ICEAGE 2026

Isogenies, Cryptography, and Explicit Arithmetic GEometry

28–30 October 2026 at the University of Lleida

Organizing Committee

Samuele Anni (Aix–Marseille Université)
Elena Berardini (CNRS; IMB, Université de Bordeaux)
Jordi Pujolàs (University of Lleida)
Benjamin Smith (Inria and LIX, Ecole polytechnique)

Invited Speakers

Leonardo Colò (University of Waterloo)
Claus Fieker (RPTU Kaiserslautern Landau)
Francesc Fité (Universitat de Barcelona)
Sabrina Kunzweiler (Centre Inria de l'Université de Bordeaux)
Elisa Lorenzo García (Aix–Marseille Université)
Christophe Ritzenthaler (Université de Rennes and Université Côte d'Azur)
Peter Stevenhagen (Universiteit Leiden)
Benjamln Wesolowski (CNRS; ENS Lyon)

Contents

Invited talks **3**

Oriented supersingular isogeny graphs with level structure – L. Colò 3
Computer–Algebra: From Toy to Tool – C. Fieker 4
Elliptic curves attached to Jacobian – F. Fité 5
Invariants for abelian fourfolds of Weil type – S. Kunzweiler 6
Sato–Tate groups of Fermat hypersurfaces, and sign ambiguities between Jacobi sums – E. Lorenzo García 7
Diving into $\mathcal{A}_2$ – C. Ritzenthaler 8
Elliptic curves and entanglements – P. Stevenhagen 9
The supersingular endomorphism ring problem – B. Wesolowski . . 10

Contributed talks **11**

Categorical equivalences for supersingular elliptic curves – S. Arpin 11
Inseparable endomorphisms of supersingular elliptic – Y. Aubry . . 12
Minimisation of quintic covers and some Hilbert modular surfaces of full level 2 – S. Frengley 13
A polred based reduction for the division polynomials of the universal elliptic curve – J. A. Galvez Gomez 14
Products of point counts of higher genus curves over finite fields – K. Kedlaya 15
Detecting splitting and real multiplication on superspecial abelian surfaces – E. Kırımlı 16
Absolutely irreducible Tate modules of Jacobians over p-adic fields – A. Konstantinou 17
Hashing-friendly elliptic curves – D. Koshelev 18
Are short proofs hard to find? – A. Sutherland 19
Supersingular Elliptic Curves Far from their Frobenius Conjugates – N. Swanson 20
Weil restriction and Coleman's conjecture – P. Tchamitchian 21
On the Semistability Defect of Hyperelliptic Curves and Cluster Picture – J. Vilà–Casadevall 22

Oriented supersingular isogeny graphs with level structure

Leonardo Colò

University of Waterloo

Supersingular isogeny graphs play an important role in both arithmetic geometry and isogeny-based cryptography. In this talk, we will explore what happens when we endow their vertices with two kinds of additional data: an orientation, coming from an embedding of an imaginary quadratic order into the endomorphism ring, and a level structure. Orientations give access to class group actions and distinguish horizontal, ascending and descending isogenies, while level structures let us work with finer moduli than the usual j-invariant, revealing additional structure in the graphs. An interesting example comes from Weber functions. Their modular polynomials are much smaller and sparser than their classical counterparts, making them useful for explicit isogeny computations. We will explain the level structures behind these functions and how they allow us to navigate supersingular isogeny graphs efficiently. Level structure also enriches the arithmetic of these graphs. Their adjacency operators describe Hecke actions on supersingular modules, connecting explicit computations in the graphs with modular forms and associated Galois representations. We will discuss how passing to higher level extends this approach and how the same computational tools serve both arithmetic and cryptographic applications. This talk is based on joint work with David Kohel.

University of Waterloo, 200 University Avenue West, Waterloo, Ontario, N2L 3G1, Canada.
e-mail: lcolo@uwaterloo.ca

Computer–Algebra: From Toy to Tool

Claus Fieker

RPTU Kaiserslautern Landau, Germany

Over the last 30+ years computer–algebra has transformed itself from being more a toy (OK, a tool for specialists) to being an indispensable tool for almost anyone working in algebra. Originally Zassenhaus defined the four main problems in computational number theory to be

- The ring of integers
- The unit group
- The class group
- The Galois group

and proceeded to develop algorithms for all of them, however at the time when I started, those were mostly endpoints, leaves in the graph of methods: the main result was that the class group e.g. is trivial - and thats it. Computation of a generator for an arbitrary ideal was a different method - not linked to the class group. Furthermore, working towards the class group tried to be independent of even the ring of integers!

