Mathematisches Forschungsinstitut Oberwolfach

Report No. 40/2024

DOI: 10.4171/OWR/2024/40

# Explicit Methods in Number Theory

Organized by
Karim Belabas, Talence
Bjorn Poonen, Cambridge MA
Fernando Rodriguez Villegas, Trieste

1 September – 6 September 2024

Abstract. The workshop brought together people attacking key modern problems in number theory via techniques involving concrete or computable descriptions. Here, number theory was interpreted broadly, including algebraic and analytic number theory, Galois theory, arithmetic of varieties, zeta and L-functions and their special values, and modular forms and functions.

*Mathematics Subject Classification (2020):* 11Yxx.



## Introduction by the Organizers

The workshop *Explicit methods in number theory*, organized by Karim Belabas (Université de Bordeaux), Bjorn Poonen (Massachusetts Institute of Technology, Cambridge, US), and Fernando Rodriguez Villegas (International Centre for Theoretical Physics, Trieste), was attended by a lively group of 45 in-person participants and 10 virtual participants.

Progress in number theory, since its ancient origins, has been informed by calculations. This has become even more true with the advent of computers and the development of the theory of computing. Our aim was to bring together people attacking key modern problems in number theory via techniques involving concrete or computable descriptions. Here, number theory was interpreted broadly, including algebraic and analytic number theory, Galois theory and inverse Galois problems, arithmetic of curves and higher-dimensional varieties, zeta and L-functions and their special values, and modular forms and functions. Considerable attention was paid to computational issues, but the emphasis was on aspects of interest to the pure mathematician.

We wanted to hear from many participants. At the same time, we wanted to allow enough breaks in the schedule to allow participants to discuss topics and work together. To balance these goals, we scheduled many talks, but limited them to 30 or 45 minutes, the length being dictated by the needs of each speaker. In the end, we had 27 talks, on a wide variety of topics. Some discussed breakthroughs on classical problems, concerning the complexity of multiplying integers and polynomials and concerning the question of which integers or rational numbers are expressible as a sum of two cubes. Some studied the local behavior of curves with bad reduction. Concerning rational points on varieties, we had a new conditional algorithm for determining the rational points on a curve of genus at least 2, a study showing that low-height rational points on hyperelliptic curves are rare, a novel study of the wild Brauer–Manin obstruction, and new results on the Manin–Peyre conjecture on points of bounded height. Some talks studied arithmetic aspects of higher-dimensional algebraic varieties and motives: 0-cycles on a product of elliptic curves, Ceresa cycles, hypergeometric motives, and K3 surfaces and abelian surfaces. On the analytic side of number theory, we had lectures on the "landscape" of L-functions, special values of Dirichlet L-functions, computation of Heegner points, 2-dimensional Artin representations, and the new phenomenon of murmurations. Finally, some talks discussed applications of number theory to quite different areas of mathematics, such as the construction of isospectral manifolds and the growth rate of hyperbolic Coxeter groups.

After the workshop ended, we asked participants to complete a survey. Participants overwhelmingly responded positively to questions on the scientific quality, organization, and importance of the workshop to them. When asked, on a scale of 1–5 (with 5 being most positive), whether the "Explicit methods in number theory" workshop series should continue, 30 of 32 respondents responded with a 5.

*Acknowledgement:* The MFO and the workshop organizers would like to thank the National Science Foundation for supporting the participation of junior researchers in the workshop by the grant DMS-2230648, "US Junior Oberwolfach Fellows".

## Workshop: Explicit Methods in Number Theory

### Table of Contents

# Abstracts

## Galois Groups of Low Degree Points on Curves

Samir Siksek
(joint work with Maleeha Khawaja)

### 1. Low Degree Points on Curves

Let $C$ be a nice curve (i.e. smooth, projective, geometrically irreducible) defined over $\mathbb{Q}$, and let $g$ be the genus of $C$. An algebraic point $P \in C(\overline{\mathbb{Q}})$ is said to have degree $n$ if its Galois orbit consists of $n$ points. This is equivalent to $[\mathbb{Q}(P) : \mathbb{Q}] = n$. The following celebrated theorem of Harris and Silverman [6] may be regarded as the beginning of the study of low degree points on curves.

**Theorem 1** (Harris and Silverman)**.** *Let $C/\mathbb{Q}$ be a curve of genus $g \geq 3$. Suppose $C$ has infinitely many quadratic points. Then $C$ is either hyperelliptic or bielliptic.*

The proof of this theorem makes use of the Mordell–Lang conjecture for subvarieties of abelian varieties which has been established by [4]. Ever since, low degree points have been a subject of intense study, both from the theoretical point of view (e.g. [12]), and from a computational point of view (e.g. [10]). One often also studies low degree integral points on hyperbolic curves, such as the unit equation (e.g. [5]).

### 2. Galois Groups of Low Degree Points

A recent trend for low degree points on curves (and more generally low degree integral points on hyperbolic curves) has been to stratify the points by Galois group (e.g. [2], [3], [7], [11]). In this talk, based on [8] and [9], we look at Galois groups of low degree points in more generality. An algebraic point $P \in C(\overline{\mathbb{Q}})$ is said to be **primitive** if $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts primitively on its Galois orbit $\{P_1, P_2, \ldots, P_n\}$. This is equivalent to the number field $\mathbb{Q}(P)$ not admitting a proper non-trivial subextension. We sketch a proof of the following theorem.

**Theorem 2** (Khawaja–S.)**.** *Let $C/\mathbb{Q}$ have genus $g$ and Jacobian $J$. Suppose*

- $3 \leq n < \sqrt{g} + 1$*;*
- *$J$ is simple.*

*If $C$ has infinitely many primitive degree $n$ points, then there exists* ***a single*** *morphism $\phi : C \to \mathbb{P}^1$ of degree $n$ such that all but finitely many occur as fibres of $\phi$.*

We call this the "single source theorem". The proof makes use of the geometry of linear systems of curves as well as the aforementioned proof by Faltings of the Mordell–Lang conjecture for subvarieties of abelian varieties.

Through a strengthening of the proof of Hilbert's irreducibility theorem (in the context of curves), and by invoking powerful results regarding fixed point ratios

of permutation groups due to Burness and Guralnick [1], we deduce the following theorem.

**Theorem 3** (Khawaja–S.)**.** *Under the same hypotheses, if $C$ has infinitely many degree $n$ points with Galois group $S_n$ or $A_n$ then $C$ has only finitely many degree $n$ points with primitive Galois group $\neq A_n$ or $S_n$.*

## 3. Open Problems

It would be interesting (and probably not too difficult) to extend the proof of Theorem 3 to other families of simple and almost simple groups. Here is a particularly interesting situation. Consider the modular curve $X_0(N)$ for large $N$. Write $j : X_0(N) \to X(1)$ for the usual $j$-map. The proof of Hilbert's irreducibility theorem constructs a thin set $S \subset X(1)(\mathbb{Q})$, such that for $\alpha \in X(1)(\mathbb{Q}) \setminus S$ the fibre $j^*(\alpha)$ has Galois group $\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z})$. Is the set $S$ finite or infinite? If it is infinite then what are the possible Galois groups that arise infinitely often? Moreover, is there an infinite family of algebraic points on $X_0(N)$ with Galois group $\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z})$ that is not arising from $j$?

## References


[1] T. C. Burness and R. M. Guralnick, *Fixed point ratios for finite primitive groups and applications*, Advances in Mathematics **411** (2022), 1–90.

[2] A. Bremner and A. Choudhry, *The Fermat cubic and quartic curves over cyclic fields*, Periodica Mathematica Hungarica **80** (2020), no. 2, 147–157.

[3] P. Bruin, M. Derickx and M. Stoll, *Elliptic curves with a point of order 13 defined over cyclic cubic fields* Funct. Approx. Comment. Math. **65** (2021), 191–197.

[4] G. Faltings, *The general case of S. Lang's conjecture*, In Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991), volume 15 of Perspect. Math., pages 175–182. Academic Press, San Diego, CA, 1994

[5] N. Freitas, A. Kraus and S. Siksek, *Local criteria for the unit equation and the asymptotic Fermat's Last Theorem*, Proceedings of the National Academy of Sciences **118** (2021), No. 12.

[6] J. Harris and J. Silverman, *Bielliptic curves and symmetric products*, Proceedings of the American Mathematical Society **(112)** (1991), 347–356.

[7] D. Joen, *Families of elliptic curves over cyclic number fields with prescribed torsion*, Mathematics of Computation **85** (2016), 1485–1502.

[8] M. Khawaja and S. Siksek, *Primitive algebraic points on curves*, Resesearch in Number Theory **10** (2024), no. 3, Paper No. 57.

[9] M. Khawaja and S. Siksek, *A single source theorem for primitive points on curves*, `arXiv:2306.17772`.

[10] S. Siksek, *Chabauty for Symmetric Powers of Curves*, Algebra & Number Theory **3** (2009), No. 2, 209–236.

[11] S. Siksek, *Integral points on punctured abelian varieties*, European Journal of Mathematics **8** (2022), 687–703.

[12] B. Viray and I. Vogt, *Isolated and parameterized points on curves*, `arXiv:2406.14353`.

## Isospectrality, regulators and torsion homology of Vignéras manifolds

Aurel Page
(joint work with Alex Bartel)

In 1966, Marc Kac [6] asked the famous question *"Can one hear the shape of a drum?"*, triggering a blossom of research on isospectrality problems. The idea is that one should start with a domain of the plane, and make a drum of that shape. When one hits the drum, it vibrates and produces sound; the question is whether this sound determines the shape, i.e. the isometry class of the domain. To eliminate complications related to where and how the drum is hit, one simplifies the problem an retains only the set of vibrating frequencies of the drum, which in turn are completely determined by the eigenvalue of the Laplace operator

$$\Delta = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}$$

acting on functions on the plane domain (with some boundary conditions).

We will shift our attention away from actual drums to compact Riemannian manifolds[1]. Such a manifold $M$ is equipped, for each integer $i$, with a Laplace operator $\Delta$ acting on the space $\Omega^i(M)$ of differential $i$-forms, which has a discrete spectrum. We say that two manifolds $M$ and $N$ are *isospectral* if for all $i$, the spectra of $\Delta$ on $\Omega^i(M)$ and $\Omega^i(N)$ agree with multiplicity. Kac's question becomes: *are isospectral manifolds always isometric?* This question was answered negatively by Vignéras [10] in all dimensions $\geq 2$, but we can fruitfully refine it.

**Question 1.** *Which isometry invariants of manifolds are isospectral invariants?*

The dimension, volume and Betti numbers are indeed isospectral invariants. On the other hand, the ring structure of the rational cohomology is not [7], and neither is the size of the $p$-power torsion of integral homology for any prime $p$ [2, 3].

We can go further by repackaging the spectrum into *spectral zeta functions*

$$\zeta_{M,i}(s) = \sum_{\lambda>0} (\dim \Omega^i(M)_{\Delta=\lambda}) \lambda^{-s}.$$

These zeta functions admit a special value formula, the Cheeger–Müller formula [4, 8]; as a consequence, isospectral 3-manifolds $M, N$ satisfy

$$\frac{\#H_1(M,\mathbb{Z})_{\mathrm{tors}}}{\mathrm{Reg}_1(M)^2} = \frac{\#H_1(N,\mathbb{Z})_{\mathrm{tors}}}{\mathrm{Reg}_1(N)^2}$$

where the regulator $\mathrm{Reg}_i(M)$ is the covolume of $H_i(M,\mathbb{Z})$ in $H_i(M,\mathbb{R})$. In particular, $\mathrm{Reg}_1(M)^2/\mathrm{Reg}_1(N)^2$ is rational. This is analogous to the situation of arithmetically equivalent number fields (i.e. having the same Dedekind zeta function) and the analytic class number formula. This equality, and its generalisation for higher dimensions, naturally leads to the following questions.

[1] or orbifolds, but we will mostly swipe this under the rug.

**Questions 2.**

- *Is* $\mathrm{Reg}_i(M)^2/\mathrm{Reg}_i(N)^2$ *rational for every isospectral* $M, N$*?*
- *When it is true, what primes enter these rational numbers?*
- *At which primes can* $H_i(M,\mathbb{Z})_{\mathrm{tors}}$ *and* $H_i(N,\mathbb{Z})_{\mathrm{tors}}$ *differ?*

Vignéras's construction of isospectral manifolds is number theoretic: they are arithmetic manifolds. In particular, the corresponding homology groups afford an action of Hecke operators, and we can expect that Questions 2 have a number theoretic significance.

The construction is as follows. We start from a quaternion algebra $A$ over a number field $F$. To each order $\mathcal{O}$ in $A$, we can associate the arithmetic group $\mathcal{O}^\times \subset G$, where $G = (\mathbb{R}\otimes A)^\times$ acts on a symmetric space $X$ (a product of hyperbolic 2- and 3-space), and we can form the arithmetic manifold $M(\mathcal{O}) = \mathcal{O}^\times\backslash X$.

**Theorem 3** (Vignéras)**.** *If* $\mathcal{O}_1$ *and* $\mathcal{O}_2$ *are maximal orders* ***and extra conditions hold****, then* $M(\mathcal{O}_1)$ *and* $M(\mathcal{O}_2)$ *are isospectral.*

The proof actually proves the stronger statement that $\mathcal{O}_1^\times$ and $\mathcal{O}_2^\times$ are *representation-equivalent*, i.e. there is an isomorphism

$$L^2(\mathcal{O}_1^\times\backslash G) \cong L^2(\mathcal{O}_2^\times\backslash G)$$

of unitary representations of $G$.

This has lead to the question of how much stronger representation-equivalence is compared to isospectrality. For hyperbolic surfaces, Doyle and Rossetti proved [5] that the two notions are equivalent, and they conjectured that this also holds in higher dimensions. However, this was too optimistic.

**Theorem 4** (Bartel–P. [1])**.** *There exists a pair of isospectral hyperbolic* 3*-manifolds of volume* $0.251\ldots$ *that are isospectral, but not representation-equivalent.*

Our example is obtained from Vignéras's construction, and is a candidate for the isospectral pair of smallest volume among hyperbolic 3-manifolds. The analysis of this example is made possible by a new method that applies both to isospectrality and to the analysis of torsion homology, contrary to the trace formula. The refined criteria that we obtain fit in the following theorem template.

**Theorem**$\langle*\rangle$ (Bartel–P. [1])**.** At least one of the following two statements is true:

(i) there exists a number field $L$ in an a-priori finite list and a $*$**-shady character** of $L$;
(ii) the manifolds $M(\mathcal{O}_1)$ and $M(\mathcal{O}_2)$ are $*$**-isospectral**.

For each instance of $*$, the $*$-shady characters are certain Hecke characters, whose existence can be checked using `PARI/GP`'s new Hecke characters package `gchar` [9]! More precisely:

- when $*$ is representation-equivalence, the $*$-shady characters are certain possibly transcendental Hecke characters;
- when $*$ is isospectrality, the $*$-shady characters are certain possibly transcendental Hecke characters of a more restricted type;

- when $*$ is "having rational regulator ratio", the $*$-shady characters are certain algebraic Hecke characters;
- when $*$ is "having the same regulators and torsion homology at $p$", the $*$-shady characters are certain mod $p$ Hecke characters.

In particular, we mostly answer Questions 2 for isospectral pairs obtained from Vignéras's construction.

The proof uses the large supply of Hecke operators between the two arithmetic manifolds; under suitable conditions, we are able to construct a Hecke operator that realises an isomorphism between the modules of interest.

In the mod $p$ case, the theorem is actually conditional on a widely believed conjecture on the existence of Galois representations attached to torsion classes in the homology of the relevant arithmetic manifolds.

**Question 5.** *Can one bypass mod p Galois representations? More precisely, can one construct and characterise mod p automorphic induction?*

On the other hand, we are able to prove that some primes are excluded from the ratios of regulators or of torsion homology, but we cannot quantify the ones that do appear.

**Question 6.** *Can one predict the p-adic valuation of* $\mathrm{Reg}_i(M(\mathcal{O}_1))^2/\mathrm{Reg}_i(M(\mathcal{O}_1))^2$ *or of* $\#H_i(M(\mathcal{O}_1),\mathbb{Z})/\#H_i(M(\mathcal{O}_2),\mathbb{Z})$ *when it is nonzero?*

This would be a mod $p$ analogue of the Labesse–Langlands multiplicity formula.

Finally, the techniques we use to analyse the regulator ratios suggest that they should have a $p$-adic avatar.

**Question 7.** *Can one define a notion of p-adic regulators, whose ratios give the same rational numbers as the real regulators?*

## References


[1] A. Bartel and A. Page, *Vignéras orbifolds: isospectrality, regulators and torsion homology*, arXiv preprint 2407.07240 (2024).

[2] A. Bartel and A. Page, *Torsion homology and regulators of isospectral manifolds*, J. Topology **9** no. 4 (2016), 1237–1256.

[3] A. Bartel and A. Page, *Group representations in the homology of 3-manifolds*, Comment. Math. Helv. **94** no. 1 (2019), 67–88.

[4] J. Cheeger, *Analytic torsion and the heat equation*, Ann. of Math. **109** (1979), 259–322.

[5] P. Doyle and J. Rossetti, *Laplace-isospectral hyperbolic 2-orbifolds are representation-equivalent*, arXiv preprint 1103.4372v2 (2014).

[6] M. Kac, *Can one hear the shape of a drum?* Amer. Math. Monthly **73** (1966), 1–23.

[7] E. Lauret, R. Miatello and J. Rossetti, *Strongly isospectral manifolds with nonisomorphic cohomology rings*, Rev. Mat. Iberoam. **29**, No. 2, 611–634 (2013).

[8] W. Müller, *Analytic torsion and R-torsion of Riemannian manifolds*, Adv. Math. **28** (1978), 233–305.

[9] The PARI Group, *PARI/GP version 2.16*, Univ. Bordeaux, 2024, `http://pari.math.u-bordeaux.fr/`.

[10] M.-F. Vignéras, *Variétés riemanniennes isospectrales et non isométriques*, Ann. of Math. (2) **112** no.1 (1980), 21–32.

## Reduction types of curves

Tim Dokchitser

In the talk I discussed the question of classifying singular fibres in 1-dimensional families of curves. These are usually called 'reduction types', and their classification is known in genus $\leq 3$ [Ko, NU, AI]. I would like to propose a classification in arbitrary genus.

One motivation for the classification is that recently several methods have emerged to compute reduction types for classes of curves in any genus, notably by Donnelly in Magma [Ma], for $\Delta_v$-regular curves [Do], and an Museli's analogue [Mu] of Tate's [Ta] and Liu's [Liu] algorithms for hyperelliptic curves.

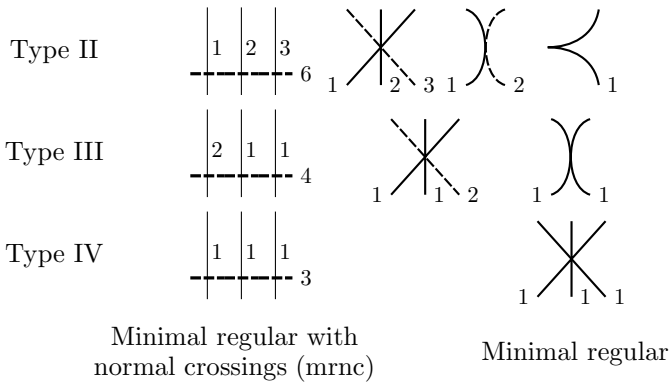
This classification problem makes sense in any genus $g$, in that there are finitely many families for a fixed genus. Their number for $g \leq 6$ turns out to be

$$10 \text{ (elliptic)}, 104\ (g=2), 1901\ (g=3), 43440, 1344722, 49483812, \ldots$$

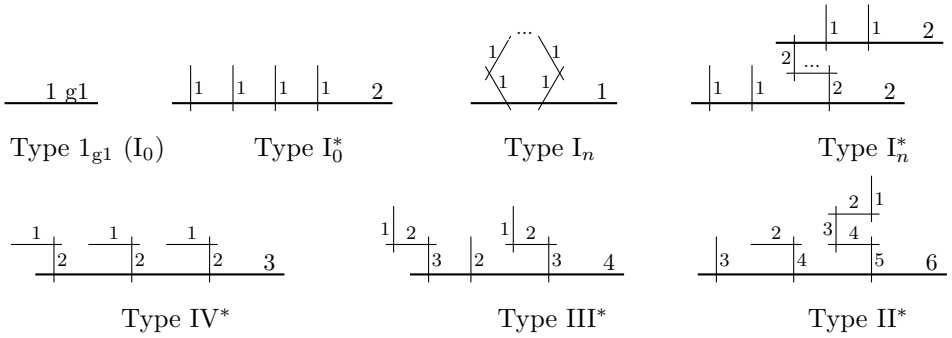
and it grows superexponentially with $g$.

A curve over a discretely valued field has a unique minimal regular model, and special fibres of these models have traditionally been used for listing reduction types. I discussed the advantages to moving to minimal models with normal crossings (mrnc), as they seem to be better suited for classification purposes. Any curve has a unique mrnc model, and one can obtain the minimal regular model from it by repeatedly blowing down exceptional curves.

