Small Units in Canonical Number Systems

Gergő Péter Batta

University of Debrecen

2026. July 06-10.

Seventeenth Algorithmic Number Theory Symposium
Bernoulli Institute
ANTS XVII
Rijksuniversiteit Groningen, Netherlands

Joint work with Attila Pethő.

Supported by the EKÖP-25-3 University Research Scholarship Program of the Ministry for Culture and Innovation from the source of the National Research, Development and Innovation Fund.

Classical Results (Intuitive Overview)

Question: How many integers have "simple" digit patterns in more than one base?

Senge–Straus (1973):

- Consider two bases q_1 and q_2 (e.g., base 10 and base 3).
- Look at integers whose digit sum is small in *both* bases.
- They proved: this set is finite *if and only if* the ratio $\log q_1 / \log q_2$ is irrational.

Stewart (1980):

- He proved explicit, computable upper bounds for such integers.

Canonical Number Systems

Let K be a number field, $\mathbb{Z}_K$ its ring of integers. A pair $(\alpha, \mathcal{N})$ is a *canonical number system* if every $0 \neq y \in \mathbb{Z}_K$ has a unique representation

$$y = g_0\alpha^{m_0} + g_1\alpha^{m_1} + \cdots + g_n\alpha^{m_n},$$

$$g_i \in \mathcal{N},\ g_i \neq 0,\ 0 \leq m_0 < m_1 < \cdots < m_n.$$

The length of the representation of y is $\ell_\alpha(y) = m_n$.

Main Theorem

Theorem (B.-Pethő) 202?

Let $(\alpha, \mathcal{N})$ be a CNS in a number field K. Let S be a finite set of places containing the archimedean ones, and assume there exists a place $v \notin S$ such that $|\alpha|_v < 1$.
If u is an S-unit whose α-representation contains at most n non-zero digits, then

$$\ell_\alpha(u) < C,$$

where C is an effectively computable constant depending only on K, α, and n.

Numerical result

Let λ be a root of $x^3 + 8x^2 + 19x + 13$. Number field: $K = \mathbb{Q}(\lambda)$. Base: $\alpha = \lambda - 2$ Digit set: $\{0, 1, \ldots, 12\}$. Choose

$$S = \{\alpha + 2,\ \alpha + 4,\ \alpha - 1\}.$$

There are exactly **67** S-units, whose α-representation has at most 4 non-zero digits.

On a Generalization of a Problem of Erdős - Selfridge

Sarthak Gupta

Department of Algebra and Number Theory

University of Debrecen

Lightening Talk

Seventeenth Algorithmic Number Theory Symposium

Main Equation

Erdős–Selfridge (1975)

The product of consecutive positive integers is never a perfect power:

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

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

Our Generalization

We introduce a gap into the product by adding t shifted, fixed terms:

$$x(x+1)\dots(x+k-1)(x+a_1)\dots(x+a_t) = by^l + c$$

where $k \geq 2$, $k+3 \leq a_1 < \cdots < a_t$, $b, c \in \mathbb{Z}$ with $b \neq 0$.

Results and Ongoing Work

Theorem 1:

For the equation $x(x+1)\dots(x+k-1)(x+a) = by^l + c$, all integer solutions with $l \geq 2$ are effectively bounded:

$$\max(|x|, |y|, l) \leq C_1.$$

Theorem 2:

For the equation $x(x+1)\dots(x+k-1)(x+a)(x+a+1) = by^l + c$ all integer solutions with $l \geq 2$ are effectively bounded:

$$\max(|x|, |y|, l) \leq C_2),$$

except for two parametric families.

Further Work

Solving for arbitrary polynomials $g(y)$ on the right-hand side.

Ten Thousand Polynomials with Small Mahler Measure

Rank	d	M	v	Coefficients
1	10	1.176280818260	1	1 1 0 −1 −1 −1
2	18	1.188368147508	1	1 1 1 1 0 0 −1 −1 −1 −1
3	14	1.200026523987	1	1 0 0 1 −1 0 0 −1
4	18	1.201396186235	2	1 1 1 0 0 −1 0 −1 0 −1
5	14	1.202616743689	1	1 0 −1 0 0 0 0 1
6	22	1.205019854225	2	1 0 1 0 0 1 −1 1 0 0 1 −1
7	28	1.207950028412	2	1 1 1 1 0 0 0 −1 −1 −1 −1 0 0 0 1
8	20	1.212824180989	2	1 1 0 0 1 1 0 −1 −1 −1 −1
9	20	1.214995700776	2	1 1 1 1 1 0 −1 −1 −1 −1 −1
10	10	1.216391661138	1	1 0 0 0 −1 1
11	20	1.218396362520	2	1 1 0 −1 0 0 0 −1 0 0 1
12	24	1.218855150304	2	1 0 0 0 0 1 0 −1 0 0 0 0 −1
13	24	1.219057507826	2	1 1 0 −1 −1 −1 −1 −1 0 1 1 1 1
14	18	1.219446875941	3	1 1 1 0 −1 −1 −1 0 0 1
15	18	1.219720859040	1	1 1 0 0 0 0 0 0 −1 −1
16	34	1.220287441693	3	1 0 1 0 0 1 −1 1 −1 0 0 −1 1 −1 0 0 −1 1
17	38	1.223447381419	3	1 1 0 −1 −1 0 0 −1 −1 0 1 1 0 0 1 1 0 −1 −1 −1
18	26	1.223777454948	3	1 1 1 0 0 −1 −1 −1 −1 0 0 1 0 1
19	16	1.224278907222	2	1 1 0 −1 −1 0 1 1 1
20	18	1.225503424104	2	1 1 0 0 1 0 −1 0 0 −1

Deg	Tot	1	2	3	4	5	6	7	8	9
8	1	1								
10	7	5	2							
12	5	1	4							
14	11	4	5	2						
16	14	1	12		1					
18	23	7	8	8						
20	35	4	22	3	6					
22	48	4	12	27	4	1				
24	46	2	29	3	11		1			
26	61	7	11	21	11	11				
28	59	1	15	14	28	1				
30	80	4	10	36	20	8	2			
32	69		12	8	35	7	7			
34	90	2	5	24	19	30	8	2		
36	88	1	15	11	36	4	20		1	
38	86		1	18	18	29	8	12		
40	87	1	9	7	32	10	23	2	3	
42	57			11	14	16	6	8	2	
44	77	1	2	4	29	5	25	4	7	
46	107	1	1	10	13	38	11	23	7	3
48	80		2	4	24	4	25	1	19	1
50	76			4	10	15	14	16	9	8

Michael Mossinghoff
Center for Communications Research, Princeton, New Jersey

- Suppose $f(x) = \sum_{k=0}^{d} a_k x^k = a_d \prod_{k=1}^{d} (x - \beta_k) \in \mathbb{Z}[x]$.
- *Mahler measure*: $\exp\left(\int_0^1 \log|f(e^{2\pi i t})|\,dt\right) = |a_d| \prod_{k=1}^{d} \max\{1, |\beta_k|\}$.
- Smallest known value > 1: $1.1762\ldots$, for a degree-10 polynomial.
- *Lehmer's problem* (1933): is 1 an accumulation point?
- Smallest known limit points: $1.255\ldots$, $1.285\ldots$, $1.309\ldots$.
- Topic of substantial computation for 50 years!
- Starting in 1996: CECM at SFU housed a database of polynomials with Mahler measure < 1.3 and degree ≤ 180. No longer available!

- New site! `github.com/mossinghoff/Mahler-Measure-Database`
- All known primitive, irreducible, noncyclotomic polynomials in $\mathbb{Z}[x]$ with Mahler measure < 1.3 and degree ≤ 200: 10236 polynomials.
- Incorporates recent finds from literature, plus 18 new with deg ≤ 180.
- Reports: best by degree, count by degree & #roots with $|z| > 1$, etc.
- All 72 known Salem numbers $< 49/37$.
- All 61 known two-variable measures < 1.37.
- Smallest and largest measures of Littlewood polynomials by degree.
- Write if you have contributions or suggestions!

Expansion Properties of the Superspecial Isogeny Graph with Level Structure

Harun Kır

École Normale Supérieure de Lyon

Seventeenth Algorithmic Number Theory Symposium ANTS XVII
6–10 July, 2026

Based on ongoing work with Maria Corte-Real Santos, Olivier Taïbi, and Benjamin Wesolowski

The g-dimensional ℓ-Superspecial Isogeny Graph $\mathcal{G}_\ell(p, g)$

Vertices V

Superspecial PPAVs (X, λ) of dimension g over $\overline{\mathbb{F}}_p$ (up to isomorphism).

The g-dimensional ℓ-Superspecial Isogeny Graph $\mathcal{G}_\ell(p, g)$

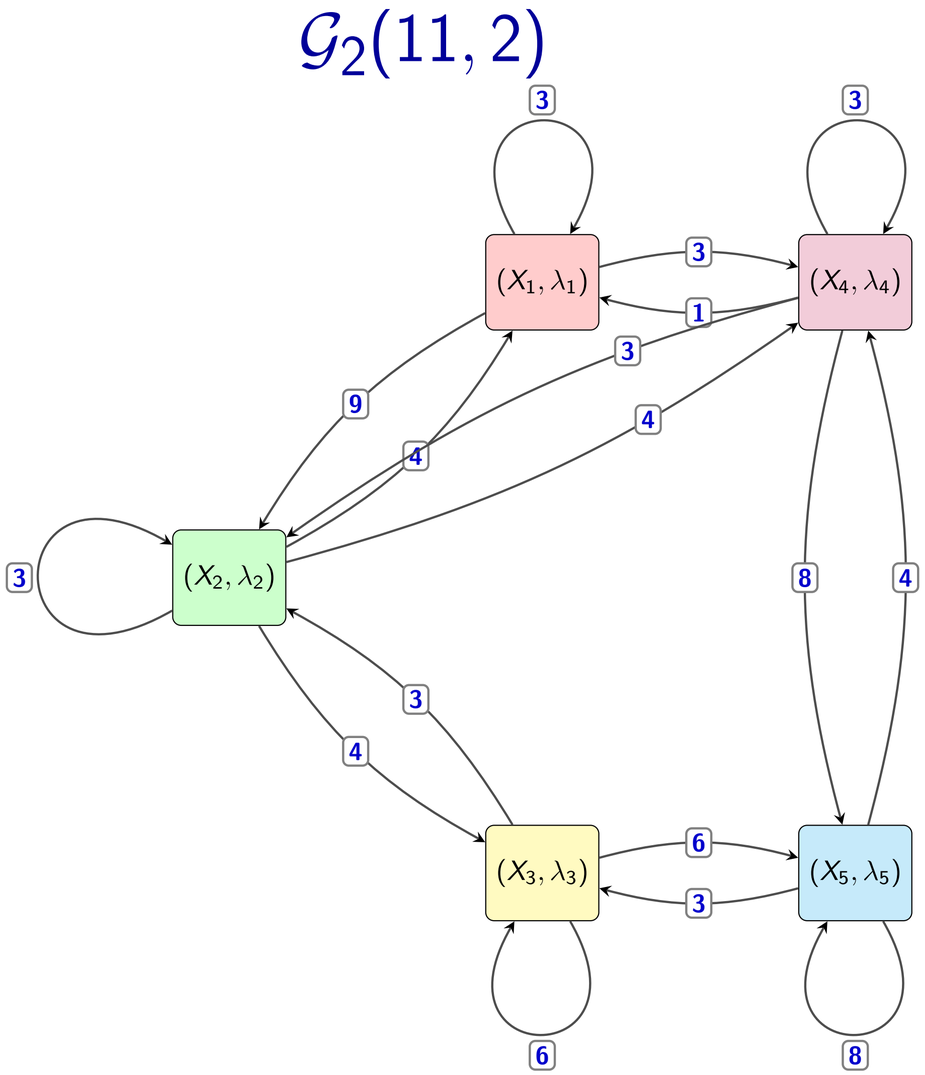
Vertices V

Superspecial PPAVs (X, λ) of dimension g over $\overline{\mathbb{F}}_p$ (up to isomorphism).

Edges E

ℓ-isogenies $(X_1, \lambda_1) \to (X_2, \lambda_2)$ (coprime to p), up to post-composition by $\mathrm{Aut}(X_2, \lambda_2)$.

The g-dimensional ℓ-Superspecial Isogeny Graph $\mathcal{G}_\ell(p, g)$



Vertices V

Superspecial PPAVs (X, λ) of dimension g over $\overline{\mathbb{F}}_p$ (up to isomorphism).

Edges E

ℓ-isogenies $(X_1, \lambda_1) \to (X_2, \lambda_2)$ (coprime to p), up to post-composition by $\mathrm{Aut}(X_2, \lambda_2)$.

Main Result

$\mathcal{G}_\ell(p,1)$ is Ramanujan by Pizer (1980): the spectral radius satisfies

$$\lambda(\mathcal{G}_\ell(p,1)) \leq 2\sqrt{\ell}.$$

Main Result

$\mathcal{G}_\ell(p,1)$ is Ramanujan by Pizer (1980): the spectral radius satisfies

$$\lambda(\mathcal{G}_\ell(p,1)) \leq 2\sqrt{\ell}.$$

Main Theorem (K., Corte-Real Santos, Taïbi, Wesolowski)

For $g \geq 2$, the spectral radius of the higher-dimensional superspecial isogeny graph $\mathcal{G}_\ell(p,g)$ satisfies:

$$\lambda(\mathcal{G}_\ell(p,g)) \leq \frac{2}{\ell^{g/2} + \ell^{-g/2}} \prod_{i=1}^{g} (1+\ell^i).$$

Main Result

$\mathcal{G}_\ell(p,1)$ is Ramanujan by Pizer (1980): the spectral radius satisfies

$$\lambda(\mathcal{G}_\ell(p,1)) \leq 2\sqrt{\ell}.$$

Main Theorem (K., Corte-Real Santos, Taïbi, Wesolowski)

For $g \geq 2$, the spectral radius of the higher-dimensional superspecial isogeny graph $\mathcal{G}_\ell(p,g)$ satisfies:

$$\lambda(\mathcal{G}_\ell(p,g)) \leq \frac{2}{\ell^{g/2} + \ell^{-g/2}} \prod_{i=1}^{g} (1+\ell^i).$$

Consequence: Rapid mixing for random walks in higher dimensions!