Over the last 30 years this has changed. One can argue that the class group itself is mostly not interesting any more, the main result is an effective *map* projecting ideals onto the class group! This change of perspective towards the maps, and thus the relations between the objects was crucial for the development of computer algebra - and in fact, one of my earliest emails with David was discussing that maps should have a proper place in the scheme of things, adhere to mathematical rules (and fit into a commutative diagram of course).

I will follow this with the development of class groups to class fields to modern computational Galois cohomology, partly in Magma, pari/gp and Oscar. We will see how it morphed from celebrating a single class group, or a single elliptic curve to being able to perform calulations involving thousands of them!

RPTU in Kaiserslautern, Gottlieb-Daimler-Straße, 67663 Kaiserslautern, Germany
claus.fieker@rptu.de

Elliptic curves attached to Jacobians with imaginary multiplication

Francesc Fité

Universitat de Barcelona, Barcelona, Catalunya

Let M be an imaginary quadratic field and A be an abelian variety of odd dimension g defined over $\mathbb{Q}$ such that A_M is endowed with a multiplication by M of signature $(\lceil g/2 \rceil, \lfloor g/2 \rfloor)$. Extending joint work with Goodman, we show the existence of an elliptic curve E over $\mathbb{Q}$ with complex multiplication by M such that $H^1_{\text{et}}(E_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)$ is a $G_{\mathbb{Q}}$-subrepresentation of $H^g_{\text{et}}(A_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell(\lfloor g/2 \rfloor))$. In this talk, I will explicitly describe E for A in two different families. First, when A is the Jacobian of the curve $y^2 = xh(x^2)$, where $h \in \mathbb{Z}[x]$ is a degree g monic separable polynomial with $h(0) \neq 0$, we show that E is given by $y^2 = x^3 + h(0)x$. Second, when A is the Jacobian of $y^3 = f(x)$, where $h \in \mathbb{Z}[x]$ is a degree 4 monic separable polynomial, we show that E is given by $y^2 = x^3 + 16\text{disc}(f)$. As an application, I will derive a practical average polynomial time algorithm to compute the Zeta functions of the reductions of a Picard curve. This is joint work with Francesc Pedret.

Universitat de Barcelona, Gran via de les Corts Catalanes 585, 08007, Barcelona, Catalunya
e-mail: francesc.fite@gmail.com

Invariants for abelian fourfolds of Weil type

Sabrina Kunzweiler

Centre Inria de l'université de Bordeaux,
Institut de Mathématiques de Bordeaux

Isogeny-based cryptography is a candidate for post-quantum cryptography. An important building block is the action of ideals on oriented elliptic curves. Recently, it was suggested by Robert to extend this idea by considering the action of modules on oriented abelian varieties. A concrete proposal is the module-isogeny key exchange (MIKE) which relies on the action of rank-2 modules. The shared keys in this protocol are principally polarized abelian fourfolds. In order to represent such fourfolds in a unique way, it is crucial to know absolute invariants.

In general, the construction of absolute invariants for principally polarized abelian fourfolds is an open problem. In this talk, we present new absolute invariants for the class of abelian fourfolds appearing in the MIKE protocol. This makes use of the fact that these abelian fourfolds are naturally equipped with an automorphism of order 4. In particular, they belong to the moduli space of *abelian fourfolds of Weil type with* $\mathbb{Q}(i)$.

The talk is based on joint work with the MIKE team (Andrea Basso, Pierrick Dartois, Max Duparc, Jonathan Komada Eriksen, Sabrina Kunzweiler, Michael Meyer, Giacomo Pope, Krijn Reijnders, Damien Robert, Ryan Rueger and Sina Schaeffler).

