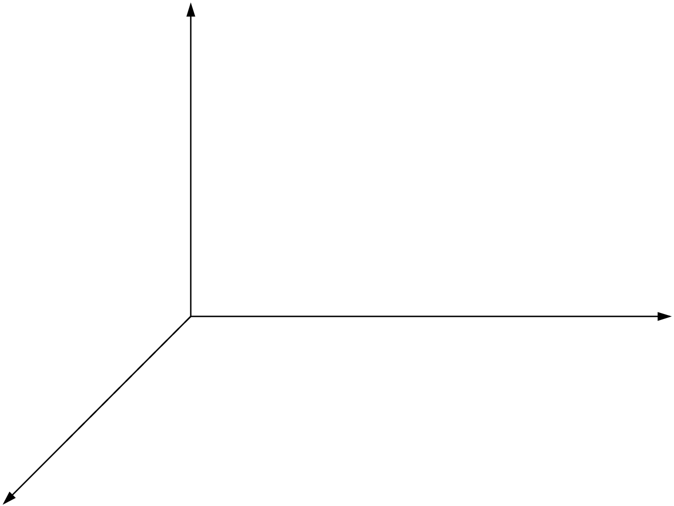
Funded by the European Union
European Research Council
Established by the European Commission

Funded by
DFG Deutsche Forschungsgemeinschaft
German Research Foundation

Orbits of linear dynamical systems

linear transformation: $\mathbf{M} \in \mathbb{Q}^{d \times d}$

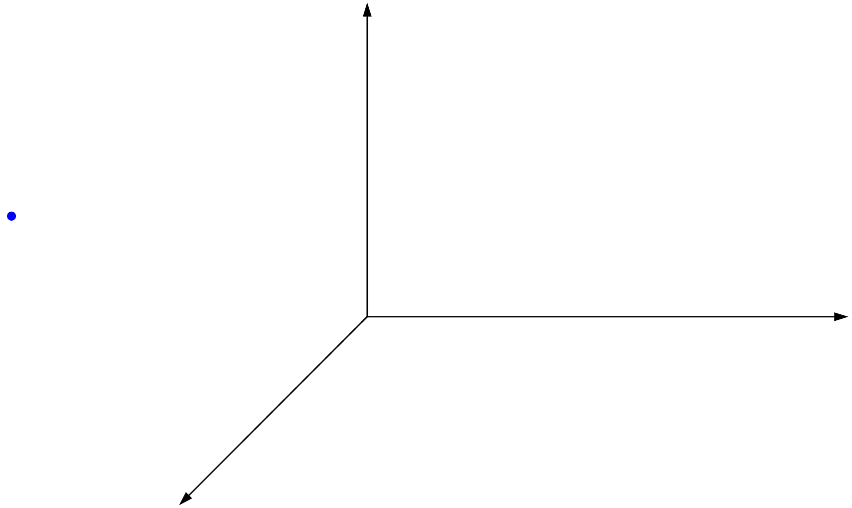
starting point: $s_0 \in \mathbb{Q}^d$



Orbits of linear dynamical systems

linear transformation: $\mathbf{M} \in \mathbb{Q}^{d \times d}$

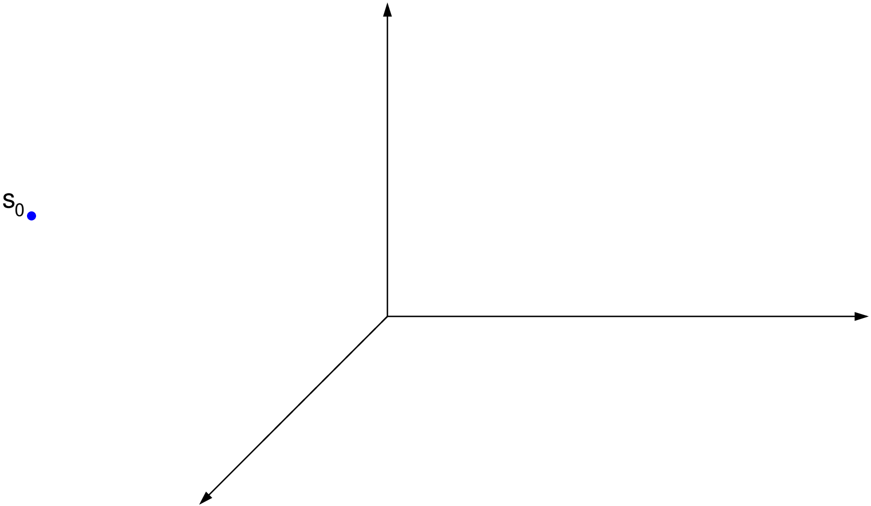
starting point: $s_0 \in \mathbb{Q}^d$



Orbits of linear dynamical systems

linear transformation: $\mathbf{M} \in \mathbb{Q}^{d \times d}$

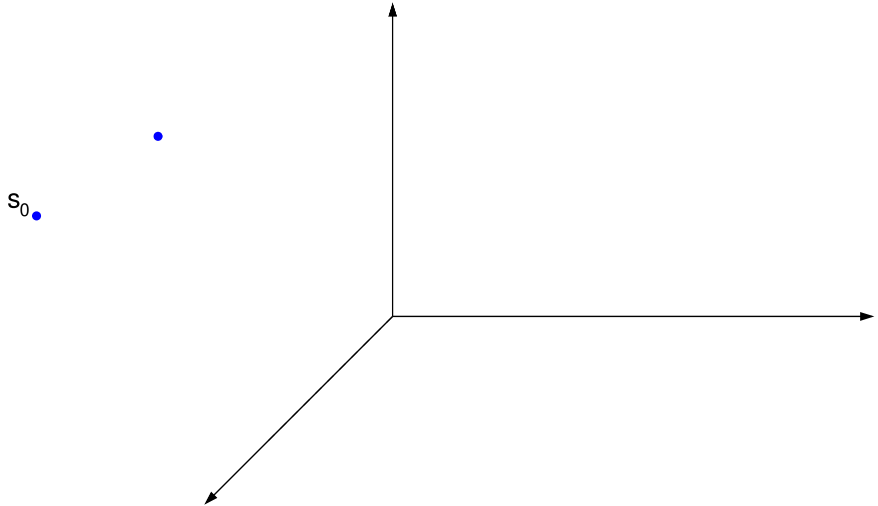
starting point: $s_0 \in \mathbb{Q}^d$



Orbits of linear dynamical systems

linear transformation: $\mathbf{M} \in \mathbb{Q}^{d \times d}$

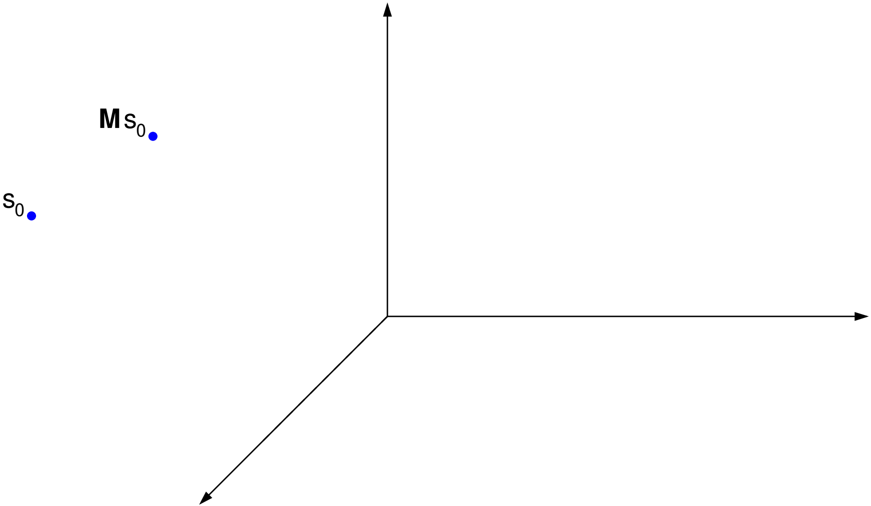
starting point: $s_0 \in \mathbb{Q}^d$



Orbits of linear dynamical systems

linear transformation: $\mathbf{M} \in \mathbb{Q}^{d \times d}$

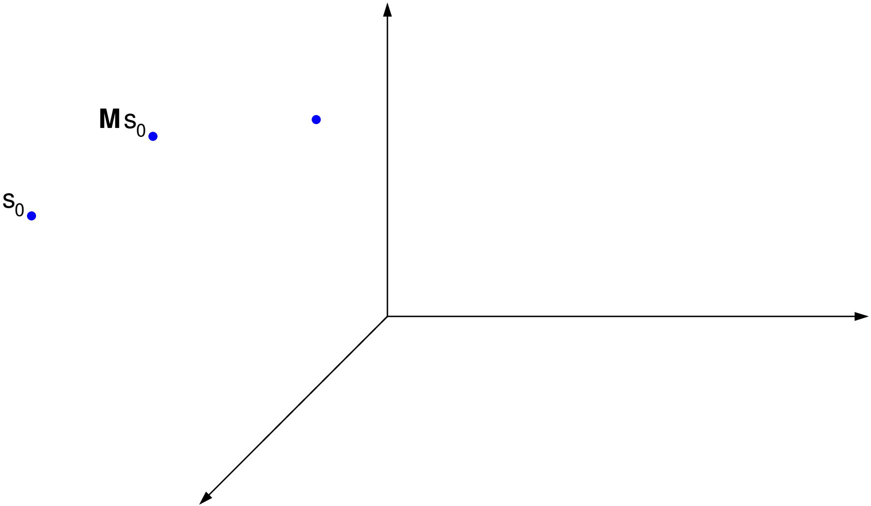
starting point: $s_0 \in \mathbb{Q}^d$



Orbits of linear dynamical systems

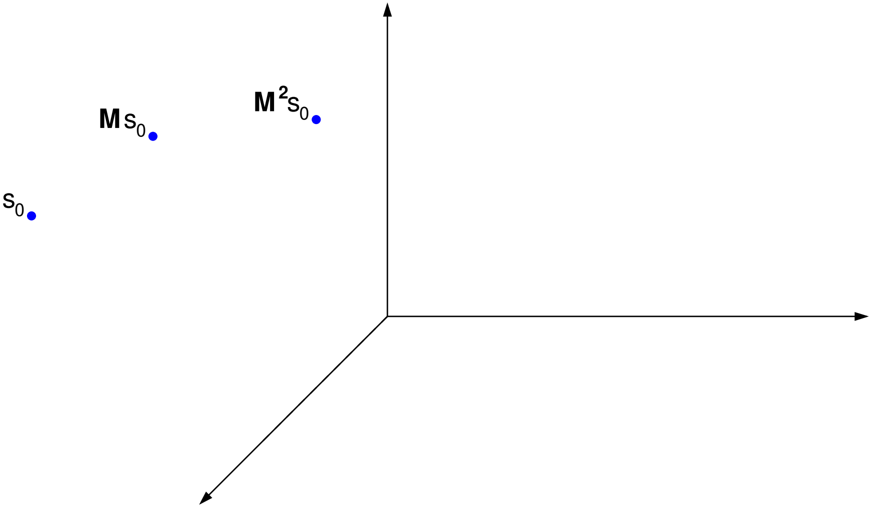
linear transformation: $\mathbf{M} \in \mathbb{Q}^{d \times d}$