Example: On $\mathcal{G}_2(p,2)$ reaching the stationary distribution within an error of p^{-r} requires only $n \approx (4.66 + 3.11r)\log(p)$ steps.

Main Result

$\mathcal{G}_\ell(p,1)$ is Ramanujan by Pizer (1980): the spectral radius satisfies

$$\lambda(\mathcal{G}_\ell(p,1)) \leq 2\sqrt{\ell}.$$

Main Theorem (K., Corte-Real Santos, Taïbi, Wesolowski)

For $g \geq 2$, the spectral radius of the higher-dimensional superspecial isogeny graph $\mathcal{G}_\ell(p,g)$ with "level structure" satisfies:

$$\lambda(\mathcal{G}_\ell(p,g)) \leq \frac{2}{\ell^{g/2} + \ell^{-g/2}} \prod_{i=1}^{g} (1+\ell^i).$$

Consequence: Rapid mixing for random walks in higher dimensions!

Example: On $\mathcal{G}_2(p,2)$ reaching the stationary distribution within an error of p^{-r} requires only $n \approx (4.66 + 3.11r)\log(p)$ steps.

On the density of coprime reduction of elliptic curves

Asimina S. Hamakiotes

joint with Sung Min Lee (Wake Forest University),
Jacob Mayle (University of Delaware),
Tian Wang (Concordia University)

Fordham University

ANTS XVII,
July 6-10, 2026

Question

Q: Given non-CM elliptic curves $E, E'/\mathbb{Q}$, what is the density of primes p of good reduction for which the orders of $E(\mathbb{F}_p), E'(\mathbb{F}_p)$ are coprime?

In particular, we are interested in understanding the asymptotic behavior of the following as $x \to \infty$:

$$\pi_{E,E'}^{\text{coprime}}(x) := \#\{p \leq x : p \nmid N_E N_{E'}, \gcd(|E_p(\mathbb{F}_p)|, |E'_p(\mathbb{F}_p)|) = 1\}.$$

Conjecture 1 (H.-Lee-Mayle-Wang)

Let $E, E'/\mathbb{Q}$ be non-CM elliptic curves that are not $\overline{\mathbb{Q}}$-isogenous. Then,

$$\pi_{E,E'}^{coprime}(x) \sim C_{E,E'}^{coprime} \cdot \frac{x}{\log x}, \qquad \text{as } x \to \infty.$$

What can we say about $C_{E,E'}^{\text{coprime}}$?

Main Results

Ignoring the finite series part in $C_{E,E'}^{\text{coprime}}$ (which is specific to the actual Galois image of $E \times E'$), the Euler product below reflects the generic case:

$$C^{\text{coprime}} := \prod_{q} \left(1 - \frac{(q+2)(q^2-q-1)}{(q-1)^3(q+1)^2}\right) \approx 0.39607 < \frac{6}{\pi^2}.$$

Theorem 1 (H.-Lee-Mayle-Wang, 2026)

Let (E, E') be a Serre pair. Then

$$0.99998 \cdot C^{coprime} \leq C_{E,E'}^{coprime} \leq 1.02914 \cdot C^{coprime}.$$

Theorem 2 (H.-Lee-Mayle-Wang, 2026)

$$\lim_{T\to\infty} \frac{1}{|\mathcal{E}(T)|} \sum_{(E,E')\in\mathcal{E}(T)} |C_{E,E'}^{coprime} - C^{coprime}|^t = 0, \quad \forall t \in \mathbb{Z}^+,$$

where $\mathcal{E}(T)$ is the set of all pairs of elliptic curves of height at most T^6.

Effective Artin–Schreier–Witt theory for curves

Christophe Levrat, Rubén Muñoz--Bertrand

Let:

p be a prime number,
q be a power of p,
n be an integer,
X be a (projective, normal, smooth) curve over $\overline{\mathbb{F}_p}$ defined over $\mathbb{F}_q$.

Problem

How to compute all unramified cyclic covers of X of degree p^n?

What is already known:

- The theory of Witt vectors (1934) enables one to compute all cyclic covers of X of degree p^n.
- There are fast[1] algorithms to compute with Witt vectors in characteristic p (Finotti, 2014, and M--B, 2025).

[1] in French: *vite*

Problem

How to compute all **unramified** cyclic covers of X of degree p^n?

AG says :

The $\mathbb{Z}/p^n\mathbb{Z}$-module $H^1_{ét}(X, \mathbb{Z}/p^n\mathbb{Z})$ encodes the data of all unramified cyclic covers of the curve X of degree p^n.

This is the module of fixed points of the Frobenius of $H^1(X, W_n(\mathcal{O}_X))$.

- We implemented an algorithm to compute fixed points of the Frobenius on $H^1(X, \mathcal{O}_X)$ in $\widetilde{\mathcal{O}}(q^{g^2})$, where g is the genus of X. It is optimal.
- We developed an algorithm to lift these fixed points to $H^1(X, W_n(\mathcal{O}_X))$.
- We expressed these points with adeles, so that we answer to the above problem.
- We implemented everything in SageMath.

Thank you for listening!

Continued fractions with the digits $\{1, 2\}$

James Rickards

Saint Mary's University

james.rickards@smu.ca

6 July 2026

Hensley's conjecture

Conjecture (Hensley, variant of Zaremba's Conjecture)

Every sufficiently large integer n can be paired with a coprime $0 < m < n$ so that the continued fraction of m/n contains only the digits $\{1, 2\}$.

Hensley's conjecture

Conjecture (Hensley, variant of Zaremba's Conjecture)

Every sufficiently large integer n can be paired with a coprime $0 < m < n$ so that the continued fraction of m/n contains only the digits $\{1, 2\}$.

- $\{1, 2, 3, 4, 5\}$: strong form of Zaremba's conjecture, expect true for all n;
- $\{1, 2, 3, 4\}$: expect true for all $n \neq 54, 120$;
- $\{1, 2, 3\}$: expect true for all $n > 6234$;

Hensley's conjecture

Conjecture (Hensley, variant of Zaremba's Conjecture)

Every sufficiently large integer n can be paired with a coprime $0 < m < n$ so that the continued fraction of m/n contains only the digits $\{1, 2\}$.

- $\{1, 2, 3, 4, 5\}$: strong form of Zaremba's conjecture, expect true for all n;
- $\{1, 2, 3, 4\}$: expect true for all $n \neq 54, 120$;
- $\{1, 2, 3\}$: expect true for all $n > 6234$;
- **Goal:** find largest exception for $\{1, 2\}$. **Issue**: growth rate is slow!

Hensley's conjecture

Conjecture (Hensley, variant of Zaremba's Conjecture)

Every sufficiently large integer n can be paired with a coprime $0 < m < n$ so that the continued fraction of m/n contains only the digits $\{1, 2\}$.

- $\{1, 2, 3, 4, 5\}$: strong form of Zaremba's conjecture, expect true for all n;
- $\{1, 2, 3, 4\}$: expect true for all $n \neq 54, 120$;
- $\{1, 2, 3\}$: expect true for all $n > 6234$;
- **Goal:** find largest exception for $\{1, 2\}$. **Issue**: growth rate is slow!
- Number of such fractions m/n with $m < n < N$ is $\approx cN^{1.063}$.
- With alphabet $\{1, 2, 3\}$, it was $\approx cN^{1.411}$.

Algorithm

- Continued fractions are "continuous":

$$285117/405197 = [0, 1, 2, 2, 1, 2, 25, 3, 17, 2, 1, 2, 1]$$
$$285118/405197 = [0, 1, 2, 2, 1, 2, 26, 1, 1, 2, 1, 15, 4, 1]$$
$$285139/405197 = [0, 1, 2, 2, 1, 1, 1, 1500, 10]$$

Algorithm

- Continued fractions are "continuous":

$$285117/405197 = [0, 1, 2, 2, 1, 2, 25, 3, 17, 2, 1, 2, 1]$$
$$285118/405197 = [0, 1, 2, 2, 1, 2, 26, 1, 1, 2, 1, 15, 4, 1]$$
$$285139/405197 = [0, 1, 2, 2, 1, 1, 1, 1500, 10]$$

- If a given m has a digit too large, you can skip a chunk.

Algorithm

- Continued fractions are "continuous":

$$285117/405197 = [0, 1, 2, 2, 1, 2, 25, 3, 17, 2, 1, 2, 1]$$
$$285118/405197 = [0, 1, 2, 2, 1, 2, 26, 1, 1, 2, 1, 15, 4, 1]$$
$$285139/405197 = [0, 1, 2, 2, 1, 1, 1, 1500, 10]$$

- If a given m has a digit too large, you can skip a chunk.
- For $n \approx 10^{16}$, $\approx$ 4sec to compute; $n \approx 10^{18}$, $\approx$ 150sec
- Current largest found is

$$69765357700255367486 \approx 6.9 \cdot 10^{19}$$

Algorithm

- Continued fractions are "continuous":

$$285117/405197 = [0, 1, 2, 2, 1, 2, 25, 3, 17, 2, 1, 2, 1]$$
$$285118/405197 = [0, 1, 2, 2, 1, 2, 26, 1, 1, 2, 1, 15, 4, 1]$$
$$285139/405197 = [0, 1, 2, 2, 1, 1, 1, 1500, 10]$$

- If a given m has a digit too large, you can skip a chunk.
- For $n \approx 10^{16}$, $\approx$ 4sec to compute; $n \approx 10^{18}$, $\approx$ 150sec
- Current largest found is

$$69765357700255367486 \approx 6.9 \cdot 10^{19}$$

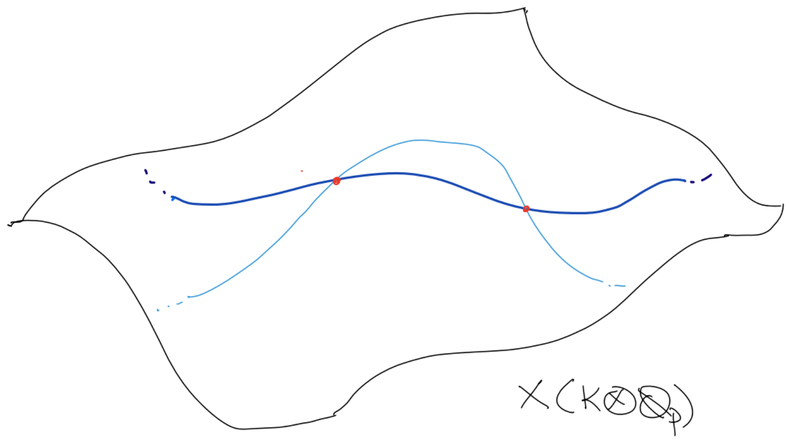
- **Issue:** integers beyond 10^{19} no longer fit inside longs.
- Standard libraries (e.g. PARI, gmp) work but *significant* slowdown.
- Need an efficient 128-bit integer implementation.

Quadratic Chabauty over number fields

Algorithmic Number Theory Symposium XVII

Aashraya Jha

Bilkent University



Joint with Jennifer Balakrishnan, L. Alexander Betts, Daniel Hast, and J. Steffen Müller

Program B

- Following Mazur's program B, Rouse, Sutherland, and Zureick-Brown propose a program to classify ℓ-adic images of elliptic curves. The classification for $\ell = 3$ was almost complete. Needed to to determine $X_{\mathsf{ns}}^{+}(27)(\mathbb{Q})$. This curve has $g = 12$.
- RSZB find a genus 3 quotient $X/\mathbb{Q}(\zeta_3)$. $J = \mathrm{Jac}(X)$ has rank 6 over $\mathbb{Q}(\zeta_3)$. There are 13 known points.

Theorem (Balakrishnan, Betts, Hast, J., Müller)

The curve $X_{\mathsf{ns}}^{+}(27)$ has exactly 8 $\mathbb{Q}$-points, all of which correspond to CM elliptic curves.

Proof

Program B

- Following Mazur's program B, Rouse, Sutherland, and Zureick-Brown propose a program to classify ℓ-adic images of elliptic curves. The classification for $\ell = 3$ was almost complete. Needed to to determine $X_{\mathsf{ns}}^{+}(27)(\mathbb{Q})$. This curve has $g = 12$.
- RSZB find a genus 3 quotient $X/\mathbb{Q}(\zeta_3)$. $J = \mathrm{Jac}(X)$ has rank 6 over $\mathbb{Q}(\zeta_3)$. There are 13 known points.

Theorem (Balakrishnan, Betts, Hast, J., Müller)

The curve $X_{\mathsf{ns}}^{+}(27)$ has exactly 8 $\mathbb{Q}$-points, all of which correspond to CM elliptic curves.

