Mathematisches Forschungsinstitut Oberwolfach

Report No. 34/2021

DOI: 10.4171/OWR/2021/34

Explicit Methods in Number Theory (hybrid meeting)

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

18 July – 24 July 2021

Abstract. The series of Oberwolfach meetings on 'Explicit methods in number theory' brings together people attacking key problems in number theory via techniques involving concrete or computable descriptions. Here, number theory is 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, modular forms and functions.

The 2021 meeting featured a seven-lecture minicourse on the distribution of class groups and Selmer groups. The other talks covered a broad range of topics in number theory ranging, for instance, from deterministic integer factorisation to the inverse Galois problem, rational points, and integrality of instanton numbers.

Mathematics Subject Classification (2020): Primary: 11Y16; Secondary: 11N05, 11R32, 11R65, 11Y05, 11Y50, 14G35, 14H25, 14K15, 14Q25.

Introduction by the Organizers

The workshop *Explicit Methods in Number Theory*, organised by Karim Belabas (Bordeaux), Bjorn Poonen (Cambridge, MA), and Fernando Rodriguez Villegas (Trieste) was run in a hybrid format due to the COVID 19 pandemic, with 14 participants at the institute and 42 participating remotely via Zoom from many time zones in Europe, the US, and Oceania. This workshop is part of a long-standing series of meetings whose goal is to present new methods and results on concrete aspects of number theory. In several cases, this included algorithmic and

experimental work, but the emphasis is on the implications for number theory. Ten previous workshops on the topic have been held in Oberwolfach since 1999.

The programme consisted of a seven-lecture minicourse on arithmetic statistics for class groups and Selmer groups, and twenty-two standalone lectures by participants. Contributions ranging from deterministic integer factorisation to the inverse Galois problem, rational points, and integrality of instanton numbers were presented, for example. Those participating remotely socialized through events hosted on the `wonder.me` platform.

Arithmetic statistics concerns itself with the distribution of arithmetic objects in a family, ordered by some natural invariant. These include class groups of number fields ordered by discriminants, and Selmer groups attached to elliptic curves ordered by the size of a Weierstrass equation or to twists of a fixed curve. Both are finite, effectively computable, abelian groups classifying global obstructions and are critical to understanding arithmetic problems like solving Diophantine equations or, equivalently, finding rational points on varieties. For instance, Selmer groups are related to the existence of rational points on elliptic curves and allow one to prove the weak Mordell–Weil theorem.

Starting from the "Cohen–Lenstra heuristics" (1983), proposing a probabilistic model for the average behavior of class groups of quadratic fields, major conjectures provide models for various such distributions and allow numerical predictions. Since class groups and Selmer groups are finite abelian groups, one can write them as the direct product of their p-Sylow subgroups and study the distribution of such p-components, for instance, by computing their moments. The minicourse was centered on Alexander Smith's proofs that the 2-parts of quadratic class groups and Selmer groups attached to twists of certain elliptic curves indeed followed the conjectured distribution. One striking consequence (obtained by Koymans and Pagano) concerns the distribution of discriminants d such that the negative Pell equation $x^2 - dy^2 = -1$ has a solution in integers x and y (Stevenhagen's conjecture).

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-1641185, "US Junior Oberwolfach Fellows".

Workshop (hybrid meeting): Explicit Methods in Number Theory

Table of Contents

Abstracts

Problems, Conjectures and Theorems in Arithmetic Statistics

Manjul Bhargava

We give an overview of some of the problems, conjectures, and known theorems (and of some of the motivations, assumptions, and methods behind them) in the subject of arithmetic statistics, with a focus on those relating to the distribution of class groups and Selmer groups. In particular, we describe the Cohen–Lenstra heuristics for class groups (and their extensions due to Gerth, Martinet, Malle, Karman, Bartel–Lenstra, and others) and the Poonen–Rains and B.–Kane–Lenstra–Poonen–Rains heuristics for Selmer groups, and the various results in the directions of these heuristics in works due to Davenport–Heilbronn, B., Fouvry–Klüners, Klagsbrun, Ho–Shankar–Varma, B.–Hanke–Shankar, Smith, Yu, Achter–Pries, Hall, Ellenberg–Venkatesh–Westerland, Heath-Brown, Swinnerton-Dyer, Kane, Klagsbrun–Mazur–Rubin, B.–Shankar, B.–Ho, B.–Gross, Shankar–Wang, Thorne, Romano–Thorne, Alpöge, B.–Shankar–Swaminathan, Milovic, Smith, Chan–Koymans–Milovic–Pagano, Koymans–Pagano, Landesman, Feng–Landesman–Rains, Boston–Bush–Hajir, Liu–Wood–Zureick-Brown, Dummit–Voight, B.–Varma, Bartel–Lenstra, Wang–Wood, Sawin, and more (as time permits). Many of the works described in this survey will be expanded upon in forthcoming lectures of this workshop.

Statistics of the Galois module structure of Mordell-Weil groups

Alex Bartel
(joint work with Adam Morgan)

The following question seems very natural, but has, to our knowledge, not been considered until now. Fix a number field K, an elliptic curve E/K, a finite group G, and a finitely generated $\mathbb{Q}[G]$-module V. By the Jordan–Zassenhaus theorem, there are only finitely many isomorphism classes of finitely generated full rank $\mathbb{Z}[G]$-lattices inside V. More precisely, there is a finite set $\mathcal{L}$ of $\mathbb{Z}$-free $\mathbb{Z}[G]$-modules such that every $\mathbb{Z}[G]$-module L satisfying $\mathbb{Q}\otimes_{\mathbb{Z}} L \cong_{\mathbb{Q}[G]} V$ is isomorphic to a unique element of $\mathcal{L}$. Let (F,ι) run over all pairs consisting of a Galois extension F of K an isomorphism ι between its Galois group and G, satisfying $\mathbb{Q}\otimes_{\mathbb{Z}} E(F) \cong_{\mathbb{Q}[G]} V$, where we may view $E(F)$ as a $\mathbb{Z}[G]$-module via the isomorphism ι. Then how often is $E(F)/E(F)_{\mathrm{tors}}$ isomorphic to any given lattice in $\mathcal{L}$? Of course, to make this question precise, we should order the family of pairs (F,ι) in some reasonable way, e.g. by the ideal norm of the discriminant of F/K, or of the product of primes of K that ramify in F (and the answer may well depend on the ordering).

In this project we consider the following special case: take $K=\mathbb{Q}$, G to be cyclic of order 2, $E/\mathbb{Q}$ to be an elliptic curve of rank 1, and V to be free of rank 1 over $\mathbb{Q}[G]$. In plain terms, we are letting F run over all quadratic number fields

over which E has rank 2. Each such F is isomorphic to $\mathbb{Q}(\sqrt{d})$ for a unique square-free integer d, and we can just order our family by $|d|$. It is not hard to see that $\mathcal{L}$ then consists of two elements: a free $\mathbb{Z}[G]$-module of rank 1, which we will just abbreviate to $\mathbb{Z}[G]$, and a direct sum of two submodules of $\mathbb{Z}$-rank 1, which we denote by $\mathbf{1} \oplus \mathrm{sign}$.

For technical reasons, we also assume that $E/\mathbb{Q}$ has full rational 2-torsion and no cyclic 4 isogeny. Our first, perhaps at first surprising, result is the following.

Theorem 1. *The proportion among fields F as just described of those for which one has $E(F)/E(F)_{\mathrm{tors}} \cong \mathbb{Z}[G]$ is asymptotically 0.*

It turns that there is a local obstruction to $E(F)/E(F)_{\mathrm{tors}}$ being isomorphic to $\mathbb{Z}[G]$: it can only happen if d is not divisible by any primes from a certain positive density set. We therefore modify the question, by restricting the family to only those F that, in addition to the constraint that the rank of $E(F)$ be 2, also satisfy the appropriate local conditions.

In that restricted family, we give a precise conjecture for the proportions with which $\mathbb{Z}[G]$ and $\mathbf{1} \oplus \mathrm{sign}$ occur as $E(F)/E(F)_{\mathrm{tors}}$, which we both conjecture to be positive. Our conjecture is closely analogous to Stevenhagen's heuristic on the solubility of the negative Pell equation. It can be summarised as follows:

- Let $\delta\colon E(\mathbb{Q}) \to H^1(\mathbb{Q}, E[2])$ be the coboundary map associated with the multiplication-by-2 Kummer sequence on E. Then the local conditions on d ensure that there is a Mordell–Weil generator P of $E(\mathbb{Q})$ such that $\delta(P) \in H^1(\mathbb{Q}, E[2]) \cong H^1(\mathbb{Q}, E_d[2])$ is contained in $\mathrm{Sel}^2(E_d/\mathbb{Q})$.
- We show that $E(F)/E(F)_{\mathrm{tors}} \cong \mathbb{Z}[G]$ if and only if there is a Mordell–Weil generator P of $E(\mathbb{Q})$ such that $\delta(P) \in \mathrm{Sel}^2(E_d/\mathbb{Q})$ is also the image of a Mordell–Weil generator of $E_d(\mathbb{Q})$ under the "twisted" coboundary map δ_d.
- We determine the proportions p_r with which one has
$$\dim_{\mathbb{F}_2}(\mathrm{Sel}^2(E_d/\mathbb{Q})/\delta_d(E_d[2])) = r$$
as d runs through our (thin!) family.
- We then conjecture that $\delta(P)$ is a uniformly "random" non-trivial element in that $\mathbb{F}_2$-vector space. This leads to the prediction that the proportion in the restricted family with which one has $E(F)/E(F)_{\mathrm{tors}} \cong \mathbb{Z}[G]$ is asymptotically $\displaystyle\sum_r \frac{p_r}{2^r - 1}$.

Remark 1. There is a lot of prior work on distributions of 2-Selmer groups in quadratic twist families, but there are additional subtleties that we have to beware of in our particular families: they are "thin" families, and by the first bullet point above, they are presisely rigged in such a way as to throw off the 2-Selmer distribution.

Remark 2. Somewhat surprisingly, our conjectured proportions turn out to be rational numbers, in contrast to the proportion in Stevenhagen's heuristic.

Graded Lie Algebras and Selmer Groups

Jack A. Thorne

Bhargava and Shankar have proved that the average size of the m-Selmer group of an elliptic curve over $\mathbb{Q}$ (these curves being ordered by the height of the coefficients in a defining Weierstrass equation) is equal to $\sigma_1(m) = \sum_{k|m} k$ for each $m = 2, 3, 4, 5$ [1–4]. In each case they introduce a pair (G, V) consisting of a reductive group G and a representation V, both defined over $\mathbb{Z}$. They relate the relevant Selmer groups to the set $G(\mathbb{Z})\backslash V(\mathbb{Z})$ of integral orbits and then use the geometry of numbers to get information about the number of orbits of bounded height, therefore about the average size of the Selmer group of an elliptic curve.

Gross observed that the pairs (G, V) appearing in the papers can all be seen as arising from stably graded Lie algebras [5]. A graded Lie algebra is a pair $(\mathfrak{g}, \theta)$, consisting of a Lie algebra $\mathfrak{g}$ (say semisimple over $\mathbb{Q}$) and homomorphism $\theta : \mu_m \to \mathrm{Aut}(\mathfrak{g})$. The homomorphism θ determines a grading $\mathfrak{g} = \oplus_{i \in \mathbb{Z}/m\mathbb{Z}} \mathfrak{g}_i$; then $\mathfrak{g}_0 \leq \mathfrak{g}$ is a Lie subalgebra which acts on $\mathfrak{g}_1$. Integrating $\mathfrak{g}_0$ to a reductive group G_0, we get a pair $(G_0, \mathfrak{g}_1)$. The grading $(\mathfrak{g}, \theta)$ is said to be stable if moreover there are stable vectors, i.e. elements in $\mathfrak{g}_1$ with closed orbit and finite stabiliser under the action of G_0.

It is therefore natural to wonder whether stably graded Lie algebras can be used to study the Selmer groups of other families of abelian varieties. Stably graded Lie algebras have been classified by Reeder, Levy, Yu, and Gross [6]. A variety of techniques have now been developed that can be used to prove theorems about Selmer groups using these stably graded Lie algebras. These include theorems concerning the average size of the 2-Selmer group of a Jacobian of a hyperelliptic curve of arbitrary genus [7–9], the 3-Selmer group of the Jacobian of a genus 2 curve [10], the 2-Selmer group of the Jacobian of a non-hyperelliptic curves of genus 3 [11], and the 2-Selmer groups of a family of (non-principally polarized) Prym abelian surfaces [12].

The techniques developed by Bhargava and Shankar to study the geometry of numbers generalise well to the context of an arbitrary stably graded Lie algebra $(\mathfrak{g}, \theta)$. More challenging is to find the relation between the rational and (in particular) integral orbits in $(G_0, \mathfrak{g}_1)$ and the Selmer groups of a family of abelian varieties. When $\mathfrak{g}$ is simply laced, the family of abelian varieties seems to be, in examples, the family of Jacobians of a versal deformation of a plane curve with a unique simple singularity. This is in particular the case for the (unique) stable $\mathbb{Z}/2\mathbb{Z}$-grading of such an algebra [13]. When $\mathfrak{g}$ is not simply laced, one expects to find a family of Pryms associated to a curves 'with fixed symmetries' (cf. [12]).

The most general construction available of rational orbits from rational points of Jacobians relies upon the existence of an interesting functor from root lattices, enriched with the data of a finite Heisenberg group, to graded Lie algebras [15]. The most general construction available of integral orbit representatives for Selmer group elements (see [11]) relies upon the observation that the compactified Jacobian of a versal $\mathbb{G}_m$-deformation of a reduced plane curve is absolutely smooth (i.e. smooth over $\mathbb{Q}$, if not over the base of the deformation) [14].