starting point: $s_0 \in \mathbb{Q}^d$



Orbits of linear dynamical systems

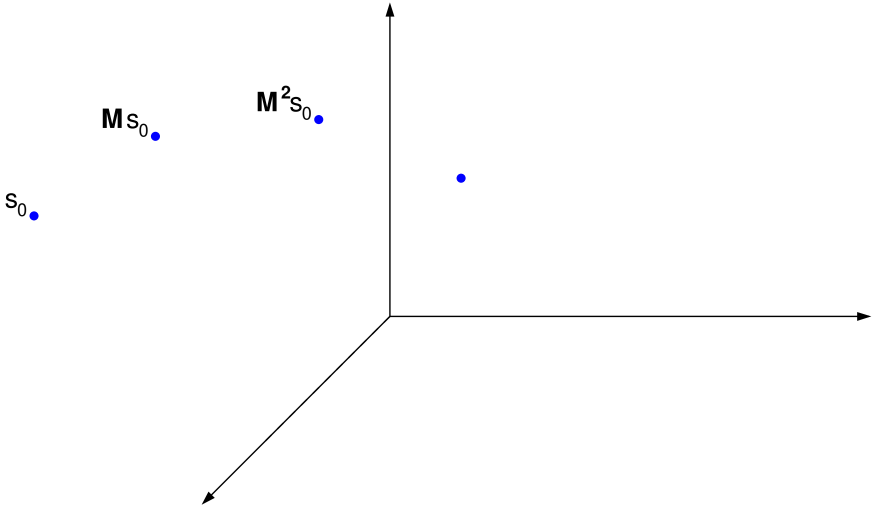
linear transformation: $\mathbf{M} \in \mathbb{Q}^{d \times d}$
starting point: $s_0 \in \mathbb{Q}^d$



Orbits of linear dynamical systems

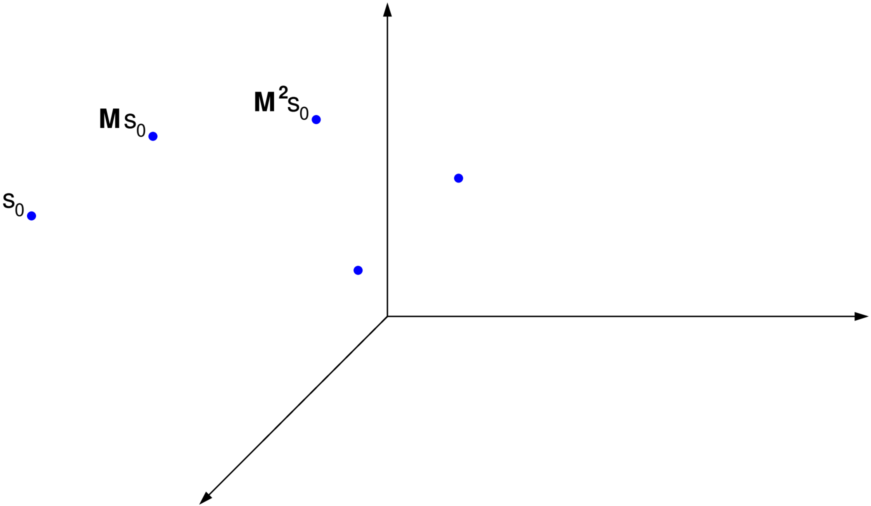
linear transformation: $\mathbf{M} \in \mathbb{Q}^{d \times d}$

starting point: $s_0 \in \mathbb{Q}^d$



Orbits of linear dynamical systems

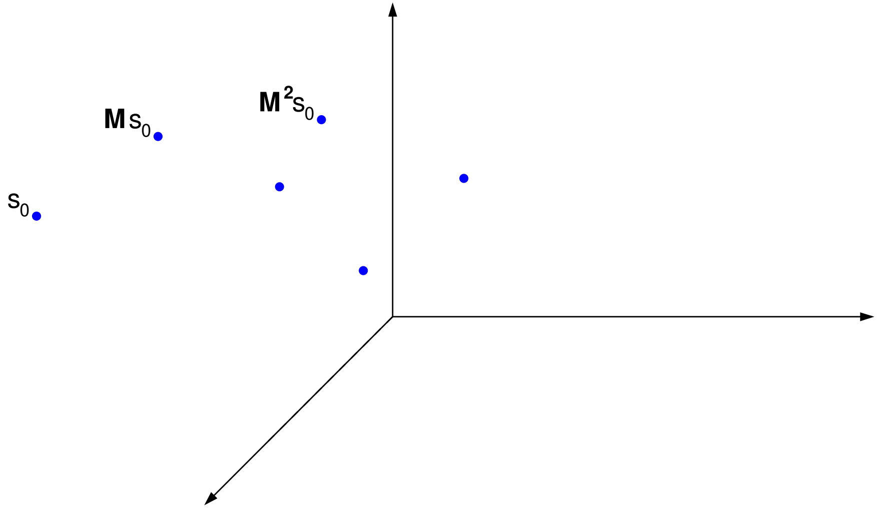
linear transformation: $\mathbf{M} \in \mathbb{Q}^{d\times d}$
starting point: $s_0 \in \mathbb{Q}^d$



Orbits of linear dynamical systems

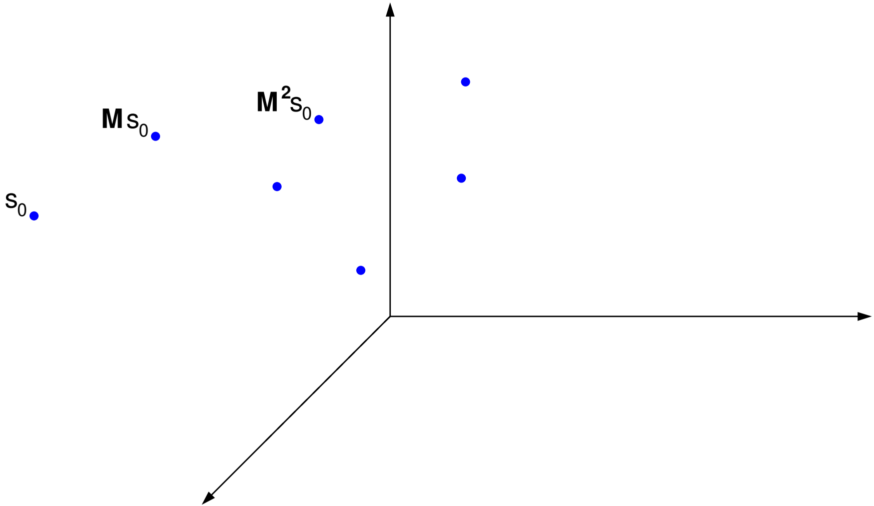
linear transformation: $\mathbf{M} \in \mathbb{Q}^{d \times d}$

starting point: $s_0 \in \mathbb{Q}^d$



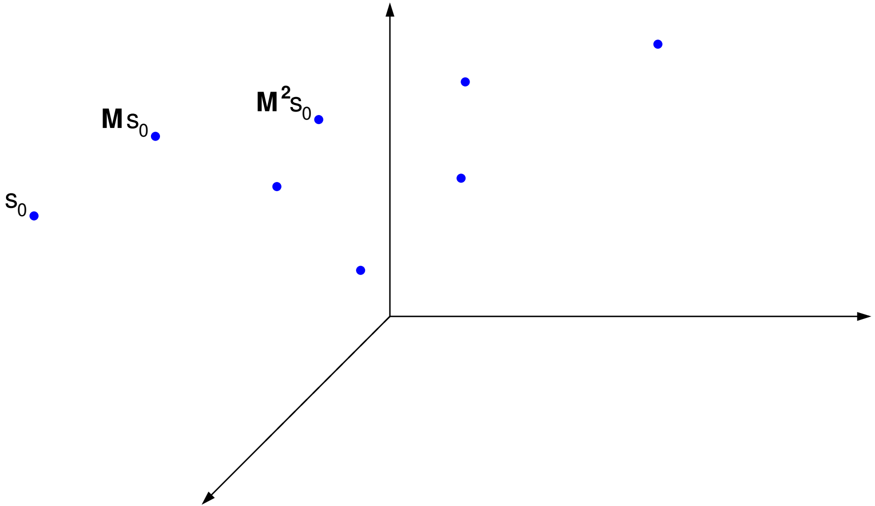
Orbits of linear dynamical systems

linear transformation: $\mathbf{M} \in \mathbb{Q}^{d \times d}$
starting point: $s_0 \in \mathbb{Q}^d$



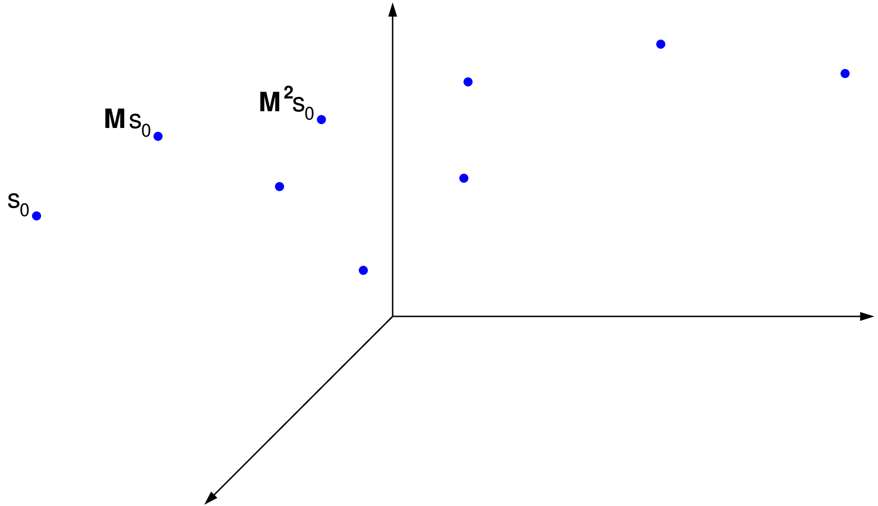
Orbits of linear dynamical systems

linear transformation: $\mathbf{M} \in \mathbb{Q}^{d\times d}$
starting point: $s_0 \in \mathbb{Q}^d$