Proof

```
Hence the set of K-rational points on the Curve over K defined by
(2*u + 2)*X1^3*Y1 + (u - 1)*X1*Y1^3 + Y1^4 - u*X1^3*Z1 - 3*u*X1^2*Y1*Z1 + (3*u
+ 2)*Y1^3*Z1 + 3*u*X1^2*Z1^2 + 3*u*X1*Y1*Z1^2 - 3*Y1^2*Z1^2 + (-u + 1)*X1*Z1^3
- 2*u*Y1*Z1^3 + (u + 1)*Z1^4 is
[ (1 : 0 : 0), (-u : 1 : 0), (0 : -u - 1 : 1), (1 : -u - 1 : 1), (u + 1 : -u -
1 : 1), (0 : -u : 1), (u + 1 : 0 : 1), (2*u + 2 : u : 1), (u : 1 : 1), (1/2*(u
- 3) : 1/2*(u + 2) : 1), (1/3*(-u - 2) : 1/3*(u + 2) : 1), (-1/2*u : -1/2 : 1),
 (1/7*(5*u + 4) : -1 : 1) ],
 where K is the Cyclotomic Field of order 3 and degree 2.This is the time taken
 8441.2108458.660
```

For quadratic fields K, given some technical conditions, we have developed a method to compute locally analytic functions $\rho\colon X(K \otimes \mathbb{Q}_p) \longrightarrow \mathbb{Q}_p$ and finite sets $T \subset \mathbb{Q}_p$, such that $\rho(X(K)) \subseteq T$. This method can compute $X(K)$ for $r = dg$.

We use this method to compute $X_{\mathrm{ns}}^{+}(27)(\mathbb{Q})$, and complete the classification of 3-adic images. :)

For quadratic fields K, given some technical conditions, we have developed a method to compute locally analytic functions $\rho\colon X(K \otimes \mathbb{Q}_p) \longrightarrow \mathbb{Q}_p$ and finite sets $T \subset \mathbb{Q}_p$, such that $\rho(X(K)) \subseteq T$. This method can compute $X(K)$ for $r = dg$.

We use this method to compute $X_{\text{ns}}^{+}(27)(\mathbb{Q})$, and complete the classification of 3-adic images. :)

Future Work

- Determine quotients of modular curves over quadratic number fields; determine rational points.
- Compute the action of correspondences and Frobenius on $H^1_{\text{dR}}(X)$ with non-hyperelliptic and non-planar models.
- Find efficient algorithms to compute zeroes of systems of p-adic power series.
- Make Tuitman's algorithm(s) more efficient.

Towards a database of genus 2 curves over quadratic fields

July 6, 2026

Hugo Nartz
hugo.nartz@loria.fr

Fix $K = \mathbb{Q}(\sqrt{d})$ and let $f(x) = A_6x^6 + \cdots + A_0$ and $h(x) = B_3x^3 + \cdots + B_0$ in $\mathcal{O}_K(A_0, \ldots, B_3)[x]$.

Same idea as Booker et al. : evaluate the formal discriminant $\Delta \in \mathcal{O}_K(A_0, \ldots, B_3)$ of

$$y^2 + h(x)y = f(x)$$

over quadratic integer boxes: $(a_0, \ldots, b_3) \in \{x + \omega y | -N \leq x \leq N, -M \leq y \leq M\}$[11].
We keep curves with $|\mathrm{N}_{K/\mathbb{Q}}(\Delta(a_0, \ldots, b_3))| \leq 10^6$.

Requires $\mathcal{O}(N^7M^7)$ evaluations. Runs at $\sim 10^8$ evaluations per second per CPU core.

Example: curve over $\mathbb{Q}(\sqrt{26})$ with discriminant of norm -256:

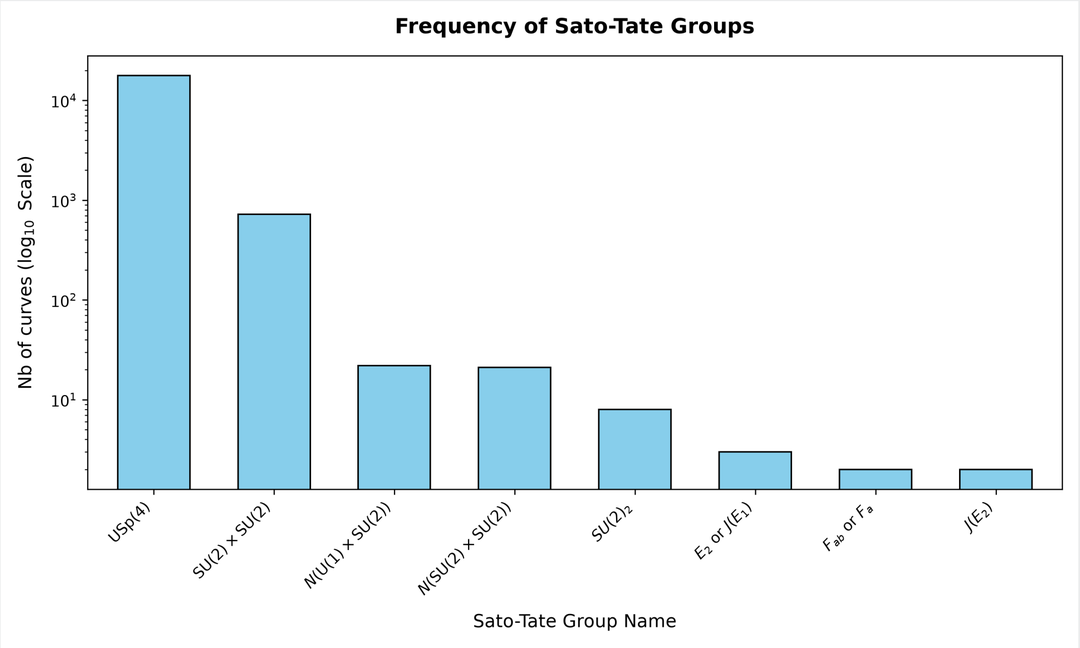
$$y^2+\left(1+x^2+(1-\sqrt{26})x^3\right)y = (-2-\sqrt{26})+(4+2\sqrt{26})x^2+(-1+2\sqrt{26})x^3+(-4-\sqrt{26})x^4+(2-3\sqrt{26})x^5+(1-\sqrt{26})x^6$$

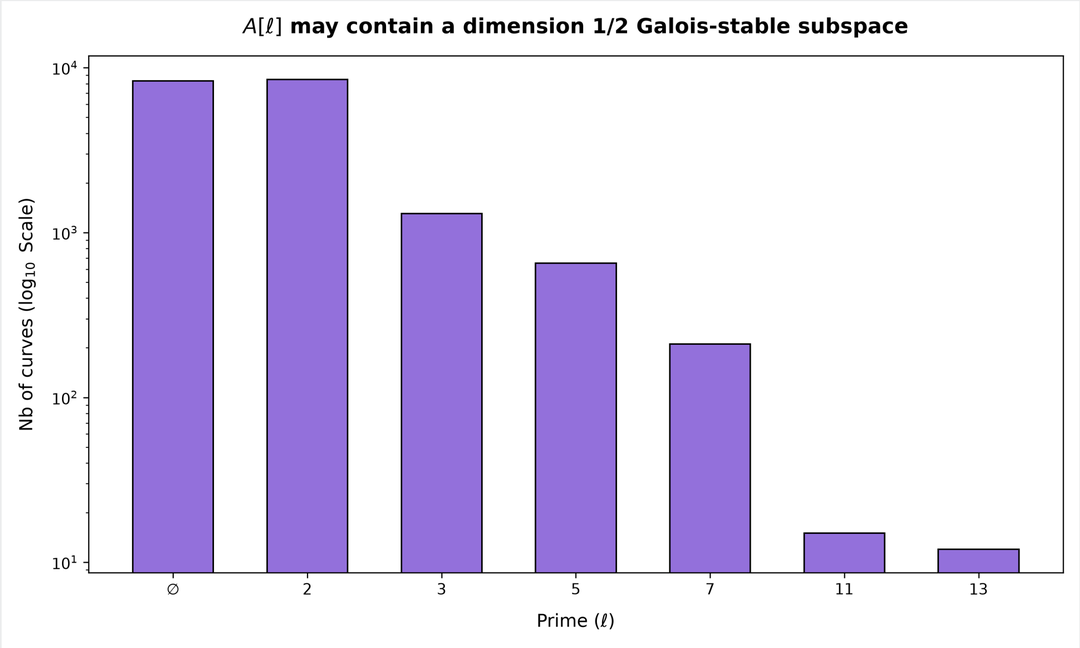
Conductor?

```
Runtime error in 'RegularModel': Currently only for principal primes, sorry
```

We hope the curves can be added to a public database at some point.
Preliminary computations: endomorphism rings, odd-conductors, Sato-Tate groups[?]...

Example: 18664 isomorphism classes over $\mathbb{Q}(\sqrt{2})$ without model over $\mathbb{Q}$.





For us: we aim to compute the isogeny class of the surfaces associated to these curves.

Contact: hugo.nartz@inria.fr

Explicit formulas for abelian varieties over number fields

Pierre Tchamitchian

Institut de Mathématiques de Marseille

06/07/2026

Mestre's explicit formulas

Let $L(s)$ be the L-function of an abelian variety $A/\mathbb{Q}$ of dimension g and conductor N, supposed to be an analytic L-function:

- $L(s) = \prod_p L_p(s)$ is defined by an Euler product.
- $L(s)$ satisfies a functional equation $\Lambda(s) = w\overline{\Lambda}(1-s)$, with
$$\Lambda(s) = N^{s/2}(\text{gamma factors})L(s).$$

For test functions $F(x)$ with Fourier transform $\Phi_F(s)$, an explicit formula gives

$$\log(N) = B(g,F) + \sum_p C(p,F) - \sum_{L(\xi)=0} \Phi_F(\xi).$$

Mestre proves

Theorem (Mestre)

An abelian variety over $\mathbb{Q}$ with analytic L-function satisfies $N \geqslant 10.323^g$.

In particular, no abelian variety with everywhere good reduction (EGR) exists over $\mathbb{Q}$. We generalize this to number fields of higher degree.

Number fields admitting no abelian variety with EGR

Computational results: The following table presents the numbers of number fields of degree d, up to root discriminant $\sqrt[d]{\Delta}$, for which the explicit formula proves non-existence of abelian varieties with EGR.

d	$\sqrt[d]{\Delta}$	fields	d	$\sqrt[d]{\Delta}$	fields
2	11.135	10	8	9.202	140
3	11.184	6	9	9.953	98
4	11.190	35	10	8.613	317
5	11.109	40	11	11.169	10
6	6.995	122	12	11.186	32
7	8.980	126	13	–	0

Including superfields L/K for which no abelian varieties with EGR exist, the same property holds for K. The updated values obtained appear in blue.

Number fields admitting no abelian variety with EGR

Computational results: The following table presents the numbers of number fields of degree d, up to root discriminant $\sqrt[d]{\Delta}$, for which the explicit formula proves non-existence of abelian varieties with EGR.

d	$\sqrt[d]{\Delta}$	fields	d	$\sqrt[d]{\Delta}$	fields
2	11.135	18	8	9.202	140
3	11.184	11	9	9.953	98
4	11.190	48	10	8.613	317
5	11.109	42	11	11.169	10
6	6.995	126	12	11.186	32
7	8.980	126	13	–	0

Including superfields L/K for which no abelian varieties with EGR exist, the same property holds for K. The updated values obtained appear in blue.

Number fields admitting no abelian variety with EGR

Computational results: The following table presents the numbers of number fields of degree d, up to root discriminant $\sqrt[d]{\Delta}$, for which the explicit formula proves non-existence of abelian varieties with EGR.

d	$\sqrt[d]{\Delta}$	fields	d	$\sqrt[d]{\Delta}$	fields
2	11.135	18	8	9.202	140
3	11.184	11	9	9.953	98
4	11.190	48	10	8.613	317
5	11.109	42	11	11.169	10
6	6.995	126	12	11.186	32
7	8.980	126	13	–	0

Including superfields L/K for which no abelian varieties with EGR exist, the same property holds for K. The updated values obtained appear in blue.

Other refinements: Mestre's method generalizes to tighter conductor bounds for abelian varieties with prescribed bad reduction and rank.

Lifting L-polynomials of genus 3 curves

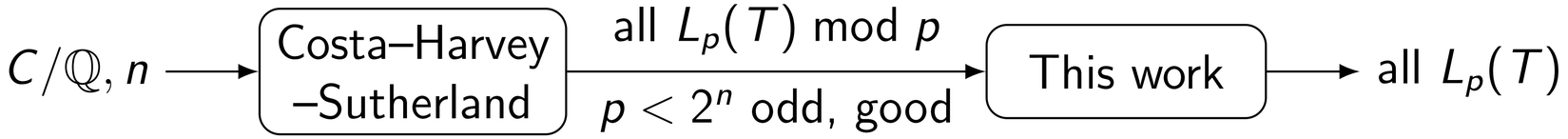
Jane Shi

Massachusetts Institute of Technology

ANTS XVII 2026

Setting

- **Goal:** compute L-polynomials of genus 3 curves.
- For a smooth projective curve C with good reduction at p, the L-polynomial $L_p(T)$ is the numerator of the zeta function of C_p.
- Shape: $L_p(T) = p^3T^6 + p^2a_1T^5 + pa_2T^4 + a_3T^3 + a_2T^2 + a_1T + 1$ with $a_1, a_2, a_3 \in \mathbb{Z}$.
- Motivation: $L(C, s) = \prod_p L_p(p^{-s})^{-1}$, which appears in the generalizations of the Sato-Tate conjecture, BSD, and the Riemann hypothesis.
- Costa–Harvey–Sutherland (CHS) give an average polynomial-time algorithm ($\tilde{O}((\log p)^4)$) to compute $L_p(T)$ mod p for genus 3 smooth plane quartic curves.
- Hasse–Weil bounds + Kedlaya-Sutherland bounds + mod p info $\xRightarrow{\text{narrows}}$ $O(\sqrt{p})$ candidates. Only 1 is correct.