Several tantalising directions remain to be explored. For example, if $(\mathfrak{g}, \theta)$ is a stably $\mathbb{Z}/2\mathbb{Z}$-graded Lie algebra and G is a simply connected algebraic group with Lie algebra $\mathfrak{g}$, one can consider the action of $G_0 = G^{\theta=1}$ on the algebraic variety $G_1 = \{g \in G \mid \theta(g) = g^{-1}\}$. The geometric invariant theory of the pair (G_0, G_1) has been studied by Richardson [17], and is very much analogous to the geometric invariant theory of the pair $(G_0, \mathfrak{g}_1)$. Moreover, there is a relation between Selmer groups and rational orbits generalising that for the pair $(G_0, \mathfrak{g}_1)$ [16]. We await a theory of the geometry of numbers of such pairs (G_0, G_1) sufficient for further applications to arithmetic statistics.

References

[1] M. Bhargava and A. Shankar, Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. *Ann. of Math.* (2) **181** (2015), no. 1, 191–242.

[2] M. Bhargava and A. Shankar, Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. *Ann. of Math.* (2) **181** (2015), no. 2, 587–621.

[3] M. Bhargava and A. Shankar, The average number of elements in the 4-Selmer groups of elliptic curves is 7. `arXiv:1312.7333`.

[4] M. Bhargava and A. Shankar, The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1. `arXiv:1312.7859`.

[5] B. H. Gross, On Bhargava's representation and Vinberg's invariant theory. *Frontiers of mathematical sciences*, 317–321, Int. Press, Somerville, MA, 2011.

[6] M. Reeder, P. Levy, J.-K. Yu and B. H. Gross, Gradings of positive rank on simple Lie algebras. *Transform. Groups* **17** (2012), no. 4, 1123–1190.

[7] M. Bhargava and B. H. Gross, 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.

[8] A. Shankar and X. Wang, Rational points on hyperelliptic curves having a marked non-Weierstrass point. *Compos. Math.* **154** (2018), no. 1, 188–222.

[9] A. N. Shankar, 2-Selmer groups of hyperelliptic curves with marked points. *Trans. Amer. Math. Soc.* **372** (2019), no. 1, 267–304.

[10] B. Romano and J. A. Thorne, E_8 and the average size of the 3-Selmer group of the Jacobian of a pointed genus-2 curve. *Proceedings of the London Mathematical Society* **122** (2021), no. 5, 678–723.

[11] J. Laga, The average size of the 2-Selmer group of a family of non-hyperelliptic curves of genus 3. `arXiv:2008.13158`.

[12] J. Laga, Arithmetic statistics of Prym surfaces. `arXiv:2101.07658`.

[13] J. A. Thorne, Vinberg's representations and arithmetic invariant theory. *Algebra Number Theory* **7** (2013), no. 9, 2331–2368.

[14] B. Fantechi, L. Göttsche and D. van Straten, Euler number of the compactified Jacobian and multiplicity of rational curves. *J. Algebraic Geom.* **8** (1999), no. 1, 115–133.

[15] B. Romano, On central extensions and simply laced Lie algebras. *J. Algebra* **568** (2021), 480–511.

[16] J. A. Thorne, Arithmetic invariant theory and 2-descent for plane quartic curves. *Algebra Number Theory* **10** (2016), no. 7, 1373–1413.

[17] R. W. Richardson, Orbits, invariants, and representations associated to involutions of reductive groups. *Invent. Math.* **66** (1982), no. 2, 287–312.

2-descent for Bloch–Kato Selmer groups

Netan Dogra

Let $X/\mathbb{Q}$ be a hyperelliptic curve of genus g given by $y^2 = f(x)$, where $f \in \mathbb{Q}[x]$ is a separable polynomial. Poonen and Schaefer [PS] showed how to relate the 2-Selmer group of the Jacobian J of X to the arithmetic of the étale algebra $\mathbb{Q}[x]/(f(x))$. One application of this 'field-theoretic' characterisation is to bounding the rank r of the Jacobian. If $r < g$, the Chabauty–Coleman method can be used to produce a finite set $X(\mathbb{Q}_p)_1 \subset X(\mathbb{Q}_p)$ of p-adic points containing $X(\mathbb{Q})$.

The subject of this talk was the problem of carrying out 2-descent to prove upper bounds on the ranks of certain Bloch–Kato Selmer groups associated to certain geometric Galois representations of weight < -1. Unlike with abelian varieties, conjecturally these ranks are, in a certain sense, 'geometric' rather than 'arithmetic' invariants [BK].

One motivation for this problem comes from the problem of computing the set of rational points of hyperelliptic curves with $r \geq g$. Minhyong Kim has defined subsets $X(\mathbb{Q}_p)_n \subset X(\mathbb{Q}_p)$ containing $X(\mathbb{Q})$ which are finite whenever r plus the sum of ranks of certain Bloch–Kato Selmer groups associated to Galois representations of weight < -1 are less than some constant depending only on g. The attraction of this approach is that the Bloch–Kato conjectures imply that, for any r, this inequality is eventually satisfied, and hence $X(\mathbb{Q}_p)_n$ is eventually finite.

By "2-descent for $H^1_f(\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}), \wedge^2 T_2 J)$" we mean that we want to bound the rank of $H^1_f(\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}), \wedge^2 T_2 J)$ by computing the rank of a subgroup of $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}), \wedge^2 J[2])$. Analogous to the classical case, to do this we relate $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}), \wedge^2 J[2])$ to the subalgebra of $\mathbb{Q}[x, y, \frac{1}{x-y}]/(f(x), f(y))$ fixed by the involution swapping x and y.

One interesting example where these methods can be applied is the genus 2, rank 3 curve

$$C : y^2 - y = x^5 - x. \tag{1}$$

In [BMSTT], Bugeaud, Mignotte, Siksek and Tengely determined the integer valued solutions to (1), using a combination of transcendence methods and Mordell–Weil sieving. Using our 2-descent algorithm we prove $\mathrm{rk} H^1_f(G_{\mathbb{Q}}, \wedge^2 T_2 \mathrm{Jac}(C)) = 2$ and determine $C(\mathbb{Q})$.

The methods used for bounding the rank of $H^1_f(\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}), \wedge^2 T_2(J))$ have been applied to verify finiteness of $X(\mathbb{Q}_2)_2$ for a large number (> 1000) of the 7224 genus 2 rank 2 curves with a rational Weierstrass point on the LMFDB. By contrast, only 29 of these curves satisfy the condition $\rho(J) > 1$ used in [BD] to guarantee finiteness of $X(\mathbb{Q}_p)_2$ when $r = g$.

References

[BD] J. Balakrishnan, N. Dogra, Quadratic Chabauty and rational points I: p-adic heights. With an appendix by J. S. Müller. Duke Math. J. 167 (2018), no. 11, 1981–2038.

[BK] S. Bloch, K. Kato, L-functions and Tamagawa numbers of motives. In "The Grothendieck Festschrift, Vol I", 333–400. Progr. Math., 86, 1990.

[BMSTT] Y. Bugeaud, M. Mignotte, S. Siksek, M. Stoll, S. Tengely, Integral points on hyperelliptic curves. Algebra & Number Theory 2, no. 8 (2008): 859–885.

[PS] B. Poonen, E. Schaefer, Explicit Descent for Jacobians of Cyclic covers of the projective line. J. Reine Angew. Math. 488 (1997), 141–188.

[Kim] M. Kim, Unipotent Albanese and Selmer Varieties. Publ. Res. Inst. Math. Sci. 45 (2009), no. 1 89–133.

Restriction of scalars Chabauty applied to cyclic covers of $\mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$

Nicholas Triantafillou

Let K be a number field, let X/K be a curve with Jacobian J, and let $\mathfrak{p}$ be a prime of good reduction for X. Chabauty's method is a p-adic technique that produces a finite subset of $X(K_\mathfrak{p})$ containing $X(K)$ when $\operatorname{rank} J(K) \leq \dim J - 1$. Given a set S of finite places of K not containing $\mathfrak{p}$, after replacing J with a suitable generalized Jacobian, one can also use Chabauty's method to compute a finite set containing the $\mathcal{O}_{K,S}$-points on an integral model of an affine curve.

If $[K : \mathbb{Q}] > 1$, one can improve the rank-versus-dimension bound by applying an analogue of Chabauty's method to the restriction of scalars $\operatorname{Res}_{K/\mathbb{Q}} X$. This approach, called *RoS Chabauty*, first appears in [3] and is attributed to Wetherell. RoS Chabauty produces a set $X(K \otimes \mathbb{Q}_p)_1$ of p-adic points containing $X(K)$ which is 'expected' to be finite when $\operatorname{rank} J(K) \leq [K : \mathbb{Q}](\dim J - 1)$. Unfortunately, this expectation fails when a (translate of a) subgroup scheme $T \subset J$ with $T(K)$ of 'large' rank intersects $\operatorname{Res}_{K/\mathbb{Q}} X$ in 'large' dimension. We call such subgroup schemes *subgroup obstructions*. As a concrete example, [3] shows that if X is the base change of a curve over $k \subset K$ for which $X(k \otimes \mathbb{Q}_p)_1$ is infinite, the RoS Chabauty set $X(K \otimes \mathbb{Q}_p)_1$ for the base change of X to K will also be infinite. Similarly, [1] shows that if $X(K \otimes \mathbb{Q}_p)_1$ is infinite and $f : Y \to X$ is a nonconstant map of curves such that the K-points of the Prym variety are p-adically dense in the $K_\mathfrak{p}$-points, $Y(K \otimes \mathbb{Q}_p)_1$ will be infinite. We call a subgroup obstruction defined by iterating these constructions a *BCP obstruction* for base change + Prym.

Working in the context of S-integral points on affine curves, we show that when q is sufficiently large and $\alpha \in \mathcal{O}_{K,S}^\times$ is not a qth power, there are no subgroup obstructions to RoS Chabauty applied to $X_{\alpha,q} := \mathbb{P}^1 \smallsetminus \{x : x^q = \alpha\}$. Let $J_{\alpha,q}$ be the Jacobian of $X_{\alpha,q}$. The proof leverages the fact that splitting field of $J_{\alpha,q}$ is nonabelian over K to prove a large gap between the rank and dimension of any subtorus of $\operatorname{Res}_{\mathcal{O}_K/\mathbb{Z}} J_{\alpha,q}$. The case of $X_{1,q}$ is much subtler. When K is totally real, for large q, one can prove $X_{1,q}(\mathcal{O}_{K,S})$ is finite using classical Chabauty, but if K contains a CM subfield, there is a BCP obstruction to RoS Chabatuy for

$X_{1,q}$. When K does not contain a CM subfield, we show that $X_{1,q}$ has no BCP obstructions. See [4] for details.

As an application/motivation for our study, we note that the points on the curves $X_\alpha \smallsetminus \{0,\infty\}$ correspond exactly to the subset of $(\mathbb{P}^1 \smallsetminus \{0,1,\infty\})(\mathcal{O}_{K,S})$ in the same class of $\mathcal{O}_{K,S}^\times$ modulo qth powers as α^{-1}. Poonen showed that these sets can be computed using classical Chabauty when $K = \mathbb{Q}$. While Poonen's results do not extend beyond $K = \mathbb{Q}$ (except for K totally real and $\alpha = 1$), our work provides evidence that RoS Chabauty could be used to compute the $X_\alpha(\mathcal{O}_{K,S})$ when K does not contain a CM subfield. This suggests that RoS Chabauty plus descent by cyclic covers gives an elementary p-adic algorithm to compute the set $(\mathbb{P}^1 \smallsetminus \{0,1,\infty\})(\mathcal{O}_{K,S})$, or equivalently the set of solutions to the S-unit equation $x + y = 1$ for $x, y \in \mathcal{O}_{K,S}^\times$.

In future work, we hope to upgrade these results to a proof that RoS Chabauty and descent can bound the set $(\mathbb{P}^1 \smallsetminus \{0,1,\infty\})(\mathcal{O}_{K,S})$ and to combine the p-adic information from RoS Chabauty with other techniques to improve existing bounds on the size of this set. It would also be interesting to extend the results presented here to the case where K contains a CM-subfield, perhaps by performing a further descent in order to compute $(X_{1,q} \smallsetminus \{0,\infty\})(\mathcal{O}_{K,S})$ and to implement the resulting algorithm on a computer.

References

[1] N. Dogra, *Unlikely intersections and the Chabauty-Kim method over number fields*, arXiv preprint:1903.05032v2, (2020).

[2] B. Poonen, *The S-integral points on the projective line minus three points via étale covers and Skolem's method*, (2020). `math.mit.edu/~poonen/papers/siegel_for_Q.pdf`, Accessed: July 27, 2021.

[3] S. Siksek, *Explicit Chabauty over number fields*, Algebra Number Theory **7** (2013), 765–793.

[4] N. Triantafillou, *Restriction of scalars Chabauty and the S-unit equation*, arXiv preprint:2006.10590v2, (2021).

Primes in very short intervals and arithmetic progressions

Andrew Granville

(joint work with Allysa Lumley)

In 1792 Gauss predicted that "the density of primes around x is about $\frac{1}{\log x}$". This suggests that in an interval of y integers,

$$\pi(x+y) - \pi(x) = \#\{\text{Primes } p \in (x, x+y]\} \approx \frac{y}{\log x}. \tag{1}$$

There are $\phi(q)$ arithmetic progressions $a \pmod q$ with $(a,q) = 1$. We guess that the primes are roughly equi-distributed amongst these progressions, so that

$$\pi(x; q, a) = \#\{\text{Primes } p \le x : p \equiv a \pmod q\} \approx \frac{1}{\phi(q)} \frac{x}{\log x}.$$

If $x = qy$ then there are y integers in the progression so we expect

$$\pi(qy; q, a) \approx \frac{q}{\phi(q)} \frac{y}{\log q}$$

when $y = q^{o(1)}$ since then $\log qy \sim \log q$. We simplify by letting q be large and prime so that $q/\phi(q) \approx 1$ and so we expect that

$$\pi(qy; q, a) \approx \frac{y}{\log q} \tag{2}$$

which is similar in structure to (1). These estimates make sense once $y > (\log x)^{1+\eta}$ (or $y > (\log q)^{1+\eta}$), and heuristics suggest they should hold "100% of the time" in these ranges.