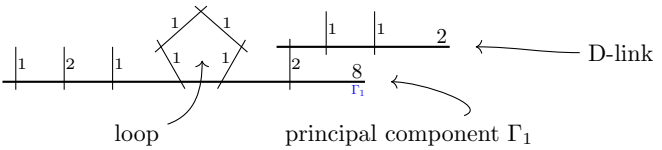
For example, for elliptic curves, there are three reduction types for which the mrnc model is different from the minimal regular one:




Blowing down exceptional curves (dashed) from left to right yields a minimal regular model. For all other reduction types of elliptic curves, the mininal regular and the mrnc model coincide:




In genus $g > 1$, one can classify reduction types roughly as follows. Say we have an mrnc model of a genus $g$ curve, and consider its special fibre. Call a component principal if it either has positive (geometric) genus or meets the rest of the special fibre in at least three points. One can associate to such a component $\Gamma$ its Euler characteristic $\chi_\Gamma$ and these add up to $2-2g$ over all principal components. In turns out that $\chi_\Gamma \leq 0$, and with one exception ($I_0^*$-like tails, called D-links), $\chi_\Gamma < 0$. Considering every a component with its loops and D-links break the special fibre into 'principal types', like this one:




It turns out to be easy to classify these principal types combinatorially, and the question of getting all reduction types reduces to glueing these together in all possible ways, which is again combinatorial, and not hard.

The classification is currently being implemented, and an interested reader is welcome to get the library from here and try it:

`https://people.maths.bris.ac.uk/~matyd/redlib/redlib.html`

This reduction type library also aims to compute reduction types of curves over discrete valuation rings in practice. It includes an implementation of Muselli's work for hyperelliptic curves in odd residue characteristic [Mu], and $\Delta_v$-regular machinery [Do].

## References

[AI] T. Ashikaga, M. Ishizaka, Classification of degenerations of curves of genus three via Matsumoto-Montesinos' theorem, Tohoku Math. J. 54 (2002), 195–226.

[Ma] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I: The user language, J. Symb. Comput. 24, No. 3–4 (1997), 235–265.

[Do] T. Dokchitser, Models of curves over discrete valuation rings, Duke Math. J. 170, no. 11 (2021), 2519–2574.

[Ko] K. Kodaira, On compact analytic surfaces II, Ann. Math. 78 (1963), 563–626.

[Liu] Q. Liu, Modèles entiers des courbes hyperelliptiques sur un corps de valuation discrète, Trans. Amer. Math. Soc. 348 no. 11 (1996), 4577–4610.

[Mu] S. Muselli, Regular models of hyperelliptic curves, arXiv:2206.10420, to appear in Indag. Math.

[NU] Y. Namikawa, K. Ueno, The Complete Classification of Fibres in Pencils of Curves of Genus Two, Manuscripta Math. 9 (1973), 143–186.

[Ta] J. Tate, Algorithm for determining the type of a singular fiber in an elliptic pencil, in: Modular Functions of One Variable IV, Lect. Notes in Math. 476, B. J. Birch and W. Kuyk, eds., Springer-Verlag, Berlin, 1975, 33–52.

## Semistable reduction of covers of curves of degree $p$

Stefan Wewers
(joint work with Ole Ossen)

### 1. Computing semistable reduction

Let $K$ be a complete, discretely valued field. We denote by $\mathcal{O}_K$ the ring of integers and by $k$ its residue field. Let $Y$ be a smooth, projective curve of genus $g$ over $K$. In my talk I reported on recent progress towards a solution of the following problem.

**Problem 1.** Compute a finite extension $L/K$, a semistable model $\mathcal{Y}$ of $Y_L$, and the action of the Galois group of $L/K$ on the special fiber $\mathcal{Y}_s$.

A solution to this problem is trivial for $g = 0$ and well known for $g = 1$. For genus $g \geq 2$ there are only partial solutions in special cases, some of which we review below.

There are many potential applications of Problem 1 to computational arithmetic geometry. For instance, in [1] (joint work with Irene Bouw) it was shown how to compute $L$-factors and conductor exponents of superelliptic curves with 'tame' exponent. More recently, in joint work with Duc Do and Irene Bouw, we extended these methods to the calculation of the Weil representation of curves with reduction of compact type, see [2]. In an article in preparation (joint work with Irene Bouw, Giovanni Bruno, Robert Nowak and Xiaodong Zhang), we extend this to the calculation of the Weil-Deligne representation of curves with bad reduction of arbitrary type.

For some of these applications, an alternative method is to compute a *regular model* of the curve in question. We refer to Tim Dokchitser's talk at this conference.

### 2. Semistable reduction of covers

Most work on Problem 1 so far is based on exploiting a particular representation of the curve $Y$ as a cover of the projective line. In this section we formulate a very general version of this approach and give a class of examples where it has been applied successfully. See [16] and Eliza Lorenzo Garcia's talk at this conference for an alternative and very different approach when $Y$ is a smooth plane quartic.

Let $K$ and $Y$ be as in §1. We choose a finite, generically etale morphism

$$\phi : Y \to X,$$

where $X$ is a smooth and projective $K$-curve whose semistable reduction is known. In practise, $X$ will mostly be the projective line, but for the following definitions, and future investigations, it makes sense to consider a more general setup.

Let $\mathcal{X}_0$ be a normal $\mathcal{O}_K$-model of $X$ and $L/K$ a finite field extension. Let $\mathcal{X}$ (resp. $\mathcal{Y}$) denote the normalization of $\mathcal{X}_0$ in the function field of $X_L$ (resp. of $Y_L$). Then $\mathcal{X}$ (resp. $\mathcal{Y}$) is a normal $\mathcal{O}_L$-model of $X$ (resp. $Y$), and we have a diagram

$$\begin{array}{ccc} \mathcal{Y} & & \\ \downarrow & & \\ \mathcal{X} & \longrightarrow & \mathcal{X}_0 \\ \downarrow & & \downarrow \\ \operatorname{Spec} \mathcal{O}_L & \longrightarrow & \operatorname{Spec} \mathcal{O}_K. \end{array}$$

**Definition 2.**

(i) We say that the model $\mathcal{X}_0$ *separates the branch points of* $\phi$ if, for some extension $L/K$, the branch locus of $\phi$ splits into distinct $L$-rational points on $X_L$ which specialize to pairwise distinct smooth points on the special fiber $\mathcal{X}_s$ of the model $\mathcal{X}$.

(ii) We say that $\mathcal{X}_0$ is *potentially semistable* if, for some extension $L/K$, the model $\mathcal{X}$ of $X_L$ is semistable.

(iii) We say that $\mathcal{X}_0$ is *potentially $\phi$-semistable* if, for some extension $L/K$, the model $\mathcal{Y}$ of $Y_L$ is semistable.

The 'cover method' for computing semistable reduction proceeds through the following steps:

(1) Choose a suitable map $\phi : Y \to X$.
(2) Find a potentially $\phi$-semistable model $\mathcal{X}_0$ fo $X$.
(3) Compute a suitable extension $L/K$ and the semistable model $\mathcal{Y}$.

The rationale for this division is that Step (3) can be implemented in a general way, without any particular assumption on the cover. To some extend, a general implementation of Step (3) has already been realized within the sofware project MCLF, see [12].

In this talk, we focused on Step (2). Here we have a good solution in a large class of examples, using the following theorem.

**Theorem 3** (Folklore)**.** *Assume that the order of the Galois group of the Galois closure of the cover $\phi$ is invertible in $\mathcal{O}_K$*[1]*. If $\mathcal{X}_0$ is potentially semistable and separates the branch locus of $\phi$, then $\mathcal{X}_0$ is also potentially $\phi$-semistable. Moreover, we can take for $L/K$ an extension which is at most tamely ramified of degree $\leq n$ over the subextension which contains the residue field of all branch points $b_i$.*

[1]For instance, this is the case if $p = \operatorname{char}(k)$ is strictly larger than the degree of $\phi$.

Theorem 3 is a consequence of basic results on tame ramification (see e.g. [8]) and the theory of *admissible covers*, first developed in [9]. It is the theoretical basis for most known results on Problem 1, for instance the results of [1] and [5].

## 3. Covers of the projective line of degree $p$

In his recent PhD thesis ([14]), Ole Ossen studies the case where the curve $Y$ can be realized as a finite, generically etale cover

$$\phi : Y \to X := \mathbb{P}^1_K$$

*of degree* $p$, where $p$ is equal to the characteristic of the residue field $k$. This is the simplest case where Theorem 3 does not apply, and its conclusion is typically false. It is then much more difficult to find a $\phi$-semistable model.

If we assume in addition that the cover $\phi$ is Galois, then the curve $Y$ is actually a superelliptic curve of degree $p$, i.e. is given by an equation of the form

$$Y : \ y^p = f(x).$$

This particular case has been much studied. Inspired by ideas of Coleman ([4]), Lehr and Matignon ([11], [10]) have essentially solved Problem 1 in this case, under the extra condition of *equidistant branch locus*.

The speaker has extended the results of Lehr and Matignon to the general case of superelliptic curves of degree $p$ (i.e. not assuming equidistant branch locus), see e.g. [3]. The results are still unpublished, but have been implemented within MCLF. More recently, the case $p = 2$ (i.e. the reduction of hyperelliptic curves at $p = 2$) has been studied by Fiore and Yelton ([6]) and also by Gehrunger and Pink ([7]).

The main result of Ole Ossen's thesis generalizes these works to the case of a general cover of degree $p$, not necessarily Galois. It can be summarized as follows.

**Theorem 4** (Ossen)**.** *Let $K$ and $Y$ be as before, and let $\phi : Y \to X$ be a cover of degree $p = \mathrm{char}(k)$. Assume that the semistable reduction of $X$ is known. Then there exists an explicit description, in terms of the equations defining $X$, $Y$ and $\phi$, of a potentially $\phi$-semistable model $\mathcal{X}_0$ of $X$.*

With this new result, the classes of curves where the cover method can be used to compute semistable reduction has been significantly expanded.

**Example 5.** Assume that $K$ has residue characteristic $p = 3$, and let $Y \subset \mathbb{P}^2_K$ be a smooth plane quartix. Assume, moreover, that $Y$ has a $K$-rational point $P$ (since we probably need to extend the base field $K$ anyway, this is not a severe restriction). Then the projection with center $P$ defines a cover $\phi : Y \to \mathbb{P}^1_K$ of degree 3. This map is never a Galois cover. We can compute the semistable reduction of $Y$ via Theorem 4 and the methods implemented in MCLF. To our knowledge, no other practical method is known in this case.

For an explict example with some arithmetic interest, see [15], [14, §5.6] and [13]. Here $K = \mathbb{Q}_3(\zeta_3)$ and $Y$ is a certain quotient of the modular curve $X^+_{\mathrm{ns}}(27)$, given by an explicit quartic equation. It has semistable reduction over a certain

totally ramified extension $L/K$ of degree 54, and the special fiber of the stable model of $Y_L$ consists of one rational curve with three tails of genus one.

## References


[1] I. I. Bouw and S. Wewers, *Computing L-functions and semistable reduction of superelliptic curves*, Glasg. Math. J. **59** (2017), no. 1, 77–108.

[2] I. I. Bouw, D. K. Do, and S. Wewers, *Computing the Weil representation of a superelliptic curve*, Indag. Math. (2024).

[3] I. I. Bouw and S. Wewers, *Semistable reduction of curves and computation of bad Euler factors of L-functions*, September 2015.

[4] R. Coleman, *Computing stable reductions*, in *Séminaire de Théorie des Nombres, Paris 1985–86*, Progr. Math., vol. 71, Birkhäuser Boston, Boston, MA, 1987, pp. 1–18.

[5] T. Dokchitser, V. Dokchitser, C. Maistret, and A. Morgan, *Arithmetic of hyperelliptic curves over local fields*, Math. Ann. **385** (2023), no. 3-4, 1213–1322.

[6] L. Fiore and J. Yelton, *Clusters and semistable models of hyperelliptic curves in the wild case*, `arXiv:2207.12490`, 2023.

[7] T. Gehrunger and R. Pink, *Reduction of hyperelliptic curves in residue characteristic 2*, `arXiv:2404.14214`, 2024.

[8] A. Grothendieck, *Revêtement étales et groupe fondamental (SGA1)*, Lecture Notes in Math., vol. 288, Springer, 1971.

[9] J. Harris and D. Mumford, *On the Kodaira dimension of the moduli space of curves*, Invent. Math. **67** (1982), no. 1, 23–88. Appendix by W. Fulton.

[10] C. Lehr and M. Matignon, *Wild monodromy and automorphisms of curves*, Duke Math. J. **135** (2006), no. 3, 569–586.

[11] M. Matignon, *Vers un algorithme pour la réduction stable des revêtements p-cycliques de la droite projective sur un corps p-adique*, Math. Ann. **325** (2003), no. 2, 323–354.

[12] J. Rüth and S. Wewers, *MCLF*, GitHub repository, 2024.

[13] O. Ossen, *Computing the semistable reduction of a particular plane quartic curve at $p = 3$*, `arXiv:2305.00288`, 2023.

[14] O. Ossen, *Semistable reduction of covers of degree p*, `arXiv:2404.16105`, 2024.

[15] J. Rouse, A. V. Sutherland, and D. Zureick-Brown, *$\ell$-adic images of Galois for elliptic curves over $\mathbb{Q}$ (and an appendix with John Voight)*, Forum Math. Sigma **10** (2022), Paper No. e62, 63.

[16] R. van Bommel, J. Docking, V. Dokchitser, R. Lercier, and E. Lorenzo García, *Reduction of Plane Quartics and Cayley Octads*, `arXiv:2309.17381`, 2023.


### Reduction of Plane Quartics and Cayley Octads


Elisa Lorenzo García

(joint work with Raymond van Bommel, Jordan Docking, Vladimir Dokchitser, Reynald Lercier)


Deligne and Mumford's proof of the irreducibility of the moduli space of smooth projective curves of genus $g \geq 2$ over an algebraically closed field consists of compacting this space by adding the curves with mild singularities, the *stable curves* [1]. Singularities of a stable curve are ordinary double points, and its irreducible components of geometric genus 0 have at least three such double points, counted with multiplicity. A consequence of the Deligne-Mumford construction is the stable reduction theorem: any curve over a local field acquires stable reduction after a finite extension of the base field. Stable models of a curve give access to

much information of arithmetic nature about the curve and its Jacobian (genus, conductor, *etc.*), and their actual calculation is a motivating question. A commonly used way to determine it is to repeatedly blow up the singular points and components of the special fibre and take normalizations [3]. However, this method can also be a difficult task from a computational point of view, even for genus 3 curves that are the focus of this work.

One of the first results that goes in the direction of greater effectivity is due to Liu, for the case of curves of genus 2 [5]. Liu gives, in terms of the Igusa invariants of a curve, $C$, not only the stable type, *i.e.* the graph of the irreducible components of $C$ as well as the genera of their normalisations, but also the $j$-invariant of the irreducible components of genus 1 when the special fibre is not smooth.

While there are only 7 possibilities for the type of stable reduction in genus 2, the situation is considerably more involved for curves of genus 3. The multiplicity of cases and also the complexity of invariant algebras complicate the generalisation of Liu's approach to genus 3. Partial results exist, however, characterising potentially good reduction of a quartic, or determining when a plane quartic reduces to a hyperelliptic curve [4]. The hyperelliptic genus 3 case, $y^2 = f(x)$, is fairly well-understood via the machinery of "cluster pictures" [2], combinatorial objects that encode $p$-adic distances between the roots of the polynomial $f(x)$.

The aim of this work is to describe a new approach to understanding the stable reduction of curves of genus 3. We believe to have identified the correct replacement for the roots of the polynomial $f(x)$ in the context of non-hyperelliptic genus 3 curves. We propose to replace the eight Weierstraß points in the hyperelliptic case by a *Cayley octad*. Fixing one of the 36 even theta characteristics $\theta$ (*i.e.* a divisor on the curve such that $2\theta$ lies in the canonical divisor class and the Riemann-Roch space of $\theta$ has even dimension) gives rise to both an embedding of the plane quartic into $\mathbb{P}^3$, and 8 points in $\mathbb{P}^3$ which form the Cayley octad. Analogous to the Weierstraß points of a hyperelliptic curve, these 8 points determine the curve. We conjecture that combinatorial data about the configuration of these eight points fully determines the stable reduction type of the curve, analogously to the cluster picture in the hyperelliptic case.

There are two natural complications compared to the hyperelliptic case. First, our eight points live in $\mathbb{P}^3$ rather than in $\mathbb{P}^1$. In particular, this means that there are new possible degenerations to consider when looking at the points over the residue field. Specifically, there are the following four basic degenerations: (i) several points coinciding (the direct analogue of a cluster), (ii) four points lying on a plane, (iii) three points lying on a line, (iv) seven points lying on a twisted cubic curve (as with cluster pictures, the case of no degenerations occurring corresponds to good reduction).

Second, unlike the case of the Weierstraß points of a hyperelliptic curve, the 8 points of a Cayley octad are not independent and satisfy an algebraic relation, under which any point is determined by the other seven. Because of this relation, the degenerations that can actually occur are harder to describe.

The central point of this work is to understand all possible degenerations (leading us to the notion of *octad* pictures and relate them to stable reduction types. We give a conjectural characterisation of the stable reduction of plane quartics over local fields in terms of their Cayley octads. This results in $p$-adic criteria that efficiently give the stable reduction type amongst the 42 possible types, and whether the reduction is hyperelliptic or not. We also construct explicit families of quartic curves that realise all possible stable types, against which we test these criteria. We give numerical examples that illustrate how to use these criteria in practice.

## References


[1] P. Deligne and D. Mumford. *The irreducibility of the space of curves of given genus*, Inst. Hautes Études Sci. Publ. Math. **36** (1969), 75–109.

[2] T. Dokchitser, V. Dokchitser, C. Maistret, and A. Morgan. *Semistable types of hyperelliptic curves*, Algebraic curves and their applications, Amer. Math. Soc., Vol. **724** (2019), 73–135.

[3] J. Harris and I. Morrison. *Moduli of curves*, Springer-Verlag, New York, Vol. **187** (1998), xiv+366.

[4] R. Lercier, Q. Liu, E. Lorenzo García, and C. Ritzenthaler. *Reduction type of smooth plane quartics*, Algebra Number Theory **15.6** (2021), 1429–1468.

[5] Q. Liu. *Courbes stables de genre 2 et leur schéma de modules*, Math. Ann. **295.2** (1993), 201–222.


## Hypergeometric motives and Fermat's generalized equation


Ariel Pacetti

(joint work with Franco Golfieri and Fernando Rodriguez Villegas)


The goal of the present talk is to show how 2-dimensional hypergeometric motives can be used to prove non-existence of solutions to the generalized Fermat equation

$$Ax^p + By^q = Cz^r, \tag{1}$$

following the strategy proposed by Darmon in [1]. In loc. cit. the author studies what he calls "Frey representations", which are representations of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}(t)}/K(t))$ (for $K$ a number field) with coefficients on a finite field. The advantage to work with hypergeometric motives is that they are also a source of "Frey representations", but with characteristic zero coefficient field.

Rank two hypergeometric motives are parametrized by pairs of rational numbers $(a,b),(c,d)$ satisfying a genericity condition. In this talk we will state their main properties (including its existence and its field of definition) in terms of the parameters. A key fact is that hypergeometric motives satisfy many congruences among themselves, an important property used to prove their modularity.

In the second part of the lecture, we will show how the parameters have to be chosen to study solutions of (1). We will focus in the particular case of exponents $(p,p,3)$ (where we can attach a new elliptic curve to a putative solution) and $(q,3,p)$. In the later case, we will prove that the motive attached to a solution is modular for all values of $p,q$ with $q>5$ and all specialization of the parameter $t$.

The talk contains results proven in the articles [2] and [3].

## References

[1] Henri Darmon. Rigid local systems, Hilbert modular forms, and Fermat's last theorem. *Duke Mathematical Journal*, 102(3):413 – 449, 2000.

[2] Franco Golfieri, Ariel Pacetti, and Fernando Rodriguez Villegas. On rank 2 hypergeometric motives. *In preparation*, 2024.

[3] Franco Golfieri and Ariel Pacetti. Hypergeometric motives and the generalized Fermat equation. *In preparation*, 2024.


## $K3$ surfaces with maximal complex multiplication

Eva Bayer-Fluckiger

Let $X$ be a complex, projective $K3$ surface, let $T_X$ be the transcendental lattice of $X$ and set $T_{X,\mathbf{Q}} = T_X \otimes_{\mathbf{Z}} \mathbf{Q}$. We denote by $E(X) = \mathrm{End}_{\mathrm{Hdg}}(T_{X,\mathbf{Q}})$ the Hodge endomorphisms of $T_{X,\mathbf{Q}}$; set $m(X) = \dim_{E(X)}(T_{X,\mathbf{Q}})$. Zarhin proved that $E(X)$ is a totally real or CM number field. It is natural to ask

**Question.** What are the possiblities for $(E(X), m(X))$ ?

The preprint [2], joint with Bert van Geemen and Matthias Schütt, gives a complete answer to this question (see the bibliography of [2] for previous results). Theorems 1 and 2 below are proved in [2] :

**Theorem 1.** *Let $E$ be a totally real number field of degree $d$ and let $m$ be an integer with $m \geq 3$ and $md \leq 21$. Then there exists an $(m-2)$-dimensional family of complex projective $K3$ surfaces such that a very general member $X$ has the properties $E(X) \simeq E$ and $m(X) = m$.*

**Theorem 2.** *Let $E$ be a CM number field of degree $d$ and let $m$ be an integer with $m \geq 1$ and $md \leq 20$.*

*If $m \geq 2$, then there exists an $(m-1)$-dimensional family of complex projective $K3$ surfaces such that a very general member $X$ has the properties $E(X) \simeq E$ and $m(X) = m$.*

*If $m = 1$, then there exist infinitely many non-isomorphic complex projective $K3$ surfaces $X$ such that $E(X) \simeq E$ and $m(X) = 1$.*

If $E(X)$ is totally real, the surface $X$ is said to have *real multiplication*; the condition $m \geq 3$ in Theorem 1 is necessary by [3], Lemma 10.1, hence Theorem 1 is optimal.