Our work: $L_p(T) \bmod p \to L_p(T)$. (See arXiv:2602.00965)

- To do this:
  - Explicit group operations in $\mathrm{Jac}(C)(\mathbb{F}_p)$+a perfect hash
  - Baby-step giant-step
  - Sutherland's algorithm for structure computation of finite abelian groups
- Complexity: Single $L_p(T)$ computation takes $O(p^{1/4+o(1)})$ on average (under heuristic assumptions), $O(p^{1/2+o(1)})$ in the worst case.
- Benchmarking: with Costa-Harvey-Kedlaya and Tuitman's algorithms, using Sutherland's genus 3 smooth plane quartic database

n	all $L_p(T) \bmod p$ [CHS]	Lift all mod p (our work)	[CHS23] + our work	Costa-Harvey-Kedlaya (estimated)	Tuitman (estimated)
14	2.96	291	294	1140	113000
16	16.4	1050	1070	15100	2490000
18	84.3	4510	4590	188000	54600000
20	427	20900	21300	3010000	1660000000
22	2420	93500	95900	245000000	49200000000

Torsion of genus 2 Jacobians over number fields

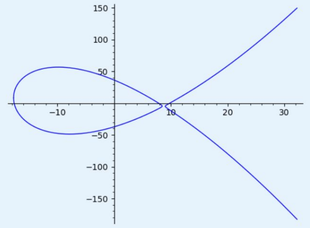
Aidan Hennessey
Dartmouth University

(largely joint with Mathilde Kermorgant and Andy Zhu, supervised by Sachi Hashimoto and Isabel Vogt)

Torsion of genus 2 Jacobians over number fields

Properties

Label	910.a4



Conductor	910
Discriminant	2153060
j-invariant	$\frac{1408317602329}{2153060}$
CM	no
Rank	1
Torsion structure	$\mathbb{Z}/6\mathbb{Z}$

Galois representations

The ℓ-adic Galois representation has maximal image for all primes ℓ except those listed in the table below.

prime ℓ	mod-ℓ image	ℓ-adic image	ℓ-adic index
2	2B	2.3.0.1	3
3	3B.1.1	3.8.0.1	8

The image $H := \rho_E(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ of the adelic Galois representation has level $10920 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 13$, index 9

$$\left(\begin{array}{cc} 7801 & 12 \\ 3126 & 73 \end{array}\right), \left(\begin{array}{cc} 5919 & 7738 \\ 3206 & 5021 \end{array}\right), \left(\begin{array}{cc} 10 & 3 \\ 4341 & 10912 \end{array}\right), \left(\begin{array}{cc} 11 & 2 \\ 10870 & 10911 \end{array}\right), \left(\begin{array}{cc} 5461 & 12 \\ 6 & 73 \end{array}\right), \left(\begin{array}{cc} 1 & 0 \\ 12 & 1 \end{array}\right), \left(\begin{array}{c} 72 \\ 18 \end{array}\right.$$

.

Input positive integer m to see the generators of the reduction of H to $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$:

Growth of torsion in number fields

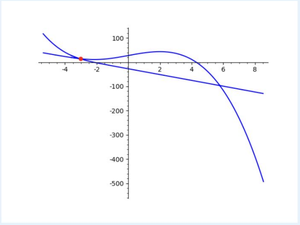
The number fields K of degree less than 24 such that $E(K)_{\mathrm{tors}}$ is strictly larger than $E(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/6\mathbb{Z}$ are as follows:

$[K:\mathbb{Q}]$	K	$E(K)_{\mathrm{tors}}$	Base change curve
2	$\mathbb{Q}(\sqrt{65})$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$	not in database
4	$\mathbb{Q}(\sqrt{11+2\sqrt{14}})$	$\mathbb{Z}/12\mathbb{Z}$	not in database
6	6.0.648270000.1	$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$	not in database
8	deg 8	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$	not in database
8	8.8.175551900160000.1	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$	not in database
9	9.3.2281096017943470000.2	$\mathbb{Z}/18\mathbb{Z}$	not in database
12	deg 12	$\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$	not in database
16	deg 16	$\mathbb{Z}/24\mathbb{Z}$	not in database
18	18.6.357245865551293427226038439470540625000000000.2	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}$	not in database

We only show fields where the torsion growth is primitive. For fields not in the database, click on the degree shown to reveal the defining polynomial.

Properties

Label	4672.a.9344.1



Conductor	4672
Discriminant	9344
Mordell-Weil group	$\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$
Sato-Tate group	$\mathrm{USp}(4)$
$\mathrm{End}(J_{\overline{\mathbb{Q}}}) \otimes \mathbb{R}$	$\mathbb{R}$
$\mathrm{End}(J_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$	$\mathbb{Q}$
$\mathrm{End}(J) \otimes \mathbb{Q}$	$\mathbb{Q}$
$\overline{\mathbb{Q}}$**-simple**	yes
GL_2**-type**	no

Galois representations

The mod-ℓ Galois representation has maximal image $\mathrm{GSp}(4, \mathbb{F}_\ell)$ for all primes ℓ except those listed.

Prime ℓ	mod-ℓ image	Is torsion prime?
2	2.10.1	no
3	3.80.1	yes
5	not computed	no

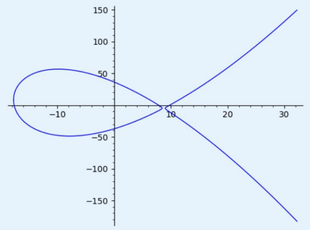
Aidan Hennessey
Dartmouth University

(largely joint with Mathilde Kermorgant and Andy Zhu, supervised by Sachi Hashimoto and Isabel Vogt)

Torsion of genus 2 Jacobians over number fields

Properties

Label	910.a4



Conductor	910
Discriminant	2153060
j-invariant	$\frac{1408317602329}{2153060}$
CM	no
Rank	1
Torsion structure	$\mathbb{Z}/6\mathbb{Z}$

Galois representations

The ℓ-adic Galois representation has maximal image for all primes ℓ except those listed in the table below.

prime ℓ	mod-ℓ image	ℓ-adic image	ℓ-adic index
2	2B	2.3.0.1	3
3	3B.1.1	3.8.0.1	8

The image $H := \rho_E(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ of the adelic Galois representation has level $10920 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 13$, index 9

$$\left(\begin{array}{cc} 7801 & 12 \\ 3126 & 73 \end{array}\right), \left(\begin{array}{cc} 5919 & 7738 \\ 3206 & 5021 \end{array}\right), \left(\begin{array}{cc} 10 & 3 \\ 4341 & 10912 \end{array}\right), \left(\begin{array}{cc} 11 & 2 \\ 10870 & 10911 \end{array}\right), \left(\begin{array}{cc} 5461 & 12 \\ 6 & 73 \end{array}\right), \left(\begin{array}{cc} 1 & 0 \\ 12 & 1 \end{array}\right), \left(\begin{array}{c} 72 \\ 18 \end{array}\right.$$

.

Input positive integer m to see the generators of the reduction of H to $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$:

Growth of torsion in number fields

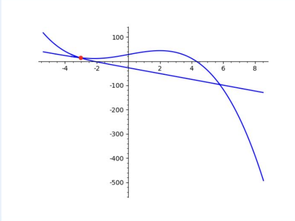
The number fields K of degree less than 24 such that $E(K)_{\mathrm{tors}}$ is strictly larger than $E(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/6\mathbb{Z}$ are as follows:

$[K:\mathbb{Q}]$	K	$E(K)_{\mathrm{tors}}$	Base change curve
2	$\mathbb{Q}(\sqrt{65})$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$	not in database
4	$\mathbb{Q}(\sqrt{11+2\sqrt{14}})$	$\mathbb{Z}/12\mathbb{Z}$	not in database
6	6.0.648270000.1	$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$	not in database
8	deg 8	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$	not in database
8	8.8.175551900160000.1	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$	not in database
9	9.3.2281096017943470000.2	$\mathbb{Z}/18\mathbb{Z}$	not in database
12	deg 12	$\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$	not in database
16	deg 16	$\mathbb{Z}/24\mathbb{Z}$	not in database
18	18.6.357245865551293427226038439470540625000000000.2	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}$	not in database

We only show fields where the torsion growth is primitive. For fields not in the database, click on the degree shown to reveal the defining polynomial.

Properties

Label	4672.a.9344.1



Conductor	4672
Discriminant	9344
Mordell-Weil group	$\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$
Sato-Tate group	$\mathrm{USp}(4)$
$\mathrm{End}(J_{\overline{\mathbb{Q}}}) \otimes \mathbb{R}$	$\mathbb{R}$
$\mathrm{End}(J_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$	$\mathbb{Q}$
$\mathrm{End}(J) \otimes \mathbb{Q}$	$\mathbb{Q}$
$\overline{\mathbb{Q}}$**-simple**	yes
GL_2**-type**	no

Galois representations

The mod-ℓ Galois representation has maximal image $\mathrm{GSp}(4, \mathbb{F}_\ell)$ for all primes ℓ except those listed.

Prime ℓ	mod-ℓ image	Is torsion prime?
2	2.10.1	no
3	3.80.1	yes
5	not computed	no

(LMFDB subgroup label 5.312.2)

$$\begin{bmatrix} * & * & * & * \\ 0 & * & * & * \\ 0 & * & * & * \\ 0 & 0 & 0 & \pm 1 \end{bmatrix}$$

Aidan Hennessey
Dartmouth University

(largely joint with Mathilde Kermorgant and Andy Zhu, supervised by Sachi Hashimoto and Isabel Vogt)

Mod-5 Galois images

Main approach: Sample Frobenius elements by reducing mod p

- The only information we can quickly compute is the characteristic polynomial and 1-eigenspace dimension.
- Compare observed distribution with subgroups of GSp4.
- Fails to distinguish certain subgroups – resolve many (but not all) ambiguities by checking for ℓ-torsion over $\boldsymbol{Q}$ and quadratic extensions.

Enough for all but 70 of the 66,158 genus 2 curves in the LMFDB.

Characteristic Polynomial	1-eigenspace dimension	Empirical Proportion	5.624.2 and 5.624.4 Proportion
x^4+4	1	12.88%	12.50%
x^4+3x^2+1	1	9.58%	9.17%
x^4+3x^2+1	2	2.32%	2.29%
$x^4+x^3+x^2+x+1$	1	4.16%	4.00%
$x^4+x^3+x^2+x+1$	2	0.97%	1.00%
$x^4+x^3+3x^2+2x+4$	0	6.58%	6.25%
$x^4+x^3+3x^2+4x+1$	1	6.49%	5.21%
$x^4+x^3+4x^2+3x+4$	0	4.36%	4.17%
$x^4+2x^3+x^2+4x+4$	0	3.58%	4.17%
$x^4+2x^3+3x^2+x+4$	0	4.07%	4.17%
$x^4+2x^3+3x^2+3x+1$	1	2.52%	4.17%
$x^4+2x^3+4x^2+2x+1$	1	3.58%	3.33%
$x^4+2x^3+4x^2+2x+1$	2	0.97%	0.83%
$x^4+3x^3+2x^2+3x+1$	1	4.94%	5.00%
$x^4+3x^3+2x^2+3x+1$	2	0.68%	1.25%
$x^4+3x^3+2x^2+4x+4$	0	5.91%	6.25%
$x^4+3x^3+3x^2+2x+1$	1	4.65%	4.17%
$x^4+3x^3+4x^2+x+4$	0	4.45%	4.17%
x^4+4x^3+4x+1	1	2.81%	3.33%
x^4+4x^3+4x+1	2	0.97%	0.83%
$x^4+4x^3+x^2+2x+4$	0	3.58%	4.17%
$x^4+4x^3+2x^2+3x+4$	0	4.94%	4.17%
$x^4+4x^3+3x^2+x+1$	1	5.03%	5.21%
$x^4+x^3+x^2+x+1$	3	0%	0.21%
$x^4+x^3+x^2+x+1$	4	0%	$< 0.01\%$

Local data for LMFDB curve 431250.a.431250.1, primes from 10,000 to 20,000

Mod-5 Galois images

Main approach: Sample Frobenius elements by reducing mod p

- The only information we can quickly compute is the characteristic polynomial and 1-eigenspace dimension.
- Compare observed distribution with subgroups of GSp4.
- Fails to distinguish certain subgroups – resolve many (but not all) ambiguities by checking for ℓ-torsion over $\boldsymbol{Q}$ and quadratic extensions.

Enough for all but 70 of the 66,158 genus 2 curves in the LMFDB.