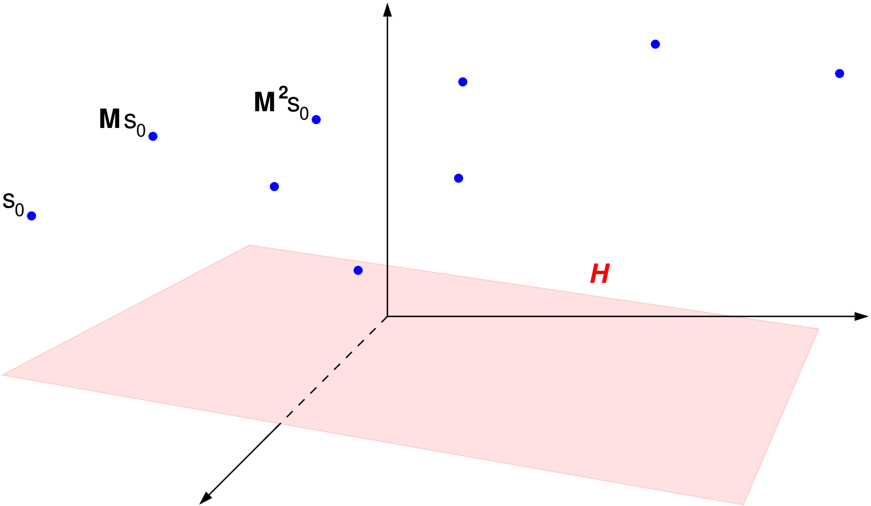
Orbits of linear dynamical systems

linear transformation: $\mathbf{M} \in \mathbb{Q}^{d \times d}$
starting point: $s_0 \in \mathbb{Q}^d$



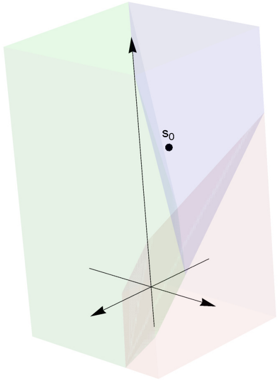
Orbits of linear dynamical systems

linear transformation: $\mathbf{M} \in \mathbb{Q}^{d \times d}$
starting point: $s_0 \in \mathbb{Q}^d$



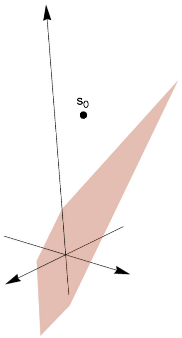
From orbits to symbolic trajectories

Partition $\mathbb{R}^d$ into



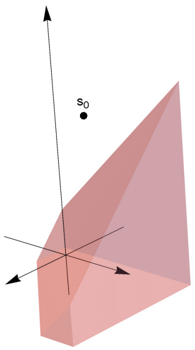
From orbits to symbolic trajectories

Partition $\mathbb{R}^d$ into S_1



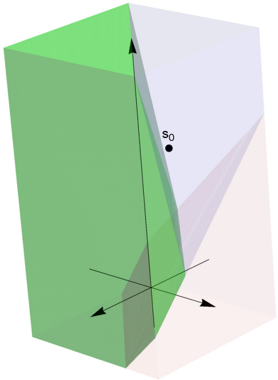
From orbits to symbolic trajectories

Partition $\mathbb{R}^d$ into S_1, S_2



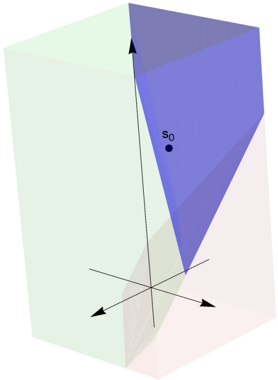
From orbits to symbolic trajectories

Partition $\mathbb{R}^d$ into S_1, S_2, S_3



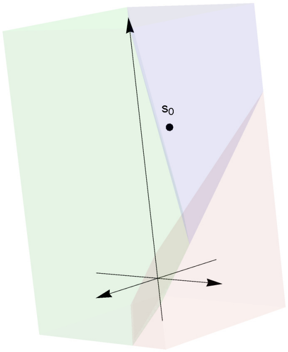
From orbits to symbolic trajectories

Partition $\mathbb{R}^d$ into S_1, S_2, S_3, S_4



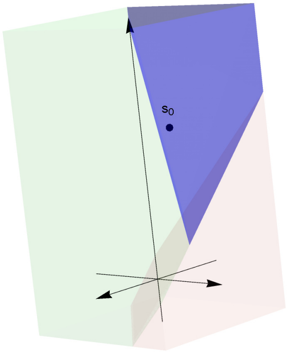
From orbits to symbolic trajectories

Partition $\mathbb{R}^d$ into S_1, S_2, S_3, S_4



From orbits to symbolic trajectories

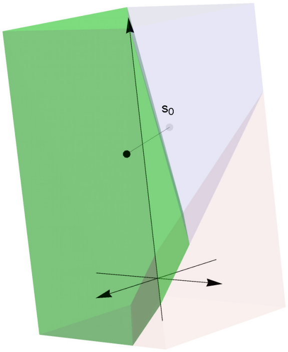
Partition $\mathbb{R}^d$ into S_1, S_2, S_3, S_4



$w=$●

From orbits to symbolic trajectories

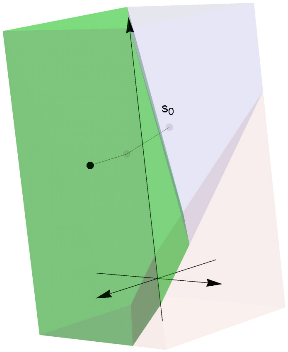
Partition $\mathbb{R}^d$ into S_1, S_2, S_3, S_4



$w=$

From orbits to symbolic trajectories

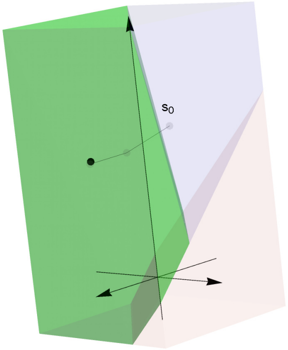
Partition $\mathbb{R}^d$ into S_1, S_2, S_3, S_4



$w =$

From orbits to symbolic trajectories

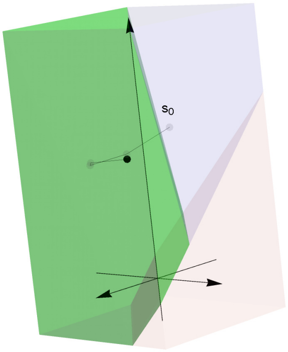
Partition $\mathbb{R}^d$ into S_1, S_2, S_3, S_4



$w=$ 

From orbits to symbolic trajectories

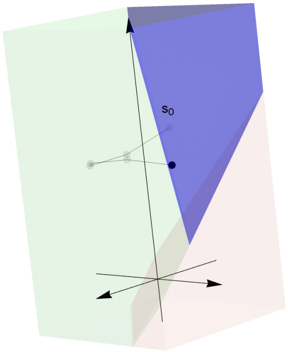
Partition $\mathbb{R}^d$ into S_1, S_2, S_3, S_4



$w =$ 

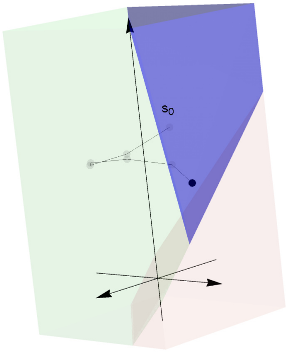
From orbits to symbolic trajectories

Partition $\mathbb{R}^d$ into S_1, S_2, S_3, S_4



From orbits to symbolic trajectories

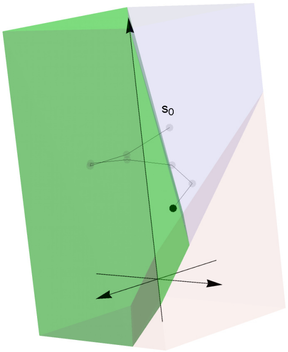
Partition $\mathbb{R}^d$ into S_1, S_2, S_3, S_4



$w=$ 

From orbits to symbolic trajectories

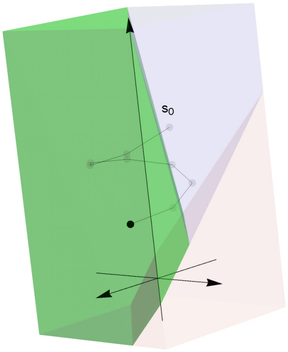
Partition $\mathbb{R}^d$ into S_1, S_2, S_3, S_4



$w=$ 

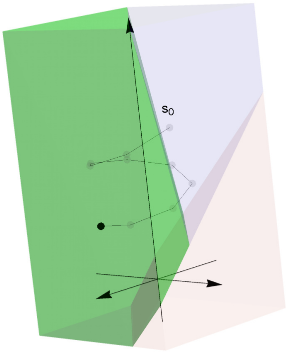
From orbits to symbolic trajectories

Partition $\mathbb{R}^d$ into S_1, S_2, S_3, S_4



From orbits to symbolic trajectories

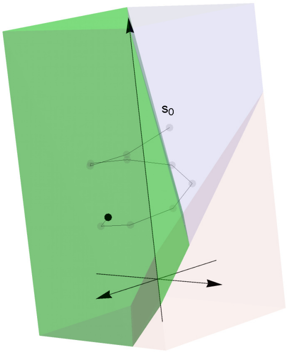
Partition $\mathbb{R}^d$ into S_1, S_2, S_3, S_4




$w=$

From orbits to symbolic trajectories

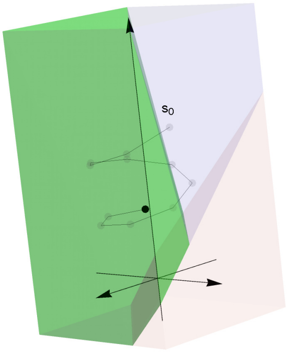
Partition $\mathbb{R}^d$ into S_1, S_2, S_3, S_4