In this talk we explore two questions: What happens when y is smaller? And what are the extreme values in these ranges, that is the maximum and minimum number of primes. We approach these questions through various heuristics and test our conjectures against computational evidence.

In 1936 Cramér suggested a model based on Gauss's observation: Let $(B_n)_{n\geq 3}$ be independent random variables for which

$$\text{Prob}(B_n = 1) = \frac{1}{\log n} \text{ with } \text{Prob}(B_n = 0) = 1 - \frac{1}{\log n}.$$

Then the distribution of $\pi(x)$ can be modeled by

$$\sum_{n\leq x} B_n \text{ which has expectation } \int_3^x \frac{dt}{\log t} + O(1)$$

which is exactly what we expect from Riemann's zeros, and indeed it suggests an error term $x^{1/2+o(1)}$ which is equivalent to the Riemann Hypothesis. Similarly one might hope to model the the distribution of $\pi(X + y) - \pi(X)$ by $\sum_{X<n\leq X+y} B_n$. This is more-or-less a binomial distribution and suggests that there exists $X \in (x, 2x]$ for which $\pi(X + y) - \pi(X) = y$ whenever $y < (\log x)^{1-\epsilon}$. However this is clearly nonsense since half the integers in any interval are even. The problem is that Cramér's model does not take account of divisibility by small primes, so we modify it to do so. The idea is to discard any integer which has a prime factor $\leq z$ (for some well-chosen $z \leq y$), and then suitably define the random variables B_n for those n with no prime factor $\leq z$. This modified model does predict the distribution of primes in arithmetic progressions, as suggested by the Generalized Riemann Hypothesis, as well as Hardy and Littlewood's prime k-tuplets conjecture (neither of which followed from the original Cramér model).

If $0 \leq a_1 < \cdots < a_k \leq y$ are integers then there cannot be infinitely many n such that

$$n + a_1, \ldots, n + a_k \text{ are all prime}$$

if some prime p divides one of the $n + a_i$ for every n. If there is no such local obstruction then $a_1 < \cdots < a_k$ is *admissible* and Hardy & Littlewood's Prime k-tuplets conjecture claims that there are infinitely many such prime k-tuples. We let $S(y)$ be the largest size k of an admissible set of length y.

On the basis of some computational evidence, a careful (conjectural) study of the range of uniformity of the prime k-tuplets conjecture, and a modification of Cramér's model, we predict that if $y \le (1-\epsilon)\log x$ then

$$\max_{x<X\le 2x} \pi(X+y) - \pi(X) = S(y),$$

and if $y \le (1-\epsilon)\log q$ with q prime then

$$\max_{(a,q)=1} \pi(qy; q, a) = S(y) \text{ or } S(y)+1.$$

We also predict that if $p_1 = 2 < p_2 = 3 < \dots$ is the sequence of prime numbers then

$$\max_{x<p_n\le 2x} p_{n+1} - p_n \gtrsim 2e^{-\gamma}(\log x)^2$$

and that perhaps these are asymptotically equal, though the data is not too convincing. Analogously we predict that if $p(q,a)$ is the least prime $\equiv a \pmod q$ then

$$\max_{(a,q)=1} p(q,a) \gtrsim 2e^{-\gamma}(\log q)^2;$$

for prime q and that perhaps these are asymptotically equal for almost all q, though the constant will get as large as $4e^{-\gamma}$ for rare q, twice the "typical value". This prediction is well backed-up by the data for the primes up to a million.

References

[1] Andrew Granville and Allysa Lumley, *Primes in short intervals: Heuristics and calculations*, Experimental mathematics (to appear)

[2] G. H. Hardy and J. E. Littlewood, *Some problems of "Partitio Numerorum", III: On the expression of a number as a sum of primes*, Acta Math. **44** (1923), 1–70.

Small Galois groups over $\mathbb{Q}$ and $\mathbb{Q}(t)$

Tim Dokchitser

The Inverse Galois Problem asks whether every finite group G occurs as a Galois group over $\mathbb{Q}$, and, stronger, over $\mathbb{Q}(\mathrm{t})$ with no constant subfields. The constructive version of this problem also asks to produce polynomials with the right Galois group. We discuss some old and new methods and new results, including realisations of some previously unknown groups, and families for all transitive groups of degree < 16 over $\mathbb{Q}(t)$ and all groups of order < 128 over $\mathbb{Q}$.

The algorithms discussed in the talk have been implemented in the Magma package available from

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

together with a list of open problems on the computational aspects of the Inverse Galois Problem.

2^∞-Selmer groups in quadratic twist families

Alexander Smith

In 1979, Goldfeld conjectured the following:

Conjecture 1 ([2])**.** *Given an elliptic curve $E/\mathbb{Q}$ with narrow Weierstrass form*

$$y^2 = x^3 + ax + b,$$

and given a nonzero integer d, take E^d to be the elliptic curve over $\mathbb{Q}$ with narrow Weierstrass form

$$E^d : y^2 = x^3 + d^2ax + d^3b.$$

This curve is a quadratic twist of E, and is isomorphic to E over $\mathbb{Q}(\sqrt{d})$.

Then, for $r \geq 0$,

$$\lim_{N\to\infty} \frac{\#\left\{d \,:\, 0 < |d| \leq N \quad \textit{and} \quad \operatorname{rank}(E^d/\mathbb{Q}) = r\right\}}{2N} = \begin{cases} 1/2 & \textit{for } r = 0 \\ 1/2 & \textit{for } r = 1 \\ 0 & \textit{for } r \geq 2. \end{cases}$$

We make progress on this conjecture by studying 2^∞-Selmer groups. For an elliptic curve $E/\mathbb{Q}$, the 2^∞-Selmer group is defined as the kernel

$$\mathrm{Sel}^{2^\infty} E = \ker\left(H^1(G_\mathbb{Q}, E[2^\infty]) \to \prod_v H^1(G_v, E[2^\infty])/\mathscr{W}_v\right).$$

Here, $G_\mathbb{Q}$ denotes the absolute Galois group of $\mathbb{Q}$, the product is over all places v of $\mathbb{Q}$, the group G_v is the absolute Galois group for the local field $\mathbb{Q}_v$, and $\mathscr{W}_v$ denotes the Bloch–Kato set of local conditions [1]. Explicitly, $\mathscr{W}_v$ the set of unramified classes at good primes for E besides 2, is 0 at bad primes besides 2, and is something more complicated at 2.

Define the 2^k-Selmer rank $r_{2^k}(E)$ to be the maximal integer r so $(\mathbb{Z}/2^k\mathbb{Z})^r$ is a subgroup of $\mathrm{Sel}^{2^\infty}(E)$, and take $r_{2^\infty}(E)$ to be the limit of the $r_{2^k}(E)$. Then $r_{2^\infty}(E) \geq \operatorname{rank}(E)$, and it is conjectured that $r_{2^\infty}(E) = \operatorname{rank}(E)$. Our main result for elliptic curves is the following:

Theorem 2. *Take $E/\mathbb{Q}$ to be an elliptic curve satisfying one of the technical conditions enumerated at the start of Section 0.2. Then*

$$\lim_{N\to\infty} \frac{\#\left\{d \,:\, 0 < |d| \leq N \quad \textit{and} \quad r_{2^\infty}(E^d/\mathbb{Q}) = r\right\}}{2N} = \begin{cases} 1/2 & \textit{for } r = 0 \\ 1/2 & \textit{for } r = 1 \\ 0 & \textit{for } r \geq 2. \end{cases}$$

0.1. **Controlling 2-Selmer ranks.** We prove Theorem 2 by finding the distribution of each 2^k-Selmer rank in turn, starting with the 2-Selmer rank. Given two primes p, q, we define a symbol $[p, q]$ that generalizes the Legendre symbol. We also define a class $[p]$, which describes the splitting behavior of p in $\mathbb{Q}(E[2])$.

Given positive squarefree integers $d = p_1 \dots p_r$ and $d' = p'_1 \dots p'_r$, we find that the 2-Selmer groups of E^d and $E^{d'}$ are isomorphic if $[p_i] = [p'_i]$ and $[p_i, p_i] = [p'_i, p'_i]$ for all $i \leq r$, and if $[p_i, p_j] = [p'_i, p'_j]$ for all $i < j \leq r$.

Because of this proposition, it is convenient to restrict our attention to a grid of twists. Fix $r > 0$ and classes $\sigma_1, \dots, \sigma_r$, and choose disjoint sets of primes $X_1, \dots, X_r$ so all X_k lie in class σ_k for $k \le r$. We say d lies in the grid $X = \prod_{k=1}^{r} X_k$ if $d = p_1 \dots p_r$ for some $p_1 \in X_1, \dots, p_r \in X_r$.

We are also able to generalize the following result of Jutila to our definition of symbols.

Proposition 3 ([3]). *Given disjoint sets X_1, X_2 of primes, take $H_1 = \max(X_1)$, $H_2 = \max(X_2)$. Then*

$$\left| \sum_{p \in X_1} \sum_{q \in X_2} \left(\frac{p}{q}\right) \right| = C \cdot H_1 H_2 \left(H_1^{-1/5} + H_2^{-1/5} \right)$$

where C is some absolute constant.

Our approach to controlling 2-Selmer groups is to carve the set of positive squarefree integers less than a given H into a set of grids with negligible leftovers, and then to control the 2-Selmer groups on each grid using a combination of our generalization of Jutila's proposition and the Chebotarev density theorem.

For any grid X, we can find a lower bound $r_{2,\min}(X, E)$ for $r_2(E)$ over X. For some grids and some elliptic curves, this lower bound can be quite large [4]. However, in all cases, we can find an isogenous curve E' to E so $r_{2,\min}(X, E') = 0$; this works just as well with the elliptic curve replaced by an abelian variety. This trick allows us to prove the following coarse result.

Theorem 4. *There is an absolute $C > 0$ so, for any abelian variety $A/\mathbb{Q}$, we have*

$$\sum_{d < H} \exp(\operatorname{rank}(A^d)) \le H \cdot e^{Cg^2}$$

for $H \gg_A 0$, where $g = \dim A$.

0.2. **Higher Selmer groups.** We need a finer result about the 2-Selmer group to deal with 4-Selmer groups and higher. For elliptic curves, we have such a fine result if

(1) $E(\mathbb{Q})[2] = 0$; or
(2) $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$ and, writing $\phi : E \to E_0$ for the unique isogeny of degree 2 over $\mathbb{Q}$, we have

$$\mathbb{Q}(E_0[2]) \ne \mathbb{Q} \quad \text{and} \quad \mathbb{Q}(E_0[2]) \ne \mathbb{Q}(E[2]); \quad \text{or}$$

(3) $E(\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$ and E has no cyclic degree 4 isogeny defined over $\mathbb{Q}$.

We will state our explicit result for the distribution of $r_2, r_4, r_8, \dots$ for curves obeying the first or third condition here. In the second case, the 2-Selmer group is large for half of the twists of E, and this complicates the distributional result.

Definition 5. Given $n \geq j \geq 0$, take

$$P^{\mathrm{Alt}}(j \,|\, n)$$

to be the probability that a a uniformly selected alternating $n \times n$ matrix with entries in $\mathbb{F}_2$ has kernel of rank exactly j. We also will define

$$P^{\mathrm{Alt}}(j \,|\, \infty) = \frac{1}{2} \lim_{n \to \infty} P^{\mathrm{Alt}}(j \,|\, 2n + j)$$

Theorem 6. *Suppose $E/\mathbb{Q}$ is an elliptic curve that fits into either the first or third case mentioned above. Given $k \geq 1$ and any sequence of integers*

$$r_2 \geq r_4 \geq \cdots \geq r_{2^k} \geq 0,$$

we have

$$\lim_{N \to \infty} \frac{\#\{d \,:\, 0 < |d| < N,\ r_2(E^d) = r_2,\ \ldots\ r_{2^k}(E^d) = r_{2^k}\}}{2N} = P^{\mathrm{Alt}}(r_{2^k} \big| r_{2^{k-1}}) \cdot P^{\mathrm{Alt}}(r_{2^{k-1}} \big| r_{2^{k-2}}) \cdot \cdots \cdot P^{\mathrm{Alt}}(r_4 \big| r_2) \cdot P^{\mathrm{Alt}}(r_2 \big| \infty).$$

These statistics correctly suggest that there is an alternating pairing on the 2-Selmer group of E whose kernel K has dimension $r_4(E)$; that there is an alternating pairing on K whose kernel has dimension $r_8(E)$; etc. These pairings are instances of the Cassels–Tate pairing. Once the 2-Selmer portion of the above theorem has been established, the rest is proved by showing that these pairings are equidistributed among alternating matrices.

Over the set of all twists $d < H$, it is not meaningful to ask for the Cassels–Tate pairings of the curves E^d be equidistributed, since we lack a method for identifying the 2-Selmer groups throughout this family. However, by restricting our scope to the set of twists in a grid X where all classes and symbols are fixed, we enter a situation where the 2-Selmer groups are all isomorphic and where it does make sense to ask if the Cassels–Tate pairings are equidistributed. With enough assumptions, we are able to prove the equidistribution result, establishing the theorem.

We finally will mention the exercise that started our sequence of lectures.