We say that $X$ has *complex multiplication* if $E(X)$ is CM and $m(X) = 1$; in this case, $X$ can be defined over a number field. Let $O(X)$ be the ring of integers of $E(X)$; we say that $X$ has *maximal complex multiplication* (or CM by the ring of integers) if $\mathrm{End}_{\mathrm{Hdg}}(T_X) = O(X)$; this notion was introduced by Domenico Valloni in [4], see also [5]. Similarly to the above question, one can ask for which CM fields do there exist $K3$ surfaces with maximal complex multiplication. In [4], Valloni proved that if $E$ is a CM field of degree $\leq 10$, then there exist infinitely many $K3$ surfaces with this property. His result can be imporved as follows.

**Theorem 3.** *If $E$ is a CM field of degree $\leq 14$, then there exist infinitely many complex projective $K3$ surfaces with CM by the ring of integers $O_E$.*

This is proved in [1], see Theorem 7.4; moreover, this results is optimal (see [1], Example 7.6).

## References


[1] E. Bayer-Fluckiger, *$K3$ surfaces with maximal complex multiplication*, preprint (2024).
[2] E. Bayer-Fluckiger, L. van Geemen, M. Schütt, *$K3$ surfaces with real or complex multiplication*, preprint (2024).
[3] B. van Geemen, *Real multiplication on $K3$ surfaces and Kuga Satake varieties*, Michigan Math. J. **56** (2008), 375–399.
[4] D. Valloni, *Complex multiplication and Brauer groups of $K3$ surfaces*, Adv. Math. **385** (2021), Paper No. 107772, 52pp.
[5] D. Valloni, *Fields of definition of K3 surfaces with complex multiplication*, J. Number Theory **242** (2023), 436–470.


## From hyperbolic growth rates to Salem numbers and back


Ruth Kellerhals
(joint work with Livio Liechti)


A hyperbolic Coxeter group $\Gamma = (W, S)$ is a discrete group $W$ generated by a finite set $S$ of hyperplane reflections in hyperbolic space $\mathbb{H}^n$. The growth series $f_S(t)$ of $\Gamma$ is the formal power series whose coefficients $a_k$ count the number of words of $S$-length equal to $k \geq 0$. The growth rate $\tau$ of $\Gamma$ as given by the inverse of the convergence radius of $f_S(t)$ turns out to be an algebraic integer $> 1$.

In fact, by means of the classical formulas of Steinberg and Solomon, one has the following systematic approach in terms of polynomial expressions $[k] := 1 + t + \ldots + t^{k-1}$ in order to deal with $f_S(t)$.

$$\frac{1}{f_S(t^{-1})} = \sum_{\substack{W_T < W \\ |W_T| < \infty}} \frac{(-1)^{|T|}}{\prod_{i=1}^{l} [m_i^T + 1]},$$

where $W_T$, $T \subset S$, is the finite Coxeter subgroup of $W$ generated by $T$, with $W_\varnothing = \{1\}$, and where $m_1^T, \ldots, m_l^T$ denote the exponents of $W_T$. In particular, the dihedral group of order $2p$ has growth polynomial $[p]$.

As a consequence, $f_S(t)$ is a rational function and quotient of two coprime integer polynomials of equal degree whose explicit form can be derived easily from the presentation of $\Gamma$ in terms of $S$. As an example, the reflection group $\Gamma$ associated to a compact hyperbolic Coxeter $k$-polygon $P = (p_1, \ldots, p_k) \subset \mathbb{H}^2$ with angles $\pi/p_i$, $1 \leq i \leq k$, can be expressed as follows.

$$f_S(t) = \frac{[2]\,[p_1] \cdots [p_k]}{[2]\,[p_1] \cdots [p_k] - \sum_{i=1}^{k} t\,[p_1] \cdots \widehat{[p_i]} \cdots [p_k]}.$$

With $f_S(t)$ given in this form, E. Hironaka [3] was able to show that the smallest growth rate of any cocompact planar hyperbolic Coxeter group is achieved in a unique way by the Coxeter triangle group $(2, 3, 7)$, and it is equal to Lehmer's number $\alpha_L \approx 1.17628$ with minimal polynomial $1+t-t^3-t^4-t^5-t^6-t^7+t^9+t^{10}$.

Observe that, by a result of C. L. Siegel, the Coxeter group $(2, 3, 7)$ is also distinguished by realising *minimal covolume* among all fundamental groups of hyperbolic orbifolds of dimension two. The analogy [minimal growth rate] $\leftrightarrow$ [minimal covolume] holds also in the 3-dimensional case (each in the cocompact and cofinite settings); see [4], for example.

Moreover, the growth rate $\tau = \alpha_L$ of $(2, 3, 7)$ is the *smallest known Salem number*, where a Salem number is a real algebraic integer $\alpha > 1$ such that all Galois conjugates have absolute value not greater than 1 and at least one of them has absolute value equal to 1. This observation is of particular interest in connection with *Lehmer's Question* restricted to Salem numbers: Is there a universal bound $\mu > 1$ such that $\alpha \geq \mu$ for any Salem number $\alpha$ ?

In fact, there are close connections between Lehmer's Question about Salem numbers and problems in hyperbolic geometry. For example, the existence of a minimal Salem number is equivalent to the so-called *Short Geodesic Conjecture* which states that there is a geodesic of minimal length amongst all simple closed geodesics on all arithmetic hyperbolic 2- and 3-orbifolds, respectively; see [1], [7] and [8].

Here, we present our result about the appearance of Salem numbers as growth rates, which constitutes a part of our joint work with L. Liechti [5]. It can be stated as follows.

**Theorem.** *Not every Salem number is the growth rate of a cocompact hyperbolic Coxeter group.*

In the proof of the above theorem, it was important to dispose of the 47 known Salem numbers less than 1.3 as displayed in the online list established by Mossinghoff.

Finally, let us look at Coxeter groups acting cocompactly on hyperbolic $n$-space for $n \geq 4$. We observed, among other things, that their growth rates are not Salem numbers anymore. Together with G. Perren [6], we then formulated the following general conjecture in terms of *Perron numbers*, that is, real algebraic integers $> 1$ such that all of whose other Galois conjugates have strictly smaller absolute value. Before doing so, let us mention, that among the Perron numbers whose minimal polynomials have degree $\leq 12$, the smallest one is about $\approx 1.06217$ and has minimal polynomial of degree 12.

**Conjecture.** *The growth rate of any cocompact hyperbolic Coxeter group is a Perron number.*

**Remark.** By means of the software designed by R. Guglielmetti [2], one can check whether the growth rate of a given cofinite hyperbolic Coxeter group is a Salem number, a Pisot number or a Perron number. Furthermore, the software computes

the group Euler characteristic and indicates whether or not the Coxeter group is arithmetic.

**Remark.** Seemingly the above conjecture remains valid under the weaker condition of finite covolume.

## References


[1] E. Ghate, E. Hironaka, *The arithmetic and geometry of Salem numbers*, Bull. AMS. **38** (2001), 293–314.

[2] R. Guglielmetti, *CoxIter* – computing invariants of hyperbolic Coxeter groups, LMS J. Computation and Math. **18** (2015), 754–773.

[3] E. Hironaka, *The Lehmer polynomial and pretzel links*, Canad. Math. Bull. European J. Combin. **44** (2001), 440–451.

[4] R. Kellerhals, *Cofinite hyperbolic Coxeter groups, minimal growth rate and Pisot numbers*, Algebr. Geom. Topol. **13** (2013), 1001–1025.

[5] R. Kellerhals, L. Liechti, *Salem numbers, spectral radii and growth rates of hyperbolic Coxeter groups*, Transform. Groups **28** (2023), 831–852.

[6] R. Kellerhals, G. Perren, *On the growth of cocompact hyperbolic Coxeter groups*, European J. Combin. **32** (2011), 1299–1316.

[7] C. Maclachlan, A. Reid, *The arithmetic of hyperbolic 3-manifolds*, Graduate Texts in Mathematics, vol. 219, Springer-Verlag, New York, 2003.

[8] C. Smyth, *Seventy years of Salem numbers*, Bull. London Math. Soc. **47** (2015), 379–395.


## The wild Brauer–Manin obstruction on K3 surfaces

Margherita Pagano

Let $V$ be a proper, smooth and geometrically integral $k$-variety. Let $\mathbb{A}_k$, the ring of adèles of $k$. We say that $V$ satisfies *weak approximation* if the image of $V(k)$ in $V(\mathbb{A}_k)$ is dense.

In 1970 Manin [1] introduced the use of the Brauer group of a variety $V$ to study the image of $V(k)$ in $V(\mathbb{A}_k)$. In particular, he used the Brauer group to build an intermediate set $V(\mathbb{A}_k)^{\mathrm{Br}}$ such that

$$V(k) \subseteq V(\mathbb{A}_k)^{\mathrm{Br}} \subseteq V(\mathbb{A}_k).$$

Using class field theory it is possible to prove that for every place $\nu \in \Omega_k$ and for every element $\mathcal{A} \in \mathrm{Br}(V)$, there is a map, called the evaluation map

$$\mathrm{ev}_{\mathcal{A}} \colon V(k_\nu) \to \mathbb{Q}/\mathbb{Z}$$

such that

$$(1) \quad V(\mathbb{A}_k)^{\mathrm{Br}} := \left\{ (x_\nu) \in X(\mathbb{A}_k) \mid \forall \mathcal{A} \in \mathrm{Br}(V), \text{ such that } \sum_{\nu \in \Omega_k} \mathrm{ev}_{\mathcal{A}}(x_\nu) = 0 \right\}$$

is a *closed* subset of $V(\mathbb{A}_k)$ that contains the set of $k$-points $V(k)$.

We say that a place $\nu$ *plays a role* in the Brauer–Manin obstruction to weak approximation on $V$ if there is an element $\mathcal{A} \in \mathrm{Br}(V)$ such that $\mathrm{ev}_{\mathcal{A}} \colon V(k_\nu) \to \mathbb{Q}/\mathbb{Z}$ is non-constant.

Let $\bar{k}$ be an algebraic closure of $k$ and $\bar{V}$ be the base change of $V$ to $\bar{k}$, i.e. $\bar{V} := V \times_k \bar{k}$. The results presented in this talk are inspired by the following question:

**Q:** Assume $\mathrm{Pic}(\bar{V})$ to be torsion-free and finitely generated. Which places can play a role in the Brauer–Manin obstruction to weak approximation on $V$?

This question is a reformulation of a question that was originally asked by Swinnerton–Dyer; he asked whether under the same assumption on $\mathrm{Pic}(\bar{V})$ as above the only places that can play a role in the Brauer–Manin obstruction to weak approximation are the archimedean ones and the ones of bad reduction for the variety.

In [2] Colliot-Thélène and Skorobogatov showed that under this assumption on $\mathrm{Pic}(\bar{V})$ if a prime of good reduction plays a role, then the corresponding element $\mathcal{A}$ in the Brauer group cannot be algebraic, i.e. it cannot lie in the kernel of $\mathrm{Br}(V) \to \mathrm{Br}(\bar{V})$[1]. If the transcendental Brauer group is finite, then the only places that can play a role are the archimedean places, the places of bad reduction and the places whose residue characteristic divides the order of the transcendental Brauer group, see [2]. Using this result, they give several examples of varieties for which the answer to Swinnerton-Dyer's question is positive.

For curves and surfaces with negative Kodaira dimension we have all the elements in the Brauer group are algebraic, i.e. $\mathrm{Br}(V) = \mathrm{Br}_1(V)$. Hence, K3 surfaces are one of the first example of varieties where the transcendental Brauer group is potentially non-trivial. However, this is not always the case: for example in [4] the authors show that, under certain conditions, the whole Brauer group of a diagonal quartic surface over $\mathbb{Q}$ is algebraic. The first example of a transcendental element in the Brauer group of a K3 surface defined over a number field was given by Wittenberg in [3]. In particular, Wittenberg constructed a 2-torsion transcendental element that obstructs weak approximation on the surface. Other examples of 2-torsion transcendental elements that obstruct weak approximation can be found in [5] and [6]. In all these articles, the obstruction to weak approximation comes from the fact that the transcendental quaternion algebra has non-constant evaluation at the place at infinity. With a construction similar to the one used in [5], Hassett and Várilly-Alvarado [7] have also built an example of a 2-torsion element on a K3 surface that obstructs the Hasse principle.

Furthermore, there are examples of transcendental elements of order 3 on K3 surfaces that obstruct weak approximation (for example, see [8], [9] and [10]). In all these cases, the evaluation map at the place at infinity has to be trivial, since $\mathrm{Br}(\mathbb{R})$ does not contain elements of order 3, and the obstruction to weak approximation comes from the evaluation map at the prime 3, which in every example is a prime of bad reduction for the K3 surface taken into account. Therefore, none of the examples mentioned above can be used to give a negative answer to the question formulated by Swinnerton-Dyer.

[1]Elements in the Brauer group that are not algebraic are called transcendental.

After Colliot-Thélène and Skorobogatov's work the main remaining difficulty was to control the evaluation map of a $p$-power element in the Brauer group on the $V(k_{\mathfrak{p}})$-points, where $\mathfrak{p}$ is a prime of good reduction with residue characteristic $p$. In 2020 Bright and Newton [11] developed new techniques that allow one to control also the behaviour of the evaluation map in this case. Roughly speaking, they use work of Kato [12] to introduce a new filtration on the Brauer group which they prove to be strongly related to the behaviour of the evaluation map attached to elements in $\mathrm{Br}(V)$. The first chapter of this thesis is devoted to introducing these new techniques and extending some results of Bright and Newton.

Bright and Newton prove that if we start with a variety $V$ with non-trivial $\mathrm{H}^0(V, \Omega^2_V)$, then for primes $\mathfrak{p}$ having good ordinary reduction we can always find a finite field extension $k'/k$ and a prime above $\mathfrak{p}$ playing a role in the Brauer–Manin obstruction to weak approximation: see [11, Theorem C] for the precise statement. Hence, if we take a variety $V$ such that:

- the geometric Picard group $\mathrm{Pic}(\bar{V})$ is torsion-free and finitely generated,
- $\mathrm{H}^0(V, \Omega^2_V)$ is non-trivial,
- there is a prime $\mathfrak{p}$ of good ordinary reduction,

then up to a base change to a finite field extension $k'/k$ we can *always* find a prime of good (ordinary) reduction that plays a role in the Brauer–Manin obstruction to weak approximation on $V_{k'}$. Since K3 surfaces satisfy all the properties listed above, Bright and Newton's result leads to a negative answer to the question asked by Swinnerton-Dyer.

However, the result does not say anything about how large the field extension $k'/k$ can be. In particular, they do not say whether it is possible to find already over $\mathbb{Q}$ a Brauer-Manin obstruction arising from a prime of good reduction.

**Theorem (Pagano, [14]).** Let $V \subseteq \mathbb{P}^3_{\mathbb{Q}}$ be the projective K3 surface defined by the equation

$$x^3y + y^3z + z^3w + w^3x + xyzw = 0. \tag{2}$$

The class of the quaternion algebra

$$\mathcal{A} = \left( \frac{z^3 + w^2x + xyz}{x^3}, -\frac{z}{x} \right) \in \mathrm{Br}\, \mathbb{Q}(V)$$

defines an element in $\mathrm{Br}(V)$. The evaluation map $\mathrm{ev}_{\mathcal{A}} \colon V(\mathbb{Q}_2) \to \mathrm{Br}(\mathbb{Q}_2)$ is non-constant. Moreover, $V(\mathbb{Q})$ is not dense in $V(\mathbb{Q}_2)$.

This is the first example of a K3 surface (defined over $\mathbb{Q}$) for which a prime of good reduction plays a role in the Brauer–Manin obstruction to weak approximation and proves that the field extension appearing in Bright and Newton's result is not always needed. At this point some natural questions arise:

(1) When is the field extension $k'/k$ appearing in Bright and Newton's result needed?
(2) Is the ordinary condition necessary?

Answering these two questions is the aim of [13].

**Theorem (Pagano, [13]).** Let $\mathfrak{p}$ be a prime of good ordinary reduction for $V$ of residue characteristic $p$. Assume that the special fibre at $\mathfrak{p}$, $\mathcal{V}(\mathfrak{p})$ has no non-trivial global 1-forms, $\mathrm{H}^1(\overline{\mathcal{V}(\mathfrak{p})}, \mathbb{Z}/p\mathbb{Z}) = 0$ and $(p-1) \not| e_{\mathfrak{p}}$. Then the prime $\mathfrak{p}$ does not play a role in the Brauer–Manin obstruction to weak approximation on $V$.

**Theorem (Pagano, [13]).** Let $V$ be a K3 surface and $\mathfrak{p}$ be a prime of good non-ordinary reduction for $V$ with $e_{\mathfrak{p}} \leq (p-1)$. Then the prime $\mathfrak{p}$ does not play a role in the Brauer–Manin obstruction to weak approximation on $V$.

## References


[1] Manin, Yuri Ivanovich, *Le groupe de Brauer-Grothendieck en géométrie diophantienne*, Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 1 (1971), 401–411.

[2] Colliot-Thélène, Jean-Louis and Skorobogatov, Alexei N., *Good reduction of the Brauer-Manin obstruction*, Transactions of the American Mathematical Society **365** (2013), 579–590.

[3] Wittenberg, Olivier, *Transcendental Brauer-Manin obstruction on a pencil of elliptic curves*, Arithmetic of higher-dimensional algebraic varieties (Palo Alto, CA, 2002), **226** (2004), 259–267.

[4] Ieronymou, Evis and Skorobogatov, Alexei N. and Zarhin, Yuri G., *On the Brauer group of diagonal quartic surfaces*, J. Lond. Math. Soc. (2) **83** (2011), 659–672.

[5] Hassett, Brendan and Várilly-Alvarado, Anthony and Varilly, Patrick, *Transcendental obstructions to weak approximation on general K3 surfaces*, Adv. Math. **228** (2011), 1377–1404.

[6] Ieronymou, Evis, *Diagonal quartic surfaces and transcendental elements of the Brauer groups*, J. Inst. Math. Jussieu **9** (2010), 769–798.

[7] Hassett, Brendan and Várilly-Alvarado, Anthony, *Failure of the Hasse principle on general K3 surfaces*, J. Inst. Math. Jussieu **12** (2013), 853–877.

[8] Preu, Thomas, *Example of a transcendental 3-torsion Brauer-Manin obstruction on a diagonal quartic surface*, London Math. Soc. Lecture Note Ser. **405** (2013), 447–459.

[9] Newton, Rachel, *Transcendental Brauer groups of products of CM elliptic curves*, J. Lond. Math. Soc. (2) **93** (2016), 397–419.

[10] Berg, Jennifer and Várilly-Alvarado, Anthony, *Odd order obstructions to the Hasse principle on general K3 surfaces*, Math. Comp. **89** (2020), 1395–1416.

[11] Bright, Martin and Newton, Rachel, *Evaluating the wild Brauer group*, Invent. Math. **234** (2023), 819–891.

[12] Kato, Kazuya, *Swan conductors for characters of degree one in the imperfect residue field case*, Contemp. Math. **83** (1989), 101–131.

[13] Pagano, Margherita, *The role of primes of good reduction in the Brauer–Manin obstruction*, https://arxiv.org/pdf/2307.16030 (2023).

[14] Pagano, Margherita, *An example of a Brauer-Manin obstruction to weak approximation at a prime with good reduction*, Res. Number Theory **8** (2022).

## The arithmetic of Dirichlet $L$-values

Frank Calegari
(joint work with Vesslin Dimitrov and Yunqing Tang)

We report on our proof [3] of the irrationality of the classical Dirichlet $L$-value

$$L(2,\chi_{-3}) = \frac{1}{1^2} - \frac{1}{2^2} + \frac{1}{4^2} - \frac{1}{5^2} + \frac{1}{7^2} - \frac{1}{8^2} + \dots.$$

Our work also establishes the $\mathbf{Q}$-linear independence of $1, \zeta(2)$ and $L(2,\chi_{-3})$. This is the first new irrationality result for such $L$-values since Apéry's proof [1, 2] in 1978 that $\zeta(3) \notin \mathbf{Q}$. We start by explaining how Apéry's argument works in terms of the radius of convergence of holonomic functions and singularities of certain ordinary differential equations of geometric origin. We then explain how one should and can exploit the analytic continuation of these $G$-functions outside the disc of radius of convergence, and how that leads to a more refined approach.

### References

[1] Alf van der Poorten, *A proof that Euler missed...Apéry's proof of the irrationality of* $\zeta(3)$, Math. Intelligencer **1** (1978/79), no. 4, 195–203, An informal report. MR 547748
[2] Henri Cohen, *Démonstration de l'irrationalité de* $\zeta(3)$ *(d'après R. Apéry)*, Séminaire de théorie des nombres de Grenoble **6** (1977–78), VI.1–9.
[3] Frank Calegari, Vesselin Dimitrov, and Yunqing Tang, *The linear independence of* $1, \zeta(2)$, *and* $L(2,\chi_{-3})$, 2021, `https://arxiv.org/abs/2408.15403`.

## Landscapes of $L$-functions

David P. Roberts
(joint work with David W. Farmer, Sally Koutsoliotas, and Stefan Lemurell)

My talk described the current state of our project to numerically tabulate many automorphic $L$-functions and to organize the results visually into landscapes. It focused on our heuristic explanation of unexpected *fine structure* visible in the landscapes.