$w =$ 

From orbits to symbolic trajectories

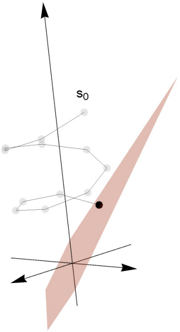
Partition $\mathbb{R}^d$ into S_1, S_2, S_3, S_4



$w =$

From orbits to symbolic trajectories

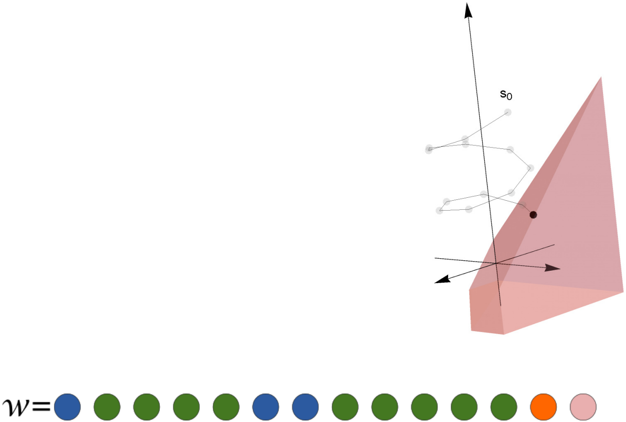
Partition $\mathbb{R}^d$ into S_1, S_2, S_3, S_4



$w=$ 

From orbits to symbolic trajectories

Partition $\mathbb{R}^d$ into S_1, S_2, S_3, S_4



The algorithmic analysis of linear dynamical systems

$w=$ 

The algorithmic analysis of linear dynamical systems

$\mathcal{W}=$ 

The Trace-Checking Problem

Instance: A word $\mathcal{W}$ and a specification Φ

Question: Does $\mathcal{W} \models \Phi$?

The algorithmic analysis of linear dynamical systems

$\mathcal{W} =$ 

The Trace-Checking Problem

Instance: A word $\mathcal{W}$ and a specification Φ

Question: Does $\mathcal{W} \models \Phi$?

The Model-Checking Problem

Instance: A system $\mathcal{S}$ and a specification Φ

Question: Does $\mathcal{W} \models \Phi$ for all $\mathcal{W}$ in $\mathcal{S}$?

The algorithmic analysis of linear dynamical systems

$\mathcal{W}=$ 

The Trace-Checking Problem

Instance: A word $\mathcal{W}$ and a specification Φ

Question: Does $\mathcal{W} \models \Phi$?

The Model-Checking Problem

Instance: A system $\mathcal{S}$ and a specification Φ

Question: Does $\mathcal{W} \models \Phi$ for all $\mathcal{W}$ in $\mathcal{S}$?

The Satisfiability Problem

Instance: A specification Φ

Question: Is there some $\mathcal{W}$ satisfying Φ?

Hallo iedereen!

Lucas Pannier

Laboratoire de Mathématiques de Versailles, UVSQ
CNRS UMR-8100

1^{st} year PhD student coadvised by Lucia Di Vizio and Alin Bostan.

Algebraicity and Differential Equations

Problem

Given a linear differential equation, decide if its solutions are algebraic.

Algebraicity and Differential Equations

Problem

Given a linear differential equation, decide if its solutions are algebraic.

Grothendieck's p-curvature conjecture

All solutions of an LDE are algebraic if and only if almost all its p-curvatures vanish.

Algebraicity and Differential Equations

Problem

Given a linear differential equation, decide if its solutions are algebraic.

Grothendieck's p-curvature conjecture

All solutions of an LDE are algebraic if and only if almost all its p-curvatures vanish.

Theorem (Kronecker, 1880)

A polynomial $f \in \mathbb{Q}[x]$ splits completely over $\mathbb{Q}$ if and only if for almost all primes p, $f \bmod p$ splits completely over $\mathbb{F}_p$.

An Effective version of Kronecker's Theorem

Theorem (Chudnovsky^2, 1985; Fürnsinn-P., 2025+)

Let $f \in \mathbb{Z}[x]$ with leading coefficient $\Delta \in \mathbb{Z}$. Let $B \in \mathbb{R}$ be an upper bound on the modulus of all complex roots of f.
Then f splits completely over $\mathbb{Q}$ if and only if $f \bmod p$ splits completely over $\mathbb{F}_p$ for all primes p not dividing Δ and at most $90B\Delta^6\log(\Delta)^6$.

Computing Mahler measures of polynomials

Berend Ringeling (Université de Montréal)
b.j.ringeling@gmail.com

July 14, 2025

Mahler measure

The *logarithmic Mahler measure* is defined as

$$\mathrm{m}(P) := \frac{1}{(2\pi i)^r} \int_{\mathbb{T}^r} \log |P(x_1, \ldots, x_r)| \frac{\mathrm{d}x_1}{x_1} \cdots \frac{\mathrm{d}x_r}{x_r}. \qquad (1)$$

Mahler measure

The *logarithmic Mahler measure* is defined as

$$\mathrm{m}(P) := \frac{1}{(2\pi i)^r} \int_{\mathbb{T}^r} \log |P(x_1, \ldots, x_r)| \, \frac{\mathrm{d}x_1}{x_1} \cdots \frac{\mathrm{d}x_r}{x_r}. \tag{1}$$

Examples (Smyth, 1981):

$$\mathrm{m}(1+x+y) = \frac{3\sqrt{3}}{4\pi} L(\chi_{-3}, 2) \quad \text{and} \quad \mathrm{m}(1+x+y+z) = \frac{7\zeta(3)}{2\pi^2},$$

(where $\chi_{-3} = \left(\frac{-3}{n}\right)$ is the quadratic character modulo 3).

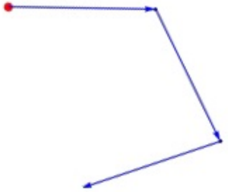
Probabilistic interpretation of $Z(P; s)$

The Mahler measure is the log-expected value of the random variable $|P(X_1, \ldots, X_r)|$, where $X_1, \ldots, X_r$ are independent and uniformly distributed random variables on the complex unit circle $\{z \in \mathbb{C} \colon |z| = 1\}$.

Probabilistic interpretation of $Z(P;s)$

The Mahler measure is the log-expected value of the random variable $|P(X_1,\ldots,X_r)|$, where $X_1,\ldots,X_r$ are independent and uniformly distributed random variables on the complex unit circle $\{z \in \mathbb{C} \colon |z| = 1\}$.

Example: $P(x,y) = 1 + x + y$.

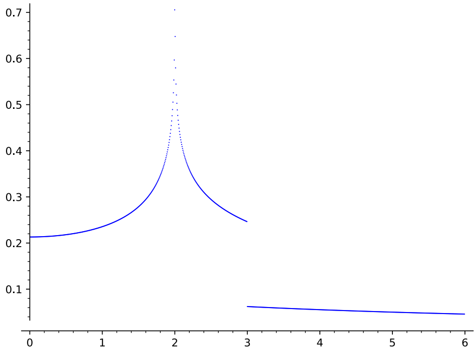


Probability density

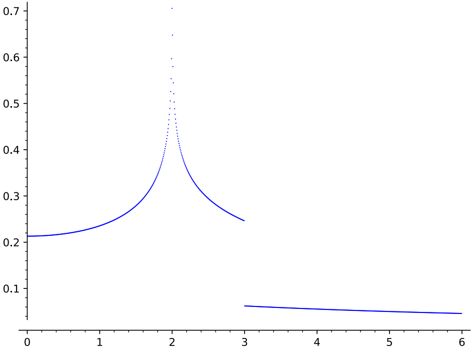
Since $|P(X_1, \ldots, X_r)|$ is a random variable, we can compute the probability density $q(x)$ and compute the Mahler measure using this!

$$\mathrm{m}(P) = \int_0^\infty \log(x) q(x) \, \mathrm{d}x.$$

These densities $q(x)$ look really cool! For example
$P = x + 1/x + y + 1/y + x/y + y/x$.



These densities $q(x)$ look really cool! For example $P = x + 1/x + y + 1/y + x/y + y/x$.



Using the differential equation for this density, one can compute Mahler measure

$$m(z + P(x, y)) = 0.6439432099\ldots.$$

Mahler measure, Class numbers, Zero-free regions, and Quadratic forms

Subham Roy

Department of Algebra (UFOCLAN group)
Charles University, Prague

Interests

My research interests lie in number theory, and include:

- Mahler measure of rational functions, $\mathrm{m}(P)$: the mean of $\log|P|$ restricted to the n-torus $\mathbb{T}^n = \{(z_j)_{j=1}^n \in (\mathbb{C}^*)^n : |z_j| = 1\}$ (with respect to the (unique) Haar measure).
    - Its relation with the special values of L-functions, and different generalizations of Mahler measure (e.g., by changing the domain, by changing the base field, etc.).
- elliptic curves and surfaces, heights.
- Class numbers of real quadratics, simple cubics, and their distribution, continued fractions.
- Solutions of polynomial equations in roots of unity.
- Universal quadratic forms over number fields.
- Zero-free region of Dirichlet L-functions.

Research works

- **Mahler measure**
  - On quantifying the effect of deforming the torus on the Mahler measure for a large family of Laurent polynomials in arbitrarily many variables—under certain conditions—including $x + \frac{1}{x} + y + \frac{1}{y} + k$.
  - (joint with Matilde Lalín, Siva Sankar Nair, Berend Ringeling) On investigating the effect of replacing the torus with unit discs on the Mahler measure for specific families of polynomials.
- (Ongoing) On the distribution of number fields in certain families with large class numbers.
- (Ongoing) On improving the zero-free region of Dirichlet L-functions for large moduli.