Centre Inria de l'université de Bordeaux, 200 Av. de la Vieille Tour, 33405 Talence, France
sabrina.kunzweiler@math.u-bordeaux.fr

Sato–Tate groups of Fermat hypersurfaces and sign ambiguities between Jacobi sums

Elisa Lorenzo García

Aix–Marseille Université

The Fermat hypersurface $X_n^m : \ x_0^m + \cdots + x_{n+1}^m = 0$ has a very convenient feature: by a theorem of Deligne, Frobenius acts diagonally on its middle cohomology with eigenvalues given by Jacobi sums, and by a theorem of Weil these Jacobi sums are Hecke characters of $\mathbb{Q}(\zeta_m)$. In my thesis I used this to compute the Sato–Tate group of X_n^m and to prove the generalized Sato–Tate conjecture for these varieties, conditionally on a conjecture about the multiplicative relations between Jacobi sums.

In this talk I will revisit those results together with several recent updates. First, the hypothesis can be dispensed with: the conjecture holds unconditionally for every $m \geq 3$ and every $n \geq 1$, over $\mathbb{Q}(\zeta_m)$ and over $\mathbb{Q}$, with identity component $\mathrm{U}(1)^{\varphi(m)/2}$. Second, the group of connected components is exactly the torsion of the group of Hecke characters generated by the Jacobi sums, so that computing it is precisely the classical problem — going back to Hasse and Yamamoto — of determining all multiplicative relations between Gauss sums. Finally, I will explain how the sign ambiguities discovered by Yamamoto disprove my original conjecture on the explicit shape of these relations, the smallest counterexamples being $m = 12$ and $m = 15$, and how they can be seen in the Sato–Tate group itself: for $m = 15$ the component group is C_{30}, and not C_{15} as predicted.

Aix–Marseille Université, Institut de Mathématiques de Marseille, 163, avenue de Luminy, 13288 Marseille Cedex 9, FRANCE
e-mail: elisa.LORENZO-GARCIA@univ-amu.fr

Diving into $\mathcal{A}_2$

Christophe Ritzenthaler

University of Rennes and University Côte d'Azur

Diving into the beautiful sea of principally polarized abelian varieties of dimension 2, we will encounter three distinct species of subvarieties: graceful rays of dimension 2, swift eels of dimension 1, and colorful coral of dimension 0, which lives in Galois orbits. Joint scuba-diving expedition with Elisa Lorenzo García.

Campus Valrose, Nice, France
chrisotphe.ritzenthaler@univ-rennes1.fr

Elliptic curves and entanglements

Peter Stevenhagen

Universiteit Leiden

Elliptic curves defined over number fields give rise to a finite abelian group of points modulo every prime of good reduction. When asking "how many" of these groups have a certain property (e.g. odd order, cyclic, generated by a given global point, ...), the associated Galois representation on the torsion points in principle answers many of these questions. I will focus on the underlying group theory that goes into finding the explicit answers – possibly under GRH. This is based on joint work with Francesco Campagna, Nathan Jones and Francesco Pappalardi.

Universiteit Leiden
e-mail: psh@math.leidenuniv.nl

The supersingular endomorphism ring problem

Benjamin Wesolowski

CNRS and ENS Lyon

In 1996, David Kohel gives the first algorithm to find endomorphisms of supersingular elliptic curves. This "endomorphism ring problem" has since become the core hard problem of isogeny-based cryptography. We will present the evolution of this problem up to the recent algorithm of complexity $p^{1/3+o(1)}$.

ENS de Lyon site Monod, UMPA UMR 5669 CNRS, 46 allée d'Italie, 69364 Lyon Cedex 07, France
e-mail:benjamin.wesolowski@ens-lyon.fr

Categorical equivalences for supersingular elliptic curves

Sarah Arpin

Virginia Tech

The Deuring correspondence connects supersingular elliptic curves over finite fields with left-ideal classes of maximal orders in a quaternion algebra. As part of his thesis, David Kohel synthesized this correspondence explicitly at the level of isogenies and ideals, and gave a novel presentation of the categorical equivalence Deuring encoded. In this talk, I will survey Kohel's refinement of the Deuring correspondence and describe how it inspired my own work extending the correspondence to supersingular elliptic curves with cyclic level structure.