**A sample landscape.** The first part of the talk explained some of the main ideas by focusing on a single landscape of $L$-functions, drawn here as Figure 1. The name $\mathcal{L}(+++,1)$ of the sample landscape captures that it is indexing automorphic $L$-functions with infinity type $\Gamma_+(s-i\lambda_1)\Gamma_+(s-i\lambda_2)\Gamma_+(s-i\lambda_3)$ and conductor 1. Here $\Gamma_+(s)$ is just another name for the standard modified $\Gamma$-function $\Gamma_{\mathbb{R}}(s) = \pi^{-s/2}\Gamma(s/2)$. Also we are imposing the normalization conditions

$$\lambda_1 + \lambda_2 + \lambda_3 = 0, \qquad \lambda_1 \le \lambda_2 \le \lambda_3. \tag{1}$$

An $L$-function gives rise to an *$L$-point* at $(\ell_1,\ell_2)$ with $\ell_j = \lambda_{j+1} - \lambda_j$. It is known that these $L$-points are distributed roughly according to Plancherel density, which is very closely approximated by a specific multiple of $\ell_1\ell_2(\ell_1+\ell_2)$.

It is currently not feasible to start in the automorphic theory and rigorously produce a generically-behaving $L$-function belonging to $\mathcal{L}(+++,1)$. Instead we

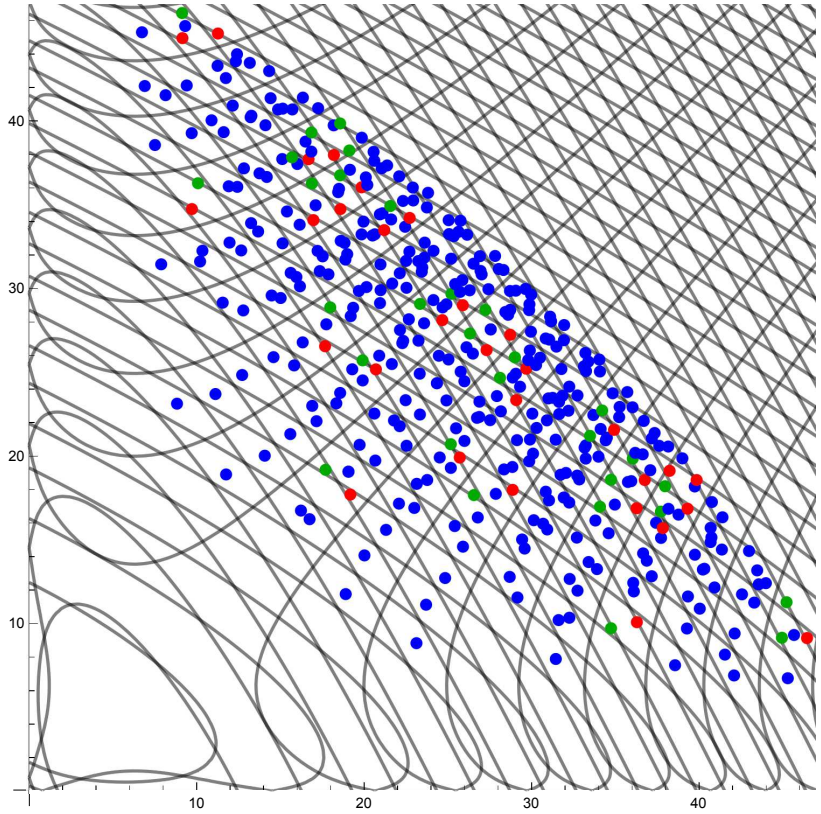



FIGURE 1. The landscape $\mathcal{L}(+++, 1)$, with all known $L$-points of radius $\leq 40$ drawn. $L$-points of class 0, 1, and 2 in $\mathbb{Z}/3\mathbb{Z}$ are respectively drawn as ●, ●, and ●.

numerically solve the functional equation that these $L$-functions are known to satisfy. Each point in Figure 1 represents what we strongly believe is indeed an $L$-function. This complicated and computationally-intensive process is sketched in [1], dates back to earlier work of my coauthors, and was not the subject of the talk. The points drawn in Figure 1 all satisfy $\lambda_1^2 + \lambda_2^2 + \lambda_3^2 \leq 40^2$. The talk explained that we expect that our list in this domain is near-complete. One source of optimism is that there is reasonably good agreement with Plancherel density. Another is that our computational method continues to produce similar $L$-points well past the radial cutoff of 40, where computations are more challenging.

One can see in Figure 1 a first aspect of fine structure, the statistical tendency of $L$-points to stay away from the drawn *ditches*. Our explanation depends on the general phenomena of *spectral rigidity* and *root repulsion*. The ditches are formed from the points $(\ell_1, \ell_2)$ where extreme spectral rigidity would predict a critical zero $\frac{1}{2} + it$ at a height $t$ coinciding with the height $\lambda_j$ of one of the three rows of

trivial zeros. From root repulsion, in this case between trivial and critical zeros, $L$-points should be less likely to occur near these ditches.

A second and more subtle aspect of fine structure is *congruence bias*. Given an $L$-function indexed by the landscape, let $z_j$ be the number of critical zeros appearing above the $j^{\text{th}}$ row but below the $(j+1)^{\text{st}}$ row of trivial zeros. In the case of Figure 1, let $c = z_1 - z_2 \in \mathbb{Z}/3\mathbb{Z}$. Then we observe that $c = 0$ arises for about 80% of the drawn $L$-points. We heuristically explain the dominance of this class by looking at the individual connected components of the complement of all the ditches. Class 0, 1, and 2 points tend to be respectively in large hexagons, small upwards-pointing triangles, and small downwards-pointing triangles.

**General formalism of landscapes.** The middle part of the talk explained, without reference to fine structure, our vision of organizing all $L$-functions into landscapes. The $L$-functions in question by definition come in the standard way from cuspidal automorphic representations of the adelic groups $\mathrm{GL}_d(\mathbb{A}_{\mathbb{Q}})$. Write $\Gamma_-(s) = \Gamma_{\mathbb{R}}(s+1)$, and $\Gamma_\omega(s) = \Gamma_{\mathbb{C}}(s+\omega)$ with $\Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s)$. Consider *shift vectors* $\Omega = (\omega_1, \ldots, \omega_v)$, with each $\omega_j$ in $\{+, -, 1, 2, 3, \ldots\}$. For each shift vector $\Omega$ and conductor $N \in \mathbb{Z}_{\geq 1}$, one has a landscape $\mathcal{L}(\Omega, N)$. The $L$-points in this landscape have infinity type

$$\Gamma_{w_1}(s - i\lambda_1) \cdots \Gamma_{w_v}(s - i\lambda_v)$$

and conductor $N$. Writing $\deg(+) = \deg(-) = 1$ and otherwise $\deg(\omega) = 2$, one has $\sum_{j=1}^{v} \deg(\omega_j) = d$. We normalize by the direct analog of (1), namely $\sum_{j=1}^{v} \deg(\omega_j)\lambda_j = 0$ and $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_{v-1} \leq \lambda_v$. So the landscape is now a $(v-1)$-dimensional orthant with coordinates $\ell_j = \lambda_{j+1} - \lambda_j$, containing $L$-points roughly distributed according to an explicit Plancherel density. In passing from $\mathcal{L}(\Omega, 1)$ to $\mathcal{L}(\Omega, N)$, Plancherel density is simply multiplied by a constant $\nu_d(N)$. Here $\nu_d$ is a complicated multiplicative function with $\nu_d(N) \approx N^d$.

An $L$-function is called *algebraic* if all its vertical shifts $\lambda_j$ are 0 and all its horizontal shifts $\omega_j$ have the same parity, counting $+$ and $-$ as even. Otherwise it is called *transcendental*. Algebraic $L$-functions are exactly the ones expected to come from algebraic geometry, with Hodge information determining $\Omega$. The talk emphasized the rarity of algebraic $L$-functions among all $L$-functions. For example, ignoring fine structure, $\mathcal{L}(+++, N)$ should look similar to $\mathcal{L}(+++, 1)$, except that the density of $L$-points has increased by about $N^3$. Correspondingly, the $L$-point-free region about the origin has shrunk. The expectation in this case is that all $L$-points at $(0, 0)$ come from totally real irreducible three-dimensional Artin representations with conductor $N$. The first such is at $N = 1947$.

**Fine structure in general landscapes.** The last part of the talk was a quick tour of various other landscapes with degree $d \leq 4$ and conductor $N = 1$. All exhibited ditch avoidance and congruence bias according to $c \in \mathbb{Z}/d\mathbb{Z}$. When all the $\omega_j$ are in $\{+, -\}$, the class $c$ is the reduced dot product $(1, \ldots, d-1) \cdot (z_1, \ldots, z_{d-1})$, with $z_j$ counting trapped zeros as before. The definition of $c$ for general $\Omega$ is the same, when one views each index $\omega_j \in \mathbb{Z}_{\geq 1}$ as contributing two rows of trivial zeros at the common height $\lambda_j$, with no critical zeros trapped

between them. Our general heuristic theory of congruence bias has as origin the fact that the root lattice of $\mathrm{GL}_d$ has index $d$ in the weight lattice, with quotient group $\mathbb{Z}/d\mathbb{Z}$. The details of the observed congruence bias always were consistent with our theory. In particular, the preferred classes depend on the ordering of the indices $\omega_j$. For example, our last exhibited pair of landscapes confirmed that $c = 2$ occurs most often for $++3$ while $c = 0$ occurs most often for $+3+$.

Fine structure for $N > 1$ is more complicated, as $L$-points must be considered in thickened landscapes, $\tilde{\mathcal{L}}(\Omega, N) = \mathcal{L}(\Omega, N) \times$ (unit circle). Here the second coordinate of an $L$-point is the contribution from finite primes to its root number. Ditches live in $\tilde{\mathcal{L}}(\Omega, N)$, not $\mathcal{L}(\Omega, N)$. But once one has moved to $\tilde{\mathcal{L}}(\Omega, N)$, ditch avoidance and congruence bias are similar to before. Time did not allow showing some of our landscapes with $N > 1$ that illustrate this more complicated theory.

## References

[1] David W. Famer, Sally Koutsoliotas, Stefan Lemurell, and David P. Roberts. *The landscape of L-functions: degree* 3 *and conductor* 1, Contemp. Math., 796, American Mathematical Society, Providence, RI, 2024, 313–338.

## On the Brauer Groups of Stacky Curves

Niven Achenjang

Brauer groups of fields were classically studied objects whose definition was generalized to rings in work of Azumaya, Auslander, and Goldman [6, 3], and then later to schemes in work of Grothendieck [7, 8, 9]. These have been cemented as important cohomological invariants for their applications to class field theory, to understanding $l$-adic cohomology (especially of curves), and to obstructions to rational points on varieties. In recent times, there has been growing interest in extending our understanding of Brauer groups from schemes to stacks. As a starting point, one can study the Brauer groups of *stacky curves*, i.e. a separated, finite-type algebraic stack $\mathcal{X}$ over a field $k$, which is pure of dimension 1 and has finite inertia. To fix ideas, given an algebraic stack $\mathcal{X}$, we define its *Brauer group* to be $\mathrm{Br}\mathcal{X} := \mathrm{H}^2_{\acute{e}t}(\mathcal{X}, \mathbb{G}_m)_{\mathrm{tors}}$.

Previous work along this direction has generally focused on a single stacky curve at a time. For example, there is the breakthrough work of Antieau and Meier [4] who computed the Brauer group of the moduli stack $\mathcal{Y}(1)$ of elliptic curves over a variety of bases of arithmetic interest (e.g. over $\mathbb{Q}, \mathbb{Z}$, or any finite or algebraically closed field of characteristic not 2). For all base schemes $S$ appearing in their main theorem [4, Theorem 1.1], they show

$$\mathrm{Br}\mathcal{Y}(1)_S \cong \mathrm{Br}\mathbb{A}^1_S \oplus \mathrm{H}^1_{\acute{e}t}(S, \mathbb{Z}/12\mathbb{Z}). \tag{1}$$

This work was later complemented by work of Shin and of di Lorenzo–Pirisi [12, 10] who were able to compute $\mathrm{Br}\mathcal{Y}(1)_k$ for *any* field $k$. Of note, they found that if $\mathrm{char}k = 2$, then there is an exact sequence

$$0 \to \mathrm{Br}\mathbb{A}^1_k \oplus \mathrm{H}^1_{\acute{e}t}(k, \mathbb{Z}/12\mathbb{Z}) \to \mathrm{Br}\mathcal{Y}(1)_k \to \mathbb{Z}/2\mathbb{Z} \to 0, \tag{2}$$

so $\mathrm{Br}\mathcal{Y}(1)_k$ is an extension of $\mathbb{Z}/2\mathbb{Z}$ by the right hand side of (1).

Separately, Bhamidipati, Jha, Ji, Lopez, and I [1] were able to extend the techniques pioneered by Antieau, Meier, and Shin in order to apply them to computing the Brauer group of the moduli stack $\mathcal{Y}_0(2)$ of elliptic curves equipped with an étale subgroup of order 2. We found that, at least when $S$ is $\mathbb{Z}[1/2]$ or a perfect field of characteristic not 2, one has

$$\mathrm{Br}\mathcal{Y}_0(2)_S \cong \mathrm{Br}(\mathbb{A}^1_S - \{0\}) \oplus \mathrm{H}^1_{\acute{e}t}(S, \mathbb{Z}/4\mathbb{Z}) \oplus \mathbb{Z}/2\mathbb{Z}. \tag{3}$$

At this point, some explanation of the terms in Eqs. (1) to (3) is in order.

- The schemes $\mathbb{A}^1_S, \mathbb{A}^1_S - \{0\}$ are the respective coarse moduli spaces of the stacks $\mathcal{Y}(1)_S$ and $\mathcal{Y}_0(2)_S$. Their Brauer groups show up as pullbacks along the maps $\mathcal{Y}(1) \to \mathbb{A}^1$ and $\mathcal{Y}_0(2) \to \mathbb{A}^1 - \{0\}$.
- The cohomology groups $\mathrm{H}^1_{\acute{e}t}(S, \mathbb{Z}/12\mathbb{Z}), \mathrm{H}^1_{\acute{e}t}(S, \mathbb{Z}/4\mathbb{Z})$ ultimately are related to the facts that, for any field $k$ (say, of characteristic not 2), one has $\mathrm{Pic}\mathcal{Y}(1)_k \cong \mathbb{Z}/12\mathbb{Z}$ and $\mathrm{Pic}\mathcal{Y}_0(2)_k \cong \mathbb{Z}/4\mathbb{Z}$.
- The fact that (1) and (2) differ is related to the fact that the stack $\mathcal{Y}(1)$ is generically tame away from characteristic 2, but is nowhere tame in characteristic 2. That is, the extra $\mathbb{Z}/2\mathbb{Z}$ in (2) should be viewed as a "wild" phenomenon.

The above gives some geometric explanation for all the terms in Eqs. (1) to (3) *except* for the $\mathbb{Z}/2\mathbb{Z}$ in (3) (note that $\mathcal{Y}_0(2)$ is everywhere tame in characteristic not 2). This brings us to the focus of our talk.

Letting $\overline{k}$ be an algebraically closed field of characteristic not 2, Eqs. (1) and (3) tell us that

$$\mathrm{Br}\mathcal{Y}(1)_{\overline{k}} = 0 \text{ while } \mathrm{Br}\mathcal{Y}_0(2)_{\overline{k}} = \mathbb{Z}/2\mathbb{Z}.$$

Recall that if $X$ is a scheme-y curve over an algebraically closed field, then $\mathrm{Br}X = 0$ always, as a consequence of Tsen's theorem. However, we see above that this result can fail for tame stacky curves.

**Question 1.** *Can one compute the Brauer group of a tame stacky curve over an algebraically closed field?*

In this talk, we address this question, at least for stacks which satisfy the following "locally Brauerless' condition (this includes, for example, all tame modular curves).

**Definition 2.** Let $\mathcal{X}$ be an algebraic stack which is tame in the sense of [5]. We say that $\mathcal{X}$ is *locally Brauerless* if, for any geometric point $x \in \mathcal{X}(\Omega)$ defined over a separably closed field $\Omega$, writing

$$0 \longrightarrow \Delta \longrightarrow \underline{\mathrm{Aut}}_{\mathcal{X}}(x) \longrightarrow G \longrightarrow 0$$

for the connected-étale sequence of its automorphism group, one has $\mathrm{H}^3(G, \mathbb{Z}) = 0$. Here, $G$ is necessarily a constant group and $\mathrm{H}^3(G, \mathbb{Z})$ denotes the group cohomology of this group acting trivially on $\mathbb{Z}$.

**Example 3.** If every geometric automorphism group of $\mathcal{X}$ is of the form $\mu_n$ for some $n$, then $\mathcal{X}$ is tame and locally Brauerless.

**Theorem 4** (A., in preparation [2])**.** *Let $\mathcal{X}$ be a locally Brauerless tame algebraic stack with coarse space $c\colon \mathcal{X} \to X$. Then, $\mathrm{R}^2 c_* \mathbb{G}_m = 0$.*

The utility of this theorem is that it simplifies the process of computing $\mathrm{H}^2_{\acute{e}t}(\mathcal{X}, \mathbb{G}_m)$ via the Leray spectral sequence $E_2^{ij} = \mathrm{H}^i_{\acute{e}t}(X, \mathrm{R}^j c_* \mathbb{G}_m) \implies \mathrm{H}^{i+j}_{\acute{e}t}(\mathcal{X}, \mathbb{G}_m)$. Its proof is rather involved, but its simplest case is exemplified by the following example.

**Example 5.** Say $\mathcal{X} = BG_k$ for a separably closed field $k$ and a finite, constant group $G$ such that $p := \mathrm{char} k \nmid \#G$. Then, $\mathbb{G}_m(k)[1/p]$ is a divisible group and so embeds inside (and hence is a direct summand of) $\mathbb{Q}^{\oplus I} \oplus (\mathbb{Q}/\mathbb{Z})^{\oplus J}$ for some sets $I, J$. Thus,

$$\mathrm{H}^2(BG, \mathbb{G}_m) \simeq \mathrm{H}^2(G, \mathbb{G}_m(k)) \simeq \mathrm{H}^2(G, \mathbb{G}_m(k)[1/p]) \hookrightarrow \mathrm{H}^2(G, \mathbb{Q})^{\oplus I} \oplus \mathrm{H}^2(G, \mathbb{Q}/\mathbb{Z})^{\oplus J}.$$

Finally, one can check that $\mathrm{H}^2(G, \mathbb{Q}) = 0$ because $G$ is finite and $\mathrm{H}^2(G, \mathbb{Q}/\mathbb{Z}) = 0$ if $\mathrm{H}^3(G, \mathbb{Z}) = 0$.

**Remark.** As was more-or-less shown already in [11], the DM case of Theorem 4 can essentially be reduced to Theorem 5.

In relation to Theorem 1, Theorem 4 allows us to prove the following.

**Setup.** *Fix $k = \bar{k}$ be a field. Suppose we're given*

$$\mathcal{X} \xrightarrow{\pi} \mathcal{Y} \xrightarrow{\rho} X, \qquad \mathcal{X} \xrightarrow{c} X$$

*where*

- *$X$ is a smooth $k$-curve.*
- *There exists distinct, closed $x_1, \ldots, x_r \in X$ and $e_1, \ldots, e_r > 1$ so that*
$$\mathcal{Y} \simeq \sqrt[e_1]{x_1/X} \times_X \cdots \times_X \sqrt[e_r]{x_r/X} \xrightarrow{\rho} X$$
- *There is a commutative, finite linearly reductive group $G/k$ so that $\mathcal{X} \to \mathcal{Y}$ is a $G$-gerbe.*

**Theorem 6** (A., in preparation [2])**.** *If $\mathcal{X}$ is locally Brauerless, then $\mathrm{Br}\mathcal{X} \simeq \mathrm{H}^1_{\acute{e}t}(X, G^\vee)$. Here, $G^\vee$ is the Cartier dual of $G$.*

*Proof Idea.* One first uses the Leray spectral sequence $E_2^{ij} = \mathrm{H}^i_{\acute{e}t}(X, \mathrm{R}^j c_* \mathbb{G}_m) \implies \mathrm{H}^{i+j}_{\acute{e}t}(\mathcal{X}, \mathbb{G}_m)$ to compute that $\mathrm{H}^2_{\acute{e}t}(\mathcal{X}, \mathbb{G}_m) \simeq \mathrm{H}^1_{\acute{e}t}(X, \mathrm{R}^1 c_* \mathbb{G}_m)$. One then uses the Grothendieck spectral sequence $F_2^{ij} = \mathrm{R}^i \rho_* \mathrm{R}^j \pi_* \mathbb{G}_m \implies \mathrm{R}^{i+j} c_* \mathbb{G}_m$ to produce an exact sequence $0 \to \mathrm{R}^1 \rho_* \mathbb{G}_m \to \mathrm{R}^1 c_* \mathbb{G}_m \to G^\vee \to 0$. Finally, $\mathrm{R}^1 \rho_* \mathbb{G}_m$ is supported on a finite $k$-scheme and so is acyclic; therefore, $\mathrm{H}^1_{\acute{e}t}(X, \mathrm{R}^1 c_* \mathbb{G}_m) \xrightarrow{\sim} \mathrm{H}^1_{\acute{e}t}(X, G^\vee)$. □

**Example 7.** If $\mathcal{X} = \mathcal{Y}(1)$ (and $\mathrm{char} k \nmid 6$), then one can take $G = \mu_2$ and Theorem 6 shows that $\mathrm{Br}\mathcal{Y}(1)_{\bar{k}} \simeq \mathrm{H}^1_{\acute{e}t}(\mathbb{A}^1_{\bar{k}}, \mathbb{Z}/2\mathbb{Z}) = 0$.