Multiple t-values: some arithmetic questions

Biswajyoti Saha

Indian Institute of Technology Delhi, New Delhi

Recurrence, transcendence, and Diophantine approximation

Multiple zeta values

- Multiple zeta values: For positive integers a_i with $a_1 \geq 2$,

$$\zeta(a_1, \ldots, a_r) := \sum_{n_1 > \cdots > n_r > 0} n_1^{-a_1} \cdots n_r^{-a_r}.$$

- Weight: The sum $a_1 + \cdots + a_r$ is called the weight of $\zeta(a_1, \ldots, a_r)$.
- Weight k vector space: Let $\mathcal{Z}_0 = \mathbb{Q}$, $\mathcal{Z}_1 = \{0\}$ and for $k \geq 2$,

$$\mathcal{Z}_k := \mathbb{Q}\langle \zeta(a_1, \ldots, a_r) : a_1 + \cdots + a_r = k, a_i \geq 1, a_1 \geq 2 \rangle.$$

- **Conjecture** (Zagier): Let $d_0 = d_2 = 1, d_1 = 0$ and $d_k = d_{k-2} + d_{k-3}$ for $k \geq 3$. Then $\dim_{\mathbb{Q}} \mathcal{Z}_k = d_k$.
- Terasoma & Deligne-Goncharov: $\dim_{\mathbb{Q}} \mathcal{Z}_k \leq d_k$.
- **Conjecture** (Hoffman): For $k \geq 2$, the set $\mathcal{B}_k$ is a $\mathbb{Q}$-basis of $\mathcal{Z}_k$, where

$$\mathcal{B}_k := \{\zeta(a_1, \ldots, a_r) : a_1 + \cdots + a_r = k, a_i \in \{2, 3\}, 1 \leq r \leq k - 1\}.$$

- Brown: $\mathcal{B}_k$ is a generating set.
- **Open question**: Linear independence.

Extending the setup: Multiple t-values

- Let $a_1, \dots, a_r$ be positive integers, $a_1 \geq 2$. Define (due to Hoffman)

$$t(a_1, \dots, a_r) := \sum_{n_1 > \cdots > n_r > 0,\ n_i \text{ odd}} n_1^{-a_1} \cdots n_r^{-a_r}.$$

- $r = 1$ case (Nielsen): $t(a) = \sum_{n \geq 1} (2n-1)^{-a} = (1 - 2^{-a})\zeta(a)$.
- Set $\mathcal{T}_0 = \mathbb{Q}$, $\mathcal{T}_1 = \{0\}$ and for an integer $k \geq 2$,

$$\mathcal{T}_k := \mathbb{Q}\langle t(a_1, \dots, a_r) : a_1 + \cdots + a_r = k, a_i \geq 1, a_1 \geq 2 \rangle.$$

- Murakami: For $k \geq 0$, $\mathcal{Z}_k \subseteq \mathcal{T}_k$.
- **Conjecture** (Hoffman): For $k \geq 4$, $\dim_{\mathbb{Q}} \mathcal{T}_k$ satisfies the recurrence relation $f_k = f_{k-1} + f_{k-2}$ with initial values $f_2 = 1, f_3 = 2$.
- **Conjecture** (BS): For $k \geq 2$, the set $\mathcal{C}_k$ is a $\mathbb{Q}$-basis of $\mathcal{T}_k$, where

$$\mathcal{C}_k := \{ t(a_1 + 1, a_2, \dots, a_r) : a_1 + \cdots + a_r = k - 1, a_i \in \{1, 2\} \}.$$

- Partial result due to Charlton, but analogue of Brown's theorem is still elusive.

Arithmetic nature of the special values of the incomplete beta function

Dr. Ekata Saha
Assistant Professor

Indian Institute Technology Delhi, New Delhi

Recurrence, transcendence, and Diophantine approximation

Beta function

- For $a, b > 0$,

$$\mathrm{B}(a,b) = \int_0^1 t^{a-1}(1-t)^{b-1}\,\mathrm{d}t.$$

  It converges for $a, b \in \mathbb{C}$ such that $\Re(a), \Re(b) > 0$.

- Relation with the gamma function:

$$\mathrm{B}(a,b) = \frac{\Gamma(a)\,\Gamma(b)}{\Gamma(a+b)}.$$

- Special values (trivial cases):
  - $a \in \mathbb{Z}$ (or $b \in \mathbb{Z}$).
  - Let $a, b \in \mathbb{Q} \setminus \mathbb{Z}$. If $a + b \leq 0$ is an integer, then $\mathrm{B}(a,b) = 0$. If $a + b \in \mathbb{N}$, then $\mathrm{B}(a,b)$ is a non-zero algebraic multiple of π.

Theorem (Schneider)

For $a, b \in \mathbb{Q} \setminus \mathbb{Z}$ such that $a + b \notin \mathbb{Z}$, $\mathrm{B}(a,b)$ is transcendental.

Incomplete beta function

- For $a, b > 0$ and $0 < x < 1$,

$$\mathrm{B}_x(a,b) := \int_0^x t^{a-1}(1-t)^{b-1}\mathrm{d}t.$$

- As $x < 1$, we can take $b \in \mathbb{R}$. In fact, we can extend the definition of the incomplete beta function for $a, b \in \mathbb{C}$ with $\Re(a) > 0$.

$$\begin{aligned}\mathrm{B}_x(a,b) &= \frac{x^a}{a}\ {}_2F_1(a, 1-b; a+1; x) \\ &= \frac{x^a(1-x)^{b-1}}{a}\ {}_2F_1\left(1-b, 1; a+1; \frac{x}{x-1}\right).\end{aligned}$$

Special values of the incomplete beta function

Joint work with S. Dhillon

Let x be an algebraic number.

- Trivial cases:
  - $a \in \mathbb{N}$ and b algebraic.
  - $b \in \mathbb{N}$ and a algebraic.
  - $a > 0$ algebraic such that $a + b \leq 0$ an integer.
  - Proof essentially uses Gelfond–Schneider theorem.
- (Not-so)-trivial cases:
  - $a \in \mathbb{Q} \setminus \mathbb{N}$ positive and $b \leq 0$ an integer.
  - $a \in \mathbb{Q} \setminus \mathbb{N}$ positive such that $a + b \in \mathbb{N}$.
  - Proof requires to view the special values as linear forms in logarithms of algebraic numbers. Hence we can use Baker's theory and some of its manifestations.
- Open question: Analogue of Schneider's theorem.

Special values of the incomplete beta function

Joint work with S. Dhillon

Let x be an algebraic number.

- Trivial cases:
  - $a \in \mathbb{N}$ and b algebraic.
  - $b \in \mathbb{N}$ and a algebraic.
  - $a > 0$ algebraic such that $a + b \leq 0$ an integer.
  - Proof essentially uses Gelfond–Schneider theorem.
- (Not-so)-trivial cases:
  - $a \in \mathbb{Q} \setminus \mathbb{N}$ positive and $b \leq 0$ an integer.
  - $a \in \mathbb{Q} \setminus \mathbb{N}$ positive such that $a + b \in \mathbb{N}$.
  - Proof requires to view the special values as linear forms in logarithms of algebraic numbers. Hence we can use Baker's theory and some of its manifestations.
- Open question: Analogue of Schneider's theorem.

Thank you for your attention!

Speed Talks

Satyabrat Sahoo

Yau Mathematical Sciences Center (YMSC), Tsinghua University

Recurrence, transcendence, and Diophantine approximation

July 14, 2025

Generalized Fermat equation

- Consider the generalized Fermat equation

$$Ax^p + By^q + Cz^r = 0, \text{ where } A, B, C, p, q, r \in \mathbb{Z} \setminus \{0\} \quad (0.1)$$

with A, B, C are coprime and $p, q, r \geq 2$ with $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$. We say (p, q, r) as the signature of the equation (0.1).

Generalized Fermat equation

- Consider the generalized Fermat equation

$$Ax^p + By^q + Cz^r = 0, \text{ where } A, B, C, p, q, r \in \mathbb{Z} \setminus \{0\} \tag{0.1}$$

  with A, B, C are coprime and $p, q, r \geq 2$ with $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$. We say (p, q, r) as the signature of the equation (0.1).
- I am working mainly on studying the asymptotic solution of the generalized Fermat equation (0.1) of signature (p, p, p), $(p, p, 2)$, $(p, p, 3)$ and (r, r, p).

Generalized Fermat equation

- Consider the generalized Fermat equation

$$Ax^p + By^q + Cz^r = 0, \text{ where } A, B, C, p, q, r \in \mathbb{Z} \setminus \{0\} \quad (0.1)$$

with A, B, C are coprime and $p, q, r \geq 2$ with $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$. We say (p, q, r) as the signature of the equation (0.1).

- I am working mainly on studying the asymptotic solution of the generalized Fermat equation (0.1) of signature (p, p, p), $(p, p, 2)$, $(p, p, 3)$ and (r, r, p).

Theorem (S. 2024)

Let K be a totally real number field. Let $A, B, C \in \mathcal{O}_K \setminus \{0\}$ and let S'_K be the set of all non-zero prime ideals of $\mathcal{O}_K$ with $\mathfrak{P} | 2ABC$.

Generalized Fermat equation

- Consider the generalized Fermat equation

$$Ax^p + By^q + Cz^r = 0, \text{ where } A, B, C, p, q, r \in \mathbb{Z} \setminus \{0\} \tag{0.1}$$

with A, B, C are coprime and $p, q, r \geq 2$ with $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$. We say (p, q, r) as the signature of the equation (0.1).

- I am working mainly on studying the asymptotic solution of the generalized Fermat equation (0.1) of signature (p, p, p), $(p, p, 2)$, $(p, p, 3)$ and (r, r, p).

Theorem (S. 2024)

Let K be a totally real number field. Let $A, B, C \in \mathcal{O}_K \setminus \{0\}$ and let S'_K be the set of all non-zero prime ideals of $\mathcal{O}_K$ with $\mathfrak{P} | 2ABC$. Suppose, for every solution (λ, μ) to the S'_K-unit equation

$$\lambda + \mu = 1, \ \lambda, \mu \in \mathcal{O}^*_{S'_K},$$

Generalized Fermat equation

- Consider the generalized Fermat equation

$$Ax^p + By^q + Cz^r = 0, \text{ where } A, B, C, p, q, r \in \mathbb{Z} \setminus \{0\} \tag{0.1}$$

with A, B, C are coprime and $p, q, r \geq 2$ with $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$. We say (p, q, r) as the signature of the equation (0.1).

- I am working mainly on studying the asymptotic solution of the generalized Fermat equation (0.1) of signature (p, p, p), $(p, p, 2)$, $(p, p, 3)$ and (r, r, p).