---

460 McBryde Hall, Virginia Tech, 225 Stanger Street, Blacksburg, VA 24061-1026
e-mail: sarpin@vt.edu

Inseparable endomorphisms of supersingular elliptic curves

Yves Aubry

Université de Toulon and Aix Marseille Université, France

Let p be a prime and E be a supersingular elliptic curve defined over $\overline{\mathbb{F}}_p$. Then the geometric endomorphism ring of E, $\mathrm{End}(E)$, is isomorphic to a maximal ideal $\mathcal{O}$ of the quaternion algebra over $\mathbb{Q}$ ramified at p and ∞.

We first prove that (see [1]), for any positive integer ℓ, there exists an endomorphism of E of degree ℓp and trace zero if and only if the Gross lattice $\mathrm{End}(E)^T$ of E contains a rank-2 sublattice of determinant $4\ell p$.

Then using this approach, we prove (see [2]) that there exists an isogeny from E to its conjugate $E^{(p)}$ of degree less than or equal to $\sqrt[3]{\frac{p}{2}}$.

Our study of the degree of isogenies $E \to E^{(p)}$ leads us naturally to define the value $\delta_E = \min_{\phi\colon E\to E^{(p)}} \deg(\phi)$, where the minimum is taken over all isogenies $\phi\colon E \to E^{(p)}$, and to define the quantity

$$\delta(p) = \max_{E \text{ ss}/\overline{\mathbb{F}}_p} \left(\min_{\phi\colon E\to E^{(p)}} \deg(\phi) \right) = \max_{E \text{ ss}/\overline{\mathbb{F}}_p} \delta_E,$$

where here E ranges over the set of isomorphism classes of supersingular elliptic curves defined over $\overline{\mathbb{F}}_p$. We give some properties and conjectures about these quantities.

This is joint works with Roger Oyono and Christelle Vincent.

References

[1] Yves Aubry and Christelle Vincent, Inseparable endomorphisms and rank-2 sublattices of the Gross lattice, arXiv:2602.05284v1 [math.NT] 5 Feb 2026.

[2] Yves Aubry, Roger Oyono and Christelle Vincent, Minimal degree of an isogeny between a supersingular elliptic curve and its conjugate, arXiv:2607.14624v1 [math.NT] 16 Jul 2026.

Institut de Mathématiques de Toulon - IMATH, Université de Toulon and Institut de Mathématiques de Marseille - I2M, Aix Marseille Univ, UMR 7373 CNRS, France

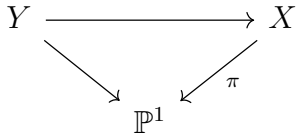
e-mail: yves.aubry@univ-tln.fr and yves.aubry@univ-amu.fr

Minimisation of quintic covers and some Hilbert modular surfaces of full level 2

Sam Frengley

INRIA Saclay

This is based on joint work with Sameera Vemulapalli [FV25]. Let X/k be a projective curve over a field k with $\mathrm{char}(k) \neq 2$ and let $\pi\colon X \to \mathbb{P}^1$ be a map of degree 5. The problem is to compute a smooth curve Y equipped with a commutative diagram



One might be tempted to write the function field $k(X)/k(\mathbb{P}^1)$ by a quintic polynomial $f(x) \in k(\mathbb{P}^1)[x]$ and then apply $\mathrm{PGL}_2(k(\mathbb{P}^1))$ transformations to $f(x)$ remove square factors from $\mathrm{disc}(f)$. This approach does not quite work (it would if $f(x)$ were cubic) but there is a fix. The modification is to use the parametrisation of qunitic rings of Casnati [Cas96] and Bhargava [Bha08] (which also works over $\mathbb{P}^1$) and then adapt "sieving" arguments used by Bhargava [Bha14].

I will illustrate this algorithm by computing a "nice equation" for the Hilbert modular surface of discriminant 13 and full level 2 (i.e., parametrising abelian surfaces with RM by $\mathbb{Z}[\frac{1+\sqrt{13}}{2}]$ and $A(k)[2] \cong (\mathbb{Z}/2\mathbb{Z})^4$).

References

[Bha08] M. Bhargava, *Higher composition laws. IV. The parametrization of quintic rings*, Ann. of Math. (2) **167** (2008), no. 1, 53–94.