**Example 8.** If $\mathcal{X} = \mathcal{Y}_0(2)$ (and $\mathrm{char}k \nmid 2$), then one can take $G = \mu_2$ and Theorem 6 shows that $\mathrm{Br}\mathcal{Y}_0(2)_{\bar{k}} \simeq \mathrm{H}^1_{\acute{e}t}(\mathbb{A}^1_{\bar{k}} - \{0\}, \mathbb{Z}/2\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$.

This gives a geometric explanation of the $\mathbb{Z}/2\mathbb{Z}$ in (3).

## References


[1] Niven Achenjang, Deewang Bhamidipati, Aashraya Jha, Caleb Ji, and Rose Lopez. The brauer group of $\mathscr{Y}_0(2)$. `https://arxiv.org/abs/2311.18132`, 2024.

[2] Niven Achenjang. On Brauer groups of tame stacks, in preparation.

[3] Maurice Auslander and Oscar Goldman. The brauer group of a commutative ring. *Transactions of the American Mathematical Society*, 97(3):367–409, 1960.

[4] Benjamin Antieau and Lennart Meier. The Brauer group of the moduli stack of elliptic curves. *Algebra & Number Theory*, 14(9):2295–2333, 2020.

[5] Dan Abramovich, Martin Olsson, and Angelo Vistoli. Tame stacks in positive characteristic. *Ann. Inst. Fourier (Grenoble)*, 58(4):1057–1091, 2008.

[6] Gorô Azumaya. On maximally central algebras. *Nagoya Mathematical Journal*, 2(none):119–150, 1951.

[7] Alexander Grothendieck. Le group de Brauer : I. Algèbres d'Azumaya et interprétations diverse. In *Séminaire Bourbaki : années 1964/65 1965/66, exposés 277-312*, number 9 in Séminaire Bourbaki. Société mathématique de France, 1966. talk: 290.

[8] Alexander Grothendieck. Le groupe de Brauer : II. Théories cohomologiques. In *Séminaire Bourbaki : années 1964/65 1965/66, exposés 277-312*, number 9 in Séminaire Bourbaki. Société mathématique de France, 1966. talk:297.

[9] Alexander Grothendieck. Le group de Brauer. III. Exemples et compléments. In *Dix exposés sur la cohomologie des schémas*, volume 3 of *Adv. Stud. Pure Math.*, pages 88–188. North-Holland, Amsterdam, 1968.

[10] Andrea Di Lorenzo and Roberto Pirisi. Cohomological invariants and brauer groups of algebraic stacks in positive characteristic. `https://arxiv.org/abs/2207.08792`, 2022.

[11] Lennart Meier. Computing brauer groups via coarse moduli – draft version. `https://webspace.science.uu.nl/~meier007/CoarseBrauer.pdf`, Febrary 2018.

[12] Minseon Shin. The Brauer group of the moduli stack of elliptic curves over algebraically closed fields of characteristic 2. *J. Pure Appl. Algebra*, 223(5):1966–1999, 2019.


## Complexity bounds for multiplication


David Harvey

(joint work with Joris van der Hoeven)


In this talk I gave an overview of what is known about upper and lower bounds for the complexity of integer multiplication and some related problems.

### 1. Upper bounds

Let $M(n)$ denote the cost of multiplying $n$-bit integers. By "cost" we mean the number of steps performed by a multitape Turing machine [Pap94].

**Theorem 1** ([HvdH21])**.** $M(n) = O(n \log n)$.

Suprisingly, the "function field case" appears to be more difficult. For a prime $p$, let $M_p(d)$ denote the cost (still in the Turing model) of multiplying polynomials in $\mathbb{F}_p[x]$ of degree $d$. Then we have the following folklore conjecture.

**Conjecture 2.** *$M_p(d) = O(n \log n)$ where $n := d \log p$ (the total bit size).*

One case of this conjecture is easy: if $\log p \gg \log d$, then we may lift the problem to $\mathbb{Z}[x]$, pack the coefficients into huge integers (this technique is known as Kronecker substitution, see [GG13, Cor. 8.27]), and apply Theorem 1. However, in general the conjecture is wide open, even for $p = 2$. The current best unconditional bound is the following.

**Theorem 3** ([HvdH19])**.** *$M_p(d) = O(n \log n \, 4^{\log^* n})$ where $n := d \log p$.*

Here $\log^* x$ is the very slowly growing "iterated logarithm" function, defined by $\log^* x := \log^*(\log x) + 1$ for $x > 1$ and $\log^* x = 0$ for $x \leq 1$.

The best evidence we have towards Conjecture 2 is the following conditional result. For relatively prime positive integers $a$ and $k$, define $P(a, k)$ to be the least prime $p \equiv a \pmod{k}$, and set $P(k) := \max_a P(a, k)$. A real number $L > 1$ is a *Linnik constant* if $P(k) = O(k^L)$; the existence of a Linnik constant was first proved by Linnik (1944). The smallest Linnik constant currently known is $L = 5.18$ [Xyl11]. Under GRH any $L > 2$ is a Linnik constant [HB92], and it is widely believed that any $L > 1$ should be a Linnik constant (see for example [LPS17]).

**Theorem 4** ([HvdH22])**.** *If $L = 1 + 2^{-1162}$ is a Linnik constant, then Conjecture 2 is true.*

## 2. Lower bounds

The upper bound in Theorem 1 is expected to be sharp:

**Conjecture 5** ([SS71])**.** *$M(n) = \Omega(n \log n)$.*

Unfortunately, we are extremely ignorant on this question. Even a super-linear lower bound for $M(n)$ has not been established. Some partial results are known:

- An $\Omega(n \log n)$ lower bound is known [PFM74] for the problem of "online" multiplication, in which the $n$-th bit of the product must be generated before the $(n + 1)$-th bits of the multiplicands are read from the input.
- A conditional $\Omega(n \log n)$ lower bound has been proved [AFKL19] for the complexity of integer multiplication in the Boolean circuit model, assuming a certain "network coding conjecture". However, it is difficult to assess how likely this conjecture is to be true, or how hard it might be to prove (I am not an expert).

In the rest of this report I discuss a new result concerning lower bounds for multiplication (not yet published), due to Joris van der Hoeven and myself.

Let $T(d, b)$ denote the cost of transposing a $d \times d$ matrix with $b$-bit entries. In the Turing model, this means rearranging the data on the tape to convert from row-major order to column-major order.

There is a simple folklore algorithm that achieves $T(d, b) = O(bd^2 \log d)$. Namely, cut the matrix into four quadrants, recursively transpose each quadrant, and recombine to obtain the result. Note that $bd^2$ is the total bit size of the matrix, and $\log d$ is the number of recursion levels.

It is reasonable to guess that this upper bound is sharp, i.e., that

$$T(d, b) = \Omega(bd^2 \log d). \tag{1}$$

I am not aware of an official conjecture along these lines.

**Theorem 6** (H. and van der Hoeven, $2024+\epsilon$)**.** *If the lower bound* (1) *holds, then* $M(n) = \Omega(n \log n)$.

In other words, if matrix transposition is as difficult as expected on a Turing machine, then integer multiplication is as difficult as expected on a Turing machine.

We give a brief sketch of the proof. The idea is to reduce transposition to multiplication. Suppose we are given a $d \times d$ matrix of $b$-bit entries, where $b \sim \log d$, and we wish to compute its transpose.

(1) Viewing the matrix as a vector in $\mathbb{C}^{d^2}$, compute the DFT (discrete Fourier transform) of this vector, using Bluestein's trick [Blu70] to convert the DFT problem to a convolution problem over $\mathbb{C}$, and then using Kronecker substitution to reduce the convolution to a large integer multiplication problem.

(2) Compute the *inverse* DFT of the result, using a different algorithm. Namely, use the Cooley–Tukey method [CT65] to decompose the DFT of size $d^2$ into a collection of DFTs of size $d$ (along the rows and columns of the matrix), and then handle each of these DFTs using the same Bluestein–Kronecker combination as in step (1).

The result of this procedure is the original vector that we started with, but in transposed order. The reason that this method performs a transposition is the same reason that textbook FFT algorithms ("decimation-in-time" or "decimation-in-frequency") naturally compute the DFT in bit-reversed order.

## References


[AFKL19] P. Afshani, C. B. Freksen, L. Kamma, and K. G. Larsen, *Lower bounds for multiplication via network coding*, 46th International Colloquium on Automata, Languages, and Programming, LIPIcs. Leibniz Int. Proc. Inform., vol. 132, Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2019, pp. Art. No. 10, 12. MR 3984828

[Blu70] L. I. Bluestein, *A linear filtering approach to the computation of discrete Fourier transform*, IEEE Transactions on Audio and Electroacoustics **18** (1970), no. 4, 451–455.

[CT65] J. W. Cooley and J. W. Tukey, *An algorithm for the machine calculation of complex Fourier series*, Math. Comp. **19** (1965), 297–301. MR 0178586

[GG13] J. von zur Gathen and J. Gerhard, *Modern Computer Algebra*, 3rd ed., Cambridge University Press, Cambridge, 2013. MR 3087522

[HB92] D. R. Heath-Brown, *Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression*, Proc. London Math. Soc. (3) **64** (1992), no. 2, 265–338. MR 1143227 (93a:11075)

[HvdH19] D. Harvey and J. van der Hoeven, *Faster polynomial multiplication over finite fields using cyclotomic coefficient rings*, J. Complexity **54** (2019), 101404, 18. MR 3983215

[HvdH21] ———, *Integer multiplication in time* $O(n \log n)$, Ann. of Math. (2) **193** (2021), no. 2, 563–617. MR 4224716

[HvdH22] ———, *Polynomial multiplication over finite fields in time* $O(n \log n)$, J. ACM **69** (2022), no. 2, Art. 12, 40. MR 4433320

[LPS17] J. Li, K. Pratt, and G. Shakan, *A lower bound for the least prime in an arithmetic progression*, Q. J. Math. **68** (2017), no. 3, 729–758. MR 3698292

[Pap94] C. H. Papadimitriou, *Computational Complexity*, Addison-Wesley Publishing Company, Reading, MA, 1994. MR 1251285 (95f:68082)

[PFM74] M. S. Paterson, M. J. Fischer, and A. R. Meyer, *An improved overlap argument for on-line multiplication*, 97–111. SIAM–AMS Proc., Vol. VII. MR 0423875

[SS71] A. Schönhage and V. Strassen, *Schnelle Multiplikation grosser Zahlen*, Computing (Arch. Elektron. Rechnen) **7** (1971), 281–292. MR 0292344 (45 #1431)

[Xyl11] T. Xylouris, *On the least prime in an arithmetic progression and estimates for the zeros of Dirichlet L-functions*, Acta Arith. **150** (2011), no. 1, 65–91. MR 2825574 (2012m:11129)

## Zero cycles on a product of elliptic curves

Kartik Prasanna

(joint work with V. Srinivas)

We discuss some computational results (unpublished) obtained many years ago when the authors were visiting the IAS in 2014/15. For recent work on this problem, the reader may consult the work of Gazaki and Love ([1], [2]) which uses a different, more geometric, method and works in greater generality. But the method used below (involving Heegner points) may be of independent interest, and seems to work in at least a few cases, of which one is described here. The computations indicated below were all done in SAGE.

Let $X$ be a smooth projective surface over a number field $k$. Let $Z^2(X)$ denote the group of zero-cycles on $X$ defined over $k$. We write $Z^2(X)_0$ for the zero-cycles of degree 0 and $Z^2(X)_{\mathrm{rat}}$ for the subgroup of cycles that are rationally equivalent to zero. The Bloch-Beilinson conjecture predicts among other things that the group $\mathrm{CH}^2(X)_0 = Z^2(X)_0/Z^2(X)_{\mathrm{rat}}$ is finitely generated and has rank equal to the order of vanishing of the $L$-function $L(h^3(X)(2), s) = L(h^1(X)(1), s)$ at the point $s = 0$. Equivalently, the group $\mathrm{CH}^2(X) = Z^2(X)/Z^2(X)_{\mathrm{rat}}$ should have rank one more than this order of vanishing.

Consider the special case $X = E_1 \times E_2$ where $E_1$ and $E_2$ are elliptic curves over $\mathbf{Q}$ of ranks $r_1$ and $r_2$ respectively. Then the conjecture predicts that

$$\mathrm{rank}\ \mathrm{CH}^2(X) = r_1 + r_2 + 1.$$

Moreover, the map

$$Z^1(E_1) \otimes Z^1(E_2) \to Z^2(X), \quad P \otimes Q \mapsto (P, Q),$$

induces a map

$$\mathrm{CH}^1(E_1) \otimes \mathrm{CH}^1(E_2) \to \mathrm{CH}^2(X).$$

Now the rank of the group on the left is $(r_1+1)(r_2+1)$ which is strictly larger than $r_1+r_2+1$ as long as both $r_1$ and $r_2$ are strictly positive. Thus the Bloch-Beilinson conjecture predicts there should be (at least) $r_1 r_2$ relations (*rational equivalence on* $X$) between the zero cycles $(P, Q)$ as $P$ and $Q$ vary over an extended Mordell-Weil basis of $E$ and $E'$ respectively. (Here, "an extended Mordell-Weil basis" of an elliptic curve is the union of a Mordell-Weil basis and the zero element of the

elliptic curve.) One can predict what these relations are from another part of the Bloch-Beilinson conjectures, which states that the Abel-Jacobi map on $\mathrm{CH}^2(X)_0$ is injective mod torsion. We use the same symbol $O$ to denote the zero elements of $E_1$ and $E_2$. It is easy to see that the cycle

$$(P-O,Q-O)=(P,Q)-(P,O)-(O,Q)+(O,O)$$

is Abel-Jacobi trivial. Thus one expects that some multiple of this cycle is rationally equivalent to zero on $X$; these should provide $r_1r_2$ relations.

We will consider the simplest nontrivial case of this phenomenon, namely when $r_1=r_2=1$ and $E_1,E_2$ are non-isogenous. For simplicity we consider the case when $E_1$ and $E_2$ have the same conductor. The first case when this happens is $N=91$. There are exactly two elliptic curves of conductor 91. These are:

$$E_1=\text{“}91a\text{”}: \quad y^2+y=x^3+x,$$

and

$$E_2=\text{“}91b\text{”}: \quad y^2+y=x^3+x^2-7x+5.$$

These are affine models, the point at infinity $[0,1,0]$ being the origin. Both curves have rank one, with the Mordell-Weil groups being given by

$$\mathrm{MW}(E_1)=\mathbf{Z}\cdot P, \quad P=(0,0),$$

and

$$\mathrm{MW}(E_2)=\mathbf{Z}\cdot Q\oplus(\mathbf{Z}/3\mathbf{Z})\cdot R, \quad Q=(-1,3),\ R=(1,0).$$

The modular curve $X_0(N)$ has genus 7 and has a canonical model over $\mathbf{Q}$. The elliptic curves $E_1$ and $E_2$ admit canonical modular parametrizations:

$$\phi_1: X_0(N)\to E_1, \quad \phi_2: X_0(N)\to E_2$$

which satisfy

$$\deg(\phi_1)=\deg(\phi_2)=4.$$

The maps $\phi_1$ and $\phi_2$ are normalized such that

$$\phi_1(c_\infty)=O, \quad \phi_2(c_\infty)=O,$$

where $c_\infty$ is the cusp at $\infty$. Let us denote the factors of $N$ by $p$ (=7) and $q$ (= 13).

The Atkin-Lehner group $W=\{1,w_p,w_q,w_{pq}\}$ acts on $X_0(N)$. Let $f$ and $g$ denote the modular forms associated to $E_1$ and $E_2$ respectively and $\omega_f$, $\omega_g$ the corresponding differential forms on $X_0(N)$. Then $w_p$ and $w_q$ both fix $f$, and send $g$ to $-g$. Thus the operator $w_{pq}$ fixes both $f$ and $g$. On the other hand, this operator acts on the orthogonal complement to the span of $f$ and $g$ in $S_2(\Gamma_0(N))$ as $-1$. Hence the map

$$X_0(N)\to E_1\times E_2$$

factors as

$$X_0(N)\xrightarrow{\psi} C\xrightarrow{\mu} E_1\times E_2=X,$$

where $C=X_0(N)/w_{pq}$. Here $C$ is nonsingular, is defined over $\mathbf{Q}$ and has genus 2 since $H^0(C,\Omega^1)=\mathbf{Q}\omega_f\oplus\mathbf{Q}\omega_g$. Let $\mu_1$ and $\mu_2$ denote the two projection maps from $C$ to $E_1$ and $E_2$ respectively. Then $\deg(\psi)=\deg(\mu_1)=\deg(\mu_2)=2$ and the map $\mu: C\to\mu(C)$ is a birational equivalence.

The idea now is to construct a function $F$ on $C$ whose divisor will give a rational equivalence on $X$. The curve $C$, being genus 2, is hyperelliptic and admits a degree-2 map $\theta$ to $\mathbf{P}^1$, which corresponds to the linear system $\mathcal{L}(K)$ where $K$ is the canonical divisor. Thus explicitly, such a map may be constructed by sending $x \mapsto [\omega_f(x), \omega_g(x)]$. Let $t$ denote the coordinate on $\mathbf{P}^1$; then for any $\lambda_1 \neq \lambda_2 \in \mathbf{P}^1$, the function

$$F_{\lambda_1,\lambda_2} := \theta^* \left( \frac{t-\lambda_1}{t-\lambda_2} \right) = \left( \frac{t-\lambda_1}{t-\lambda_2} \right) \circ \theta$$

is a rational function on $C$ and is a natural candidate to look at since its divisor is a linear combination of four points on $C$. If we further choose $\lambda_1, \lambda_2 \in \mathbf{P}^1_{\mathbf{Q}}$, then the zero cycle $(F_{\lambda_1,\lambda_2})$ on $C$ will be defined over $\mathbf{Q}$. Note that

$$\psi^*(F_{\lambda_1,\lambda_2}) = \frac{f(\tau) - \lambda_1 g(\tau)}{f(\tau) - \lambda_2 g(\tau)}, \tag{1}$$

viewed as a function on $\Gamma_0(N)\backslash\mathfrak{h}$, where $\mathfrak{h}$ denotes the complex upper half plane.

In choosing $\lambda_1$ and $\lambda_2$, it is natural to use the theory of Heegner points. First, we pick an imaginary quadratic field $K$ that satisfies the Heegner hypothesis for $N$; this means that $K$ must be split at both $p$ and $q$. The simplest choice is $K = \mathbf{Q}(\sqrt{-3})$. This field has class number equal to one, so the corresponding Heegner points on $X_0(N)$ are defined over $K$. There are four of these Heegner points on $X_0(N)$ that are permuted by the action of the Atkin-Lehner group. The operator $w_{pq}$ identifies two pairs, so that on the curve $C$ one gets two "Heegner points" that are permuted by the action of $W/ < w_{pq} >$.

We will pick one of these points; call it $x \in C(K)$. We can take for $x$ the image of the point $\tau_1 \in \mathfrak{h}$ under the composition $\mathfrak{h} \to \Gamma_0(N)\backslash\mathfrak{h} = Y_0(N) \to C$,

$$\tau_1 := \frac{1}{182}\sqrt{-3} - \frac{19}{182}.$$

Computationally, we find that:

$$\mu_1(x) = (3, -6) = \ominus 3P, \quad \mu_2(x) = (5/4, -5/8) = Q \oplus R.$$

Here we use $\oplus$ and $\ominus$ to denote addition and subtraction in the group law. Since $\mu_1(x)$ and $\mu_2(x)$ are both $\mathbf{Q}$-rational points, we find that $x$ lies in $C(\mathbf{Q})$. (One can also deduce this in this case from the theory of Heegner points.)

Next we evaluate $f/g$ at $\tau_1$. We find that $f$ and $g$ both vanish to order two at $\tau_1$ and $(f/g)(\tau_1) = 1/3$. Thus it is natural to take $\lambda_1 = 1/3$. There is one more point $y \in C(\mathbf{Q})$ for which $(f/g)(y) = 1/3$. We find experimentally that this is the image of the point $\tau_2 \in \mathfrak{h}$ where

$$\tau_2 := 0.07339952702407614276263 2... + i \cdot 0.07484330579051746448107 8...$$

*Remark:* The point $\tau_2$ was computed as follows. We need to find a zero of $\frac{f(\tau)}{g(\tau)} - \frac{1}{3}$ on the upper half plane. For this we use Newton's method after making an initial guess. Note that $\tau_2$ is unrelated to the other Heegner point since $(f/g)$ takes the value $-1/3$ at that Heegner point, the $w_p$ eigenvalue of $f/g$ being $-1$.