Theorem (S. 2024)

Let K be a totally real number field. Let $A, B, C \in \mathcal{O}_K \setminus \{0\}$ and let S'_K be the set of all non-zero prime ideals of $\mathcal{O}_K$ with $\mathfrak{P} | 2ABC$. Suppose, for every solution (λ, μ) to the S'_K-unit equation

$$\lambda + \mu = 1, \ \lambda, \mu \in \mathcal{O}^*_{S'_K},$$

there exists some prime $\mathfrak{P}$ of $\mathcal{O}_K$ with $\mathfrak{P}|2$ that satisfies

$$\max\{|v_{\mathfrak{P}}(\lambda)|, |v_{\mathfrak{P}}(\mu)|\} \leq 4v_{\mathfrak{P}}(2).$$

Generalized Fermat equation

- Consider the generalized Fermat equation

$$Ax^p + By^q + Cz^r = 0, \text{ where } A, B, C, p, q, r \in \mathbb{Z} \setminus \{0\} \qquad (0.1)$$

  with A, B, C are coprime and $p, q, r \geq 2$ with $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$. We say (p, q, r) as the signature of the equation (0.1).
- I am working mainly on studying the asymptotic solution of the generalized Fermat equation (0.1) of signature (p, p, p), $(p, p, 2)$, $(p, p, 3)$ and (r, r, p).

Theorem (S. 2024)

Let K be a totally real number field. Let $A, B, C \in \mathcal{O}_K \setminus \{0\}$ and let S'_K be the set of all non-zero prime ideals of $\mathcal{O}_K$ with $\mathfrak{P} | 2ABC$. Suppose, for every solution (λ, μ) to the S'_K-unit equation

$$\lambda + \mu = 1, \ \lambda, \mu \in \mathcal{O}^*_{S'_K},$$

there exists some prime $\mathfrak{P}$ of $\mathcal{O}_K$ with $\mathfrak{P} | 2$ that satisfies

$$\max \{|v_{\mathfrak{P}}(\lambda)|, |v_{\mathfrak{P}}(\mu)|\} \leq 4 v_{\mathfrak{P}}(2).$$

Then $Ax^p + By^p = Cz^p$ has no asymptotic solution $(a, b, c) \in \mathcal{O}^3_K$ with $2 | abc$.

Lehmer-type bounds

- Let K denote a number field and A/K denote an abelian variety defined over K.

Lehmer-type bounds

- Let K denote a number field and A/K denote an abelian variety defined over K.
- Let $\mathcal{L}$ be a symmetric ample line bundle on A and let $\hat{h}_{\mathcal{L}}$ be the Néron-Tate height on $A(\overline{K})$ associated with $\mathcal{L}$.

Lehmer-type bounds

- Let K denote a number field and A/K denote an abelian variety defined over K.
- Let $\mathcal{L}$ be a symmetric ample line bundle on A and let $\hat{h}_{\mathcal{L}}$ be the Néron-Tate height on $A(\overline{K})$ associated with $\mathcal{L}$.

Conjecture (Lehmer's conjecture)

There exists a constant $C > 0$ such that

$$\hat{h}_{\mathcal{L}}(P) \geq \frac{C}{D^{(1/g(P))}}$$

for all non-torsion points $P \in A(\overline{K})$, where $D := [K(P) : K]$ and $g(P)$ denotes the dimension of the smallest algebraic subgroup of A containing P.

Lehmer-type bounds

- Let K denote a number field and A/K denote an abelian variety defined over K.
- Let $\mathcal{L}$ be a symmetric ample line bundle on A and let $\hat{h}_{\mathcal{L}}$ be the Néron-Tate height on $A(\overline{K})$ associated with $\mathcal{L}$.

Conjecture (Lehmer's conjecture)

There exists a constant $C > 0$ such that

$$\hat{h}_{\mathcal{L}}(P) \geq \frac{C}{D^{(1/g(P))}}$$

for all non-torsion points $P \in A(\overline{K})$, where $D := [K(P) : K]$ and $g(P)$ denotes the dimension of the smallest algebraic subgroup of A containing P.

Theorem (Kumar-S. 2024)

1. $\hat{h}_{\mathcal{L}}(P) \geq \frac{C}{(\mathbf{D} \log \mathbf{D})^{\mathbf{2g}}}$;
2. For any $\epsilon > 0$, $\hat{h}_{\mathcal{L}}(P) \geq \frac{C}{\mathbf{D}^{\mathbf{2g}+\epsilon}}$,

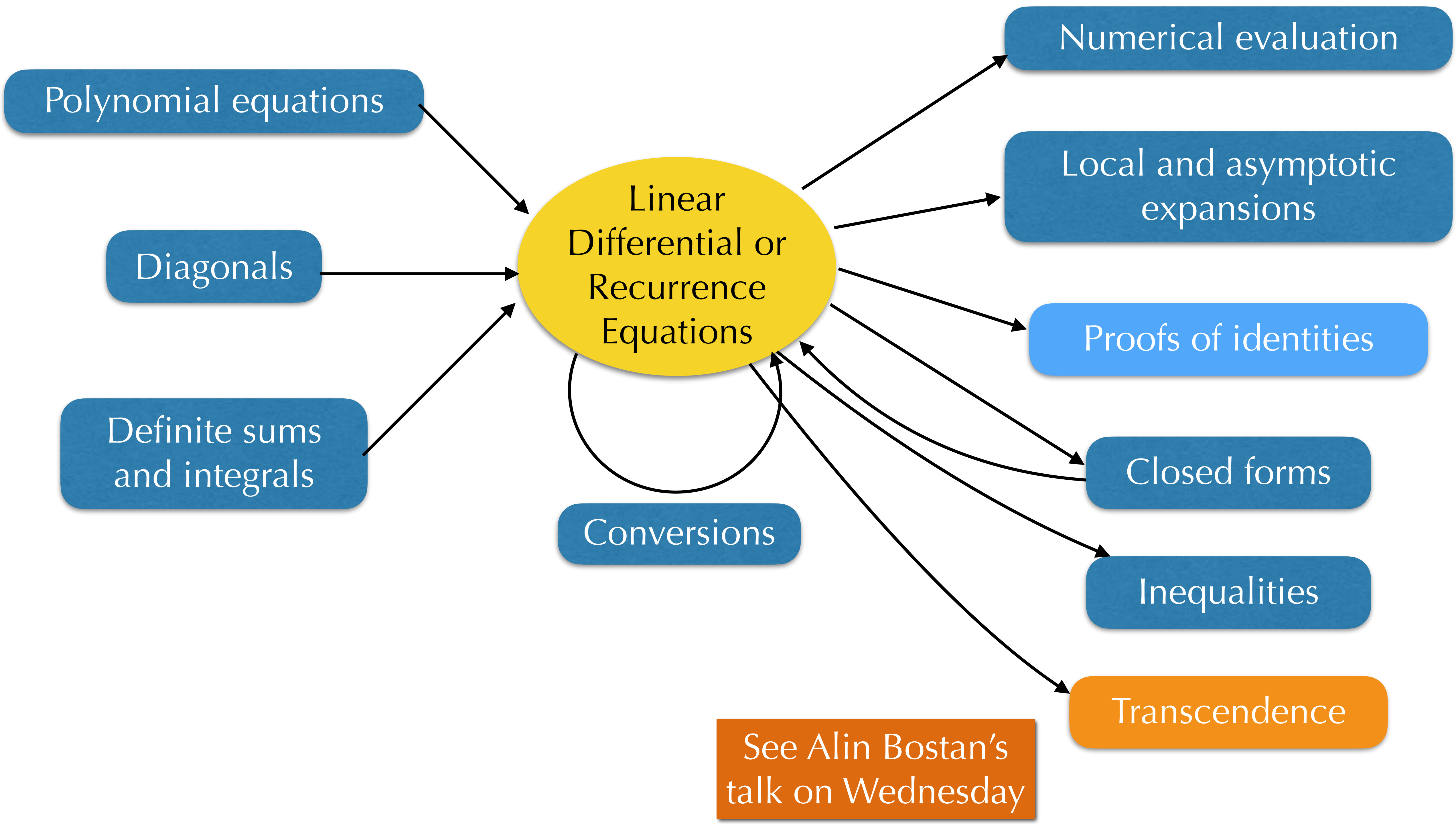
for all non-torsion points $P \in A(\overline{K})$ with $K(P)$ is a Galois extension of degree D over K.

Bruno Salvy

Inria at ENS de Lyon (France)

Main interest: Computer Algebra

LDE/LREs as Data-Structures



Work Related to the Workshop (1/2)

Transcendental solutions of LDE

```
> L:=[seq(add(binomial(n,k)^2*binomial(n+k,k)^2,k=0..n),n=0..30)]:
> deq:=gfun:-listtodiffeq(L,y(z),[ogf])[1];
```

$$\mathrm{deq} := \{ \left(z-5\right) y(z) + \left(7z^2 - 112z + 1\right) y'(z) + \left(6z^3 - 153z^2 + 3z\right) y''(z) + \left(z^4 - 34z^3 + z^2\right) y'''(z), y(0) = 1, y'(0) = 5, y''(0) = 146 \}$$

```
> istranscendental(deq,y(z));
```

true, "multiple root of multiplicity 3 of the indicial equation ==> ln at 0"

Joint work with
Alin Bostan & Michael Singer

Work Related to the Workshop (2/2)

Algebraic values of E-functions

```
> deq:=gfun:-holexprtodiffeq(diff(BesselJ(0,z),z$4),y(z));
```

$$\text{deq} := \left\{ \left(z^{11} - 12z^9 + 54z^7 - 108z^5 + 81z^3\right) y^{(4)}(z) + \cdots \right.$$

$$\left. +(z^{11} - 12z^9 + 54z^7 + 36z^5 + 945z^3 + 6480z)y(z), y(0) = \frac{3}{8} \right\}$$

```
> algvalues(deq,y(z));
```

$$\{y(\mathrm{RootOf}(Z^2 - 3)) = 0\}$$

Meaning:
$J_0^{(4)}(\pm\sqrt{3}) = 0$

Joint work with
Alin Bostan & Tanguy Rivoal

Periods, Heights, and Transcendence

Emre Can Sertöz

July 2025

Who I Am

- Assistant professor at Leiden University, since 2023.

Who I Am

- Assistant professor at Leiden University, since 2023.
- PhD (2017): Humboldt University of Berlin
  Enumerative Geometry of Double Spin Curves

Who I Am

- Assistant professor at Leiden University, since 2023.
- PhD (2017): Humboldt University of Berlin
  Enumerative Geometry of Double Spin Curves
- My research lies at the interface of algebraic geometry and transcendence theory, with a focus on developing effective methods.

Recent Projects

- **Effective transcendence of single variable integrals**
  (w/ Ouaknine and Worrell, following Huber and Wüstholz)
  An explicit algorithm to compute $\overline{\mathbb{Q}}$-linear relations between 1-periods. Gives transcendence results methodically.