Definition 7. Given a group G acting on an abelian group M and a homomorphism $\chi : G \to \{\pm 1\}$, there is a unique G-module M^χ and isomorphism $\beta^\chi : M^\chi \to M$ of abelian groups so

$$\beta^\chi(\sigma m) = \chi(\sigma)\sigma\beta^\chi(m)$$

for all σ in G and m in M. This is known as the quadratic twist of the module M.

For example, for any nonzero integer d, we may define $\chi_d : G_{\mathbb{Q}} \to \{\pm 1\}$ so $\chi_d(\sigma) = \sigma(\sqrt{d})/\sqrt{d}$ for all $\sigma \in G_{\mathbb{Q}}$. Choose an elliptic curve $E/\mathbb{Q}$. If we take $M = E\left(\overline{\mathbb{Q}}\right)$, then we have

$$M^{\chi_d} \cong E^d\left(\overline{\mathbb{Q}}\right).$$

Exercise 8. Given $n > 1$ and $H > 0$, what is the smallest $G_{\mathbb{Q}}$-module N so that, for any positive integer d less than H, there is an equivariant embedding

$$\left(\tfrac{1}{n}\mathbb{Z}/\mathbb{Z}\right)^{\chi_d} \hookrightarrow N?$$

- For $n = 2$, $N = \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ suffices, since $\chi_d(\sigma) \equiv 1 \mod 2$.
- For $n = 3$, we can do no better than

$$N = \left(\tfrac{1}{3}\mathbb{Z}/\mathbb{Z}\right) \oplus \bigoplus_{\substack{d<H \\ d \text{ squarefree}}} \left(\tfrac{1}{3}\mathbb{Z}/\mathbb{Z}\right)^{\chi_d},$$

  which has dimension around $\frac{6}{\pi^2}H$. This sort of behavior continues for all odd n.
- For $n = 4$, the module

$$N = \left(\tfrac{1}{4}\mathbb{Z}/\mathbb{Z}\right) \oplus \bigoplus_{\substack{p<H \\ p \text{ prime}}} \left(\tfrac{1}{4}\mathbb{Z}/\mathbb{Z}\right)^{\chi_p}$$

  suffices. This has dimension around $H/\log H$ by the prime number theorem. Higher powers of two lead to similarly small dimensions for N.

This exercise leads us to the following heuristic for identifying arithmetic-statistical problems that could plausibly be solved using methods like ours.

Heuristic 9. *Given finite $G_{\mathbb{Q}}$ modules $M_1, M_2, \ldots$ decorated with some local conditions, we have hope that we can find the distribution of*

$$\operatorname{Sel} M_1, \operatorname{Sel} M_2, \ldots$$

if

$$\frac{\log \# N_H}{\sum_{i<H} \log \# M_i}$$

tends to 0*, where N_H is the minimal $G_{\mathbb{Q}}$ module containing $M_1, \ldots, M_H$ as subquotients.*

References

[1] Spencer Bloch and Kazuya Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift, Springer, 2007, pp. 333–400. MR1086888

[2] Dorian Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Number theory, Carbondale 1979, Springer, 1979, pp. 108–118.

[3] Matti Jutila, *On mean values of Dirichlet polynomials with real characters*, Acta Arithmetica **27** (1975), no. 1, 191–198.

[4] Zev Klagsbrun and Robert J. Lemke Oliver, *The distribution of the Tamagawa ratio in the family of elliptic curves with a two-torsion point*, Res. Math. Sci. **1** (2014), Art. 15, 10.

Effective height bounds for odd-degree totally real points on some curves

Levent Alpöge

My talk was on the following theorem.

Theorem. *There is a finite-time algorithm (i.e. Turing machine which terminates on all inputs) which, on input $(K, C/K)$ with $K/\mathbb{Q}$ totally real of odd degree and C/K a smooth projective hyperbolic curve which admits a map defined over K to a Hilbert modular variety, outputs $C(K)$.*

Just for concreteness, what follows is an example application. The relevant family of abelian varieties is the hypergeometric family corresponding to the triangle group $\Delta(3,6,6)$ (which is, crucially, arithmetic).

Theorem. *Let $a \in \overline{\mathbb{Q}}^{\times}$ be totally real of odd degree (e.g. $a = 1$). Then: there is a finite-time algorithm which, on input K with $K/\mathbb{Q}(a)$ totally real of odd degree, outputs the finitely many pairs (x, y) with $x, y \in K$ and $x^6 + 4y^3 = a^2$.*

In what remains we will describe the argument, keeping the ideas and also the points which led to the hypotheses on the number fields and curves in consideration, and dropping the usual mass of notation.

Parshin's reduction of the Mordell conjecture to Shafarevich's finiteness conjecture for abelian varieties uses a construction of Kodaira to produce, for a smooth projective hyperbolic curve C/K, a finite-to-one map $C \to A_g$ for some $g \in \mathbb{Z}^+$ (not the genus of C/K), without loss of generality defined over K. Letting $\mathcal{C}/\mathfrak{o}_K$ be the minimal proper regular model of C/K, this extends to a map $\mathcal{C} \to \mathcal{A}_g$ defined over $\mathfrak{o}_{K,S}$ once S is explicitly sufficiently large, and thus produces a finite-to-one map $C(K) = \mathcal{C}(\mathfrak{o}_{K,S}) \to \mathcal{A}_g(\mathfrak{o}_{K,S})$, the first equality by compactness (and since S is explicitly sufficiently large).

Rather than use Kodaira's family, we begin with curves mapping to a Hilbert modular variety. Thus the same argument reduces us to considering S-integral K-points on a Hilbert modular variety, and thus to considering abelian varieties A/K with $\mathfrak{o} \hookrightarrow \mathrm{End}_K(A)$ with $\mathrm{rk}_{\mathbb{Z}}(\mathfrak{o}) = \dim A$ ("of $\mathrm{GL}_2(\mathfrak{o})$-type over K") with good reduction outside S, treating $(\mathfrak{o}, K, S)$ as given. To effectivize Faltings' argument, we must find all such abelian varieties in finite time.

We do this by using potential modularity *and* a standard construction of motives out of automorphic forms. This second point forces us to further impose that K is totally real of odd degree (the first would only require K CM [1]).

So now let us describe how to find all A/K of $\mathrm{GL}_2(\mathfrak{o})$-type over K with good reduction outside S. Let us first explain how to find all such A/K which are modular over K. This means that one of the degree two L-functions of A (associated to a λ-adic Tate module $T_\lambda(A)$) matches the L-function of a parallel weight two Hilbert modular eigencuspform, say f. It is standard (and due to Hida [3]) that there is a quotient of the Jacobian of an explicit Shimura curve (depending on K and S) which is also of GL_2-type over K with a degree two L-function matching $L(s, f)$. So by Faltings' proof of the Tate conjecture for endomorphisms of abelian

varieties it follows that A/K is a K-isogeny factor of an explicit abelian variety B/K (namely a bounded power of said Jacobian).

But then $h(A)$ is explicitly bounded: $B \sim_K A \times A'$ by Poincaré complete reducibility, whence $h(A) + h(A') = h(A \times A') \ll_{h(B),[K:\mathbb{Q}],\dim B} 1$ by Masser-Wüstholz [5] (Raynaud's isogeny estimate would also suffice). But $h(A') \gg -\dim A' \geq -\dim B$ by Bost, so $h(A) \ll_{h(B),K,\dim B} 1$.

So it remains to show that, given $(\mathfrak{o}, K, S)$, we may compute in finite time a finite set $\mathcal{F}$ of odd-degree totally real L/K such that all relevant A/K are modular over some $L \in \mathcal{F}$.

We first effectivize work of Dimitrov [2] to prove that, once $\operatorname{Nm}\mathfrak{p} \gg_{\mathfrak{o},K,S} 1$ (explicit implied constant), the two-dimensional mod-$\mathfrak{p}$ residual representation associated to an abelian variety A/K of $\mathrm{GL}_2(\mathfrak{o})$-type over K with good reduction outside S has large image (i.e. containing a conjugate of $\mathrm{SL}_2(\mathbb{F}_p)$). So we may pick an explicit such $\mathfrak{p}$ and then produce the explicit finite set of residual representations that could possibly arise (Hermite-Minkowski finiteness). Writing $\overline{\rho}$ for one such, following Taylor's proof of his potential modularity theorem it remains only to produce[1] a totally real Galois extension $\widetilde{L}/K$ such that a particular subvariety of projective space $X_{\overline{\rho}} \hookrightarrow \mathbb{P}^N_{/K}$ (a Hilbert modular variety with level structure depending on $\overline{\rho}$ and another chosen auxiliary $\mathfrak{p}' \neq \mathfrak{p}$) has $X_{\overline{\rho}}(\widetilde{L}) \neq \emptyset$. This can be done by a finite-time algorithm: as Taylor proves, there is *some* such $\widetilde{L}/K$ by a theorem of Moret-Bailly [6], so therefore e.g. a brute force search through all totally real points of larger and larger height and degree will terminate in finite time.

So we produce a finite list of totally real Galois extensions $\widetilde{L}/K$ such that all relevant A/K are modular over some $\widetilde{L}/K$ in our list. Finally, as in Snowden's [7], by Langlands' solvable descent for GL_2 [4], if A/K is modular over $\widetilde{L}$ then it is modular over the odd-degree $\widetilde{L}^H$, where $H \subseteq \mathrm{Gal}(\widetilde{L}/K)$ is a 2-Sylow subgroup (thus solvable). This produces our desired $\mathcal{F}$ and we conclude.

References

[1] Patrick B. Allen, Frank Calegari, Ana Caraiani, Toby Gee, David Helm, Bao V. Le Hung, James Newton, Peter Scholze, Richard Taylor, and Jack A. Thorne. Potential automorphy over CM fields. 2018. https://arxiv.org/abs/1812.09999.

[2] Mladen Dimitrov. Galois representations modulo p and cohomology of Hilbert modular varieties. *Ann. Sci. École Norm. Sup. (4)*, 38(4):505–551, 2005.

[3] Haruzo Hida. On abelian varieties with complex multiplication as factors of the Jacobians of Shimura curves. *Amer. J. Math.*, 103(4):727–776, 1981.

[4] Robert P. Langlands. *Base change for* GL(2), volume 96 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1980.

[1] We are abbreviating a bit here: this is not quite the setup that arises in Taylor's argument, though the differences are immaterial (for example there is a bit more data that goes into defining $X_{\overline{\rho}}$, and it is not quite defined over K but over an explicit finite totally real extension K'/K — see Snowden's [7] (particularly his proof of his Proposition 5.3.1) for the precise construction which we follow).

[5] David Masser and Gisbert Wüstholz. Isogeny estimates for abelian varieties, and finiteness theorems. *Ann. of Math. (2)*, 137(3):459–472, 1993.
[6] Laurent Moret-Bailly. Groupes de Picard et problèmes de Skolem. I, II. *Ann. Sci. École Norm. Sup. (4)*, 22(2):161–179, 181–194, 1989.
[7] Andrew Snowden. On two dimensional weight two odd representations of totally real fields. 2009. https://arxiv.org/abs/0905.4266.

Integral points on punctured curves and punctured abelian varieties

Samir Siksek

1. A conjecture

The talk is intended to give some evidence for the following conjecture.

Conjecture 1 (S.)**.** *Let $X/\mathbb{Q}$ be a hyperbolic curve, and let $\mathcal{X}$ be a model over $\mathbb{Z}$. Let $n \geq 1$. Then*

$$\mathcal{X}(\mathcal{O}_K) \;=\; \mathcal{X}(\mathbb{Z})$$

for 100% of primitive number fields K of degree n, when ordered by discriminant.

There are some weak results towards this conjecture for $X = \mathbb{P}^1 - \{0, 1, \infty\}$ thanks to the efforts of Triantafillou [5] and others [1], [2], [3]. Our talk is based on [4] and concerned with punctured curves of genus ≥ 1.

Let $C/\mathbb{Q}$ be a smooth projective curve of genus ≥ 1, and let J be the Jacobian of C. Let $Q_0 \in C(\mathbb{Q})$, and consider the punctured curve $C - Q_0$. This is a curve of Euler characteristic $1 - 2g < 0$ and therefore hyperbolic. It is natural to study the integral points on X using the Abel–Jacobi map

$$C \to J, \qquad Q \mapsto [Q - Q_0].$$

An integral point on $C - Q_0$ is sent via the Abel–Jacobi map to an integral point on $J - 0$. In view of this we study integral points on abelian varieties punctured at the origin.

2. A theorem for punctured abelian varieties

Theorem 2 (S.)**.** *Let ℓ be a rational prime. Let A be an abelian variety defined over $\mathbb{Q}$. Suppose that*

(i) $A(\mathbb{Q}) = 0$;
(ii) There is $p \equiv 1 \pmod{\ell}$ of good reduction for A such that $\ell \nmid \#A(\mathbb{F}_p)$.

Then $(A - 0)(\mathcal{O}_K) = \emptyset$ for 100% of cyclic degree ℓ number fields K.

Example 3. Let

$$C/\mathbb{Q} \;:\; y^2 + (x+1)y = x^5 - 55x^4 - 87x^3 - 54x^2 - 16x - 2.$$

This is a curve of genus 2 with `LMFDB` label `8969.a`. We let $A = J$ be the Jacobian of C. From the `LMFDB` we learn that $A(\mathbb{Q}) = 0$. We checked that condition (ii) is satisfied for all primes ℓ with the help of an algorithm of Dieulefait for checking the surjectivity of mod ℓ representations of genus 2 Jacobians. From the theorem we have the following conclusions.

- Fix a prime ℓ. Then $(A-0)(\mathcal{O}_K) = \emptyset$ for 100% of cyclic degree ℓ number fields K.
- Fix a prime ℓ. Then $(C-\infty)(\mathcal{O}_K) = \emptyset$ for 100% of cyclic degree ℓ number fields K.