Computationally, we find that

$$\mu_1(y) = (33/4, -195/8) = \oplus 5P, \quad \mu_2(y) = (3, -5) = \ominus Q \oplus R.$$

For $\lambda_2$, one natural choice is $\lambda_2 = 1$ since $(f/g)[c_\infty] = 1$. Thus $f/g$ takes the value 1 at the cusp at infinity and at one more point, which we find computationally to be the image of

$$\tau_3 := 0.120879120879120879424 48.... + i \cdot 0.00634450845263325023023 24....$$

Let $z$ denote the image of $\tau_3$ in $C$; it is a point in $C(\mathbf{Q})$. Computationally, we find:

$$\mu_1(z) = (1, -2) = \oplus 2P, \quad \mu_2(z) = (1, -1) = \oplus 2R.$$

Finally, let $u$ denote the cusp $[c_\infty]$ in $C(\mathbf{Q})$. Then the divisor of $F_{1/3,1}$ on $C$ (pushed forward to $E_1 \times E_2$) is given by

$$(F_{1/3,1}) = (\ominus 3P, Q \oplus R) + (\oplus 5P, \ominus Q \oplus R) - (\oplus 2P, \oplus 2R) - (O, O).$$

Since $\oplus 3R \sim_{E_2} O$ ($\sim_{E_2}$ denotes rational equivalence on $E_2$) and $\oplus nS \sim_E nS - (n-1)O$ on $E_1$ and likewise on $E_2$, we find that

$$\begin{aligned} 3(F_{1/3,1}) &\sim_X 3\left[(\ominus 3P, Q) + (\oplus 5P, \ominus Q) - (\oplus 2P, O) - (O, O)\right] \\ &\sim_X 3\left[(4O - 3P, Q) + (5P - 4O, 2O - Q) - (2P - O, O) - (O, O)\right] \\ &= -24\left[(P, Q) - (P, O) - (O, Q) + (O, O)\right]. \end{aligned}$$

Thus

$$24\left[(P, Q) - (P, O) - (O, Q) + (O, O)\right]$$

is rationally equivalent to zero on $X$.

## References


[1] E. Gazaki & J. Love. *Torsion phenomena for zero-cycles on a product of curves over a number field,Res. Num. Thy* **10**, 35(2024). https://doi.org/10.1007/s40993-024-00519-4

[2] E. Gazaki & J. Love. *Hyperelliptic curves mapping to abelian varieties and Applications to Beilinson's Conjecture for zero-cycles*, https://arxiv.org/abs/2309.06361


## 100 % of odd hyperelliptic Jacobians have no rational points of small height


Jef Laga

(joint work with Jack Thorne)


Let $g \geq 1$ be an integer and consider the family of polynomials

$$\mathcal{F} = \{f(x) = x^{2g+1} + c_2 x^{2g-1} + \cdots + c_{2g+1} \in \mathbb{Z}[x] \colon \operatorname{disc}(f) \neq 0\}.$$

For each $f(x) \in \mathcal{F}$, let $C_f$ be the smooth projective curve with affine equation $y^2 = f(x)$; this is a hyperelliptic curve of genus $g$ with a unique point $P_\infty \in C(\mathbb{Q})$ at infinity. Let $J_f$ be the Jacobian variety of $C_f$, a $g$-dimensional abelian variety. In this work, we are interested in the statistical behaviour of $C_f(\mathbb{Q})$ and $J_f(\mathbb{Q})$ when $f$ varies over $\mathcal{F}$ and ordered by the height $\operatorname{ht}(f) = \max |c_i|^{1/i}$.

Bhargava–Gross [1] have shown that the average Mordell–Weil rank of $J_f$ is at most 3/2, by computing the average size of the 2-Selmer group of $J_f$. Poonen and Stoll [6] used this to show that a positive proportion of $f$ satisfy $C_f(\mathbb{Q}) = \{P_\infty\}$,

and that this proportion tends to 100% as $g \to +\infty$. Moreover, Poonen and Rains [5] developed a remarkable set of heuristics modelling all the Selmer groups of $J_f$, suggesting that 50% of $J_f$ should have rank zero and 50% should have rank one, generalizing the $g = 1$ case.

The work I presented at the workshop tries to answer the following question: how complicated will the points of $J_f(\mathbb{Q})$ or $C_f(\mathbb{Q})$ typically be?

To formalize this, we first need to define a height on $J_f(\mathbb{Q})$. Say an effective divisor $D = P_1 + \cdots + P_m$ on $C_f$ is *reduced* if $m \leq g$, $P_i \neq P_\infty$ and $P_i$ is not conjugate to $P_j$ under the hyperelliptic involution for all $i \neq j$. Then every nonzero element of $J_f(\mathbb{Q})$ is of the form $[D - mP_\infty]$ for some unique reduced divisor $D$. We then define the naive height of such an element to be

$$h^\dagger([D - mP_\infty]) = h(x(P_1)) + \cdots + h(x(P_m)),$$

where $x(P_i) \in \bar{\mathbb{Q}}$ denotes the $x$-coordinate of $P_i$ and $h(\alpha)$ denotes the logarithmic (normalized) Weil height of $\alpha \in \bar{\mathbb{Q}}$. If $g = 1$, we recover (up to a factor of 2) the usual naive height of points on elliptic curves.

Our result [4] states that, typically, if $f(x)$ has large height, then nonzero elements in $J_f(\mathbb{Q})$ must also have large height, in the following sense:

**Theorem 1.** *Let $\varepsilon > 0$ be arbitrary. Then for 100% of $f \in \mathcal{F}$, every nonzero $P \in J_f(\mathbb{Q})$ satisfies*

$$h^\dagger(P) \geq (2g - 1 - \varepsilon)\log(\mathrm{ht}(f)).$$

The proof method uses an auxiliary object, namely the representation of the split orthogonal group $G = \mathrm{SO}_{2g+1}$ acting on the space $V$ of trace-zero self-adjoint $(2g+1) \times (2g+1)$ matrices. The rational and integral orbits of $G$ on $V$ are used in the study of 2-descent on $J_f$, and Bhargava and Gross counted such orbits (with appropriate conditions) in their study of the 2-Selmer group of $J_f$. The proof of Theorem 1 follows from relating the reduction theory of the representation $(G, V)$ to the arithmetic of points in $J_f(\mathbb{Q})$.

In slightly more detail, we assign to every element $T \in V(\mathbb{Z})$ of nonzero discriminant an inner product $H_T$ on $\mathbb{R}^{2g+1}$ satisfying some additional conditions. We call this inner product the 'reduction covariant' associated to $T$, since it is analogous to the reduction covariant employed in descent algorithms on elliptic curves [2] and the Julia covariant used in reducing binary forms [3].

We show that if $J_f(\mathbb{Q})$ admits a point of "small" height in a certain sense, there exists a matrix $T \in V(\mathbb{Z})$ with characteristic polynomial $f$ and a vector $v \in \mathbb{Z}^{2g+1}$ with "small" $H_T$-norm. On the other hand, we show that the assignment $T \mapsto H_T$ equidistributes over irreducible integral orbits, where the target is the moduli space of lattices with additional structure, implying that there cannot be too many $T$ for which $H_T$ has a small integral vector. It is this tension that underlies the proof of Theorem 1.

## References

[1] Bhargava, Manjul and Gross, Benedict H., *The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point*, Automorphic representations and L-functions, 23–91, Tata Inst. Fundam. Res. Stud. Math., 22, Tata Inst. Fund. Res., Mumbai, 2013.

[2] Cremona, John E. and Fisher, Tom A. and Stoll, Michael, *Minimisation and reduction of 2-, 3- and 4-coverings of elliptic curves*, Algebra Number Theory 4 (2010), no. 6, 763–820.

[3] Cremona, John E. and Stoll, Michael, *On the reduction theory of binary forms* J. Reine Angew. Math. 565 (2003), 79–99.

[4] Laga, Jef and Thorne, Jack, 100% *of odd hyperelliptic Jacobians have no rational points of small height*, Arxiv preprint, available at `https://arxiv.org/abs/2405.10224`.

[5] Poonen, Bjorn and Rains, Eric, *Random maximal isotropic subspaces and Selmer groups*, J. Amer. Math. Soc. 25 (2012), no. 1, 245–269.

[6] Poonen, Bjorn and Stoll, Michael, *Most odd degree hyperelliptic curves have only one rational point*, Ann. of Math. (2) 180 (2014), no. 3, 113–1166.


## Heegner Points on Twists of Elliptic Curves


Henri Cohen

(joint work with Bill Allombert)


### 1. The Classical Heegner Point Method

The classical theory of Heegner points was extensively developed both in theory and in practical implementations by Heegner, Birch, Gross, Zagier, Cremona, Stephens, Delaunay, Watkins, Silverman, Darmon, Allombert, and many others. Probably most efficient implementation is due to B. Allombert in `Pari/GP`, and it allows the practical computation of a nontrivial rational point on an elliptic curve (over $\mathbb{Q}$) of *rank 1* with reasonably small conductor.

Rough sketch: let $E/\mathbb{Q}$ be an elliptic curve of rank 1, of conductor $N$, let $f(\tau) = \sum_{n\geq 1} a(n)q^n$ be the corresponding modular form of weight 2 on $\mathbb{G}amma_0(N)$, let $F(\tau) = \sum_{n\geq 1} a(n)q^n/n$ be its antiderivative vanishing at $\infty$. Up to factors 2, $E$ is parametrized by $(x, y) = (\wp(F(\tau)), \wp'(F(\tau)))$ with $\wp$ the Weierstrass P function (proof: $(x, y)$ satisfies the Weierstrass equation for $E$ by definition of $\wp$, and $dx/y = F'(\tau)d\tau = f(\tau)d\tau$).

By CM theory, if $\tau \in \mathcal{H}$ is a *CM point* of discriminant $D < 0$ (i.e., $A\tau^2 + B\tau + C = 0$ with $A > 0$, $\gcd(A, B, C) = 1$, and $B^2 - 4AC = D$) then $\wp(F(\tau))$ is an *algebraic number* with *known conjugates* by Shimura reciprocity.

The natural idea is to sum over all conjugates, either directly on he elliptic curve, or better, the values of $F(\tau) \in \mathbb{C}$ and then send to $E$ using $\wp$. Under suitable assumptions, this will give a nontrivial point in $E(\mathbb{Q}(\sqrt{D}))$, and this point will be either in $E(\mathbb{Q})$ or in the twist $E^{(D)}(\mathbb{Q})$, and it will be in $E(\mathbb{Q})$ because root number $\varepsilon = -1$.

The *defining assumption* of Heegner points: the discriminant of $N\tau$ must be equal to that of $\tau$. This implies $N \mid A$, hence $D = B^2 - 4AC$ must be a square modulo $4N$. Usually but not always, we require $\gcd(D, N) = 1$.

We thus need to compute (essentially $h(D)$) sums of the form

$$\sum_{n\geq 1} \frac{a(n)}{n} \exp\left(2\pi i \frac{-B+\sqrt{D}}{2A}\right)$$

Since $N \mid A$, this is *very slow* when $N > 10^8$, say. For instance, in the special case of the congruent number curves $y^2 = x^3 - n^2x$, the conductor $N$ is proportional to $n^2$, so the method is impractical if $n > 10^4$.

Best timings, using Allombert's `ellheegner` for $N = 157$ (0.4s), $N = 1013$ (40s), for $N = 958957$ (hundreds of years ?).

## 2. The Monsky Surprise

In 1990, Paul Monsky published a paper [1] on congruent numbers, giving first a new algorithm (specific to congruent numbers), and second proving that certain primes and almost primes are congruent. This paper is well-known and often cited, but its *practical* efficiency was apparently forgotten.

History: in 1996, PhD of A. Robatino [3], a student of G. Stevens, who implements in `Pari/GP` Monsky's algorithm (together with algorithms for *quartic* twists, with $n^2$ replaced by $N$), noting its amazing speed (note: an important algorithm already using Pari/GP in 1996!). Recently, R. Rathbun (who has apparently been using Robatino's script for some time) sent us the script translated into 2024 `GP` format. He had already used it to find generators for all congruent numbers up to $10^6$, now in the LMFDB.

The algorithm's speed is not so easy to estimate, but very roughly for a given height of the point, it takes time proportional to $n$ (possibly $n^{1+\alpha}$ for a small $\alpha$) instead of $n^2$ for classical Heegner.

Many improvements added by our group (only by a large constant factor). For instance for the three above examples: $N = 157$ (0.01s), $N = 1013$ (0.04s), $N = 958957$ (22s); note a slight cheat because the new method uses parallelism, a feature of `Pari/GP` due to Bill, without it multiply the times by 4 or 5.

Monsky achieves this by working directly on the curves $E$: $y^2 = x^3 - x$ (for odd $n$) and $y^2 = x^3 - 4x$ (for even $n$), using an explicit modular parametrization using *Weber functions*, and *NOT* on their quadratic twists such as $y^2 = x^3 - n^2x$. He also uses an auxiliary discriminant $D$, which is now *fixed*: $D = -4n$ for $n$ odd and $D = -8n$ for $n$ even.

Using the image by this parametrization of a CM point of discriminant $D$ he obtains a point on the *ring class field* of discriminant $D$. This class field contains $K = \mathbb{Q}(\sqrt{\pm n})$, and as in standard Heegner he computes a (twisted) elliptic trace $(x, y) \in E(K)$. Trivially $(X, Y) = (nx, n^{3/2}y) \in E_n(\mathbb{Q}(\sqrt{n}))$ (with $E_n$: $Y^2 = X^3 - n^2X$), and the initial choices ensures that in fact $(X, Y) \in E_n(\mathbb{Q})$.

The resulting point *may* be torsion, apparently never in practice when $E_n$ has rank 1 (if it was, one could choose slightly different $D$). There exist partial results of Gross–Zagier type for this construction.

The main advantage of this method is that there is no need for complicated *modular parametrization* of $y^2 = x^3 - n^2x$, instead we use the *trivial* ones of

$y^2 = x^3 - x$ or $y^2 = x^3 - 4x$, for instance using Weber functions, so no need to compute millions of terms of series of the type $\sum_{n\geq 1}(a(n)/n)q^n$.

The important fact concerning this method is the fact that one works directly on a *very small* elliptic curve such as $y^2 = x^3 - x$ (instead of the very large $y^2 = x^3 - n^2x$). The specific modular parametrization used is *not* important, but Weber functions have added benefit of being *very fast* to compute.

For definiteness, here is one parametrization (there exist at least 4 more interesting ones). The three Weber functions are:

$$f(\tau) = e^{-i\pi/24}\frac{\eta((\tau+1)/2)}{\eta(\tau)}\,, f_1(\tau) = \frac{\eta(\tau/2)}{\eta(\tau)}\,, f_2(\tau) = \sqrt{2}\frac{\eta(2\tau)}{\eta(\tau)}$$

The parametrization used by Robatino is:

$$X = \frac{f_1^6}{\sqrt{8}}\,, \quad Y = \frac{f_1^{12}(f^{24} + f_2^{24})}{8\sqrt{2}(f_1^{24} + 16)}\,,$$

$$x = \frac{1 + X^2 + 2Y}{(X-1)^2}\,, \quad y = \frac{2(1+X)(1-X+X^2+Y)}{(X-1)^3}\,,$$

$$\text{then} \qquad 2Y^2 = X^4 + 1 \quad \text{and} \quad y^2 = x^3 - x\,.$$

Note that it is even faster to work directly on $2Y^2 = X^4 + 1$.

Note that the classical Heegner method is essentially due to B. Birch, while Monsky's method is closer to Heegner's original papers.

In a second paper [2], Monsky also considers *quartic twists*, i.e. finding points on the more general curve $y^2 = x^3 - Nx$ with $N$ not necessarily square nor positive, but with congruence restrictions. Also impressively fast, but less so than when $N = n^2$.

Finally, note that N. Elkies, and later J. Voight et al. have used similar techniques for *cubic twists* of $y^2 = x^3 + 1$.

## 3. Generalizing Monsky

There is no reason to restrict to quadratic twists of the specific curve $y^2 = x^3 - x$. The advantage of that curve (because it has CM) is that there exist very simple parametrizations as above. But any curve with reasonably small conductor (CM or not) can be explicitly parametrized with little difficulty. Even if not, computing the antiderivative $F(\tau) = \sum_{n\geq 1}(a(n)/n)q^n$ is very fast if the conductor is small and $\tau$ not too close to the real axis.

Thus our goal is to generalize Monsky: given *any elliptic curve* $E$ over $\mathbb{Q}$ (of any rank) and an integer $d$ such that the *quadratic twist* $E_d$ of $E$ by $d$ has *rank 1*, compute explicitly a nontrivial rational point on $E_d$ by working only on the initial curve $E$, assumed to be simpler.

The main work has been done by B. Allombert, and the gain is similar to Monsky, several orders of magnitude faster. Assume $d$ squarefree (not a restriction) coprime to $N$ (for general case see below). As in classical Heegner, we find a negative fundamental discriminant $D$ such that $d \mid D$ and $D$ is a square modulo

$4N$, and work on the twist by $D$ (which may be of rank 0). Find classical Heegner points for the curve $E$ (not its twist, this is the main point) corresponding to $D$, their image in the Hilbert class field $H_D$ of $K = \mathbb{Q}(\sqrt{D})$. Since $H_D$ contains $\mathbb{Q}(\sqrt{d})$, trace down not to $E(K)$ (would give trivial point if twist by $D$ of rank 0) but to $E(\mathbb{Q}(\sqrt{d})) \simeq E_d(\mathbb{Q}(\sqrt{d}))$, and only now descend to $E_d(\mathbb{Q})$.

Explicit example: $E = 37a1$ ($N = 37$), $d = 197$. We choose $D = -3d = -591$, which works. The Hilbert class field is of degree 22 over $\mathbb{Q}(\sqrt{-591})$ (so absolute degree 44) but contains also $\mathbb{Q}(\sqrt{197})$. We compute the 22 Heegner points $\tau = (-B + \sqrt{D})/(2A)$ of level 37 and discriminant $D$: note that for $A = N$ we have $\Im(\tau) = \sqrt{|D|}/(2A) \approx 0.32\cdots$, so is *large* (which is excellent!), while the conductor of $E_{197}$ is the *huge* $37 \cdot 197^2$ which would need to divide all the $A$'s occuring as denominator of $\tau$ if we worked directly on $E_{197}$. We trace down to $E(\mathbb{Q}(\sqrt{197}))$ and then to $E_{197}(\mathbb{Q})$ as above (we find a point with about 230 decimal digits numerator and denominator of the $x$-coordinate).

If $d$ is *not* coprime to the conductor $N$, crucial idea of Allombert is to use a modified version of Heegner points, i.e., use $\tau$ such that the discriminant of $\tau$ equals that of $Q\tau$ for some $Q \| N$ coprime to $D$ (including $Q = 1$!) such that $N/Q \mid \gcd(d, N)$ (classical Heegner being $Q = N$).

Example timings:

| Curve | ellheegner | Monsky/Bill |
|---|---|---|
| $11a1$ twisted by $-195$ | 1.63s | 0.07s |
| $11a1$ twisted by $-491$ | 15.3s | 0.09s |
| $11a1$ twisted by $-1999$ | 178.s | 0.64s |
| $37a1$ twisted by 197 | 6.4s | 0.21s |
| $37a1$ twisted by 509 | 59s | 0.17s |
| $37a1$ twisted by $-772$ | 98s | 3.6s |
| $389a1$ twisted by 301 | 51s | 1.27s |

## References


[1] P. Monsky, *Mock Heegner Points and Congruent Numbers*, Math. Z. **204** (1990), 45–68.

[2] P. Monsky, *Three constructions of rational points on* $Y^2 = X^3 \pm NX$, Math. Z.**209** (1992), 445–462.

[3] A. Robatino, *Computation of mock Heegner points on modular elliptic curves*, PhD Dissertation, Boston U. (1996).

[4] The PARI Group, PARI/GP version `2.16.2`, Univ. Bordeaux, 2024, http://pari.math.u-bordeaux.fr/.


## Integers expressible as the sum of two rational cubes


Manjul Bhargava

(joint work with Levent Alpöge, Ari Shnidman)


We prove that a positive proportion of integers are expressible as the sum of two rational cubes, and a positive proportion are not so expressible, thus proving a conjecture of Davenport. More generally, we prove that a positive proportion (in

fact, at least one sixth) of elliptic curves in any cubic twist family have rank 0, and a positive proportion (in fact, at least one sixth) of elliptic curves with good reduction at 2 in any cubic twist family have rank 1.

Our method involves proving that the average size of the 2-Selmer group of elliptic curves in any cubic twist family, having any given root number, is 3. We accomplish this by generalizing a parametrization, due to Bhargava and Ho [3], of elliptic curves with extra structure by pairs of binary cubic forms. We then count integer points satisfying suitable congruences on a quadric hypersurface in the space of real pairs of binary cubic forms in a fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$, using a novel combination of geometry-of-numbers methods and the circle method that builds on earlier work of Ruth [5] and Alpöge [1]. In particular, we make use of a new interpretation of the singular integral and singular series arising in the circle method in terms of real and $p$-adic Haar measures on the relevant group $\mathrm{SL}_2 \times \mathrm{SL}_2$. We prove a new uniformity estimate for integral points on such a quadric, which along with a sieve allows us to prove that the average size of the 2-Selmer group over the full cubic twist family is 3. By suitably partitioning the subset of curves in the family with given root number, we carry out a further sieve to show that the root number is equidistributed and that the same average, now taken over only those curves of given root number, is again 3. Finally, we apply the $p$-parity theorem of Dokchitser and Dokchitser[4] and a new $p$-converse theorem, proven by Burungale and Skinner in the Appendix of [2], to conclude.

We also prove the analogue of the above results for the sequence of square numbers: namely, we prove that a positive proportion of square integers are expressible as the sum of two rational cubes, and a positive proportion are not so expressible.

## References


[1] L. H. A. Alpöge, *Points on Curves,* Princeton University Ph.D. thesis (2020).

[2] L. Alpöge and M. Bhargava and A. Shnidman, *Integers expressible as the sum of two rational cubes*, arXiv: 2210.10730, (2022).