Characteristic Polynomial	1-eigenspace dimension	Empirical Proportion	5.624.2 and 5.624.4 Proportion
x^4+4	1	12.88%	12.50%
x^4+3x^2+1	1	9.58%	9.17%
x^4+3x^2+1	2	2.32%	2.29%
$x^4+x^3+x^2+x+1$	1	4.16%	4.00%
$x^4+x^3+x^2+x+1$	2	0.97%	1.00%
$x^4+x^3+3x^2+2x+4$	0	6.58%	6.25%
$x^4+x^3+3x^2+4x+1$	1	6.49%	5.21%
$x^4+x^3+4x^2+3x+4$	0	4.36%	4.17%
$x^4+2x^3+x^2+4x+4$	0	3.58%	4.17%
$x^4+2x^3+3x^2+x+4$	0	4.07%	4.17%
$x^4+2x^3+3x^2+3x+1$	1	2.52%	4.17%
$x^4+2x^3+4x^2+2x+1$	1	3.58%	3.33%
$x^4+2x^3+4x^2+2x+1$	2	0.97%	0.83%
$x^4+3x^3+2x^2+3x+1$	1	4.94%	5.00%
$x^4+3x^3+2x^2+3x+1$	2	0.68%	1.25%
$x^4+3x^3+2x^2+4x+4$	0	5.91%	6.25%
$x^4+3x^3+3x^2+2x+1$	1	4.65%	4.17%
$x^4+3x^3+4x^2+x+4$	0	4.45%	4.17%
x^4+4x^3+4x+1	1	2.81%	3.33%
x^4+4x^3+4x+1	2	0.97%	0.83%
$x^4+4x^3+x^2+2x+4$	0	3.58%	4.17%
$x^4+4x^3+2x^2+3x+4$	0	4.94%	4.17%
$x^4+4x^3+3x^2+x+1$	1	5.03%	5.21%
$x^4+x^3+x^2+x+1$	3	0%	0.21%
$x^4+x^3+x^2+x+1$	4	0%	$< 0.01\%$

Local data for LMFDB curve 431250.a.431250.1, primes from 10,000 to 20,000

Mod-5 Galois images

Main approach: Sample Frobenius elements by reducing mod p

- The only information we can quickly compute is the characteristic polynomial and 1-eigenspace dimension.
- Compare observed distribution with subgroups of GSp4.
- Fails to distinguish certain subgroups – resolve many (but not all) ambiguities by checking for ℓ-torsion over $\boldsymbol{Q}$ and quadratic extensions.

Enough for all but 70 of the 66,158 genus 2 curves in the LMFDB.

Characteristic Polynomial	1-eigenspace dimension	Empirical Proportion	5.624.2 and 5.624.4 Proportion
x^4+4	1	12.88%	12.50%
x^4+3x^2+1	1	9.58%	9.17%
x^4+3x^2+1	2	2.32%	2.29%
$x^4+x^3+x^2+x+1$	1	4.16%	4.00%
$x^4+x^3+x^2+x+1$	2	0.97%	1.00%
$x^4+x^3+3x^2+2x+4$	0	6.58%	6.25%
$x^4+x^3+3x^2+4x+1$	1	6.49%	5.21%
$x^4+x^3+4x^2+3x+4$	0	4.36%	4.17%
$x^4+2x^3+x^2+4x+4$	0	3.58%	4.17%
$x^4+2x^3+3x^2+x+4$	0	4.07%	4.17%
$x^4+2x^3+3x^2+3x+1$	1	2.52%	4.17%
$x^4+2x^3+4x^2+2x+1$	1	3.58%	3.33%
$x^4+2x^3+4x^2+2x+1$	2	0.97%	0.83%
$x^4+3x^3+2x^2+3x+1$	1	4.94%	5.00%
$x^4+3x^3+2x^2+3x+1$	2	0.68%	1.25%
$x^4+3x^3+2x^2+4x+4$	0	5.91%	6.25%
$x^4+3x^3+3x^2+2x+1$	1	4.65%	4.17%
$x^4+3x^3+4x^2+x+4$	0	4.45%	4.17%
x^4+4x^3+4x+1	1	2.81%	3.33%
x^4+4x^3+4x+1	2	0.97%	0.83%
$x^4+4x^3+x^2+2x+4$	0	3.58%	4.17%
$x^4+4x^3+2x^2+3x+4$	0	4.94%	4.17%
$x^4+4x^3+3x^2+x+1$	1	5.03%	5.21%
$x^4+x^3+x^2+x+1$	3	0%	0.21%
$x^4+x^3+x^2+x+1$	4	0%	$< 0.01\%$

Local data for LMFDB curve 431250.a.431250.1, primes from 10,000 to 20,000

Mod-5 Galois images

Main approach: Sample Frobenius elements by reducing mod p

- The only information we can quickly compute is the characteristic polynomial and 1-eigenspace dimension.
- Compare observed distribution with subgroups of GSp4.
- Fails to distinguish certain subgroups – resolve many (but not all) ambiguities by checking for ℓ-torsion over $\boldsymbol{Q}$ and quadratic extensions.

Enough for all but 70 of the 66,158 genus 2 curves in the LMFDB.

$$\begin{bmatrix} \pm 1 & * & * & * \\ 0 & * & * & * \\ 0 & * & * & * \\ 0 & 0 & 0 & * \end{bmatrix}$$

Has ℓ-torsion over a quadratic extension

$$\begin{bmatrix} * & * & * & * \\ 0 & * & * & * \\ 0 & * & * & * \\ 0 & 0 & 0 & \pm 1 \end{bmatrix}$$

Does *not* have ℓ-torsion over any quadratic extension

Missing functionality in Magma

0.1s Run Format More 3

In [12]:
```
_<x> := PolynomialRing(Rationals());
K<b> := NumberField(x^2-5);
_<xk> := PolynomialRing(K);
f := xk^6 + 2*xk^2 + 2;
J := Jacobian(HyperellipticCurve(f));

J;
TorsionSubgroup(J);
```

Out[12]:
```
Jacobian of Hyperelliptic Curve defined by y^2 = x^6 + 2*x^2 + 2 over K

In line 8, column 16:
>> TorsionSubgroup(J);
                   ^
Runtime error: TorsionSubgroup is only implemented for Jacobians of genus 2 curves over the rationals.
```

Missing functionality in Magma

0.1s Run Format More 3

In [12]:
```
_<x> := PolynomialRing(Rationals());
K<b> := NumberField(x^2-5);
_<xk> := PolynomialRing(K);
f := xk^6 + 2*xk^2 + 2;
J := Jacobian(HyperellipticCurve(f));

J;
TorsionSubgroup(J);
```

Out[12]:
```
Jacobian of Hyperelliptic Curve defined by y^2 = x^6 + 2*x^2 + 2 over K

In line 8, column 16:
>> TorsionSubgroup(J);
                   ^
Runtime error: TorsionSubgroup is only implemented for Jacobians of genus 2 curves over the rationals.
```

So we did it ourselves!

https://github.com/MaxPosthumus/MasterProject/tree/main

https://github.com/Aidan-Hennessey/genus2_jacobian_torsion/

Power sums over subspaces of finite fields

ANTS XVII

Yağmur Sak
Charles University, Prague

Joint work with Faruk Göloğlu, Gohar Kyureghyan and Alexander Pott

July 2026

The Idea

$V : \mathbb{F}_q$-subspace of $\mathbb{F}_{q^{m+1}}$, where $\mathbb{F}^*_{q^{m+1}} = \langle \omega \rangle$
For any $1 \leq t \leq q^{m+1} - 1$ and $c \in \mathbb{F}_{q^{m+1}}$,

$$S_t(V, c) = \sum_{v \in V} (v + c)^t.$$

For a subset T of $\mathbb{F}_{q^{m+1}}$,

$$S_t(T, c) = \sum_{x \in \mathbb{F}_{q^{m+1}}} \chi_T(x - c)x^t,$$

where $\chi_T : \mathbb{F}_{q^{m+1}} \to \{0, 1\}$ is the characteristic function of T.

$$\chi_T(x - c) \longrightarrow g(x) \longrightarrow g(\omega^k) \longrightarrow a_k \implies S_t(T, c) = \sum_{k=1}^{q^{m+1}-1} a_k \omega^{kt} \text{ for } 1 \leq t \leq q^{m+1} - 1$$

$$(S_1(T, c), \ldots, S_{q^{m+1}-1}(T, c)) \xleftrightarrow{\text{Fourier vector}} a_{q^{m+1}-1}x^{q^{m+1}} + \cdots + a_2x + a_1$$

Our Results

Conditions on t for $S_t(V, c) = 0$, V is a hyperplane of $\mathbb{F}_{p^{m+1}}$. *(Byott and Chapman)*

$S_t(V, c)$ values for all t when V is a hyperplane of $\mathbb{F}_{p^{m+1}}$.

Conditions on t for $S_t(V, c) = 0$, V is a hyperplane of $\mathbb{F}_{q^{m+1}}$. *(Chandler, Wu, and Xiang)*

$S_t(V, c)$ values for all t when V is a hyperplane of $\mathbb{F}_{q^{m+1}}$.

Question: What are the necessary & sufficient conditions on t for $S_t(V, c) = 0$ when the $\dim(V) < m$? *(Chandler, Wu, and Xiang)*

$S_t(V, c)$ values for all t when V is an $(m-1)$-dimensional subspace of $\mathbb{F}_{2^{m+1}}$.

A study on a family of the elliptic curves of rank at least 2

Pankaj Patel

Department of Mathematics
BITS Pilani Hyderabad Campus, India

Seventeenth Algorithmic Number Theory Symposium
Bernoulli Institute
University of Groningen, Netherlands
July 6–10, 2026

Family and Main Result

We study the family

$$E_{m,t}: \qquad y^2 = x^3 + m^2x^2 - t^2x,$$

where

$$m^2 = 3t^2 + 1.$$

Key observations

- $E_{m,t}(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$.
- Two explicit rational points are

$$P_1 = (t, mt), \qquad P_2 = (-1, 2t).$$

- The Pell equation

$$m^2 - 3t^2 = 1$$

has infinitely many integer solutions, producing infinitely many curves in the family.

Idea of the Proof

Compute canonical heights from the growth of $x([2^N]P)$.
The canonical height is defined by

$$\hat{h}(P) = \frac{1}{2} \lim_{N\to\infty} \frac{H([2^N]P)}{4^N}.$$

For the constructed points,

$$\hat{h}(P_1) = \frac{1}{4}, \qquad \hat{h}(P_2) = \frac{1}{2}, \qquad \hat{h}(P_1 + P_2) = \frac{5}{2}.$$

Hence the Néron–Tate height pairing matrix is

$$H = \begin{pmatrix} \langle P_1, P_1\rangle & \langle P_1, P_2\rangle \\ \langle P_1, P_2\rangle & \langle P_2, P_2\rangle \end{pmatrix} \implies H = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix}$$

Since $\det(H) = \frac{1}{4} > 0$
the points P_1 and P_2 are linearly independent.

Conclusion:

$$\operatorname{rank}(E_{m,t}(\mathbb{Q})) \geq 2.$$

Models of Kummer lines and Galois representations

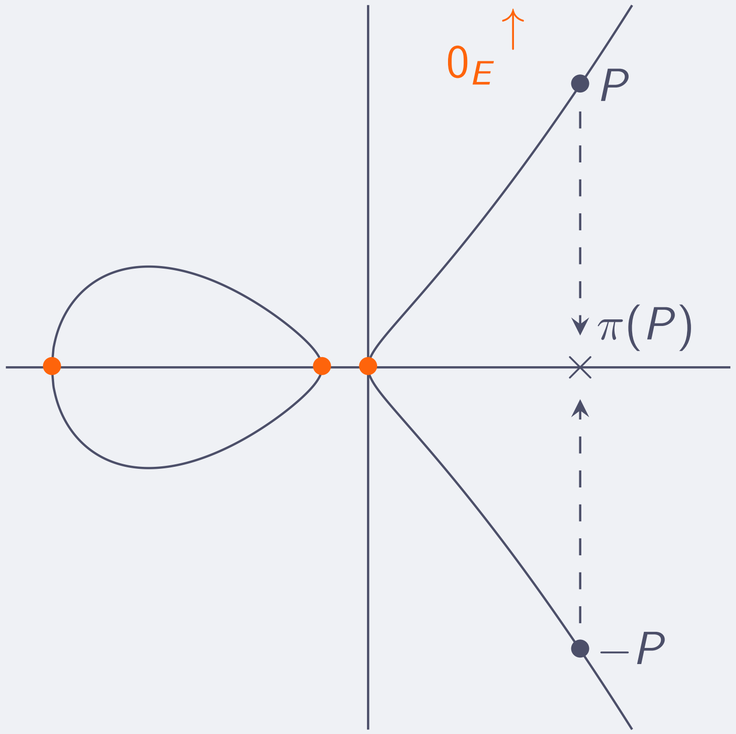
Razvan Barbulescu[1], Damien Robert[1], *Nicolas Sarkis*[2]

[1] Institut de Mathématiques de Bordeaux, France
[2] Inria Saclay, France

July 6, 2026 — Groningen, Netherlands

Pre-print (not revised yet): `ia.cr/2025/543`

Arithmetic on elliptic curves



$\pi : E \to \mathbb{P}^1$ deg. 2 cover with ramification at 2-torsion points (colored) and $\pi(P) = \pi(-P)$. Computing $n \cdot P$?