Recent Projects

- **Effective transcendence of single variable integrals** (w/ Ouaknine and Worrell, following Huber and Wüstholz) An explicit algorithm to compute $\overline{\mathbb{Q}}$-linear relations between 1-periods. Gives transcendence results methodically.
- **Separation bounds for K3 periods** (with Pierre Lairez) For instance, we can prove that the Liouville-type number

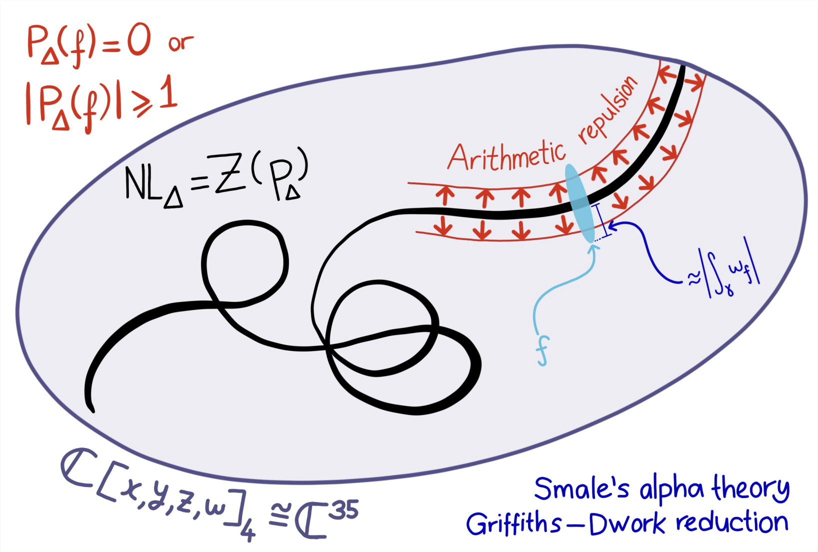
$$\sum_{n \geq 0} (2 \uparrow\uparrow 3n)^{-1}$$

is not the ratio of two periods of a quartic K3 over $\overline{\mathbb{Q}}$.

Recent Projects

- **Effective transcendence of single variable integrals**
  (w/ Ouaknine and Worrell, following Huber and Wüstholz)
  An explicit algorithm to compute $\overline{\mathbb{Q}}$-linear relations between 1-periods. Gives transcendence results methodically.
- **Separation bounds for K3 periods** (with Pierre Lairez)
  For instance, we can prove that the Liouville-type number
  $$\sum_{n \geq 0} (2 \uparrow\uparrow 3n)^{-1}$$
  is not the ratio of two periods of a quartic K3 over $\overline{\mathbb{Q}}$.
- **Arithmetic of limit periods**
  (with Spencer Bloch and Robin de Jong)
  We relate limit periods in degenerating families to Néron–Tate and Bloch–Beilinson heights.

Separating periods of K3s using moduli spaces



Math Stuff that I Enjoy

Joe Silverman

Brown University

Leiden Speed Talk

14 July 2025

Who Am I?: Faculty at Brown University (RI, USA) since 1988. PhD Harvard (1982) w/John Tate.

Mathematical Interests:

- Arithmetic geometry, especially rational and integral points on (elliptic) curves and surfaces.
- Arithmetic dynamics.
- (Dabble in) cryptography.

Some Favorite Math, Both Old and New

- (w/ H. Pasten) **Conjecture/Theorem** (New '23): For

$$f : X \to X \text{ and } X(K) \text{ is Zariski dense,}$$

there should be "lots" of "widely spaced" f-orbits. True for various (X, f). [Details later!]

Some Favorite Math, Both Old and New

- (w/ H. Pasten) **Conj./Thm.** Orbit spacing. . .

- **Project** (New '25) Dynamics of **Folding Maps**. Study the commuting familys of polynomial maps

$$F_{\mathcal{L},n} : \mathbb{A}^N \to \mathbb{A}^N$$

coming from quotients by the Weyl group of Cartan subalgebras of a Lie algebra $\mathcal{L}$.

Some Favorite Math, Both Old and New

- (w/ H. Pasten) **Conj./Thm.** Orbit spacing...

- **Project** Folding Maps...

- (w/ J.H. Evertse) **Theorem** (Old '86) With suitable defs and hypotheses:

$$\#\left\{(x,y) \in R_S : y^n = f(x)\right\} \le 17^{[L:K](6[K:\mathbb{Q}]+\#S)} \cdot n^{2[L:K]\#S+\operatorname{rank}_n \mathcal{H}_L}.$$

Some Favorite Math, Both Old and New

- (w/ H. Pasten) **Conj./Thm.** Orbit spacing...

- **Project** Folding Maps...

- (w/ J.H. Evertse) **Theorem** $\#V(R_S, f, n) \leq \cdots$

- (w/ J. Hoffstein, J. Pipher) **Invention** (Old '98) Construction of NTRU, the first practical public key cryptosystem whose security relies on the difficulty of solving hard lattice problems (CVP).

Some Favorite Math, Both Old and New

- (w/ H. Pasten) **Conj./Thm.** Orbit spacing. . .

- **Project** Folding Maps. . .

- (w/ J.H. Evertse) **Theorem** $\#V(R_S, f, n) \le \cdots$

- (w/ J. Hoffstein, J. Pipher) **Invention** NTRU. . .

Some Non-Mathematical Interests: Theatre (both attending and performing), poker and duplicate bridge, and last (but far from least!) grandchildren.

Some Favorite Math, Both Old and New

- (w/ H. Pasten) **Conj./Thm.** Orbit spacing...

- **Project** Folding Maps...

- (w/ J.H. Evertse) **Theorem** $\#V(R_S, f, n) \le \cdots$

- (w/ J. Hoffstein, J. Pipher) **Invention** NTRU...

Some Non-Mathematical Interests: Theatre (both attending and performing), poker and duplicate bridge, and last (but far from least!) grandchildren.

Thank you for your attention

Marco Streng – Speed talk

name: Marco Streng

affiliation: Leiden University

favourite recurrence relation:

Marco Streng – Speed talk

name: Marco Streng

affiliation: Leiden University

favourite recurrence relation:

$$B_{k+l+m}B_{k-l}B_{n+m}B_n + B_{l+n+m}B_{l-n}B_{k+m}B_k + B_{n+k+m}B_{n-k}B_{l+m}B_l = 0$$

Marco Streng – Speed talk

name: Marco Streng

affiliation: Leiden University

favourite recurrence relation:

$$B_{k+l+m}B_{k-l}B_{n+m}B_n + B_{l+n+m}B_{l-n}B_{k+m}B_k + B_{n+k+m}B_{n-k}B_{l+m}B_l = 0$$

- elliptic divisibility sequences,
- also $[n]P = \left(\frac{A_n}{B_n^2}, \frac{C_n}{B_n^3}\right)$,
- my results in this area:
  - primitive prime divisors even for $n \in \mathrm{End}(E)$,
  - results for B_n in function fields (with Ingram-Mahé-Silverman-Stange / with Naskręcki),
  - sharper lower bounds on heights of points on elliptic curves over function fields (with Naskręcki, in progress).

What else?

Explicit and computation methods related to curves and abelian varieties, and their moduli spaces.

E.g.

- reconstructing algebraic curves from their periods (complex analytically),
- creating tables of curves wose Jacobians have complex multiplication (CM),
- bounding their primes of bad reduction,
- using them for explicit class field theory.

(with various others, see my web page)

`www.math.leidenuniv.nl/~streng`

Lola Thompson

Associate Professor

Universiteit Utrecht

Key Words: multiplicative number theory, anatomy of integers, sieve methods, distribution of values of arithmetic functions, statistical questions about arithmetic objects, applications of analytic number theory to problems in spectral geometry, Salem numbers, algorithmic questions.

Recent research themes

- Let $s(n)$ be the sum of proper divisors function. For sets of integers $\mathcal{A}$ with asymptotic density 0, what can we say about $\#s^{-1}(\mathcal{A})$?

www.lolathompson.com

Recent research themes

- Let $s(n)$ be the sum of proper divisors function. For sets of integers $\mathcal{A}$ with asymptotic density 0, what can we say about $\#s^{-1}(\mathcal{A})$?
- How can we calculate the sum of $f(n)$ for arithmetic functions f and integers $n \leq x$ using as little time and space as possible?

www.lolathompson.com

Recent research themes

- Let $s(n)$ be the sum of proper divisors function. For sets of integers $\mathcal{A}$ with asymptotic density 0, what can we say about $\#s^{-1}(\mathcal{A})$?
- How can we calculate the sum of $f(n)$ for arithmetic functions f and integers $n \leq x$ using as little time and space as possible?
- What proportion of Salem numbers of degree up to N are realized by a classical arithmetic hyperbolic lattice of a given dimension defined over $\mathbb{Q}$? What does this tell us about the lengths of geodesics on certain arithmetic, hyperbolic orbifolds?

www.lolathompson.com

Overview of current research

Riccardo Tosi

University of Duisburg-Essen

14.07.2025

Irrationality proofs for zeta values

- Irrationality proofs.
- Zeta values and multiple zeta values:

$$\zeta(s_1, \ldots, s_r) = \sum_{1 \leq n_1 < \cdots < n_r} \frac{1}{n_1^{s_1} \ldots n_r^{s_r}}$$

  for $s_1, \ldots, s_r \in \mathbb{Z}_{\geq 1}$, $s_r \geq 2$.
- Multiple polylogarithms.
- Hyperplane arrangements and their periods.
- Mixed Tate motives.

Irrationality proofs for zeta values

- Irrationality proofs.
- Zeta values and multiple zeta values:

$$\zeta(s_1, \ldots, s_r) = \sum_{1 \le n_1 < \cdots < n_r} \frac{1}{n_1^{s_1} \ldots n_r^{s_r}}$$

  for $s_1, \ldots, s_r \in \mathbb{Z}_{\ge 1}$, $s_r \ge 2$.
- Multiple polylogarithms.
- Hyperplane arrangements and their periods.
- Mixed Tate motives.

Irrationality proofs for zeta values

- Irrationality proofs.
- Zeta values and multiple zeta values:

$$\zeta(s_1, \ldots, s_r) = \sum_{1 \le n_1 < \cdots < n_r} \frac{1}{n_1^{s_1} \ldots n_r^{s_r}}$$

  for $s_1, \ldots, s_r \in \mathbb{Z}_{\geq 1}$, $s_r \geq 2$.
- Multiple polylogarithms.
- Hyperplane arrangements and their periods.
- Mixed Tate motives.