References

[1] N. Freitas, A. Kraus and S. Siksek, *On Asymptotic Fermat over $\mathbb{Z}_p$ extensions of $\mathbb{Q}$*, Algebra & Number Theory **14** (2020), No. 9, 2571–2574.

[2] N. Freitas, A. Kraus and S. Siksek, *The unit equation over cyclic number fields of prime degree*, Algebra & Number Theory, to appear.

[3] 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, 1–5.

[4] S. Siksek, *Integral points on punctured abelian varieties*, `arXiv:2105.00570`.

[5] N. Triantafillou, *The unit equation has no solutions in number fields of degree prime to 3 where 3 splits completely*, `arXiv:2003.02414`.

Low degree points and linear configurations

Borys Kadets

(joint work with Isabel Vogt)

Let k be a number field, and let X/k be a nice (smooth, proper, geometrically irreducible) algebraic curve. The following natural question is an extension of Mordell's conjecture.

Question. Given an integer d and a nice curve X, is the number of degree d points on X finite or infinite?

If the curve X is fixed and the number d is large, then having a single degree d point is equivalent to having infinitely many of them (by Riemann-Roch and Hilbert's irreducibility). Therefore, the question has an answer in terms of the index of the curve.

If we think of d as being fixed and allow X to vary, the question has a different flavor.

Definition. The arithmetic degree of irrationality $\mathrm{a.irr}_k X$ of a nice curve X over a number field k is the minimal d such that X has infinitely many points of degree d.

For example, if X is a degree d cover of $\mathbb{P}^1$, then pulling back rational points from $\mathbb{P}^1$ gives an infinite family of degree d points on X, and so $\mathrm{a.irr}_k X \leqslant d$. Similarly, the arithmetic irrationality is bounded by d for degree d covers of elliptic curves of positive rank. Harris and Silverman [3] and Abramovich and Harris [1] showed that the converse holds for $d = 2$ and $d = 3$ respectively, at least after extending the base field. However Debarre and Fahlaoui [2] showed that for $d \geqslant 4$ curves can have infinitely many degree d without being low degree covers of $\mathbb{P}^1$ or elliptic curves. The existence of these examples makes analyzing arithmetic irrationality a challenging problem.

In a work in progress, joint with Isabel Vogt, we developed a method for analyzing arithmetic irrationality using geometry of subspace configurations. The methods allow us to prove a number of new results.

Theorem 1 (K. - Vogt)**.** *Suppose* $\text{a.irr}\, X = d$*. Then one of the following holds:*

(1) There exists a covering $f : X \to Y$ *of degree* $m \geqslant 2$ *such that* $\text{a.irr}\, Y = d/m$*;*

(2) The genus of X *satisfies* $g \leqslant \frac{d(d-1)}{2} + 1$*.*

Note that in case (1) there is a clear reason for X to have infinitely many degree d points: they can be obtained as pullbacks of low degree points on Y under f. Theorem 1 is a generalization of the results of Harris-Silverman [3] and Abramobich-Harris [1], who handled the cases $d = 2$ and $d = 3$ respectively. Debarre and Fahlaoui [2] proved that for $d \geqslant 4$ there exists curves of genus $\frac{d(d-1)}{2} + 1$ that do not have maps of degree less than d to other curves; thus case 2 of Theorem 1 does occur and the genus bound is optimal.

Theorem 1 is proved by attaching to every curve of arithmetic irrationality d a certain discrete-geometric invariant: an algebraic family of linear configurations in projective spaces. By carefully studying the combinatorics and geometry of these configurations we can shed light on the geometry of low degree points. For example, this invariant includes a sequence of numbers r_i, $i = 2, 3, ...$ which describe dimensions of the relevant linear spaces. For the purposes of this abstract the exact definition of r_i does not matter, but the usefullness of these invariants can be demonstrated by the following finer classification of curves of arithmetic irrationality d.

Theorem 2 (K.-Vogt)**.** *Suppose* X/k *has arithmetic irrationality* d*. Then one of the following holds:*

(1) $r_2 = 1$ *and* X *is a degree* d *cover of an elliptic curve of positive rank;*

(2) $r_2 \geqslant 2$*, and there exists a covering* $f : X \to Y$ *of degree* $m \geqslant 2$ *such that* $\text{a.irr}\, Y = d/m$*;*

(3) $r_2 = 2$ *and* X *is a curve of Debarre-Fahlaoui type*[1] *(see* [2]*);*

(4) $r_2 > 2$ *and the genus of* X *satisfies* $g \leqslant \frac{(d-1)(d-2)}{2} + 2$*.*

In particular, the construction of Debarre-Fahlaoui [2] can be naturally arrived at by studying configurational invariants.

References

[1] Dan Abramovich, and Joe Harris, *Abelian varieties and curves in* $W_d(C)$. Compositio Mathematica **78.2** (1991): 227–238.

[2] Olivier Debarre and Rachid Fahlaoui, *Abelian varieties in* $W^r_d(C)$ *and points of bounded degree on algebraic curves.* Compositio Mathematica **88.3** (1993): 235-249.

[3] Joe Harris and Joe Silverman, *Bielliptic curves and symmetric products.* Proceedings of the American Mathematical Society **112.2** (1991): 347–356.

[1] a straightforward generalization of the construction in [2]; these do *not* necessarily have genus $\frac{d(d-1)}{2}$

A geometric approach to the Cohen-Lenstra heuristics

Aaron Landesman

It is well known to experts that moduli spaces exist whose integer points parameterize n-torsion elements in class groups of quadratic number fields. In particular, counting points of bounded height on these spaces is tantamount to solving cases of the Cohen-Lenstra heuristics. We explain why many of these moduli spaces have the following relatively simple form: They are the quotient of the complement of a hypersurface in affine space by the action of an algebraic group. We will also describe how this lets us view n-torsion in class groups of quadratic fields as n-Selmer groups of singular genus 1 curves.

This investigation is motivated by the Cohen-Lenstra heuristics, which describe the average number of n-torsion elements in class groups of quadratic number fields. It is an important open question in arithmetic statistics to count the asymptotic number of these n-torsion elements in quadratic fields.

A simple-to-state consequence of our approach is the following:

Theorem 1 Under the correspondence between quadratic forms and line bundles on spectra of rings of integers of quadratic fields, a quadratic form q corresponds to an n-torsion line bundle if and only if there exists a degree n homogeneous polynomial $f := \sum_{i=0}^{n} t_i x^i y^{n-i} \in \mathbb{Z}[x, y]$ whose resultant with q is ± 1, where the resultant is defined below in (1).

In fact, our approach gives a more precise parameterization of n-torsion elements in quadratic fields, as detailed in [1, Theorem 1.3]. Namely, n-torsion elements in class groups of varying quadratic extensions of $\mathbb{Z}$ are in bijection with $\mathbb{Z}$ points of the quotient stack $[U/G]$, with U and G defined as follows. Consider the affine space $\mathbb{A}_{\mathbb{Z}}^{3+(n+1)}$ parameterizing the coefficients $(a, b, c), (t_0, \ldots, t_n)$, where a, b, c are the coefficients of a quadratic form $q := ax^2 + bxy + cy^2$ and t_i are the coefficients of a degree n binary form $f := \sum_{i=0}^{n} t_i x^i y^{n-i}$. Then, define U as the complement of the hypersurface $\mathrm{Res}(q, f) = 0$, where $\mathrm{Res}(q, f)$ denotes the resultant given as the determinant of the matrix

$$\mathrm{Res}(q, f) := \begin{pmatrix} a & 0 & \cdots & 0 & t_0 & 0 \\ b & a & \cdots & 0 & t_1 & t_0 \\ c & b & \ddots & 0 & t_2 & t_1 \\ \vdots & \vdots & \ddots & 0 & \vdots & \vdots \\ 0 & 0 & \ddots & 0 & t_{n-2} & t_{n-3} \\ 0 & 0 & \ddots & a & t_{n-1} & t_{n-2} \\ 0 & 0 & \ddots & b & t_n & t_{n-1} \\ 0 & 0 & \cdots & c & 0 & t_n \end{pmatrix}. \tag{1}$$

The group G is most naturally realized as the automorphism group of the Hirzebruch surface $\mathrm{Proj}_{\mathbb{P}^1}(\mathcal{O}_{\mathbb{P}^1}(2) \oplus \mathcal{O}_{\mathbb{P}^1}(n))$. It can also be explicitly described as generated by the actions of $\mathbb{G}_m, \mathrm{GL}_2, \mathbb{G}_a^{n-1}$, where $\lambda \in \mathbb{G}_m$ acts by sending $(q, f) \mapsto$

$(\lambda q, \lambda f)$, $g \in \mathrm{GL}_2$ acts by sending $(q(x,y), f(x,y)) \mapsto \frac{1}{\det(g)} \cdot (q(gx,gy), f(gx,gy))$ and $(\alpha_0, \ldots, \alpha_{n-2}) \in \mathbb{G}_a^{n-1}$ sends $(q,f) \mapsto (q, f + \sum_{i=0}^{n-2} \alpha_i x^i y^{n-2-i} q)$.

It turns out there is a nearly equivalent description of the above quotient stack, which we describe next. Let S denote the secant variety to the rational normal curve in $\mathbb{P}^n$, and let $W \subset S$ denote the open subscheme where one removes the rational normal curve. Then, then $[U/G]$ can be identified with $[W/\mathrm{PGL}_2]$, acting as automorphisms of the rational normal curve, see [2, Proposition 6.1.1].

Given the above relatively simple moduli spaces, it is natural to ask whether there is any way to use them to count n-torsion elements in class groups of quadratic fields.

Question 2 Is it possible to use these moduli spaces to obtain bounds on the asymptotic number of n-torsion elements in class groups of quadratic fields?

The above moduli spaces are in fact closely connected to Selmer groups of certain singular genus 1 curves, or equivalently Selmer groups of tori which are the smooth locus of these singular genus 1 curves. More precisely, suppose we start with a degree 2 cover $g : \operatorname{Spec} \mathcal{O}_K \to \operatorname{Spec} \mathbb{Z}$. One can then relate $\mathrm{Cl}(\mathcal{O}_K)[n]$ to the n-Selmer group of the relative dimension 1 torus $g_* \mathbb{G}_m / \mathbb{G}_m$ as in [1, Lemma 10.2].

Example 3 In the case that $n = 3$, the moduli space $[U/G]$ described above parameterizes G-orbits of pairs (q,f) where $q = ax^2 + bxy + cy^2$ and $f = t_0x^3 + t_1x^2y + t_2xy^2 + t_3y^3$. Associated to this, one can form the singular genus 1 curve given as the vanishing locus of $zq + f = z(ax^2 + bxy + cy^2) + (t_0x^3 + t_1x^2y + t_2xy^2 + t_3y^3)$ in $\mathbb{P}^2_{[x,y,z]}$. This is singular at at the point $x = y = 0$. By chasing various cohomological exact sequences as in [1, Lemma 10.2], one can relate the n-Selmer group of the relative Jacobian of this genus 1 curve to the n-torsion in the class group of the quadratic extension whose discriminant is $b^2 - 4ac$.

The above observation that class groups of quadratic fields can be described in terms of Selmer groups of 1-dimensional tori suggests the following question.

Question 4 Can one create a unified set of heuristics which govern n-Selmer groups of (not necessarily proper) algebraic groups that also imply the Cohen-Lenstra-Martinet heuristics for class groups of number fields?

References

[1] A. Landesman, *A geometric approach to the Cohen-Lenstra heuristics*, https://arxiv.org/abs/2106.10357v1, (2021).
[2] A. Landesman, *A thesis of minimal degree: two*, Thesis (Ph.D.)–Stanford University, (2021).

On pairs of 17-congruent elliptic curves

Tom Fisher

Elliptic curves E_1 and E_2 are *n-congruent* if their n-torsion subgroups $E_1[n]$ and $E_2[n]$ are isomorphic as Galois modules. We say that a congruence is *trivial* if it is arises from an isogeny (of degree coprime to n). Frey and Mazur conjectured that for n sufficiently large there are no non-trivial n-congruences between elliptic curves defined over the rationals. With the aim of refining their conjecture, we look for examples with n as large as possible, concentrating on the case n is prime.

It is natural to classify congruences not just by their level n, but by their power k, where an n-congruence has *power* k if it raises the Weil pairing to the power k. We write $X_E(n,k)$ for the curve parametrising all elliptic curves n-congruent with power k to a given elliptic curve E, and $Z(n,k)$ for the surface parametrising all pairs of elliptic curves that are n-congruent with power k. Composing a congruence with multiplication by an integer multiplies k by a square, so when n is an odd prime, there are just two cases: if k is a quadratic residue mod n then we say the congruence is *symplectic*, otherwise it is *anti-symplectic*.

Equations for $X_E(7,1)$ and $X_E(7,3)$, depending on the coefficients a and b of a Weierstrass equation for E, were computed by Halberstadt and Kraus [HK] and Poonen, Schaefer and Stoll [PSS]. From these it follows [C], [F2] that $Z(7,1)$ is rational, and $Z(7,3)$ is birational to the elliptic K3-surface

$$y^2 = x^3 + (4T^4 + 4T^3 - 51T^2 - 2T - 50)x^2 + (6T + 25)(52T^2 - 4T + 25)x.$$

Equations for $X_E(11,1)$ and $X_E(11,2)$ were computed by Fisher [F1]. From these it follows [F2] that $Z(11,1)$ is birational to the properly elliptic surface

$$y^2+(T^3+T)xy = x^3-(4T^5-17T^4+30T^3-18T^2+4)x^2+T^2(2T-1)(3T^2-7T+5)^2x.$$

According to Kani and Schanz [KS], the surface $Z(11,2)$ and all the surfaces $Z(n,k)$ for $n \geqslant 13$ are surfaces of general type. Equations for $Z(11,2)$, $Z(13,1)$ and $Z(13,2)$ were computed by Kumar [K] and Fisher [F3]. Each is a double cover of a rational surface, where the rational surface is the quotient $W(n,k)$ of $Z(n,k)$ by the involution that swaps over the two elliptic curves.