[Bha14] ———, *The geometric sieve and the density of squarefree values of invariant polynomials*, arXiv:1402.0031 (2014).

[Cas96] G. Casnati, *Covers of algebraic varieties. II. Covers of degree* 5 *and construction of surfaces*, J. Alg. Geom. **5** (1996), no. 3, 461–477.

[FV25] S. Frengley and S. Vemulapalli, *Tschirnhausen bundles of quintic covers of* $\mathbb{P}^1$, arXiv:2507.06942 (2025).

Inria and Laboratoire d'Informatique de l'École polytechnique, CNRS, Institut Polytechnique de Paris, Palaiseau, France
e-mail:samuel.frengley@inria.fr

A polred based reduction for the division polynomials of the universal elliptic curve

José Ángel Gálvez Gómez

Universitat Politècnica de Catalunya, Spain

Cohen and Diaz's [1] `polred` algorithm is an LLL based [2] lattice reduction method applied to the ring of integers of a number field $K = \mathbb{Q}[x]/(f)$. This algorithm generally obtains a better polynomial f_* (in the sense of smaller coefficients) such that $K = \mathbb{Q}[x]/(f_*)$.

We apply `polred` to several specializations of the nth division polynomial ψ_n of the universal elliptic curve $E/\mathbb{Q}(t)$ given by $E\colon y^2 = x^3 - 3(t-1728)tx - 2(t-1728)^2t$ (or some other universal family of elliptic curves over $X_G(p)$ with $G \leq \mathrm{GL}_2(\mathbb{F}_p)$). As a result of a selected interpolation process we end up with meaningfully reduced polynomials $\psi_{n,*}$. These universal reduced descriptions of ψ_n enable us to work more easily with the field $K = \mathbb{Q}(t)[x]/(\psi_n) = \mathbb{Q}(t)[x]/(\psi_{n,*})$. We present some theorems that we are able to prove using this reduction. This is joint work with Joan Carles Lario.

References

[1] H. Cohen and F. D. Diaz. A polynomial reduction algorithm. *Journal de théorie des nombres de Bordeaux*, 3(2):351–360, 1991.

[2] A. K. Lenstra, H. W. Jr. Lenstra, and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534, 1982.

Universitat Politècnica de Catalunya, Departament de matemàtiques, Campus Diagonal Sud, Edifici U, C. Pau Gargallo, 14, 08028 Barcelona
e-mail:jose.angel.galvez@upc.edu

Products of point counts of higher genus curves over finite fields

Kiran Kedlaya

University of California San Diego, USA

The original form of the conjecture of Birch and Swinnerton-Dyer was formulated not in terms of the L-function of an elliptic curve over $\mathbb{Q}$, but as an asymptotic for the product $\prod_{p \leq x} \frac{N_p}{x}$ where N_p is the number of points on the reduction of the elliptic curve mod p. Later, Mestre and Nagao considered the related asymptotic for the sum $\sum_{p \leq x} \frac{a_p \log p}{p}$ where $a_p = p + 1 - N_p$ is the Frobenius trace. We formulate an analogue of the original BSD conjecture for a curve of arbitrary genus, in which there is a curious discrepancy with respect to the analogue of the Mestre–Nagao sum: whereas the asymptotic of the latter is controlled by the (analytic) rank of the Jacobian as in the genus 1 case, the former also includes a contribution from the Sato–Tate group of the curve. Joint work with Alina Bucur (UC San Diego) and Arshay Sheth (TIFR, Mumbai).

University of California San Diego, Department of Mathematics, 9500 Gilman Drive #0112, La Jolla, CA 92093, USA
e-mail: kedlaya@ucsd.edu

Detecting splitting and real multiplication on superspecial abelian surfaces

Eda Kırımlı

University of Birmingham

We study principally polarized superspecial abelian surfaces over finite fields through their refined Humbert invariants. Primitive representations by these invariants characterize the existence of (N, N)-isogenies from Jacobians to products of elliptic curves, leading to a study of splitting levels and minimum walks to the product locus in the corresponding isogeny graphs. Primitive representations also give information about embeddings of real quadratic orders into endomorphism rings, and hence on real multiplication. This is joint work with Gaurish Korpal.