Irrationality proofs for zeta values

- Irrationality proofs.
- Zeta values and multiple zeta values:

$$\zeta(s_1, \ldots, s_r) = \sum_{1 \le n_1 < \cdots < n_r} \frac{1}{n_1^{s_1} \ldots n_r^{s_r}}$$

  for $s_1, \ldots, s_r \in \mathbb{Z}_{\geq 1}$, $s_r \geq 2$.
- Multiple polylogarithms.
- Hyperplane arrangements and their periods.
- Mixed Tate motives.

Irrationality proofs for zeta values

- Irrationality proofs.
- Zeta values and multiple zeta values:

$$\zeta(s_1, \dots, s_r) = \sum_{1 \le n_1 < \cdots < n_r} \frac{1}{n_1^{s_1} \dots n_r^{s_r}}$$

  for $s_1, \dots, s_r \in \mathbb{Z}_{\ge 1}$, $s_r \ge 2$.
- Multiple polylogarithms.
- Hyperplane arrangements and their periods.
- Mixed Tate motives.

Let k be a subfield of $\mathbb{C}$. Let $\mathcal{A}$ be a finite set of hyperplanes in $\mathbb{A}^n_k$ and $Y_{\mathcal{A}} = \mathbb{A}^n \setminus \bigcup_{H \in \mathcal{A}} H$. Let $\overline{Y}_{\mathcal{A}}$ be the De Concini-Procesi compactification of $Y_{\mathcal{A}}$.

Theorem (T.)

Suppose that $\mathcal{A}$ has enough modular elements.
Then period integrals of $\overline{Y}_{\mathcal{A}}$ relative to $\overline{Y}_{\mathcal{A}} \setminus Y_{\mathcal{A}}$ are $k(2\pi i)$-linear combinations of multiple polylogarithms of weight at most n evaluated at a specific finite set of points of k.
This set depends only on the one-dimensional arrangements obtained from $\mathcal{A}$ through iterated restrictions and deletions.

Example: Fix $q \geq 1$ and let $\mu \in \mathbb{C}$ be a primitive q-th root of unity. Write $\mathbb{A}_k^n = \operatorname{Spec} k[t_1, \ldots, t_n]$ and consider

$$\mathcal{A}_q = \bigcup_{i \neq j} \bigcup_{p=1}^{q} \{\{t_i = 0\}, \{t_i = \mu^p\}, \{t_i = \mu^p t_j\}\}.$$

Then period integrals of $\overline{Y}_{\mathcal{A}}$ relative to $\overline{Y}_{\mathcal{A}} \setminus Y_{\mathcal{A}}$ are generated by $2\pi i$ and values of multiple polylogarithms at roots of unity.

Transcendental number theory

- Methods from Diophantine approximation.
- Algebraic independence of periods of Abelian varieties and their exponentials.
  Example: there are at least two algebraically independent numbers among

$$B\left(\frac{1}{12},\frac{1}{12}\right),\ B\left(\frac{5}{12},\frac{5}{12}\right),\ \pi,\ e^{\pi^2},\ e^{i\pi^2}.$$

- Simultaneous approximations for exponentials and logarithms (joint with Veekesh Kumar).
  Lower bound for the distance of $\left(\frac{\log\alpha_1}{\log\alpha_2},\alpha_1^\beta,\alpha_2^\beta\right)$ from curves in $\mathbb{P}^3$ defined over $\mathbb{Q}$, with α_1,α_2 algebraic and multiplicatively independent, β quadratic irrational.

Transcendental number theory

- Methods from Diophantine approximation.
- Algebraic independence of periods of Abelian varieties and their exponentials.

  Example: there are at least two algebraically independent numbers among

$$B\left(\frac{1}{12},\frac{1}{12}\right),\ B\left(\frac{5}{12},\frac{5}{12}\right),\ \pi,\ e^{\pi^2},\ e^{i\pi^2}.$$

- Simultaneous approximations for exponentials and logarithms (joint with Veekesh Kumar).

  Lower bound for the distance of $\left(\frac{\log\alpha_1}{\log\alpha_2},\alpha_1^\beta,\alpha_2^\beta\right)$ from curves in $\mathbb{P}^3$ defined over $\mathbb{Q}$, with α_1,α_2 algebraic and multiplicatively independent, β quadratic irrational.

Transcendental number theory

- Methods from Diophantine approximation.
- Algebraic independence of periods of Abelian varieties and their exponentials.
  Example: there are at least two algebraically independent numbers among
  $$B\left(\frac{1}{12},\frac{1}{12}\right),\ B\left(\frac{5}{12},\frac{5}{12}\right),\ \pi,\ e^{\pi^2},\ e^{i\pi^2}.$$
- Simultaneous approximations for exponentials and logarithms (joint with Veekesh Kumar).
  Lower bound for the distance of $\left(\frac{\log\alpha_1}{\log\alpha_2},\alpha_1^\beta,\alpha_2^\beta\right)$ from curves in $\mathbb{P}^3$ defined over $\mathbb{Q}$, with α_1,α_2 algebraic and multiplicatively independent, β quadratic irrational.

Mihir Vahanwala

PhD Student
Foundations of Algorithmic Verification group
Max Planck Institute for Software Systems

My research interests include **dynamical systems**, **word combinatorics**, number-theoretic problems in CS, logic, and concurrency

Recurrence, transcendence, and
Diophantine approximation workshop
Leiden, July 2025

Automata on S-adic words

Berthé, Karimov, V. [1]

For any omega-regular language, the set of S-adic expansions that direct a word in the language is itself omega-regular

[1] https://arxiv.org/abs/2506.17460

Automata on S-adic words

Berthé, Karimov, V. [1]

For any omega-regular language, the set of S-adic expansions that direct a word in the language is itself omega-regular

Let $L \subseteq \Sigma^\omega$ be an ω-regular language, and let S be a set of non-erasing substitutions $\Sigma \to \Sigma$. We can compute a finite alphabet Ξ, a map $h : S \to \Xi$, and an ω-regular language $L' \subseteq \Xi^\omega$ such that a sequence $\sigma_0, \sigma_1, \ldots$ directs a word in L if and only if the word $h(\sigma_0)h(\sigma_1)\cdots \in L'$.

[1] https://arxiv.org/abs/2506.17460

Preservation theorems for transducer outputs

Berthé, Goulet-Ouellet, Karimov, Perrin, V. (forthcoming)

For certain nice combinatorial properties of infinite words which imply the existence of factor frequencies, we can show that if a word enjoys the property, then so does the output obtained by feeding it to a deterministic finite transducer

Preservation theorems for transducer outputs

Berthé, Goulet-Ouellet, Karimov, Perrin, V. (forthcoming)

For certain nice combinatorial properties of infinite words which imply the existence of factor frequencies, we can show that if a word enjoys the property, then so does the output obtained by feeding it to a deterministic finite transducer

Let $x \in \Sigma^\omega$, **and let** $\mathscr{A} : \Sigma^\infty \to \Gamma^\infty$ **be a deterministic finite transducer.**

For each of the following properties P, **we have that**

if $x \models P$ **and** $\mathscr{A}(x) \in \Gamma^\omega$, **then** $\mathscr{A}(x) \models P$.

(i) has a uniformly recurrent suffix

(ii) has a linearly recurrent suffix

(iii) has a (primitive) morphic suffix

(iv) has a uniformly recurrent suffix whose shift satifies Boshernitzan's condition

Properties (ii), (iii), (iv) imply, in particular, that the word admits factor frequencies.

Ronald van Luijk (Universiteit Leiden)

Rational points on surfaces

Question 1. (Del Pezzo surfaces)
Are there any $x, y, z, w \in \mathbb{C}(A, B)$ with $zw \neq 0$ and

$$y^2 = x^3 + Az^6 + Bw^6 \quad ?$$

Question 2. (K3 surfaces)
Is it true that for every integer t, there are integers x, y, z, w with

$$t = \frac{x^4 - y^4}{z^4 - w^4} \quad ?$$

Algorithmic Arithmetic Geometry

Madhavan Venkatesh

Indian Institute of Technology, Kanpur

Recurrence, Transcendence, and Diophantine Approximation
July 14 2025, Lorentz Center, Leiden

- Effective methods and algorithms.
- Computational number theory.
- Point counting.
- Rational points.

Main results

Theorem 1 (Kweon-V, '24).

For an n – dimensional smooth projective variety X, can recover $P_{n-1}(X/\mathbb{F}_q, T) := \left(1 - TF_q^\star \mid \mathrm{H}_{\acute{e}t}^{n-1}(X, \mathbb{Q}_\ell)\right)$ from $P_{n-1}(Y_i/\mathbb{F}_Q, T)$ for two randomly chosen hyperplane sections Y_i of X, and a polynomially bounded extension $\mathbb{F}_Q/\mathbb{F}_q$, with high probability.
Effective, probabilistic version of Deligne's 'théoréme du pgcd'.

Proof Ideas

- Hard-Lefschetz, big mod-ℓ monodromy of vanishing cycles.
- Equidistribution of Frobenius mod-ℓ.

Theorem 2 (Saxena-V, '25).

There is a randomised algorithm to compute the local zeta function of a fixed smooth projective surface over the rationals, at any prime p of good reduction, running in time polynomial in $\log p$.

Proof ideas

- Compute mod-ℓ étale coho: Lefschetz pencils, use Puiseux series to compute vanishing cycles and monodromy.
- Compute Galois action on part fixed by monodromy in ℓ–torsion of trivialising cover by moving to positive char.
- Arakelov theory to bound heights and ensure polynomial precision is sufficient.

Speed Talk

James Worrell, Department of Computer Science
University of Oxford

July 13, 2025

Decision Problems for Linear Recurrence Sequences

Theorem

It is decidable whether a linear recurrence sequence of order at most 5 is ultimately positive. The Ultimate Positivity Problem for simple linear recurrence sequences is $\forall\mathbb{R}$-complete.

Theorem

Assuming the p-adic Schanuel Conjecture and Skolem's Conjecture, there is an algorithm to decide the Skolem Problem for simple linear recurrence sequences

Transcendence

Theorem

Let β be an algebraic integer with $|\beta| > 1$. For any non-constant polynomial $f(x) \in \mathbb{Z}[x]$ and $\theta, \alpha \in \mathbb{R}$ with θ irrational, the Hecke-Mahler series $\sum_{n=0}^{\infty} f(\lfloor n\theta + \alpha \rfloor)\beta^{-n}$ is transcendental.