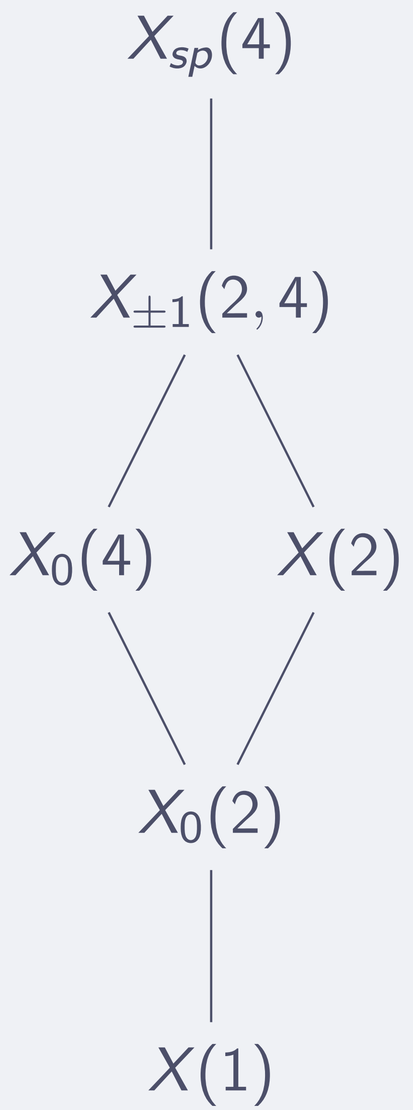
$$\left.\begin{array}{r} \pi(P), \pi(Q), \pi(P-Q) \mapsto \pi(P+Q) \\ \pi(P) \mapsto \pi(2 \cdot P) \end{array}\right\} \rightsquigarrow \text{Montgomery ladder}$$

Kummer line	$\pi(P)$
Montgomery XZ	$(X_P : Z_P)$
Theta level 2	$(\theta_0(P) : \theta_1(P))$
Theta level 2 squared	$(\theta_0(P)^2 : \theta_1(P)^2)$
Theta level 2 twisted	$(\theta_0(0_E)\theta_0(P) : \theta_1(0_E)\theta_1(P))$

How to find curves with a given Kummer line?

Point on a modular curve $P \in X \rightsquigarrow E$ with a chosen Kummer line.

Modular curve	Galois image lies in	Kummer line
$X_0(4)$	$\left\{\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \bmod 4\right\}$	Montgomery XZ
$X_{sp}(4)$	$\left\{\left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right) \bmod 4\right\}$	Theta lvl 2
$X_{\pm 1}(2,4)$	$\left\{\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \bmod 4, \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \bmod 2\right\}$	Theta lvl 2 squared
$X_{\pm 1}(2,4)$	$\left\{\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \bmod 4, \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \bmod 2\right\}$	Theta lvl 2 twisted



Montgomery type (MT) for $T \in E[2](k)$ (let $2 \cdot T_0 = T$):

$\rightsquigarrow$ when the 4-isogeny $f : E \to E/\langle T_0 \rangle$ is rational

- Montgomery XZ: one MT point
- Theta level 2: two MT points
- Theta level 2 squared / twisted: one MT point + $E[2] = E[2](k)$

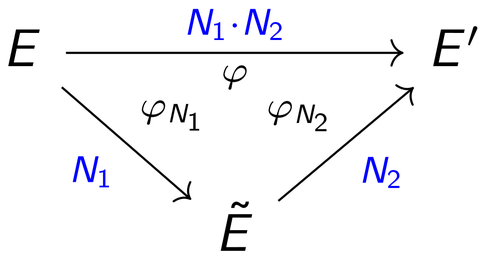
Computing 2D Cyclic Isogenies: An Approach using Kani's Reducibility Criterion

Raul Arturo Hernandez-Gonzalez

University of Virginia

Joint w/ Blair Butler, Luciano Maino, Nicolas Swanson, Suo-Jun Tan

July 6, 2026

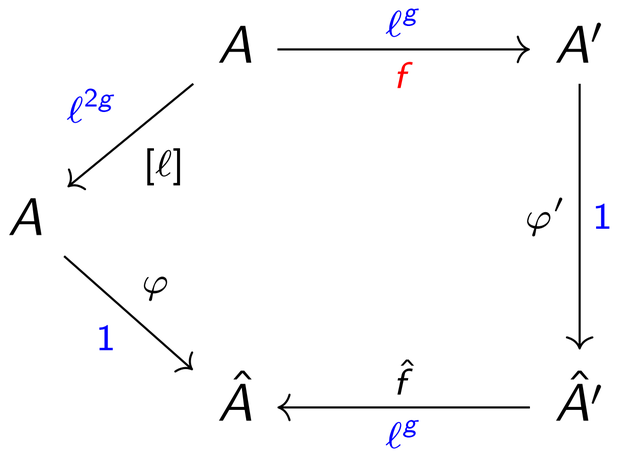


Problem: Computing isogenies is slow, specially for higher degrees.

Idea: Can we "factor" a 2-dimensional $(2, 2)$-isogeny?

Approach: Degrees in *cyclic isogenies* don't grow with dimension g.
Goal:

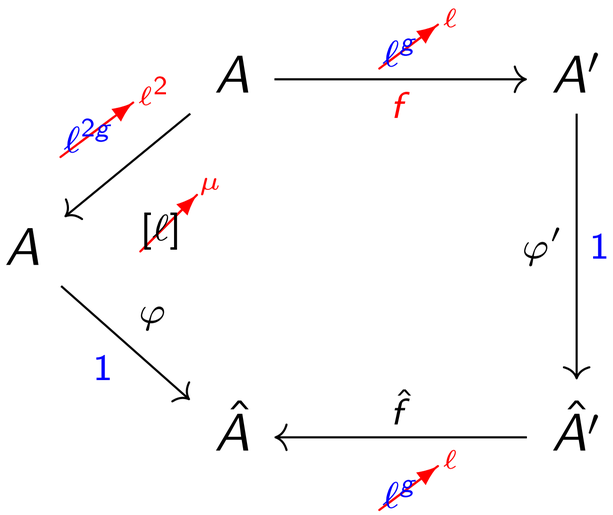
- Compute *ONE* 2D cyclic isogeny using Kani's Reducibility Criterion.

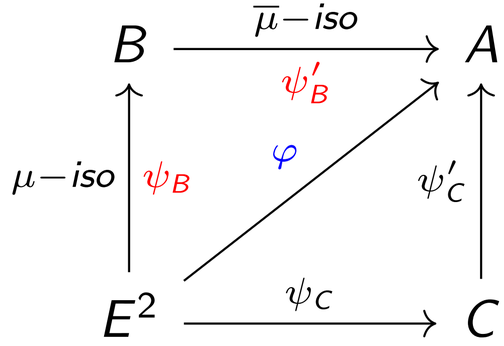


$$[\ell] : A \to A, \text{ where}$$
$$\deg(f) = \text{Norm}_*([\ell]) = \ell^g$$
$$f \text{ is a } (\ell, \cdots, \ell)\text{-isogeny}$$

Research focus on these isogenies!

- Though, cyclic isogenies have potential of outperfoming them in higher dimensions.





ℓ prime, t smooth, ℓ, t coprime.
φ is (ℓ, ℓ)-isogeny

What if: $\mu : A \to A$, where
$\deg(f) = \mathrm{Norm}_*(\mu) = \ell$
Want: f to be cyclic μ-isogeny

Φ is (t, t, t, t)-isogeny w/

$$\Phi = \begin{pmatrix} \psi_B & -\tilde{\psi}'_B \\ \psi_C & \tilde{\psi}'_C \end{pmatrix} : E^2 \times A \to B \times C$$

To compute cyclic isogenies ψ_B, ψ'_B, we need to:

- Compute an (ℓ, ℓ)-isogeny φ. (Easy!)
- Compute a (t, t, t, t)-isogeny Φ. (Hard!)

Generating endomorphism rings of supersingular elliptic curves

Jonathan Love (Leiden University)

BIRS 2025 project with Kirsten Eisenträger, Eyal Goren, Annamaria Iezzi, Harun Kir, Eda Kirimli, Will Mahaney, Jennifer Park, and Maria Sabitova

Lightning Talks @ ANTS XVII
Groningen, July 2026

Theorem (EGIKKLMPS '26++)

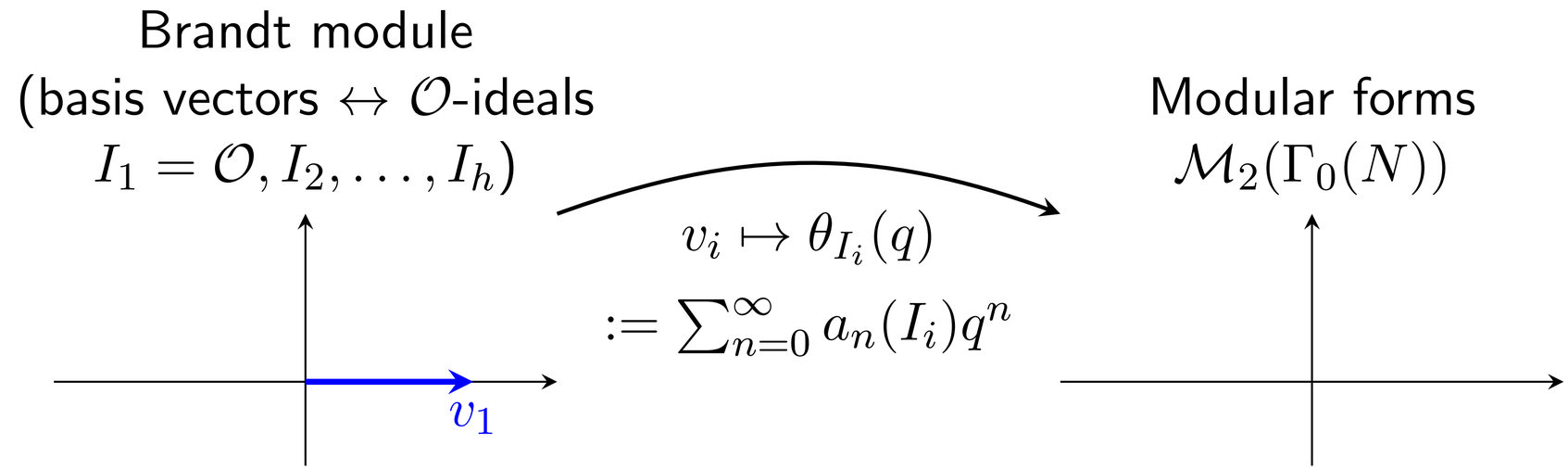
Let p, ℓ prime, $p > \ell^{30}$, and $E/\overline{\mathbb{F}}_p$ supersingular elliptic curve. If $k > \frac{5}{2}\log_\ell(3p)$ then $\mathrm{End}(E)$ is generated as a $\mathbb{Z}$-algebra by endomorphisms of degree ℓ^k.

Proof.

Let $C = \{\alpha \in \mathrm{End}(E) \mid \deg \alpha = \ell^k\}$. $\mathrm{End}(E)$ is a maximal order in a quaternion algebra $B_{p,\infty}$, and $\mathbb{Z}[C]$ is a suborder containing C.

The number of elements of norm ℓ^k in a maximal order of $B_{p,\infty}$ is strictly larger than the number in any non-maximal order, so $\mathbb{Z}[C] = \mathrm{End}(E)$. □

We need explicit bounds on $a_n(\mathcal{O}) := |\{\alpha \in \mathcal{O} \mid \mathrm{nrd}(\alpha) = n\}|$.



coefficient of q^n: $\underset{a_n(\mathcal{O})}{\theta_{\mathcal{O}}(q)} = \underset{\text{computable}}{E(q)} + \sum \underset{???}{c_i} \underset{\substack{\text{bounded} \\ \text{(Deligne)}}}{f_i(q^{e_i})}$

Brandt operator B_n: the i,j entry counts $J \subseteq I_j$ of prescribed index with $[J] = [I_i]$. (We can express θ in terms of B_n: $a_n(\mathcal{O}) = |\mathcal{O}^\times| B_n(1,1)$)

Theorem (EGIKKLMPS '26++)

For any quaternion $\mathbb{Z}$-order $\mathcal{O}$, the operators B_n pairwise commute.

$\Rightarrow$ Brandt module has an orthogonal basis of simultaneous eigenvectors.
Use this to show $\theta_{\mathcal{O}}$ lands in a certain **compact** region.

Number of point counts of abelian varieties determining the zeta function

Shiva Chidambaram

University of Wisconsin-Madison
chidambaram3@wisc.edu

Joint work with Timo Keller

ANTS XVII, Groningen

The problem: how many point counts pin down the zeta function?

Let $A/\mathbf{F}_q$ be an abelian variety of dimension g. Its zeta function is determined by the L-polynomial

$$L(A,T) = \det\bigl(1 - \mathrm{Frob}_q\, T \mid \mathrm{H}^1_{\text{ét}}\bigr) = \prod_{i=1}^{2g}(1-\alpha_i T) \quad \text{with } |\alpha_i| = q^{1/2} \quad \text{and } \alpha_i\alpha_{i+g} = q$$

Its reverse $f_A(T) = \prod_{i=1}^{2g}(T-\alpha_i) = \sum_{i=0}^{2g} a_i T^{2g-i} \in \mathbf{Z}[T]$, where $a_{g+i} = q^i a_{g-i}$ is a q-Weil polynomial.

- (Honda-Tate) Knowing $f_A \iff$ zeta function $\iff$ isogeny class
- The point counts are: $c_n := \#A(\mathbf{F}_{q^n}) = \prod_{i=1}^{2g}(1-\alpha_i^n) = \prod_{\zeta^n=1} f_A(\zeta) = \mathrm{Res}(f_A(T), T^n - 1)$.

Kedlaya's question.
How few counts $c_1, \ldots, c_N$ recover f_A?
(Kedlaya 2006): The first $2g$ point counts $c_1, \ldots, c_{2g}$ suffice once $q > 256\, g^2$.

Sturmfels–Zworski conjecture.
A monic reciprocal polynomial p of even degree $2g$ is determined by the first $g+1$ cyclic resultants
$r_m(p) = \mathrm{Res}(p(x), x^m - 1), \qquad m \le g+1.$

Question: Are the first g point counts $c_1, \ldots, c_g$ enough to recover f_A?