School of Computer Science, University of Birmingham, Edgbaston, Birmingham, B15 2TT, United Kingdom
e-mail: e.kirimli@bham.ac.uk

Absolutely irreducible Tate modules of Jacobians over p-adic fields

Alexandros Konstantinou

Max-Planck-Institut für Mathematik, Bonn, Germany

Over a number field, absolutely irreducible Tate modules of Jacobians occur in every positive even dimension. Over p-adic fields, however, the possible dimensions are constrained by the residue field and by the action of inertia. For odd p and $\ell \neq p$, I will describe a classification of the dimensions of absolutely irreducible ℓ-adic representations with rational traces on inertia, together with constructions realising every permitted even dimension as the Tate module of a Jacobian of a curve. I will also determine the genera in which hyperelliptic curves can have absolutely irreducible Tate modules, and discuss the further restrictions that arise when the curve has potentially good reduction. The emphasis will be on explicit examples.

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn, Germany
e-mail: konstantinou@mpim-bonn.mpg.de

Hashing-friendly elliptic curves

Dimitri Koshelev

University of Lleida, Catalonia, Spain

This talk aims to consider batch hashing to elliptic curves. The given kind of hash functions found numerous applications in elliptic curve cryptography. In practice, a hash-to-curve function is often evaluated at a time by the same entity at many different inputs. It turns out that under certain mild conditions simultaneous evaluation can be carried out several times faster than separate ones. In this regard, one introduces a new class of elliptic curves over finite fields, more appropriate for multiple hashing to them. Moreover, two explicit hashing-friendly Montgomery/twisted Edwards curves (of ≈ 128 security bits) are generated: one of CM discriminant -7, i.e., a GLV-friendly curve and one of huge CM discriminant, i.e., a CM-secure curve. The new elliptic curves are intentionally covered by so-called Klein's and Bring's curves of geometric genera 3 and 4, respectively. The latter are well studied in various algebraic geometry contexts, although they have not yet been (reasonably) applied in cryptography to the speaker's knowledge. Such a mathematical complication is justified, since conventional curves (from existing standards or of j-invariants 0, 1728) are seemingly less efficient for batch hashing.

University of Lleida, Department of Mathematics
Carrer de Jaume II, 71, 25001, Lleida, Catalonia, Spain
dimitri.koshelev@gmail.com

Are short proofs hard to find?

Andrew Sutherland

MIT Mathematics, USA

Elliptic curve primality proving algorithms due to Goldwasser-Kilian and Atkin-Morain produce primality certificates that can be deterministically verified in quasi-cubic time, faster than even randomized variants of the polynomial-time AKS algorithm due to Bernstein. In 1987 Pomerance proved that every sufficiently large prime admits an elliptic curve primality proof that can be verified in quasi-quadratic time, but no efficient algorithm is known for finding such a proof: the best known algorithms take exponential time. In this talk I will present a subexponential-time algorithm that produces an elliptic curve primality proof that can be verified in quasi-quadratic time. Its running time of $L(1/3, (3/2)^{1/3})$ is asymptotically faster than the general number field sieve and can be practically applied to primes with well over 1000 bits.

This is joint work with Alexa McLain that relies heavily on the use of AI coding agents.

Massachusetts Institute of Technology, Department of Mathematics, Headquarters Office, Simons Building (Building 2), Room 106, 77 Massachusetts Avenue, Cambridge, MA 02139-4307
e-mail: drew@math.mit.edu

Supersingular Elliptic Curves Far from their Frobenius Conjugates

Nicolas Swanson

University of Waterloo, Canada

For a prime p, let $\delta(p)$ denote the smallest degree bound needed to guarantee an isogeny from any supersingular elliptic curve $E/\overline{\mathbb{F}}_p$ to its Frobenius conjugate $E^{(p)}$. Aubry, Oyono, and Vincent [1] proved that $\delta(p) \leq \lfloor \sqrt[3]{p/2} \rfloor$. This bound raises natural arithmetic questions: is it attained for infinitely many primes, and how large is the gap for a typical prime?