In [F4] we use invariant-theoretic arguments to compute the surfaces $Z(17,k)$ and $W(17,k)$ as quotients of $X(17) \times X(17)$. In particular we find that $W(17,1)$ and $W(17,3)$ are each birational to the elliptic K3-surface

$$y^2 + (T+1)(T-2)xy + T^3y = x^3 - x^2.$$

For each prime $p < 17$, the papers cited above show that there are infinitely many non-trivial pairs of p-congruent elliptic curves, both symplectic and anti-symplectic, and with infinitely many pairs of j-invariants. In contrast, searching for rational points on $Z(17,1)$ and $Z(17,3)$, we have only found two non-trivial 17-congruences: one symplectic and one anti-symplectic. The anti-symplectic pair, with conductors 3675 and 47775, was previously found by Cremona. The symplectic pair, with conductors 279809270 and 3077901970, is new. We conjecture that these examples (and their simultaneous quadratic twists) are the only non-trivial pairs of p-congruent elliptic curves for $p \geqslant 17$.

A further study of n-congruences for n composite is currently being made by my PhD student Sam Frengley. In particular he has extended ideas of Halberstadt [H] and Cremona and Freitas [CF] to give an example of an elliptic curve that is non-trivially 48-congruent to one of its quadratic twists.

I would like to thank Noam Elkies, Bjorn Poonen, Will Sawin and Michael Stoll for interesting discussions following my talk relating to the surfaces $W(17,1)$ and $W(17,3)$, and the fact that these surfaces are birational.

References

[C] Z. Chen, *Congruences of elliptic curves*, PhD thesis, University of Cambridge, 2016. http://zc231.user.srcf.net/Maths/PhDThesis.pdf

[CF] J.E. Cremona and N. Freitas, Global methods for the symplectic type of congruences between elliptic curves, to appear in *Rev. Mat. Iberoam.*, doi:10.4171/RMI/1269

[F1] T.A. Fisher, On families of 7- and 11-congruent elliptic curves, *LMS J. Comput. Math.* **17** (2014), no. 1, 536–564.

[F2] T.A. Fisher, Explicit moduli spaces for congruences of elliptic curves, *Math. Z.* **295** (2020), no. 3-4, 1337–1354.

[F3] T.A. Fisher, On families of 13-congruent elliptic curves, arXiv:1912.10777[math.NT]

[F4] T.A. Fisher, On pairs of 17-congruent elliptic curves, arXiv:2106.02033[math.NT]

[H] E. Halberstadt, Sur la courbe modulaire $X_{\text{ndép}}(11)$, *Experiment. Math.* **7** (1998), no. 2, 163–174.

[HK] E. Halberstadt and A. Kraus, Sur la courbe modulaire $X_E(7)$, *Experiment. Math.* **12** (2003), no. 1, 27–40.

[KS] E. Kani and W. Schanz, Modular diagonal quotient surfaces, *Math. Z.* **227** (1998), no. 2, 337–366.

[K] A. Kumar, Hilbert modular surfaces for square discriminants and elliptic subfields of genus 2 function fields, *Res. Math. Sci.* **2** (2015), Art. 24.

[PSS] B. Poonen, E.F. Schaefer and M. Stoll, Twists of $X(7)$ and primitive solutions to $x^2+y^3=z^7$, *Duke Math. J.* **137** (2007), no. 1, 103–158.

ℓ-adic images of Galois for elliptic curves over $\mathbb{Q}$

Andrew V. Sutherland

(joint work with Jeremy Rouse and David Zureick-Brown)

In joint work with Jeremy Rouse and David Zureick-Brown we obtain a conjecturally complete classification of the possible images of ℓ-adic Galois representations attached to an elliptic curve $E/\mathbb{Q}$ without complex multiplication [4]. This complements prior work of Rouse and Zureick-Brown, who determined the 2-adic images in [3], and of Sutherland and Zywina, who determined the ℓ-adic images that arise for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves in [5].

We exploit previous results that determine the rational points on several of the corresponding modular curves that we must consider; this notably includes the recent work of Balakrishnan et al. who determined the rational points on the modular curves $X_{\text{sp}}^+(13)$, $X_{\text{ns}}^+(13)$, $X_{S_4}(13)$ in [1, 2]. This still leaves several dozen modular curves whose rational points we must determine in order to obtain a complete classification, and we introduce a number of new techniques for doing so.

Aside from the ℓ-adic images known to arise for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves $E/\mathbb{Q}$, we find only 22 exceptional images that arise for any prime ℓ and any non-CM $E/\mathbb{Q}$. We conjecture that this list of exceptional images is complete, and show that any counterexamples must arise from unexpected rational points on $X_{\mathrm{ns}}^{+}(N)$ with $N = 3^3, 5^2, 7^2, 11^2$ or a prime $\ell \geq 17$, or one of two modular curves of level 49 and genus 9.

This yields a fast algorithm that takes as input a non-CM elliptic curve $E/\mathbb{Q}$ and outputs an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ for each prime ℓ where the representation $\rho_{E,\ell^\infty} \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ is nonsurjective. We have applied this algorithm to all of the non-CM elliptic curves in the LMFDB, as well as the non-CM elliptic curves in two larger databases that together contain approximately 380 million elliptic curves over $\mathbb{Q}$. We found no counterexamples to our conjecture.

A key ingredient to our work is a moduli-theoretic approach to counting $\mathbb{F}_p$-rational points on modular curves X_H. This allows us to quickly rule out $\mathbb{Q}$-rational points on modular curves that have no $\mathbb{F}_p$-rational points for some prime $p \neq \ell$. This applies to 11 of the arithmetically maximal curves we must consider, including one of genus 12 and one of genus 4 whose Jacobian has analytic rank 4. This point-counting algorithm also allows us to explicitly determine (with multiplicity) the weight-2 modular forms f whose corresponding modular abelian varieties A_f appear as simple isogeny factors of the Jacobian of X_H, and in particular, to determine its analytic rank. Here we rely on a joint result with John Voight that generalizes Ribet's observation that simple abelian varieties attached to weight-2 newforms on $\Gamma_1(N)$ are of GL_2-type; this extends Kolyvagin's theorem that analytic rank zero implies algebraic rank zero to isogeny factors of the Jacobian of X_H.

References

[1] Jennifer S. Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk, *Explicit Chabauty-Kim for the split Cartan modular curve of level* 13, Annals of Mathematics **189** (2019), 885–944.

[2] Jennifer S. Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk, *Quadratic Chabauty for modular curves: Algorithms and examples*, arXiv:2021.01862.

[3] Jeremy Rouse and David Zureick-Brown, *Elliptic curves over* $\mathbb{Q}$ *and* 2*-adic images of Galois*, Research in Number Theory **1** (2015), article 12, 34 pages.

[4] Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown (and an appendix with John Voight), *ℓ-adic images of Galois for elliptic curves over* $\mathbb{Q}$, arXiv:2106.11141.

[5] Andrew V. Sutherland and David Zywina, *Modular curves of prime-power level with infinitely many rational points*, Algebra and Number Theory **5** (2017), 1199–1229.

Recent progress on deterministic integer factorisation

David Harvey
(joint work with Markus Hittmeir)

We consider integer factorisation algorithms that are *deterministic* and whose time complexity bounds have been *rigorously established*. These requirements exclude many well-known factoring algorithms such as the Number Field Sieve [CP05, §6.2], the Elliptic Curve Method [Len87], rigorous randomised variants of the class group approach [LP92], and quantum factoring algorithms [Sho94].

Unfortunately, all known rigorous deterministic algorithms for factoring an integer N run in fully exponential time, i.e., in time $N^{C+o(1)}$ for some $C > 0$. The first improvement on the ancient trial division algorithm ($C = \frac{1}{2}$) was Lehman's $C = \frac{1}{3}$ algorithm [Leh74]. (Is it unclear to this author whether Shanks' slightly earlier $C = \frac{1}{4}$ algorithm [Sha71] was fully rigorous.) Shortly afterwards, Pollard [Pol74] and Strassen [Str77] gave two closely related algorithms achieving $C = \frac{1}{4} = 0.25$, and somewhat later Coppersmith gave yet another algorithm [Cop96] achieving $C = \frac{1}{4}$.

The exponent remained stuck at $C = \frac{1}{4}$ for over 40 years, until the very recent breakthrough of Hittmeir [Hit21], who managed to push the exponent down to $C = \frac{2}{9} = 0.222\ldots$. The present author [Har20] subsequently simplified and improved Hittmeir's algorithm, achieving $C = \frac{1}{5} = 0.2$. Roughly speaking, the new algorithms combine ideas from Lehman's and Pollard's algorithms mentioned above. The best current bit-complexity bound, established in joint work of Hittmeir and the present author [HH21], is

$$O\left(\frac{N^{1/5}(\log N)^{16/5}}{(\log\log N)^{3/5}}\right).$$

It seems likely that the power of $\log N$ can be further improved.

We give a brief sketch of the new algorithms. Assume for simplicity the hardest case, where N is a product of distinct primes $p, q \asymp N^{1/2}$. Using the theory of Diophantine approximation, there (usually) exist integers $a, b \ll N^{1/10}$ such that

$$\frac{a}{b} = \frac{p}{q}(1+\epsilon), \qquad \epsilon \ll N^{-1/5}.$$

A brief calculation then shows that

$$aq + bp - \lfloor 2\sqrt{abN} \rfloor = j \qquad \text{for some } j \ll N^{1/5}.$$

Let $\alpha \in (\mathbb{Z}/N\mathbb{Z})^*$; then Fermat's little theorem yields

$$\alpha^{aN+b-\lfloor 2\sqrt{abN}\rfloor} \equiv \alpha^j \pmod{p}.$$

This may be regarded as a collision modulo p between two subsets of $\mathbb{Z}/N\mathbb{Z}$: the "giant steps" $\alpha^{aN+b-\lfloor 2\sqrt{abN}\rfloor}$ ranging over $a, b \ll N^{1/10}$, and the "baby steps" α^j ranging over $j \ll N^{1/5}$. We now form the polynomial

$$f(x) = \prod_{a,b}(x - \alpha^{aN+b-\lfloor 2\sqrt{abN}\rfloor}) \in (\mathbb{Z}/N\mathbb{Z})[x],$$

and evaluate it at the points $x = \alpha^j$ for $j \ll N^{1/5}$. Computing the GCDs of these values with N enables us to discover the collision alluded to above, provided that α has sufficiently large multiplicative order. This in turn reveals a and b, and then immediately p and q.

To turn this sketch into a rigorous algorithm, there are several technical issues to address, notably, dealing with the parenthetical "usually" in the paragraph above, and deterministically finding an α of sufficiently large order. Both of these problems admit satisfactory solutions.

References

[Cop96] D. Coppersmith, *Finding a small root of a bivariate integer equation; factoring with high bits known*, Advances in cryptology—EUROCRYPT '96 (Saragossa, 1996), Lecture Notes in Comput. Sci., vol. 1070, Springer, Berlin, 1996, pp. 178–189. MR1421585

[CP05] R. Crandall and C. Pomerance, *Prime Numbers: a Computational Perspective*, second ed., Springer, New York, 2005. MR2156291 (2006a:11005)

[Har20] D. Harvey, *An exponent one-fifth algorithm for deterministic integer factorisation*, to appear in Mathematics of Computation, arXiv preprint `https://arxiv.org/abs/2010.05450`, 2020.

[HH21] D. Harvey and M. Hittmeir, *A log-log speedup for exponent one-fifth deterministic integer factorisation*, arXiv preprint `https://arxiv.org/abs/2105.11105`, 2021.

[Hit21] M. Hittmeir, *A time-space tradeoff for Lehman's deterministic integer factorization method*, Math. Comp. **90** (2021), no. 330, 1999–2010. MR4273122

[Leh74] R. S. Lehman, *Factoring large integers*, Math. Comp. **28** (1974), 637–646. MR340163

[Len87] H. W. Lenstra, Jr., *Factoring integers with elliptic curves*, Ann. of Math. (2) **126** (1987), no. 3, 649–673. MR916721

[LP92] H. W. Lenstra, Jr. and C. Pomerance, *A rigorous time bound for factoring integers*, J. Amer. Math. Soc. **5** (1992), no. 3, 483–516. MR1137100

[Pol74] J. M. Pollard, *Theorems on factorization and primality testing*, Proc. Cambridge Philos. Soc. **76** (1974), 521–528. MR0354514 (50 #6992)

[Sha71] D. Shanks, *Class number, a theory of factorization, and genera*, 1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969), 1971, pp. 415–440. MR0316385

[Sho94] P. W. Shor, *Algorithms for quantum computation: discrete logarithms and factoring*, 35th Annual Symposium on Foundations of Computer Science (Santa Fe, NM, 1994), IEEE Comput. Soc. Press, Los Alamitos, CA, 1994, pp. 124–134. MR1489242

[Str77] V. Strassen, *Einige Resultate über Berechnungskomplexität*, Jber. Deutsch. Math.-Verein. **78** (1976/77), no. 1, 1–8. MR0438807 (55 #11713)

Quadratic Chabauty for modular curves

Jennifer S. Balakrishnan

The *quadratic Chabauty method* is the first step of Minhyong Kim's nonabelian extension [7–9] of the method of Chabauty–Coleman, which has been used to determine rational points on certain curves. Recently, quadratic Chabauty has been developed in a few directions in joint work with A. Besser, N. Dogra, J. S. Müller, J. Tuitman, and J. Vonk [2–5] and can be applied when the Mordell–Weil rank r of the Jacobian of the curve is equal to the genus g and the Néron–Severi rank of the Jacobian. The quadratic Chabauty method produces a finite set of p-adic points containing $X(\mathbb{Q})$, and this finite set is cut out using double p-adic

integrals arising as solutions to p-adic differential equations described by p-adic heights.