Theorem (C–Keller)

If $q > Q(g) = \left(16\, g^3 p(2g)\right)^{2g+2}$, then the g point counts $\#A(\mathbf{F}_{q^i})$, $1 \le i \le g$, determine f_A.

- Power sums $s_n = \sum_i \alpha_i^{-n}$: as $q^n s_n = \mathrm{Tr}(\mathrm{Frob}^n) \in \mathbf{Z}$, can round once error is $< \frac{1}{2} q^{-n}$.
- Counts give $\log(q^{gn}/c_n) = \sum_j s_{jn}/j$, which can be inverted by Möbius inversion.
- recursive error bound on s_n for $g/2 < i \le g$, using Newton-Girard identities + functional equation

Question: Is this optimal, i.e., are g point counts necessary?

Let $N(g) :=$ least number of points counts that can recover *every* isogeny class (for large enough q).

- g=3**:** $N(3) = 2$ — c_1, c_2 give the *linear* data $f_A(\pm 1)$; the fibre line has lattice points $\sim q^2$ apart, the Weil region only $\sim q^{3/2}$ wide $\Rightarrow \le 1$ q-Weil polynomial (for $q \ge 16$).
- g=4**:** $N(4) = 4$. Two "$\mathbf{Z}[q]$-families" of non-isogenous fourfolds sharing c_1, c_2, c_3 but not c_4.
  $T^8 - (q+1)T^5 - (q^2+q+2)T^4 - q(q+1)T^3 + q^4$; $\quad T^8 - 2T^6 - (q+1)T^5 + (q^2-q)T^4 - q(q+1)T^3 - 2q^2T^2 + q^4$
- g=5, 6**:** no two "$\mathbf{Z}[q]$-families" share the first 4 point counts (Gröbner elimination)

Challenge: Prove or disprove: $N(5) = 4$; $N(6) = 4$. What is the least k such that $N(g) \sim kg$?

Simultaneous Approximation for Lattice-Based Cryptography

Julia VanLandingham

Clemson University

What You Probably Already Know

- Cryptography is very useful and important 🙂

What You Probably Already Know

- Cryptography is very useful and important 🙂
- Shor's algorithm puts classical cryptography at risk ☹

What You Probably Already Know

- Cryptography is very useful and important 🙂
- Shor's algorithm puts classical cryptography at risk ☹
- Lattices are very popular for quantum-secure algorithms 🙂

What You Probably Already Know

- Cryptography is very useful and important 🙂
- Shor's algorithm puts classical cryptography at risk ☹
- Lattices are very popular for quantum-secure algorithms 🙂
- Naive implementations take n^2 numbers to describe ☹

What You Probably Already Know

- Cryptography is very useful and important 🙂
- Shor's algorithm puts classical cryptography at risk ☹
- Lattices are very popular for quantum-secure algorithms 🙂
- Naive implementations take n^2 numbers to describe ☹
- Ideal lattices can be described with n numbers! 🙂

What You Probably Already Know

- Cryptography is very useful and important 🙂
- Shor's algorithm puts classical cryptography at risk ☹
- Lattices are very popular for quantum-secure algorithms 🙂
- Naive implementations take n^2 numbers to describe ☹
- Ideal lattices can be described with n numbers! 🙂
- Ideal lattices may not be as secure as general lattices ☹

What You Probably Don't Know

- Martin defined Simultaneous Approximation (SA) Lattices (2020)

What You Probably Don't Know

- Martin defined Simultaneous Approximation (SA) Lattices (2020)
  - Only require $n + 1$ numbers to describe!

What You Probably Don't Know

- Martin defined Simultaneous Approximation (SA) Lattices (2020)
  - Only require $n + 1$ numbers to describe!
  - SVP in these lattices is the same as SAP!

What You Probably Don't Know

- Martin defined Simultaneous Approximation (SA) Lattices (2020)
  - Only require $n + 1$ numbers to describe!
  - SVP in these lattices is the same as SAP!
- Martin gave reduction from SVP to SAP using SA lattices (2020)

What You Probably Don't Know

- Martin defined Simultaneous Approximation (SA) Lattices (2020)
  - Only require $n + 1$ numbers to describe!
  - SVP in these lattices is the same as SAP!
- Martin gave reduction from SVP to SAP using SA lattices (2020)
  - So these are as secure as general lattices!

What You Probably Don't Know

- Martin defined Simultaneous Approximation (SA) Lattices (2020)
  - Only require $n + 1$ numbers to describe!
  - SVP in these lattices is the same as SAP!
- Martin gave reduction from SVP to SAP using SA lattices (2020)
  - So these are as secure as general lattices!
- V. defined CVP and SIVP in SA lattices (2026)

What You Probably Don't Know

- Martin defined Simultaneous Approximation (SA) Lattices (2020)
  - Only require $n + 1$ numbers to describe!
  - SVP in these lattices is the same as SAP!
- Martin gave reduction from SVP to SAP using SA lattices (2020)
  - So these are as secure as general lattices!
- V. defined CVP and SIVP in SA lattices (2026)
- V. gave reductions from CVP and SIVP to SA counterparts (2026)

What You Probably Don't Know

- Martin defined Simultaneous Approximation (SA) Lattices (2020)
  - Only require $n + 1$ numbers to describe!
  - SVP in these lattices is the same as SAP!
- Martin gave reduction from SVP to SAP using SA lattices (2020)
  - So these are as secure as general lattices!
- V. defined CVP and SIVP in SA lattices (2026)
- V. gave reductions from CVP and SIVP to SA counterparts (2026)
  - Also improved the SVP case from Martin's results

What You Probably Don't Know

- Martin defined Simultaneous Approximation (SA) Lattices (2020)
  - Only require $n + 1$ numbers to describe!
  - SVP in these lattices is the same as SAP!
- Martin gave reduction from SVP to SAP using SA lattices (2020)
  - So these are as secure as general lattices!
- V. defined CVP and SIVP in SA lattices (2026)
- V. gave reductions from CVP and SIVP to SA counterparts (2026)
  - Also improved the SVP case from Martin's results
  - Approximate a general lattice by an SA lattice and transform the problem

On a conjecture of Lenny Jones about some monogenic polynomials

Sumandeep Kaur

Department of Mathematics,
Shanghai University, China-200444

Monogenic Polynomial

A monic irreducible polynomial $f(x)$ with integer coefficients is said to be monogenic if $\mathbb{Z}[\theta]$ is the ring of integers of $\mathbb{Q}(\theta)$, where θ is a root of $f(x)$.

Question: Given a monic irreducible polynomial $f(x) \in \mathbb{Z}[x]$ with a root θ, when is $\mathbb{Q}(\theta)$ monogenic?

If $f(x)$ is the minimal polynomial of an algebraic integer θ over $\mathbb{Q}$, then the discriminant $\triangle_f$ of $f(x)$ and the discriminant d_K of $K = \mathbb{Q}(\theta)$, are related by the formula

$$\triangle_f = [\mathbb{Z}_K : \mathbb{Z}[\theta]]^2 d_K, \tag{1}$$

where $\mathbb{Z}_K$ is the ring of integers of K. The group index $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ will be denoted by $\mathrm{ind}_K(\theta)$.

Conjecture by L. Jones [Bull. Aust. Math. Soc. 100 (2019), 239-244]

Let p be a prime number, n, m and B be positive integers with $m < n,\ n > 2$ and $\gcd(n, mB) = 1$. Then $f(x) = x^n + p(Bx + 1)^m$ is monogenic if and only if $n^n + (-1)^{n+m} B^n (n - m)^{n-m} m^m p$ is square-free.

Theorem 1.1. (-, Kumar), 2024

Let A and B are integers, n and m are positive integers with $m < n, n > 2$ and $B \neq 0$. Assume that $\gcd(n, mB) = 1$. Then an irreducible polynomial of the type $f(x) = x^n + A(Bx + 1)^m$ is monogenic if and only if both A and $n^n + (-1)^{n+m} B^n (n - m)^{n-m} m^m A$ are square-free.

It may be pointed out that in the above theorem the assumption '$\gcd(n, mB) = 1$' cannot be dropped.

Ours Goes to 211:

Euler pseudoprimes to 47 prime bases from Carmichael numbers

ALEJANDRA ALCANTARILLA SANCHEZ[1], JOLIJN COTTAAR[1], TANJA LANGE[1,2], AND BENNE DE WEGER[1]

[1]Eindhoven University of Technology, [2]Academia Sinica Taiwan

TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY

How far can a composite number pretend to be prime?

How far can a composite number pretend to be prime?

The Test

How far can a composite number pretend to be prime?

The Test

Proving primality is often too expensive

How far can a composite number pretend to be prime?

The Test

Proving primality is often too expensive

Need for compositeness tests

How far can a composite number pretend to be prime?

The Test

Proving primality is often too expensive

⇩

Need for compositeness tests

⇩

Solovay-Strassen

$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \ (mod\ n)$$

How far can a composite number pretend to be prime?

The Test

Proving primality is often too expensive

⇩

Need for compositeness tests

⇩

Solovay-Strassen

$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \ (mod\ n)$$

⇧

Non-prime n passing this test is Euler pseudoprime to base a

How far can a composite number pretend to be prime?

The Test

Proving primality is often too expensive

⇩

Need for compositeness tests

⇩

Solovay-Strassen

$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \ (mod\ n)$$

⇧

Non-prime n passing this test is Euler pseudoprime to base a

The Suspects

How far can a composite number pretend to be prime?

The Test

Proving primality is often too expensive

⇩

Need for compositeness tests

⇩

Solovay-Strassen

$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \ (mod\ n)$$

⇧

Non-prime n passing this test is Euler pseudoprime to base a

The Suspects

Maximum number of Euler liars?

How far can a composite number pretend to be prime?

The Test

Proving primality is often too expensive

⇩

Need for compositeness tests

⇩

Solovay-Strassen

$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \ (mod\ n)$$

⇧

Non-prime n passing this test is Euler pseudoprime to base a

The Suspects

Maximum number of Euler liars?

⇩

Carmichael Number n:
$a^{n-1} \equiv 1\ (mod\ n)$
for all a coprime to n.

How far can a composite number pretend to be prime?

The Test

Proving primality is often too expensive

⇩

Need for compositeness tests

⇩

Solovay-Strassen

$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \ (mod\ n)$$

⇧

Non-prime n passing this test is Euler pseudoprime to base a

The Suspects

Maximum number of Euler liars?

⇩

Carmichael Number n:
$a^{n-1} \equiv 1\ (mod\ n)$
for all a coprime to n.

⇩

If $\frac{n-1}{\lambda(n)}$ is even:

$\frac{1}{2}\varphi(n)$ Euler liars
(Class A)

How far can a composite number pretend to be prime?

The Test

Proving primality is often too expensive

⇩

Need for compositeness tests

⇩

Solovay-Strassen

$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \ (mod\ n)$$

⇧

Non-prime n passing this test is Euler pseudoprime to base a

The Suspects

Maximum number of Euler liars?

⇩

Carmichael Number n:
$a^{n-1} \equiv 1\ (mod\ n)$
for all a coprime to n.

⇩

If $\frac{n-1}{\lambda(n)}$ is even:

$\frac{1}{2}\varphi(n)$ Euler liars
(Class A)

The Method

How far can a composite number pretend to be prime?

The Test

Proving primality is often too expensive

⇩

Need for compositeness tests

⇩

Solovay-Strassen

$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \ (mod\ n)$$

⇧

Non-prime n passing this test is Euler pseudoprime to base a

The Suspects

Maximum number of Euler liars?

⇩

Carmichael Number n:
$a^{n-1} \equiv 1\ (mod\ n)$
for all a coprime to n.

⇩

If $\frac{n-1}{\lambda(n)}$ is even:

$\frac{1}{2}\varphi(n)$ Euler liars
(Class A)

The Method

List of Carmichael numbers
(See Shallue & Webster,
Friday 11:30)

How far can a composite number pretend to be prime?

The Test

Proving primality is often too expensive

⇩

Need for compositeness tests

⇩

Solovay-Strassen

$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \ (mod\ n)$$

⇧

Non-prime n passing this test is Euler pseudoprime to base a

The Suspects

Maximum number of Euler liars?

⇩

Carmichael Number n:
$a^{n-1} \equiv 1\ (mod\ n)$
for all a coprime to n.

⇩

If $\frac{n-1}{\lambda(n)}$ is even:

$\frac{1}{2}\varphi(n)$ Euler liars
(Class A)

The Method

List of Carmichael numbers
(See Shallue & Webster, Friday 11:30)

⇩

Solovay-Strassen test
for small prime bases

How far can a composite number pretend to be prime?

The Test

Proving primality is often too expensive

⇩

Need for compositeness tests

⇩

Solovay-Strassen

$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \ (mod\ n)$$

⇧

Non-prime n passing this test is Euler pseudoprime to base a

The Suspects

Maximum number of Euler liars?

⇩

Carmichael Number n:
$a^{n-1} \equiv 1\ (mod\ n)$
for all a coprime to n.