In this talk, we approach these questions through the geometry of ternary quadratic forms. In a recent preprint [3], we reformulate Aubry and Vincent's characterization of inseparable endomorphism degrees [2] in terms of these forms. Namely, a positive integer n is the least degree of an isogeny $E \to E^{(p)}$ for some supersingular curve E in characteristic p if and only if there is a positive definite integral ternary quadratic form with minimum n and discriminant p. Thus, determining when $\delta(p)$ is close to its upper bound reduces to studying forms whose minima are close to the largest values allowed by their discriminants.

We give an explicit classification of these forms. In particular, for sufficiently large primes p, we show that $\delta(p) = \lfloor \sqrt[3]{p/2} \rfloor$ if and only if $p = P_i(n)$ for some $n \in \mathbb{Z}$ and one of nine explicit cubics $P_1, \ldots, P_9$. Thus, the upper bound for $\delta(p)$ proposed by [1] is attained infinitely often if and only if at least one of these cubics takes prime values infinitely often. Extending this analysis, we also use a counting argument to show that $\delta(p) \leq \lfloor \sqrt[3]{p/2} \rfloor - p^{1/6-o(1)}$ for almost all primes p.

[1] Y. Aubry, R. Oyono, and C. Vincent. *Minimal degree of an isogeny between a supersingular elliptic curve and its conjugate*. arXiv:2607.14624 (2026).

[2] Y. Aubry and C. Vincent. *Inseparable endomorphisms and rank-2 sublattices of the Gross lattice*. arXiv:2602.05284 (2026).

[3] N. Swanson. *Supersingular elliptic curves without inseparable small degree endomorphisms*. arXiv:2609.03839 (2026).

University of Waterloo, Department of Combinatorics and Optimization

Mathematics and Computers

200 University Ave W

Waterloo, Ontario N2L 3G1

e-mail: nicswanson@uwaterloo.ca

Weil restriction and Coleman's conjecture

Pierre Tchamitchian

Aix-Marseille Université

We study the link between the endomorphism rings of abelian varieties over number fields and their Weil restriction. In particular, We show that Weil restriction of elliptic curves over number fields of a fixed odd degree have finitely many possible endomorphism rings.

Aix-Marseille Université & Institut de Mathématiques de Marseille, Campus de Luminy, Case 907, 13288 Marseille Cedex 9
e-mail:pierre.tchamitchian@univ-amu.fr

On the Semistability Defect of Hyperelliptic Curves and Cluster Picture

Jordi Vilà-Casadevall

University of Bristol

Given an abelian variety $A/\mathbb{Q}_p^{nr}$, there exists a minimal (finite) extension $L/\mathbb{Q}_p^{nr}$ over which A_L acquires semistable reduction. The Galois group of this extension is sometimes referred to as the *monodromy group* of A, usually denoted by Φ. Philip gave in [1] a characterization of the abstract groups that occur as monodromy groups of abelian varieties. However, determining the monodromy group of a given abelian variety remains a difficult problem.

When A is the Jacobian of a curve $C/\mathbb{Q}_p^{nr}$, Halle gave in [3] a criterion for determining Φ in terms of the special fiber of the minimal regular model of C, provided that $L/\mathbb{Q}_p^{nr}$ is tamely ramified. In this talk I will present a different criterion for determining Φ for hyperelliptic curves, based on the notion of *cluster picture* introduced in [2]. This criterion applies both in the tame case and in the wild case, provided that p is sufficiently large compared to the genus of C. This is joint work with G. Jakovác (Bristol), J. Martínez-Marín (Bristol), A. Pérez (Bristol) and J. Shi (MIT).

References

[1] S. Philip, *The (p,t,a)-inertial groups as finite monodromy groups*, arXiv:2503.21199, 2025.

[2] T. Dokchitser, V. Dokchitser, C. Maistret, A. Morgan *Arithmetic of hyperelliptic curves over local fields*, Mathematische Annalen, 385(3), 2023, pp. 1213–1322.

[3] L. H. Halle, *Stable reduction of curves and tame ramification*, Mathematische Zeitschrift, 265(3), 2010, pp. 529–550.

University of Bristol, School of Mathematics, Fry Building, Woodland Road, Clifton Campus, BS8 1UG Bristol, UK
jordi.vilacasadevall@bristol.ac.uk