In recent joint work with N. Dogra, J. S. Müller, J. Tuitman, and J. Vonk [6], we have extended the quadratic Chabauty method to consider modular curves that may have few known rational points or nontrivial local height contributions. We describe a selection of modular curves where we have used quadratic Chabauty to determine rational points: certain genus 2 and 3 curves arising from Mazur's Program B, including $X_{S_4}(13)$ (the last remaining modular curve of level 13^n), and various genus 2 and 3 curves in the family of Atkin–Lehner quotient curves $X_0^+(\ell)$, of prime level ℓ. We also note the recent work of N. Adžaga, V. Arul, L. Beneish, M. Chen, S. Chidambaram, T. Keller, and B. Wen [1], where they have determined rational points on the genus 4, 5, and 6 curves in the family $X_0^+(\ell)$ of Atkin–Lehner quotient curves of prime level ℓ.

References

[1] N. Adžaga, V. Arul, L. Beneish, M. Chen, S. Chidambaram, T. Keller, and B. Wen. Quadratic Chabauty for Atkin-Lehner quotients of modular curves of prime level and genus 4, 5, 6. 2021.

[2] J. S. Balakrishnan, A. Besser, and J. S. Müller. Quadratic Chabauty: p-adic heights and integral points on hyperelliptic curves. *J. Reine Angew. Math.*, 720:51–79, 2016.

[3] J. S. Balakrishnan and N. Dogra. Quadratic Chabauty and rational points, I: p-adic heights. *Duke Math. J.*, 167(11):1981–2038, 2018. With an appendix by J. Steffen Müller.

[4] J. S. Balakrishnan and N Dogra. Quadratic Chabauty and rational points II: Generalised height functions on Selmer varieties. *IMRN*, 2020. rnz362.

[5] J. S. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman, and J. Vonk. Explicit Chabauty–Kim for the split Cartan modular curve of level 13. *Ann. of Math. (2)*, 189(3):885–944, 2019.

[6] J. S. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman, and J. Vonk. Quadratic Chabauty for modular curves: Algorithms and examples. 2021.

[7] M. Kim. The motivic fundamental group of $\mathbf{P}^1 \setminus \{0, 1, \infty\}$ and the theorem of Siegel. *Invent. Math.*, 161(3):629–656, 2005.

[8] M. Kim. The unipotent Albanese map and Selmer varieties for curves. *Publ. Res. Inst. Math. Sci.*, 45(1):89–133, 2009.

[9] M. Kim. Massey products for elliptic curves of rank 1. *J. Amer. Math. Soc.*, 23:725–747, 2010.

Idèlic Approach in Enumerating Heisenberg Extensions

Jürgen Klüners

(joint work with Jiuya Wang)

Let ℓ be an odd prime and k be a number field. Let $G \leq S_{\ell^2}$ be a transitive permutation group which can occur as a Galois group of a tower of fields $L/F/k$, where the two extensions L/F and F/k are Galois with cyclic group C_ℓ. We will call these groups generalized and twisted Heisenberg groups.

The goal of this talk is to prove the strong Malle conjecture for the asymptotics of number fields with given Galois group G of the above mentioned type.

Let us first classify the possible Galois groups G. It is easy to see that those groups are subgroups of the wreath product $C_\ell \wr C_\ell = C_\ell^\ell \rtimes C_\ell$. We denote the

normal subgroup C_ℓ^ℓ by W_ℓ which we identify with the $\mathbb{F}_\ell$-vector space $\mathbb{F}_\ell^\ell$. Denote by σ a generator of the quotient C_ℓ and consider W_ℓ as an $\mathbb{F}_\ell[H]$-module. In order to determine all possible groups G it is useful to compute all $\mathbb{F}_\ell[H]$-submodules W_d of W_ℓ. Since W_ℓ consists of one Jordan block, we see that there is exactly one module W_d of dimension d for all $1 \leq d \leq \ell$. This gives rise to an exact sequence of groups

$$1 \to W_d \to G \to H = \langle \sigma \rangle \to 1.$$

In case that this sequence is split we call the resulting group $H(\ell, d)$ generalized Heisenberg group. Up to isomorphism there is for $d < \ell$ only one non-split group $\tilde{H}(\ell, d)$ which we call twisted Heisenberg group. Note that these groups are abelian for $d = 1$ and that $H(\ell, 2)$ is the usual Heisenberg group of order ℓ^3.

In order to formulate our main result we introduce the counting function

$$N_k(G, X) := \#\{L/k : \mathrm{Gal}(L/k) = G, \mathrm{Norm}_{k/\mathbb{Q}}(d_{L/k}) \leq X\}.$$

Theorem 1. *Let k be a number field, ℓ be a prime number, and $G = H(\ell, d)$ or $G = \tilde{H}(\ell, d)$ be a transitive subgroup of S_{ℓ^2}. Then the strong Malle conjecture is true, i.e. there exists a constant $c(k, G) > 0$ such that*

$$N_k(G, X) \sim c(k, G) X^{a(G)} \log(X)^{b(k,G)} \text{ for } X \to \infty,$$

and the constants $a(G)$ and $b(k, G)$ are given as predicted by Malle (see [2, 3]).

We remark that the cases $d = 1$ (abelian groups) and $d = \ell$ have been proved before. In a first step we prove the corresponding statement for a fixed C_ℓ-extension F/k and we denote the corresponding counting function by

$$N_{F/k}(H, X) := \#\{L/F : \mathrm{Gal}(L/k) = H, \mathrm{Norm}_{k/\mathbb{Q}}(d_{L/k}) \leq X\}.$$

Theorem 2. *Let F/k be a C_ℓ-extension and $G = H(\ell, d)$ or $\tilde{H}(\ell, d)$ for $1 < d < \ell$. Then*

$$N_{F/k}(G, X) \sim c(d, F) X^{a(G)} \log(X)^{b(k,G)-1} \text{ for } X \to \infty.$$

We derive our main theorem by a summation using the method of Lemke Oliver, Wang, and Wood [4]. In order to control the constants we bound the ℓ-torsion of Cl_F:

Theorem 3 ([1])**.** *Let F/k be an ℓ-group-extension. Then*

$$|\mathrm{Cl}_F[\ell]| = O_{\epsilon,k}(\mathrm{Norm}_{k/\mathbb{Q}}(d_{F/k})^\epsilon) \text{ for all } \epsilon > 0.$$

An important ingredient of the proof of Theorem 2 is the possibility to compute the global Galois group of L/k by local computations. Let us denote the idèle class group of F by C_F. Then C_ℓ-extensions L/F are in bijection with $\rho \in C_F^\vee := \mathrm{Hom}(C_F, F_\ell)$. It is easy to see that $C_F^\vee$ is an H-module and this action partitions C_F into the blocks

$$I_F(\mathfrak{p}) := (F \otimes_k k_\mathfrak{p})^\times = \prod_{\mathfrak{P}|\mathfrak{p}} F_\mathfrak{P}^\times \text{ for } \mathfrak{p} \in \mathbb{P}(k).$$

Therefore the global object $\rho \in C_F^\vee$ can be described by the local objects $\rho_\mathfrak{p} \in I_F(\mathfrak{p})^\vee$ for all $\mathfrak{p} \in \mathbb{P}(k)$. Note that our Galois group G is determined by d and the

information if the exact sequence is split or not. The number d is the rank of ρ. We get:

Theorem 4. *For $\rho \in C_F^\vee$ we have*

$$\mathrm{rk}(\rho) = \max_{\mathfrak{p}\in\mathbb{P}(k)} \mathrm{rk}(\rho_{\mathfrak{p}}) = \max_{\mathfrak{p}\in S_k} \mathrm{rk}(\rho_{\mathfrak{p}}),$$

where $S_k := \{\mathfrak{P}\cap k \mid \mathfrak{P}\in S\}$ and $S\subseteq\mathbb{P}(F)$ contains all ramified primes of F/k and it is large enough to generate Cl_F.

We use this information to enumerate all ρ with $\mathrm{rk}(\rho)\le d$. Note that S_k is a finite set. We fix one inert prime ideal $\mathfrak{p}_0\in\mathbb{P}(k)$. The extension is non-split if the corresponding Frobenius element lifts to an element of order ℓ^2 which can be easily checked.

References

[1] J. Klüners and J. Wang. ℓ-torsion bounds for the class group of number fields with an ℓ-group as Galois group. *ArXiv: 2003.12161*, 2020.

[2] G. Malle. On the distribution of Galois groups. *J. Number Theory*, 92(2):315–329, 2002.

[3] G. Malle. On the distribution of Galois groups. II. *Experiment. Math.*, 13(2):129–135, 2004.

[4] R. J. Lemke Oliver, J. Wang, and M. M. Wood. Inductive methods for proving Malle's conjecture. In K. Belabas, B. Poonen, and F. Rodriguez Villegas, editors, *Explicit Methods in Number Theory*, Oberwolfach Reports, pages 2064–2066, 2018.

p-integrality of instanton numbers

Frits Beukers

(joint work with Masha Vlasenko)

The motivation for this subject comes from the striking paper of Candelas, De la Ossa, Green and Parkes [5] in the study of mirrorsymmetry of quintic threefolds from 1991. Our short story starts with the differential operator

$$L = -\theta^4 + 5^5 t(\theta+1/5)(\theta+2/5)(\theta+3/5)(\theta+4/5),$$

where θ denotes $t\frac{d}{dt}$. The unique holomorphic solution to $L(y)=0$ is of hypergeometric type and given by

$$F_0 := \sum_{n\ge 0} \frac{(5n)!}{(n!)^5} t^n.$$

The equation $L(y)=0$ has a unique basis of solutions of the form

$$y_0 = F_0,\ y_1 = F_0\log t + F_1,\ y_2 = \frac{1}{2}F_0\log^2 t + F_1\log t + F_2,$$

$$y_3 = \frac{1}{6}F_0\log^3 t + \frac{1}{2}F_1\log^2 t + F_2\log t + F_3,$$

where F_0 is given above and $F_1, F_2, F_3 \in t\mathbb{Q}[[t]]$. Straightforward computation shows that the coefficients of F_1 are certainly not integral. The surprise is that $q := t\exp(F_1/F_0) \in t\mathbb{Z}[[t]]$. The function $q(t)$ is called the *canonical coordinate*. It is a power series in t. The inverse power series $t(q)$ is called the *mirror map*.

Using this inverse series one can rewrite the solutions y_i as power series in q. In particular,

$$y_1/y_0 = \log q, \quad y_2/y_0 = \frac{1}{2}\log^2 q + V(q)$$

for some $V(q) \in q\mathbb{Q}[[q]]$. Let $\theta_q = q\frac{d}{dq}$. Then $K(q) := 1+\theta_q^2 V$ is called the *Yukawa coupling* for reasons coming from theoretical physics. In [5] the Yukawa coupling is expanded as

$$K(q) = 1 + \sum_{n\geq 1} \frac{A_n q^n}{1-q^n}.$$

Motivated by arguments that come from mirrorsymmetry, Candelas et al conjectured that the numbers $a_n = 5A_n/n^3$ are integers which are equal to the (virtual) number of degree n rational curves on a generic quintic threefold in $\mathbb{P}^3$. This is predicted by mirror-symmetry theory from theoretical physics. The numbers a_n are called *instanton numbers*. In particular their integrality has been an intriguing riddle.

It turns out that integrality of instanton numbers also occurs experimentally for a large number of related fourth order differential equation. With this in mind, Almkvist, Van Enckevort, Van Straten and Zudilin [1] compiled a large collection of so-called Calabi-Yau equations, which display instanton numbers which are presumably p-integral for almost all primes p. It is suspected that all equations in this list arise as Picard-Fuchs equations corresponding to a one parameter family of Calabi-Yau threefolds. The quintic example of Candelas et al certainly belongs to this class. For more background we like to refer to the excellent paper [6].

One of the approaches to p-integrality is to use Dwork's methods in p-adic cohomology. This was started by Jan Stienstra [8] with partial success and later Kontsevich, Schwarz and Vologodsky [7],[9] laid out the ideas for a more complete approach. Unfortunately it is hard to find a account of their work which does not depend on certain assumptions.

In our work on so-called Dwork crystals, [2],[3],[4] we obtained as by-product an approach which yields p-integrality for almost all primes p of instanton numbers for a limited number of differential equations, including the quintic example. The advantage of our method is its explicitness, using only p-adic expansions of rational functions. Unfortunately this explicitness also sets limitations on the generality of our results. The actual results will appear on arXiv in September 2021.

References

[1] G. Almkvist, C. van Enckevort, D. van Straten, W. Zudilin, *Tables of Calabi-Yau operators*, arXiv:math/0507430.

[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 II*, Int. Math. Res. Notices, 2021 (2021), 4427–4444, online: https://doi.org/10.1093/imrn/rnaa120

[4] F.Beukers, M.Vlasenko, *Dwork crystals III*, arXiv:math/2105.14841(2021).

[5] P. Candelas, X. de la Ossa, P. Green, L. Parkes, *An exactly soluble superconformal theory from a mirror pair of Calabi-Yau manifolds*, Phys. Lett. B 258 (1991), no. 1-2, 118 - 126.

[6] Straten, D. van, *Calabi-Yau operators*, in Uniformization, Riemann-Hilbert Correspondence, Calabi-Yau Manifolds & Picard-Fuchs Equations (Eds. Lizhen Ji, Shing-Tung Yau), Advanced Lectures in Mathematics, Vol. 42, 2018; arXiv:1704.00164.
[7] M.Kontsevich, A.Schwarz, V.Vologodsky, *Integrality of instanton numbers and p-adic B-model*, Physics Letters B, 637 (2006), 97–101.
[8] J.Stienstra, *Ordinary Calabi-Yau-3 Crystals*, Proc. Workshop on Calabi-Yau Varieties and Mirror Symmetry, Fields Institute Communications volume 38 (2003), pp. 255-271, arXiv:math/0212061.
[9] V.Vologodsky, *Integrality of instanton numbers*, arXiv:0707.4617.