⇩

If $\frac{n-1}{\lambda(n)}$ is even:

$\frac{1}{2}\varphi(n)$ Euler liars
(Class A)

The Method

List of Carmichael numbers
(See Shallue & Webster, Friday 11:30)

⇩

Solovay-Strassen test for small prime bases

⇩

Multiplication between class A

The result: Ours goes to 211

- 1230-bit Euler pseudoprime
- Passes first 47 prime bases… until 211

The result: Ours goes to 211

- 1230-bit Euler pseudoprime
- Passes first 47 prime bases… until 211

297180253242403184105341150390525401177755979450850674143574534366013877426704534
593555915420699343889059073145832891673993841274696136803836427921670679792296684
633516565295275589915225338961827697395774510820672522818570055652099552788792514
216529771842300258718279723455898329630840119845009750759993111718562286885100243
830307487082192012147931844333404766921904576 01

The result: Ours goes to 211

- 1230-bit Euler pseudoprime
- Passes first 47 prime bases… until 211

297180253242403184105341150390525401177755979450850674143574534366013877426704534
593555915420699343889059073145832891673993841274696136803836427921670679792296684
633516565295275589915225338961827697395774510820672522818570055652099552788792514
216529771842300258718279723455898329630840119845009750759993111718562286885100243
830307487082192012147931844333404766921904576 01

Check the paper and poster for more info!

Sums of two units in number fields

17th Algorithmic Number Theory Symposium (ANTS XVII)
Bernoulli Institute, Rijksuniversiteit Groningen

Robin Visser
(based on joint work with Magdaléna Tinková (Charles), Pavlo Yatsyna (Charles), and Volker Ziegler (Salzburg))

Faculty of Mathematics and Physics
Charles University

06 July 2026

Motivation

Let K be a number field with ring of integers $\mathcal{O}_K$. We study the equation

$$\varepsilon + \delta = n, \qquad n \in \mathbb{Z}_{>0}, \quad \varepsilon, \delta \in \mathcal{O}_K^\times.$$

Motivation

Let K be a number field with ring of integers $\mathcal{O}_K$. We study the equation

$$\varepsilon + \delta = n, \qquad n \in \mathbb{Z}_{>0}, \quad \varepsilon, \delta \in \mathcal{O}_K^{\times}.$$

For a fixed nonzero n, Siegel's theorem gives only finitely many solutions (ε, δ), and Baker's theory of linear forms in logarithms makes them effectively computable.

Motivation

Let K be a number field with ring of integers $\mathcal{O}_K$. We study the equation

$$\varepsilon + \delta = n, \qquad n \in \mathbb{Z}_{>0}, \quad \varepsilon, \delta \in \mathcal{O}_K^\times.$$

For a fixed nonzero n, Siegel's theorem gives only finitely many solutions (ε, δ), and Baker's theory of linear forms in logarithms makes them effectively computable.

What if we don't fix n? Let's define

$$\mathcal{N}_K := \left\{ n \in \mathbb{Z}_{>0} \mid n = \varepsilon + \delta \text{ for some } \varepsilon, \delta \in \mathcal{O}_K^\times \right\}.$$

Motivation

Let K be a number field with ring of integers $\mathcal{O}_K$. We study the equation

$$\varepsilon + \delta = n, \qquad n \in \mathbb{Z}_{>0}, \quad \varepsilon, \delta \in \mathcal{O}_K^\times.$$

For a fixed nonzero n, Siegel's theorem gives only finitely many solutions (ε, δ), and Baker's theory of linear forms in logarithms makes them effectively computable.

What if we don't fix n? Let's define

$$\mathcal{N}_K := \left\{ n \in \mathbb{Z}_{>0} \mid n = \varepsilon + \delta \text{ for some } \varepsilon, \delta \in \mathcal{O}_K^\times \right\}.$$

We are interested in the following two questions:

1. For which number fields K is $\mathcal{N}_K$ finite?
2. When $\mathcal{N}_K$ is finite, can we compute it explicitly?

Finiteness of $\mathcal{N}_K$

Theorem (Tinková–V–Yatsyna 2025)

Let K be a number field not containing any real quadratic subfield. Then $\mathcal{N}_K$ is finite.

Finiteness of $\mathcal{N}_K$

Theorem (Tinková–V–Yatsyna 2025)

Let K be a number field not containing any real quadratic subfield. Then $\mathcal{N}_K$ is finite.

- Let $\varepsilon^{(1)}, \ldots, \varepsilon^{(d)}$ and $\delta^{(1)}, \ldots, \delta^{(d)}$ be the d distinct conjugates of ε and δ resp.
  If $\varepsilon + \delta = n$, then $\varepsilon^{(i)} + \delta^{(i)} - \varepsilon^{(j)} - \delta^{(j)} = 0$: a unit equation in several unknowns.
  The non-degenerate solutions are finite (Evertse, van der Poorten–Schlickewei).

Finiteness of $\mathcal{N}_K$

Theorem (Tinková–V–Yatsyna 2025)

Let K be a number field not containing any real quadratic subfield. Then $\mathcal{N}_K$ is finite.

- Let $\varepsilon^{(1)}, \ldots, \varepsilon^{(d)}$ and $\delta^{(1)}, \ldots, \delta^{(d)}$ be the d distinct conjugates of ε and δ resp. If $\varepsilon + \delta = n$, then $\varepsilon^{(i)} + \delta^{(i)} - \varepsilon^{(j)} - \delta^{(j)} = 0$: a unit equation in several unknowns. The non-degenerate solutions are finite (Evertse, van der Poorten–Schlickewei).

Theorem (V–Ziegler 2026)

Let K be a number field such that either $D = [K : \mathbb{Q}]$ is odd, or $D \geq 3$ and K primitive. Then $\mathcal{N}_K$ is effectively computable: i.e. there is an effectively computable constant C_K with $n \leq C_K$ for all $n \in \mathcal{N}_K$.

Finiteness of $\mathcal{N}_K$

Theorem (Tinková–V–Yatsyna 2025)

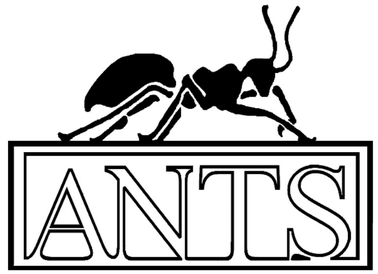
Let K be a number field not containing any real quadratic subfield. Then $\mathcal{N}_K$ is finite.

- Let $\varepsilon^{(1)}, \ldots, \varepsilon^{(d)}$ and $\delta^{(1)}, \ldots, \delta^{(d)}$ be the d distinct conjugates of ε and δ resp. If $\varepsilon + \delta = n$, then $\varepsilon^{(i)} + \delta^{(i)} - \varepsilon^{(j)} - \delta^{(j)} = 0$: a unit equation in several unknowns. The non-degenerate solutions are finite (Evertse, van der Poorten–Schlickewei).

Theorem (V–Ziegler 2026)

Let K be a number field such that either $D = [K : \mathbb{Q}]$ is odd, or $D \geq 3$ and K primitive. Then $\mathcal{N}_K$ is effectively computable: i.e. there is an effectively computable constant C_K with $n \leq C_K$ for all $n \in \mathcal{N}_K$.

- Given $\varepsilon^{(i)} + \delta^{(i)} - \varepsilon^{(j)} - \delta^{(j)} = 0$, the unit matching techniques of Bajpai and Bennett gives a lower bound for the *second smallest* element of $|\varepsilon^{(i)}|$, $|\delta^{(i)}|$, $|\varepsilon^{(j)}|$, $|\delta^{(j)}|$. Applying known effective bounds on linear forms on logarithms proves the result.



Seventeenth Algorithmic Number Theory

Symposium ANTS XVII

Groningen, Netherlands

Families of Real Biquadratic Fields with 2-Iwasawa Module Rank 3

Presented by : **IKRAME DAQAQ**

Joint Work with: **Pr. M. M. Chems-eddin**

Sidi Mohamed Ben Abdellah University, Morocco (FSDM)

July 6, 2026

Notation

- Let k be a number field. We denote by $A(k)$ the 2-class group of k. A $\mathbb{Z}_2$-extension of k is an infinite extension of k denoted by k_∞/k such that $\mathrm{Gal}(k_\infty/k) \simeq \mathbb{Z}_2$, where $\mathbb{Z}_2$ denotes the ring of 2-adic integers.
  For each $n \geq 1$, let $\mathbb{Q}_{2,n} = \mathbb{Q}\left(2\cos\left(\frac{2\pi}{2^{n+2}}\right)\right)$, and put $k_n = k\mathbb{Q}_{2,n}$. Then $k = k_0 \subset k_1 \subset k_2 \subset \cdots \subset k_n \subset \cdots \subset k_\infty = \bigcup_{n\geq 0} k_n$.
  The inverse limit $A_\infty(k) := \varprojlim A(k_n)$, with respect to the norm maps, is called the Iwasawa module for k_∞/k.

Notation

- Let k be a number field. We denote by $A(k)$ the 2-class group of k. A $\mathbb{Z}_2$-extension of k is an infinite extension of k denoted by k_∞/k such that $\mathrm{Gal}(k_\infty/k) \simeq \mathbb{Z}_2$, where $\mathbb{Z}_2$ denotes the ring of 2-adic integers.
  For each $n \geq 1$, let $\mathbb{Q}_{2,n} = \mathbb{Q}\left(2\cos\left(\frac{2\pi}{2^{n+2}}\right)\right)$, and put $k_n = k\mathbb{Q}_{2,n}$. Then $k = k_0 \subset k_1 \subset k_2 \subset \cdots \subset k_n \subset \cdots \subset k_\infty = \bigcup_{n\geq 0} k_n$.
  The inverse limit $A_\infty(k) := \varprojlim A(k_n)$, with respect to the norm maps, is called the Iwasawa module for k_∞/k.
- In previous work, M. Chems Eddin classified all real biquadratic fields satisfying :

$$\mathrm{rank}(A(k)) = \mathrm{rank}(A_\infty(k)) \leq 2.$$

Notation

- Let k be a number field. We denote by $A(k)$ the 2-class group of k. A $\mathbb{Z}_2$-extension of k is an infinite extension of k denoted by k_∞/k such that $\mathrm{Gal}(k_\infty/k) \simeq \mathbb{Z}_2$, where $\mathbb{Z}_2$ denotes the ring of 2-adic integers.

  For each $n \geq 1$, let $\mathbb{Q}_{2,n} = \mathbb{Q}\left(2\cos\left(\frac{2\pi}{2^{n+2}}\right)\right)$, and put $k_n = k\mathbb{Q}_{2,n}$. Then $k = k_0 \subset k_1 \subset k_2 \subset \cdots \subset k_n \subset \cdots \subset k_\infty = \bigcup_{n\geq 0} k_n$.
  The inverse limit $A_\infty(k) := \varprojlim A(k_n)$, with respect to the norm maps, is called the Iwasawa module for k_∞/k.
- In previous work, M. Chems Eddin classified all real biquadratic fields satisfying :

$$\mathrm{rank}(A(k)) = \mathrm{rank}(A_\infty(k)) \leq 2.$$

- Let K be a real biquadratic number field such that K_1/K is a ramified extension of QO-fields, where $K_1 = K(\sqrt{2})$ is the first layer of the cyclotomic $\mathbb{Z}_2$-extension of K.
  Consider the following problems:

  What are the real biquadratic fields K such that

$$\mathrm{rank}(A(K_\infty)) = 3 \qquad \text{and} \qquad \mathrm{rank}(A(K_\infty)) = \mathrm{rank}(A(K))?$$

Theorem

Let F be a real biquadratic number field that is of the form $F := \mathbb{Q}(\sqrt{q}, \sqrt{d})$. Then $\text{rank}(A(F_\infty)) = 3$ and $\text{rank}(A(F_\infty)) = \text{rank}(A(F))$ if and only if F takes one of the following forms:

1. $F := \mathbb{Q}(\sqrt{q}, \sqrt{d})$ where $q \equiv 3 \pmod 4$ is a prime number and $d > 2$ is square free integer relatively prime to q, and $d = rst$, where r, s and t are two prime numbers such that $\left(\frac{q}{s}\right) = \left(\frac{q}{r}\right) = \left(\frac{q}{t}\right) = 1$ and one of the following conditions holds
   1. $q \equiv 3 \pmod 8$ and $r \equiv t \equiv 3 \pmod 8$ and $s \equiv 5 \pmod 8$
   2. $q \equiv 3 \pmod 8$ and $r \equiv 3 \pmod 8$ and $s \equiv t \equiv 5 \pmod 8$
   3. $q \equiv 3 \pmod 8$ and $r \equiv 3 \pmod 8$ and $s \equiv 5 \pmod 8$, $t \equiv 7 \pmod 8$, in this case $rank(A(F_1)) \in \{3,4\}$ and it's equal to 3 if and only if $\overline{\sqrt{\varepsilon_{2q}}} \notin < \overline{-1}, \overline{\varepsilon_2}, \overline{\sqrt{\varepsilon_q}} >$
   4. $q \equiv 3 \pmod 8$ and $r \equiv t \equiv 5 \pmod 8$ and $s \equiv 7 \pmod 8$ $rank(A(F_1)) \in \{3,4\}$ and it's equal to 3 if and only if $\overline{\sqrt{\varepsilon_{2q}}}, \notin < \overline{-1}, \overline{\varepsilon_2}, \overline{\sqrt{\varepsilon_q}} >$
   5. $q \equiv 7 \pmod 8$ and $r \equiv t \equiv 3 \pmod 8$ and $s \equiv 5 \pmod 8$
   6. $q \equiv 7 \pmod 8$ and $r \equiv 3 \pmod 8$ and $s \equiv t \equiv 5 \pmod 8$
   7. $q \equiv 3 \pmod 8$, $r \equiv 3 \pmod 8$, $s \equiv 7 \pmod 8$ and $t \equiv 3 \pmod 8$ and such that $\overline{\sqrt{\varepsilon_{2q}}}, \overline{\sqrt{\varepsilon_q}} \notin < \overline{-1}, \overline{\varepsilon_2}, >$