[3] M. Bhargava and W. Ho, *Coregular spaces and genus one curves,* Camb. J. Math., **4**(1) (2016), 1–119.

[4] T. Dokchitser and V. Dokchitser, *Regulator constants and the parity conjecture,* Invent. Math., **178**(1) (2009), 23–71.

[5] S. Ruth, *A bound on the average rank of j-invariant 0 elliptic curves,* Princeton University Ph.D. thesis, (2013).


## Sums of rational cubes and the 3-Selmer group


Alexander Smith

(joint work with Peter Koymans)


We are interested in the following question:

**Question 1.** *What proportion of the positive integers can be expressed as the sum of two rational cubes?*

In other words, as $d$ varies among the positive integers, how often does the affine curve with equation $x^3 + y^3 = d$ have a rational point?

The projective curve associated with this equation is the elliptic curve with Weierstrass form $E^d : y^2 = x^3 - 432d^2$. With finitely many exceptions among cubefree integers $d$, $E^d$ has positive rank if and only if $d$ is the sum of two rational cubes. The global root number of $E^d$ is $+1$ for 50% of $d$ and $-1$ for 50% of $d$, so we have the following:

**Proposition 2.** *Assume that the Birch and Swinnerton–Dyer conjecture holds. Then at least* 50% *of positive integers are the sum of two rational cubes.*

In analogy with Goldfeld's conjecture for quadratic twist families [2], one might predict that exactly 50% of positive integers are the sum of two rational cubes.

As reported in the previous abstract, Alpöge, Bhargava, and Shnidman have recently made progress towards this conjecture by studying the 2-Selmer groups in cubic twist families of elliptic curves [1]. We make progress instead by studying the 3-Selmer groups, but we run into a problem noted in [1].

**Proposition 3.** *For any $r > 0$, the 3-Selmer rank of $E^d$ is greater than $r$ for* 100% *of positive integers $d$.*

But note that $E^d$ has CM by the ring $\mathbb{Z}[\sqrt{-3}]$, and $\sqrt{-3}$ defines a 3-isogeny from $E^d$ to the curve $E_0^d : y^2 = x^3 + 16x$. Take

$$r_3(E_0^d) = -1 + \dim_{\mathbb{F}_3} \mathrm{Sel}^3 E_0^d;$$

$E_0^d$ has a nontrivial rational 3-torsion point, so this is an upper bound on the rank of $E_0^d$, and hence of $E^d$.

**Theorem 4** ([3])**.** *Among the curves $E_0^d$ of global root number $+1$,* 63% *have* 3*-Selmer rank* 0*. Furthermore, among the curves $E_0^d$ of global root number $-1$, at least* 95.8% *have* 3*-Selmer rank* 1*.*

To prove this theorem, we consider the exact sequence

$$0 \to \mathrm{Sel}^{\sqrt{-3}} E_0^d \to \mathrm{Sel}^3 E_0^d \to \mathrm{Sel}^{\sqrt{-3}} E^d$$

For 100% of $d$, the group $\mathrm{Sel}^{\sqrt{-3}} E_0^d$ is trivial. Furthermore, the image of the final map in this sequence equals the kernel of the Cassels–Tate pairing

$$\mathrm{CTP}_{E^d} : \mathrm{Sel}^{\sqrt{-3}} E^d \times \mathrm{Sel}^{\sqrt{-3}} E^d \to \tfrac{1}{3}\mathbb{Z}/\mathbb{Z}.$$

To prove the result, we need to show that the pairings $\mathrm{CTP}_{E^d}$ behave approximately like uniformly selected random alternating pairings.

This is similar to the approach to proving distributional results for Selmer groups appearing in [4, 5]. However, the distributional results of those papers are built on delicate combinatorial arguments that cannot handle the large Selmer groups $\mathrm{Sel}^{\sqrt{-3}} E^d$.

To prove Theorem 1, Koymans and I replaced the bilinear character sum estimates at the heart of [4, 5] with a trilinear character sum estimate. A simple form of this estimate takes the following form:

**Theorem 5** ([3]). *Given integers $d_1, d_2, d_3$, take $[d_1,\ d_2,\ d_3] \in \{-1, 0, 1\}$ to be the Rédei symbol, as defined in* [3, Example 2.5]. *Choose three functions*

$$a_{12}, a_{13}, a_{23} : \mathbb{Z} \times \mathbb{Z} \to \mathbb{C}$$

*of magnitude at most* 1. *Then, given real numbers $H_1, H_2, H_3 \geq 3$, we have*

$$\left| \sum_{|d_1|<H_1} \sum_{|d_2|<H_2} \sum_{|d_3|<H_3} a_{12}(d_1, d_2) \cdot a_{13}(d_1, d_3) \cdot a_{23}(d_2, d_3) \cdot [d_1,\ d_2,\ d_3] \right| \ll H_1 H_2 H_3 \cdot \log(H_1 H_2 H_3)^{1792} \cdot \left( H_1^{-1/512} + H_2^{-1/512} + H_3^{-1/512} \right)$$

*with the implicit constant absolute.*

The flexibility of the general form of this result allows us to bypass the combinatorial steps of [4, 5], allowing us to prove Theorem 1.

## References


[1] L. Alpöge, M. Bhargava and A. Shnidman, *Integers expressible as the sum of two rational cubes*, with an appendix by Ashay Burungale and Christopher Skinner (2022). arXiv:2210.10730.

[2] D. Goldfeld, "Conjectures on elliptic curves over quadratic fields", *Number Theory Carbondale 1979*. Springer (1979), 108–118.

[3] P. Koymans and A. Smith, *Sums of rational cubes and the* 3*-Selmer group*, (2024). arXiv:2405.09311

[4] A. Smith, *The distribution of $\ell^\infty$-Selmer groups in degree $\ell$ twist families I* (2022). arXiv:2207.05674.

[5] A. Smith, *The distribution of $\ell^\infty$-Selmer groups in degree $\ell$ twist families II* (2022). arXiv:2207.05143.


## Enumerating exceptional 2-dimensional Artin representations by conductor


Bill Allombert

(joint work with Aurel Page)


### 1. Summary

The purpose of this talk is to show how computational class field theory can be applied to the construction of low-dimensional Artin representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ given the conductor. For technical reasons, we will assume the GRH for Dedekind zeta functions.

## 2. Motivation

Around 2016, Henri Cohen and Karim Belabas wrote the PARI/GP[1] package *mfinit*[2] for computing spaces of modular forms for $\Gamma_0(N)$, given a level $N$, a weight and a character, using the trace formula method and Miyake's criterion for CM forms.

In the weight-1 case, according to Deligne-Serre's theorem, modular forms are associated to Artin $L$-function of 2-dimensional odd Galois representations, the converse being true due to Langlands-Tunnell and Khare-Wintenberger[4].

A natural question is how to compute efficiently such Galois representations in the exceptional case.

The trick is to use Brauer's theorem which allows to write the Artin $L$-function as a quotient of two Hecke-$L$ functions in a very efficient way, which is much faster than computing the modular form coefficients using *mfinit*. So we worked on a way to compute the Galois representations without the knowledge of the modular forms.

Using the trace formula method, the implementation of Kieran Child [3] reached level 10000 using a cluster. Our method can handle much larger levels.

## 3. Computing the projective representation

The first step is to compute the number field cut by the projective representation of the Galois group.

There are known algorithms using computational class field theory to build all fields of Galois group $A_4$ or $S_4$ of a given discriminant, by using towers of Abelian extensions. Aurel Page modified them to build all fields leading to a representation of a given conductor. These algorithms are subexponential in the logarithm of the conductor.

3.1. **The $A_5$ case.** For the case $A_5$ a full table of all number fields with Galois group $A_5$ with conductor less than $10^6$ has been computed by the authors, by using a targeted Hunter search and using the *ratpoints*[5] program to find the values of the last coefficient that makes the discriminant a square. This required about 300 core×months.

For this computation we worked with Michael Stoll to improve ratpoints to take advantage of the new SIMD capabilities (AVX256) in modern CPUs.

## 4. Lifting to $\mathrm{GL}_2$

The second step is to lift the projective representation to the twist-minimal linear representation. This is a cyclic extension of the field, so it can also be expressed in terms of class field theory.

Using Brauer's theorem, we write the 2-dimensional representation as a difference of representations induced by 1-dimensional characters, which can be identified as Hecke characters.

For $A_4$ and $S_4$ they are attached to extensions of $\mathbb{Q}$ of degree 6 and 4, for $A_5$ of degree 12 and 10.

## 5. Algebraic Maass forms and higher-dimensional representations

The exact same technique works in principle for algebraic Maass forms with the caveat that we cannot prove that the resulting $L$-function is holomorphic and that they are attached to an actual Maass form.

It is in principle possible to use the same technique for higher dimensional representations as long as the projective image is solvable, with the same caveat. For example in dimension 3, we can handle the projective groups $6T10 = F_{36}(6) = (C_3 \times C_3) \rtimes C_4$ and $9T14$.

## References


[1] The PARI Group, Univ. Bordeaux. *PARI/GP version 2.16.2*, 2024. available from `http://pari.math.u-bordeaux.fr/`.

[2] Karim Belabas and Henri Cohen. Modular forms in PARI/GP, 2018. arXiv 1810.00547 (`https://arxiv.org/abs/1810.00547`).

[3] Kieran Child. Computation of weight 1 modular forms with exotic representations, 2022. arXiv 2201.08873 (`https://arxiv.org/abs/2201.08873`).

[4] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture (i). *Inventiones mathematicae*, 178(3):485–504, Dec 2009.

[5] Michael Stoll. *The ratpoints program*, 2022. arXiv 0803.3165 (`https://arxiv.org/abs/0803.3165`), software available from `https://www.mathe2.uni-bayreuth.de/stoll/programs/index.html`.


## Random modular symbols


Dan Yasaki

(joint work with Avner Ash)


Let $\Gamma$ denote the subgroup $\Gamma_0^{\pm}(N)$ of $\mathrm{GL}_2(\mathbb{Z})$, with $N$ prime. Let $V$ be the space of holomorphic modular forms for $\Gamma$. Let

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_k \oplus E$$

denote decomposition into Hecke eigenspaces, with the last $E$ denoting the one-dimensional Eisenstein subspace. We investigate the set of modular symbols in $V$. If $M \in V$ is a modular symbol, define the type of $M$ to be $(t_1, t_2, \ldots, t_k, t_E)$, where $t_\alpha = 1$ if the projection of $M$ to $V_\alpha$ is nonzero, and $t_\alpha = 0$ otherwise. Our talk presented the results of a computational investigation of the types of the modular symbols in an increasing series of concentric boxes. We prove some of the observations made in the data hold in general, while other observations are still open questions. We discussed the following results:

(1) Most random modular symbols are cuspidal in the following sense. Let $(t_1, t_2, \ldots, t_k, t_E)$ be the type of a modular symbol. Choosing modular symbols in a "rectangular box" and letting the box grow to infinity, the probability that $t_E = 0$, i.e., the symbol is cuspidal, is $\frac{1+N^2}{(1+N)^2}$, and the probability that $t_E = 1$ is $\frac{2N}{(1+N)^2}$.

(2) Let $U \subset$ be the set of modular symbols, and let $U' \subset$ be the cuspidal symbols. Let $\Lambda \subset V$ be the $\mathbb{Z}$-lattice generated by $U$, and let $\Lambda' \subset V$ be the $\mathbb{Z}$-lattice generated by $U'$. Then
   (a) the set of cuspidal symbols is the cuspidal lattice, $U' = \Lambda'$;
   (b) the modular symbols is the union of three cosets in $\Lambda/\Lambda'$,

$$U = \Lambda' \cup ([e, f]_\Gamma + \Lambda') \cup (-[e, f]_\Gamma + \Lambda').$$

   It follows that if there are no cuspforms of level $N$, then $U$ consists of three points. When the cuspidal space is nontrivial, $U$ is infinite.

(3) There is an obstruction for a given type to occur, related to the existence of "Eisenstein primes" [5, 6]. Let $\Lambda_i$ be the projection of $\Lambda$ to $V_i$, and let $\Lambda_i'$ be the projection of $\Lambda'$ to $V_i$. Suppose $[\Lambda_i \colon \Lambda_i'] \neq 1$, and let $[v, w]_\Gamma \in V$ have type $(t_1, t_2, \ldots, t_k, t_E)$. Then $t_E = 1$ implies that $t_i = 1$.

   For any given type that survives this obstruction, we give computational evidence that the proportion of its occurrence in a box stabilizes as the boxes grow larger. We interpret the limit of this ratio (assuming it exists) as the box size goes to infinity as the probability that a random modular symbol will have this type. See [1] for several plots. Contrary to our original expectation, it does not appear to be the case that with probability 1 a random symbol will project nontrivially to each $V_i$. Whether the limit actually exists, and why the limits have the various values that appear in our computations, are open questions.

(4) A corollary of the Eisenstein obstruction predicts the existence of cuspforms that are congruent to Eisenstein series. Namely, if prime $\ell > 2$ divides the index $[\Lambda_i \colon \Lambda_i']$, then there is a newform of level $N$ and weight 2 whose Hecke eigenvalue $a_p$ is congruent modulo $\ell$ to $p + 1$ for all $p \neq N$. Such a prime $p$ divides $N - 1$.

For details, we refer to [1]. This work was partially supported by the Simons Foundation (848154).

## References

[1] Avner Ash and Dan Yasaki, *Random modular symbols*, preprint, 2024.
[2] Avner Ash and Dan Yasaki, *Steinberg homology, modular forms, and real quadratic fields*, J. Number Theory **224** (2021), 323–367. MR 4244157
[3] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR MR1484478
[4] The LMFDB Collaboration, *The L-functions and modular forms database*, `http://www.lmfdb.org`, 2023, [Online; accessed 1 November 2023].
[5] Barry Mazur and Jean-Pierre Serre, *Points rationnels des courbes modulaires $X_0(N)$ (d'après A. Ogg)*, Séminaire Bourbaki (1974/1975), Exp. No. 469, Lecture Notes in Math, vol. Vol. 514, Springer, Berlin, 1976, pp. pp 238–255. MR 485882
[6] Preston Wake and Carl Wang-Erickson, *The Eisenstein ideal with squarefree level*, Adv. Math. **380** (2021), Paper No. 107543, 62. MR 4200464

## Vanishing criteria for Ceresa cycles

Ari Shnidman
(joint work with Jef Laga)

Let $C$ be a smooth, projective, and connected curve of genus $g \geq 2$ over $\mathbb{C}$ and $J$ its Jacobian variety. Embed $C \hookrightarrow J$ via $x \mapsto x - e$, where $e$ is a degree 1 divisor $e \in \mathrm{Pic}(C)$ such that $(2g-2)e$ is canonical. The Ceresa cycle $\kappa(C) \in \mathrm{CH}_1(J)$ in the Chow group with $\mathbb{Q}$-coefficients is the class of $[C] - (-1)^*[C]$. This is arguably the simplest example of an algebraic cycle that is homologically trivial but not in general algebraically trivial (as was proven by Ceresa [4]).

Recently, some non-hyperelliptic examples have been found with $\kappa(C) = 0$, among curves with non-trivial automorphism group. Other examples have been found proving the vanishing of the image $\bar{\kappa}(C)$ of $\kappa(C)$ in the Griffiths group $\mathrm{Gr}_1(J)$. Let $G = \mathrm{Aut}(C)$ be the finite group of automorphisms of $C$. Our first result is a general criteria: if $\mathrm{H}^3(J)^G_{\mathrm{prim}} = 0$, then $\kappa(C)$. Here, $H^3(J)_{\mathrm{prim}}$ denotes the primitive part of cohomology, the quotient of $H^3(J)$ by $H^1(C)(-1)$. This extends a recent result of Qiu-Zhang [9]. The assumption forces the relevant part of the intermediate Jacobian to vanish; we use this to show that not only does the Abel-Jacobi image of $\kappa(C)$ vanish, but $\kappa(C)$ itself. This gives several interesting examples of non-hyperelliptic curves with $\kappa(C) = 0$. However it is still quite rare, for example the criteria applies to exactly two plane quartic curves.

Our second result concerns the more general case where $H^3(J)^G$ is not zero, but rather, is isomorphic to $H^1(A)(-1)$ for some abelian variety $A$. Let $V = H^0(C, \Omega_C)$, the $g$-dimensional space of holomorphic differentials. Assuming the Hodge conjecture for $J \times A$, we show that the condition $(\wedge^3 V)^G = 0$ implies $\bar{\kappa}(C) = 0$. For example, this applies to all Picard curves, i.e. plane quartics of the form $y^3 = x^4 + ax^2 + bx + c$; the relevant Hodge conjecture in this case has been shown by Schoen. There are several other families of higher genus examples satisfying $(\wedge^3 V)^G = 0$, but it is not clear to the authors whether non-hyperelliptic examples exist in arbitrarily large genus. Even in genus 3, it is not clear the true strength of the criteria, since it may be combined with the fact that if $D \to C$ is a cover, and $\kappa(D) = 0$ then $\kappa(C) = 0$, and similarly for the classes $\bar{\kappa}(C)$ and $\bar{\kappa}(D)$. For example, the genus 7 Fricke-Macbeath curve satisfies both criteria but has a genus 3 quotient which satisfies neither.

Our final result concerns families of curves where $\kappa(C) = 0$, but for non-group theoretic reasons. Namely, we given an exact criteria for the vanishing of $\kappa(C)$ in the aforementioned family of Picard curves. Roughly, we may view the Picard modular surfaces as fibered over the $j$-invariant 0 elliptic curve $E\colon y^2 = x^3 + 1$ (more precisely, a quotient of it) and $\kappa(C) = 0$ if and only if $C$ lives in the fiber above a torsion point of $E$. As a result, we find that there are infinitely many plane quartic curves over $\mathbb{Q}$ with $\kappa(C) = 0$, and in fact, the Picard modular surface (viewed inside $\mathcal{M}_3$) contains a countable sequence of rational curves on which $\kappa(C) = 0$ identically. On the other hand, we also show that there is a uniform bound on the *order* of a torsion Picard curve Ceresa cycle (in the Chow

group with $\mathbb{Z}$-coefficients, appropriately defined) defined over a given number field, where the bound depends only on the degree of the number field.

The strategy of our proof of the vanishing criterion for $\kappa(C)$ of Picard curves makes sense more generally in any situation where one has a non-trivial family of curves with fiber-wise algebraically trivial Ceresa cycle. We give several other examples of such families, and it would be interesting in the future to: find more, implement our strategy for all of them (which will require some non-trivial work, including proving the relevant case of the Hodge conjecture if necessary), as well as to unify or characterize these examples to whatever extent possible. Indeed, the families we are aware of seem to exhibit certain common features, but the overall picture is still a mystery.

## References


[1] A. Beauville. A non-hyperelliptic curve with torsion Ceresa class. *C. R. Math. Acad. Sci. Paris*, 359:871–872, 2021.

[2] A. Beauville and C. Schoen. A non-hyperelliptic curve with torsion Ceresa cycle modulo algebraic equivalence. *Int. Math. Res. Not. IMRN*, (5):3671–3675, 2023.

[3] D. Bisogno, W. Li, D. Litt, and P. Srinivasan. Group-theoretic Johnson classes and non-hyperelliptic curves with torsion Ceresa class. *Épijournal Géom. Algébrique*, 7:Art. 8, 19, 2023.

[4] G. Ceresa, $C$ is not algebraically equivalent to $C^-$ in its Jacobian, Ann. of Math. (2) **117** (1983), no. 2, 285–291; MR0690847

[5] J. Laga and A. Shnidman. Ceresa cycles of bielliptic Picard curves. Arxiv preprint, available at https://arxiv. org/abs/2312.12965v1, to appear in *J. Reine Angew. Math.*

[6] J. Laga and A. Shnidman. Vanishing criteria for Ceresa cycles. Arxiv preprint, available at https://arxiv.org/ abs/2406.03891v1, 2024+

[7] R. Laterveer. On the tautological ring of Humbert curves. *manuscripta math.*, 172:1093–1107, 2023.

[8] D. T.-B. G. Lilienfeldt and A. Shnidman. Experiments with Ceresa classes of cyclic Fermat quotients. *Proc. Amer. Math. Soc.*, 151(3):931–947, 2023.

[9] C. Qiu and W. Zhang, Vanishing results in Chow groups for the modified diagonal cycles, *Tunis. J. Math.* **6** (2024), no. 2, 225–247; MR4765500


## Gauss' congruences and supercongruences for rational functions in several variables


Masha Vlasenko

(joint work with Frits Beukers)


A sequence of integers $\{a(n); n \geq 0\}$ satisfies the Gauss congruences for a prime number $p$ if

$$a(n) \equiv a(n/p) \mod p^{ord_p(n)} \qquad \forall n.$$

Examples of such sequences include $a(n) = a^n, a \in \mathbb{Z}$ and, more generally, $a(n) = \mathrm{tr}(A^n)$ where $A$ is a matrix with coefficients in $\mathbb{Z}$. In [2] we prove Gauss' congruences for expansion coefficients of multivariable rational functions, generalising the results in [1]:

**Theorem 1.** *Consider Laurent polynomials $P, Q \in \mathbb{Z}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$. Let $\Delta_Q \subset \mathbb{R}^n$ be the Newton polytope of $Q$ ($\Delta_Q$ = convex hull of its support $supp(Q)$). Assume that $supp(P) \subset \Delta_Q$ and $\Delta_Q \cap \mathbb{Z}^n = \{vertices\}$. Then for any prime $p$ not dividing any of the coefficients of $Q$, the coefficients of the formal expansion*

$$\frac{P}{Q} = \sum_{u \in \mathbb{Z}^n} a(u) x_1^{u_1} \cdots x_n^{u_n}$$

*at any vertex of $\Delta_Q$ satisfy multivariable Gauss' congruences*

$$a(u_1, \ldots, u_n) \equiv a(u_1/p, \ldots, u_n/p) \mod p^{\min_j ord_p(u_j)} \qquad \forall u.$$

For example, the conditions of this theorem are satisfied by the Delannoy numbers

$$\frac{1}{1 - x_1 - x_2 - x_1 x_2} = \sum_{u \in \mathbb{Z}^2_{\geq 0}} D(u_1, u_2) x_1^{u_1} x_2^{u_2}$$

and the binomial coefficients

$$\frac{1}{1 - x_1 - x_2} = \sum_{m=0}^{\infty} (x_1 + x_2)^m = \sum_{u \in \mathbb{Z}^2_{\geq 0}} \binom{u_1 + u_2}{u_1} x_1^{u_1} x_2^{u_2}.$$

While the $p$-adic order in this theorem is the best possible in general, the binomial coefficients provide an example of a *supercongruence*:

$$\binom{u_1 + u_2}{u_1} \equiv \binom{(u_1 + u_2)/p}{u_1/p} \mod p^{2 \min(ord_p(u_1), ord_p(u_2))}.$$

In the talk we sketched a homological proof of the above theorem and explained a generalisation of this method given in [3], which allows one to prove supercongruences.

## References


[1] F. Beukers, M. Houben, A. Straub, *Gauss congruences for rational functions in several variables*, Acta Arithmetica 184 (2018), 341–362

[2] F. Beukers, M. Vlasenko, *Dwork crystals I*, Int. Math. Res. Notices, 2021 (2021), 8807–8844, online: https://doi.org/10.1093/imrn/rnaa119

[3] F. Beukers, M. Vlasenko, *Dwork crystals III: Excellent Frobenius lifts towards supercongruences*, Int. Math. Res. Notices, online: https://doi.org/10.1093/imrn/rnad101

## Genus 2 curves over $\mathbb{Q}$ of small conductor

Andrew V. Sutherland
(joint work with Andrew R. Booker)

In his invited talk at the Algorithmic Number Theory Symposium in 1996, Poonen proposed a list "reasonable projects for the near future" in the development of algorithms for curves of genus 2 or more [12]. Proposed projects included faster point-counting algorithms for genus 2 curves over finite fields, practical algorithms to compute the conductor, Mordell-Weil group, and endomorphism ring of the Jacobian of a genus 2 curve $X/\mathbb{Q}$, implementation of the Chabauty–Coleman method for determining rational points, methods to enumerate all genus 2 curves whose Jacobians are isogenous to the Jacobian of a given curve, and a list of genus 2 $X/\mathbb{Q}$ for which $\mathrm{Jac}(X)$ has good reduction away from 2. Substantial progress has been made on all the projects Poonen proposed, with one notable exception:

> *Assemble a list of genus 2 curves over $\mathbb{Q}$ of small conductor, analogous to the lists of elliptic curves in* [5] *and* [8].

A database of genus 2 curves over $\mathbb{Q}$ of small *discriminant* constructed in 2016 is part of the L-functions and Modular Forms Database (LMFDB) [7]. It is believed to include a substantial proportion (perhaps 90 percent) of all genus 2 curves over $\mathbb{Q}$ with discriminant $|\Delta| \le 10^6$, but only a tiny proportion (less than one percent) of those with conductor $N \le 10^6$, because most curves with $N \le 10^6$ have $|\Delta| > 10^6$. Indeed, the genus 2 curve with smallest possible conductor $N = 11^2 = 121$, the modular curve $X_0(22)$, has $\Delta = 2^{12} \cdot 11^4 = 59969536 > 10^6$.

The tables of elliptic curves compiled by Cremona [8] have been expanded over the years to include all elliptic curves $E/\mathbb{Q}$ of conductor $N \le 500000$ and are now part of the LMFDB. These tables were compiled using the following approach:

(1) Assume modularity (now proved), which gives a bijection between isogeny classes of elliptic curves $E/\mathbb{Q}$ and rational newforms $f \in S_2^{\mathrm{new}}(\Gamma_0(N))$.
(2) Enumerate rational newforms $f \in S_2^{\mathrm{new}}(\Gamma_0(N))$ for $N = 1, 2, 3, \ldots$.
(3) Use Eichler-Shimura to construct an elliptic curve $E_f$ for each $f$.
(4) Find all elliptic curves $E/\mathbb{Q}$ isogenous to $E_f$.

Steps (1), (2), and (4) are all expected to generalize, at least in principle, to abelian varieties of dimension $g > 1$. For $g = 2$ there has been substantial recent progress on steps (1) and (4); see [3] and [6]. Step (2) is much more challenging, and currently only practical for $g = 2$ and very small $N$ (it is difficult to get rigorous results due to a lack of dimension formulae for spaces of paramodular forms). But even if one could make step (2) practical, this will still be insufficient, because there is simply no analog of step (3) for $g > 1$ (not even in principle).

Another approach for $g = 1$ uses Thué–Mahler solvers to enumerate all $E/\mathbb{Q}$ with good reduction away from a fixed set of primes $S$ [2, 9]. One can in principle similarly determine all genus 2 curves $X/\mathbb{Q}$ with good reduction away from $S$ using $S$-unit solvers, but this is very hard to do in practice and it is not sufficient. For $g > 1$, a curve may have bad reduction at a prime where its Jacobian has good reduction (such primes divide the discriminant but not the conductor). The

curve $X_0(22)$ is an example: it has bad reduction at 2, but its Jacobian has good reduction at 2. There are many genus 2 curves $X/\mathbb{Q}$ of small conductor that have bad reduction at large primes, including primes much larger than the conductor.

Thus for $g > 1$ a new approach seems to be required. In recent joint work with Andrew Booker, we extend the axiomatic approach of Farmer, Koutsoliotas, and Lemurell [10] to explicitly enumerate $L$-functions of small conductor. We restrict to $L$-functions in the Selberg class (with polynomial Euler factors), which, under the Hasse–Weil conjecture (implied by modularity), includes all $L$-functions of abelian varieties. We focus on arithmetic $L$-functions $L(s) = \sum a_n n^{-s}$ with $a_n \in \mathbb{Z}$. This is a countable set, and if one fixes the conductor, degree, motivic weight, and gamma factors (the last three are the same for every abelian surface over $\mathbb{Q}$), it is a finite set. For any positive integer $m$ one can provisionally compute the finite set of prefixes $(a_1, a_2, \ldots, a_m)$ that arise among these $L$-functions by using the functional equation to eliminate other possibilities, and by making $m = O(\sqrt{N})$ sufficiently large, one can ensure each prefix corresponds to at most one $L$-function.

To obtain a practical algorithm, we treat the $a_n$ as unknown integer variables that satisfy the Ramanujan/Hasse-Weil bounds and multiplicative relations implied by the Euler product, and use the approximate functional equation for $L(s)$ and its twists (Rankin-Selberg convolutions of $L(s)$ with known $L$-functions) to obtain a system of inequalities that we solve using an iterative process that exploits high-performance implementations of the simplex method and LLL. This allows us to substantially extend the feasible range of conductors.

In order to prove that every prefix output by our algorithm corresponds to an $L$-function (and only one of them), we search for abelian varieties, and in particular, Jacobians of genus 2 curves, that realize each prefix. Once we have an abelian variety $A/\mathbb{Q}$ that realizes a particular prefix, assuming modularity, we can prove that any abelian variety $A'/\mathbb{Q}$ realizing the same prefix must be isogenous to $A$.

As in the recent work of Alpöge and Lawrence presented by Alpöge at this workshop, our results conditionally provide an effective form of the Shafarevich conjecture proved by Faltings: the set of $g$-dimensionally abelian varieties $A/\mathbb{Q}$ with good reduction outside of a fixed set of primes is finite. Assuming modularity of abelian varieties over $\mathbb{Q}$, we can in principle enumerate this finite set for any given set of primes as follows. Results of Brumer and Kramer [4] provide an explicit finite set of conductors to consider, results of Masser and Wustholz imply that we can effectively enumerate all the abelian varieties $A'/\mathbb{Q}$ isogenous to an $A/\mathbb{Q}$ that realizes a prefix output by our algorithm, and assuming modularity, we are guaranteed to find an $A/\mathbb{Q}$ for each prefix if we simply enumerate $A/\mathbb{Q}$ by height using brute force (for perfect power conductors we cannot restrict our search to $A$ of dimension $g$, we may also need to consider $A$ of dimension $ng$ whose $L$-function may be the $n$th power of the $L$-function we seek). While the brute force part of this algorithm is highly impractical, as a whole the algorithm is arguably less impractical than the Alpöge-Lawrence algorithm, and it depends on fewer (and weaker) conjectures. As explained in [1], this also yields an effective version of Faltings' proof of the Mordell conjecture, which with our approach is conditional only on the modularity of abelian varieties.

We do not yet have a practical algorithm that is guaranteed to find the $A/\mathbb{Q}$ whose $L$-functions we seek (even assuming modularity), but we can do much better than brute force, especially when $g = 2$ and when $A$ can be realized as the Jacobian of a curve (which is not always true, even for $g = 2$). Here we use two approaches. The first leverages our knowledge of the prefix we seek, using a CRT approach to produce global candidates that are locally compatible at many small primes. The second uses the approximate functional equation to very quickly compute provisional conductors (and missing Euler factors), which allows us to extend the methods previously used to efficiently enumerate curves of small height that were filtered for small discriminants in [7] to instead filter for small conductors. Together these yield the following provisional theorem, whose proof is still in progress.

**Theorem 1.** *Assume the paramodular conjecture. There are 456 $L$-functions of abelian surfaces $A/\mathbb{Q}$ with conductor $N \leq 1000$, of which*

- *360 arise from products of elliptic curves over $\mathbb{Q}$;*
- *17 arise from weight-2 newforms with quadratic coefficients;*
- *2 arise from the Weil restriction of an elliptic curve over a quadratic field;*
- *77 arise from generic abelian surfaces, of which at least 67 are Jacobians.*

## References


[1] Levent Alpöge and Brian Lawrence, *Conditional algorithmic Mordell*, arXiv preprint 2408.11653v1, posted on August 21, 2024.

[2] Michael A. Bennett, Adela Gherga, Andrew Rechnitzer, *Computing elliptic curves over* $\mathbb{Q}$, Math. Comp. **88** (2019), 1341-1390.

[3] George Boxer, Frank Calegari, Toby Gee, Vincent Pilloni, *Abelian surfaces over totally real fields are potentially modular*, Publ. Math. Inst. Hautes Études Sci. **134** (2021), 153–501.

[4] Armand Brumer and Kenneth Kramer, *The conductor of an abelian variety*, Comp. Math. **92** (1994), 227–248.

[5] Bryan J. Birch and Willem Kuyk, eds., *Modular functions of one variable IV*, Lecture Notes in Math. **476**, Springer–Verlag, 1975.

[6] Raymond van Bommel, Shiva Chidambaram, Edgar Costa, Jean Kieffer, *Computing isogeny classes of typical principally polarized abelian surfaces over the rationals*, pages 187–214 in LuCaNT: LMFDB, Computation, and Number Theory, Contemp. Math. **796**, American Mathematical Society, 2024.

[7] Andrew R. Booker, Jeroen Sijsling, Andrew V. Sutherland, John Voight, Dan Yasaki, *A database of genus* 2 *curves over the rational numbers*, Twelfth Algorithmic Number Theory Symposium (ANTS XII), LMS J. Comput. Math **19** (2016), 235–254.

[8] John E. Cremona, *Algorithms for modular curves*, Cambridge University Press, 1992.

[9] Adela Gherga and Samir Siksek, *Efficient resolution of Thue–Mahler equations*, Algebra Number Theory, to appear.

[10] David Farmer, Sally Koutsoliotas, and Stefan Lemurell, *Varieties via their L-functions*, J. Number Theory **196** (2019), 264–380.

[11] David Masser and Gisbert Wustholz, *Isogeny estimates for abelian varieties and finiteness theorems*, Annals of Mathematics **137** (1993), 459–472.

[12] Bjorn Poonen, *Computational aspects of curves of genus at least* 2, Algorithmic Number Theory, Second International Symposium (ANTS II), pages 283–306, in Lecture Notes in Comput. Sci. **1122**, Springer, 1996.


*Reporter: Mieke Wessel*

## Participants

**Asem Abdelraouf**
SISSA
International School for Advanced Studies
Via Beirut n. 2-4
34014 Trieste
ITALY

**Niven Achenjang**
Department of Mathematics
Massachusetts Institute of Technology
Cambridge, MA 02139
UNITED STATES

**Dr. Bill Allombert**
CNRS
Institut de Mathématiques de Bordeaux
Université de Bordeaux
351, cours de la Liberation
33405 Talence Cedex
FRANCE

**Levent Alpöge**
Department of Mathematics
Harvard University
1 Oxford Street
Cambridge, MA 02138
UNITED STATES

**Dr. Jennifer S. Balakrishnan**
Department of Mathematics
Boston University
665 Commonwealth Avenue
Boston, MA 02215-2411
UNITED STATES

**Prof. Dr. Eva Bayer-Fluckiger**
EPFL
SB IMB CSAG (Batiment MA)
Station 8
1015 Lausanne
SWITZERLAND

**Prof. Dr. Karim Belabas**
Institut de Mathématiques
Université de Bordeaux
351, cours de la Liberation
33405 Talence Cedex
FRANCE

**Prof. Dr. Manjul Bhargava**
Department of Mathematics
Princeton University
Fine Hall
Washington Road
Princeton, NJ 08544-1000
UNITED STATES

**Prof. Dr. Irene I. Bouw**
Institut für Algebra und Zahlentheorie
Universität Ulm
Helmholtzstraße 18
89081 Ulm
GERMANY

**Prof. Dr. Frank Calegari**
Department of Mathematics
The University of Chicago
5734 South University Avenue
Chicago, IL 60637-1514
UNITED STATES

**Prof. Dr. Henri Cohen**
Institut de Mathématiques
Université de Bordeaux
351, cours de la Liberation
33405 Talence Cedex
FRANCE

**Dr. Edgar Costa**
Department of Mathematics
Massachusetts Institute of Technology
77 Massachusetts Avenue
Cambridge, MA 02139-4307
UNITED STATES

**Prof. Dr. John E. Cremona**
Department of Mathematics
University of Warwick
Coventry CV4 7AL
UNITED KINGDOM

**Prof. Dr. Tim Dokchitser**
Department of Mathematics
University of Bristol
Fry Building
Woodland Road
Bristol BS8 1UG
UNITED KINGDOM

**Prof. Dr. Noam D. Elkies**
Department of Mathematics
Harvard University
Science Center
One Oxford Street
Cambridge, MA 02138-2901
UNITED STATES

**Dr. David Harvey**
School of Mathematics and Statistics
The University of New South Wales
6108 Anita B. Lawrence Centre
Sydney NSW 2052
AUSTRALIA

**Prof. Dr. Ruth Kellerhals**
Département de Mathématiques
Université de Fribourg
Perolles
Chemin du Musee 23
1700 Fribourg
SWITZERLAND

**Dr. Sabrina Kunzweiler**
Institut de Mathématiques de Bordeaux,
Inria Bordeaux
Université de Bordeaux
351, cours de la Liberation
33405 Talence Cedex
FRANCE

**Vadym Kurylenko**
SISSA
International School for Advanced
Studies
Via Beirut n. 2-4
34014 Trieste
ITALY

**Dr. Jef Laga**
Department of Pure Mathematics
and Mathematical Statistics
University of Cambridge
Wilberforce Road
Cambridge CB3 0WB
UNITED KINGDOM

**Prof. Dr. Hendrik W. Lenstra**
Mathematisch Instituut
Universiteit Leiden
P.O. Box 9512
2300 RA Leiden
NETHERLANDS

**Dr. Wanlin Li**
Washington University in St. Louis
One Brookings Drive
St. Louis, MO 63130
UNITED STATES

**Dr. Elisa Lorenzo Garcia**
U. F. R. Mathématiques
I. R. M. A. R.
Université de Rennes I
Campus de Beaulieu
35042 Rennes Cedex
FRANCE

**Dr. Céline Maistret**
Department of Mathematics
University of Bristol
Woodland Road
Bristol BS8 1UG
UNITED KINGDOM

**Prof. Dr. Ariel Martin Pacetti**
Math. Department, University of Aveiro
Campus Universitário de Santiago
Aveiro 3810-193
PORTUGAL

**Dr. Margherita Pagano**
Rijksuniversiteit te Leiden
Mathematisch Instituut
Niels Bohrweg 1
5238 CA Leiden
NETHERLANDS

**Dr. Aurel Page**
Inria – CANARI Team
Institut de Mathématiques de Bordeaux
Université de Bordeaux
351, cours de la Libération
33405 Talence
FRANCE

**Prof. Dr. Jennifer Park**
Department of Mathematics
The Ohio State University
231 W 18th Ave
43215 Columbus, OH 43215
UNITED STATES

**Prof. Dr. Bjorn Poonen**
Department of Mathematics
Massachusetts Institute of Technology
77 Massachusetts Avenue
Cambridge, MA 02139-4307
UNITED STATES

**Prof. Dr. Kartik Prasanna**
Department of Mathematics
University of Michigan, Ann Arbor
2074 East Hall
530 Church Street
Ann Arbor, MI 48109-1043
UNITED STATES

**Prof. Dr. Rachel Pries**
Department of Mathematics
Colorado State University
Weber Building
Fort Collins, CO 80523-1874
UNITED STATES

**Dr. Danylo Radchenko**
Université Lille I
Laboratoire Paul Painleve
UFR de Mathématiques
59655 Villeneuve d'Ascq Cedex
FRANCE

**Dr. Damien Robert**
Mathématiques et Informatique
Université Bordeaux I
351, cours de la Liberation
33405 Talence Cedex
FRANCE

**Prof. Dr. David Roberts**
Division of Science and Mathematics
University of Minnesota – Morris
Morris, MN 56267
UNITED STATES

**Prof. Dr. Fernando Rodriguez-Villegas**
Mathematics Section
The Abdus Salam International Centre for Theoretical Physics (ICTP)
Strada Costiera, 11
34151 Trieste
ITALY

**Dr. David Roe**
Department of Mathematics
Massachusetts Institute of Technology
77 Massachusetts Avenue
Cambridge, MA 02139-4307
UNITED STATES

**Dr. Will Sawin**
Department of Mathematics
Princeton University
Fine Hall, Washington Road
Princeton, NJ 08540
UNITED STATES

**Prof. Dr. Damaris Schindler**
Mathematisches Institut
Georg-August-Universität Göttingen
Bunsenstr. 3-5
37073 Göttingen
GERMANY

**Prof. Dr. René Schoof**
Dipartimento di Matematica
Università degli Studi di Roma II -
"Tor Vergata"
Via della Ricerca Scientifica
00133 Roma
ITALY

**Prof. Dr. Ari Shnidman**
Einstein Institute of Mathematics
The Hebrew University
Givat-Ram
91904 Jerusalem
ISRAEL

**Prof. Dr. Samir Siksek**
Department of Mathematics
University of Warwick
Warwick CV4 7AL
UNITED KINGDOM

**Dr. Alexander Smith**
UCLA
Department of Mathematics
520 Portola Plaza
Los Angeles 90024
UNITED STATES

**Prof. Dr. Padmavathi Srinivasan**
Department of Mathematics
Boston University
665 Commonwealth Avenue
Boston, MA 02215-2411
UNITED STATES

**Prof. Dr. Michael Stoll**
Mathematisches Institut
Universität Bayreuth
95440 Bayreuth
GERMANY

**Andrew Sutherland**
Department of Mathematics
Massachusetts Institute of Technology
77 Massachusetts Avenue
Cambridge, MA 02139-4307
UNITED STATES

**Dr. Jack Thorne**
Department of Pure Mathematics
and Mathematical Statistics
University of Cambridge
Wilberforce Road
Cambridge CB3 0WB
UNITED KINGDOM

**Prof. Dr. Gonzalo Tornaría**
Centro de Matemática
Facultad de Ciencias
Igua 4225
Montevideo 11400
URUGUAY

**Dr. Raymond van Bommel**
School of Mathematics
University of Bristol
Fry Building, Woodland Road
Bristol BS8 1UG
UNITED KINGDOM

**Dr. Masha Vlasenko**
Institute of Mathematics
of the Polish Academy of Sciences
Sniadeckich 8
00-656 Warszawa
POLAND

**Prof. Dr. John Voight**
Department of Mathematics
Dartmouth College
6188 Kemeny Hall
Hanover, NH 03755-3551
UNITED STATES

**Mieke Wessel**
Mathematisches Institut
Georg-August-Universität Göttingen
Bunsenstr. 3-5
37073 Göttingen
GERMANY

**Prof. Dr. Stefan Wewers**
Institut für Algebra und Zahlentheorie
Universität Ulm
89069 Ulm
GERMANY

**Dr. Dan Yasaki**
Department of Mathematics & Statistics
University of North Carolina at
Greensboro
116 Petty Building
Greensboro, NC 27402-6170
UNITED STATES

**Prof. Dr. Don B. Zagier**
Max Planck Institut für Mathematik
Vivatsgasse 7
53111 Bonn
GERMANY

**Dr. Nina Zubrilina**
Department of Mathematics
Princeton University
Fine Hall
Washington Road
Princeton, NJ 08544-1000
UNITED STATES