Stable and regular models for $X_{\mathrm{ns}}(p)$ and $X^+_{\mathrm{ns}}(p)$

Bas Edixhoven
(joint work with Pierre Parent)

Our work on *stable* models of the modular curves in the title, over suitable extensions of $\mathbb{Z}_p$, has appeared in [3]. *This* talk reported on our work on *regular* models, over the maximal unramified extension $\mathbb{Z}_p^{\mathrm{unr}}$ of $\mathbb{Z}_p$. These results are still being written up, and at this moment we are not yet completely happy with all proofs and computations. The details will appear later.

Let $p \geq 3$ be a prime number. Let $Y(p)$ be the modular curve over $\mathbb{Q}$ defined by the property that for every $\mathbb{Q}$-algebra A the set $Y(p)(A)$ of A-valued points of $Y(p)$ is the set of isomorphism classes of $(E/A, \varphi)$ with E and elliptic curve over A and ϕ an isomorphism of A-group schemes from $(\mathbb{Z}/p\mathbb{Z})^2_A$ to $E[p]$. Then $Y(p)$ is a smooth affine curve over $\mathbb{Q}$. Its compactification is denoted $X(p)$.

The group $G := \mathrm{GL}_2(\mathbb{F}_p)$ acts on $X(p)$, and for each subgroup H of G we denote the quotient by $X(H)$. Let $\Gamma_{\mathrm{ns}}(p)$ be a cyclic subgroup of G of order p^2-1, and $\Gamma^+_{\mathrm{ns}}(p)$ its normaliser in G (unique up to conjugation). Then $X_{\mathrm{ns}}(p)$ is $X(\Gamma_{\mathrm{ns}}(p))$ and $X^+_{\mathrm{ns}}(p)$ is $X(\Gamma^+_{\mathrm{ns}}(p))$.

A well-known problem is to determine $X(\Gamma^+_{\mathrm{ns}}(p))(\mathbb{Q})$. For $p = 13$ this was done in [1], using the *quadratic Chabauty* method. For applying this method, or its *geometric* variant of [2], one needs information on how $X(\Gamma^+_{\mathrm{ns}}(p))$ extends as a curve over $\mathbb{Z}$. Over $\mathbb{Z}[1/p]$ it extends as a smooth projective curve. A stable model over $\mathbb{Z}_p^{\mathrm{unr}}[\pi]$, with $\pi^{(p^2-1)/2}$, is decribed in [3]. The intertia group $\mu_{(p^2-1)/2}$ acts on it, compatibly with its action on $\mathbb{Z}_p^{\mathrm{unr}}[\pi]$. We get a regular model over $\mathbb{Z}_p^{\mathrm{unr}}$ by taking the quotient, and resolving its singularities. A curious, but not unexpected fact (by analogy with the split Cartan case), is that all irreducible components of the special fibre whose multiplicities are greater than 1 can be successively contracted, so that the minimal regular model has reduced special fibre.

References

[1] J. S. Balakrishnan, N. Dogra, J.S. Müller, J. Tuitman and J. Vonk, *Explicit Chabauty-Kim for the Split Cartan Modular Curve of Level* 13, Ann. of Math. **189** (2019), no. 3, 885–944.
[2] B. Edixhoven, G. Lido, *Geometric quadratic Chabauty*, J. Inst. Math. Jussieu (2021), 1–55.
[3] B. Edixhoven, P. Parent, *Semistable reduction of modular curves associated with maximal subgroups in prime level*, Doc. Math. 26 (2021), 231–269.

Separation of periods of quartic surfaces

Emre Can Sertöz
(joint work with Pierre Lairez)

Kontsevich–Zagier periods form a natural number system that extends the algebraic numbers by adding constants coming from geometry and physics. Because there are countably many periods, one would expect to be able to compute effectively in this number system. This would require an effective height function and the ability to separate periods of bounded height, neither of which are currently possible.

Jointly with Pierre Lairez (Inria, France) we determined an *explicit* height function to separate periods of quartic surfaces [LS20]. More precisely, given a smooth quartic surface $X = Z(f) \subset \mathbb{P}^3$ with 2-holomorphic differential ω_f and two topological cycles $\gamma_1, \gamma_2 \in \mathrm{H}_2(X(\mathbb{C}), \mathbb{Z})$ we would like to check for the equality

$$\int_{\gamma_1} \omega_f \stackrel{?}{=} \int_{\gamma_2} \omega_f. \tag{1}$$

Equivalently, we need to check if the period of $\gamma = \gamma_1 - \gamma_2$ vanishes,

$$\int_{\gamma_1-\gamma_2} \omega_f \stackrel{?}{=} 0. \tag{2}$$

Let $\Delta(\gamma) = (h \cdot \gamma)^2 - 4\gamma^2$ be the discriminant of γ where $h \in \mathrm{H}_2(X, \mathbb{Z})$ is the hyperplane class. Then, we give an effective bound $\varepsilon(f, \Delta(\gamma)) > 0$ such that

$$\int_{\gamma} \omega_f = 0 \quad \text{or} \quad \left| \int_{\gamma} \omega_f \right| > \varepsilon(f, \Delta(\gamma)). \tag{3}$$

By Lefschetz theorem on $(1,1)$-cycles, the period $\int_\gamma \omega_f$ vanishes precisely when γ is represented by algebraic curves on X. Moreover, the existence of an algebraic cycle of discriminant Δ on X is an algebraic criterion on the coefficients of the polynomial f. That is, there is a (Noether–Lefschetz) polynomial p_Δ on the space of quartics so that $p_\Delta(f) = 0$ precisely when X admits an algebraic cycle of discriminant Δ.

To get bounds on the period integrals, we determined a height bound on the coefficients of p_Δ in terms of Δ. We used relative Hilbert schemes and their explicit representation, combined with the theory of heights of multi-projective varieties [DKS13], to bound the height of p_Δ.

Our methods also give bounds on the degrees of p_Δ that are exponential in Δ. From the work of Maulik and Pandharipande [MP13], we know that $\deg p_\Delta$ grows at most polynomially in Δ. We suspect that using modular forms as in [Kud03] one might be able to improve our height bounds for p_Δ. This would make the separation bounds $\varepsilon(f, \Delta)$ not only effective but useful for practical computations to check the equality of periods by approximation only.

References

[DKS13] C.D'Andrea, T Krick, and M. Sombra, "Heights of varieties in multiprojective spaces and arithmetic Nullstellensätze," *Ann. Sci. Éc. Norm. Supér.*, vol. 46, no. 4, pp. 549-627, 2013. DOI:10/gbdc5k.

[Kud03] S. S. Kudla, "Modular forms and arithmetic geometery," in *Current developments in mathematics, 2002*, Int. Press, Somerville, MA, 2003, pp. 135-179

[LS20] P. Lairez and E. C. Sertöz, "Separation of periods of quartic surfaces," Nov. 24, 2020. arXiv: 2011.12316 [math.AG]

[MP13] D. Maulik and R. Pandharipande, "Gromov-Witten theory and Noether-Lefschetz theory," in *A Celebration of Algebraic Geometry*, ser. Clay Math. Proc. Vol. 18, Amer. Math. Soc., Providence, RI, 2013, pp. 469–507.

The negative Pell equation

Peter Koymans

(joint work with Carlo Pagano)

For fixed squarefree $d > 0$, consider the equation

$$C_d : x^2 - dy^2 = 1 \text{ to be solved in } x, y \in \mathbb{Z}.$$

The curve C_d is known as Pell's equation and already appears as the final part of Archimedes' cattle problem. Systematic study of Pell's equation was undertaken by the Indian mathematicians Brahmagupta and Bhaskara II. Their work led to an algorithm to find non-trivial integral solutions of the above equation.
Here we are interested in the negative Pell equation, which is

$$x^2 - dy^2 = -1 \text{ to be solved in } x, y \in \mathbb{Z}. \tag{1}$$

It is not hard to see that the negative Pell equation is not always soluble over $\mathbb{Z}$. In fact, it follows from the Hasse–Minkowski theorem that

$$x^2 - dy^2 = -1 \text{ is soluble with } x, y \in \mathbb{Q} \iff d \in \mathcal{D},$$

where $\mathcal{D}$ is the set of squarefree integers satisfying $p \mid d \Rightarrow p \not\equiv 3 \bmod 4$. Here we shall be concerned with the following question: how often is the negative Pell equation soluble? More precisely, writing $\mathcal{D}^-$ for the set of squarefree integers d for which equation (1) is soluble, what is the density

$$\lim_{X \to \infty} \frac{\#\{d \in \mathcal{D}^- : d \leq X\}}{\#\{d \in \mathcal{D} : d \leq X\}},$$

if it exists. Nagell conjectured in the 1930s that the above limit exists and lies in the open interval $(0, 1)$. This was refined by Stevenhagen [11], who conjectured that

$$\lim_{X \to \infty} \frac{\#\{d \in \mathcal{D}^- : d \leq X\}}{\#\{d \in \mathcal{D} : d \leq X\}} = 1 - \alpha, \quad \alpha = \prod_{j \text{ odd}} (1 - 2^{-j}) \approx 0.41942.$$

Fouvry and Klüners [3] made substantial progress towards Stevenhagen's conjecture by proving that

$$\alpha \leq \liminf_{X\to\infty} \frac{\#\{d \in \mathcal{D}^- : d \leq X\}}{\#\{d \in \mathcal{D} : d \leq X\}} \leq \limsup_{X\to\infty} \frac{\#\{d \in \mathcal{D}^- : d \leq X\}}{\#\{d \in \mathcal{D} : d \leq X\}} \leq \frac{2}{3}.$$

The lower bound was further improved by Fouvry and Klüners [4] to $5\alpha/4$. These works rely on an estimation of certain character sums with some of the key ideas going back to Heath-Brown [6]. The lower bound was improved once more in [1] building on ideas of Smith [9].

From now on we write $\mathrm{Cl}^+(K)$ for the narrow class group of a number field K. A classical criterion for the solubility of equation (1) is that the element $(\sqrt{d})$ is trivial in $\mathrm{Cl}^+(\mathbb{Q}(\sqrt{d}))$. Since the element $(\sqrt{d})$ is 2-torsion, we proceed by studying the 2-part of the class group $\mathrm{Cl}^+(\mathbb{Q}(\sqrt{d}))[2^\infty]$. The p-parts of class groups are conjecturally well-understood thanks to the work of Cohen–Lenstra [2] for odd p, which was adapted to the case $p = 2$ by Gerth [5]. Recently, Smith [10] showed that Gerth's modification of the Cohen–Lenstra conjectures is correct.

Theorem 1 (Smith, 2017)**.** *We have for all finite, abelian 2-groups A*

$$\frac{|\{K \text{ im. quadr.} : |D_K| \leq X, 2\mathrm{Cl}(K)[2^\infty] \cong A\}|}{|\{K \text{ im. quadr.} : |D_K| \leq X\}|} = \frac{\prod_{i=1}^{\infty}(1-2^{-i})}{|\mathrm{Aut}(A)|}.$$

We adapt Smith's work to the family of *real quadratic* fields $\mathbb{Q}(\sqrt{d})$ with $d \in \mathcal{D}$. Since

$$\#\{d \in \mathcal{D} : d \leq X\} \sim C \cdot \frac{X}{\sqrt{\log X}}$$

by classical work of Landau, one sees that we are in a thin subfamily of all real quadratic fields. This subfamily is particularly difficult, since $\mathcal{D}$ ends up in the error term when one would naively adapt Smith's work.

To overcome these issues, we develop two novel reflection principles that replace Smith's key algebraic result [10, Theorem 2.8]. These reflection principles use earlier ideas of the authors [7], which describes the maximal unramified multiquadratic extension of a multiquadratic extension of $\mathbb{Q}$. An application of Hilbert reciprocity then gives the first reflection principle. A slightly weaker version of this reflection principle can already be found in [8].

The second reflection principle is more specific to the Pell family. This reflection principle ultimately also follows from an application of Hilbert reciprocity in a multiquadratic extension of $\mathbb{Q}$, but uses in an essential way that the ramified primes in this multiquadratic extension are all 1 modulo 4. The 2-cocycle to which we apply Hilbert's reciprocity is also of a more complicated nature. Once these obstacles are overcome, the rest of the proof is a relatively straightforward adaptation of Smith's work. This leads to the following result

Theorem 2 (K.-Pagano, 2021)**.** *We have*

$$\lim_{X\to\infty} \frac{\#\{d \in \mathcal{D}^- : d \leq X\}}{\#\{d \in \mathcal{D} : d \leq X\}} = 1 - \alpha,$$

i.e. Stevenhagen's conjecture is true.

References

[1] S. Chan, P. Koymans, D.Z. Milovic and C. Pagano. On the negative Pell equation. *arXiv preprint*, 1908.01752.
[2] H. Cohen and H.W. Lenstra. Heuristics on class groups of number fields. Number theory, Noordwijkerhout 1983, *Lecture Notes in Math.*, *Springer, Berlin*, 1984, 33-62.
[3] É. Fouvry and J. Klüners. On the negative Pell equation. *Ann. of Math. (2)* 172:2035-2104, 2010.
[4] É. Fouvry and J. Klüners. The parity of the period of the continued fraction of $\sqrt{d}$. *Proc. Lond. Math. Soc. (3)* 101:337-391, 2010.
[5] F. Gerth. The 4-class ranks of quadratic fields. *Invent. Math.* 77:498-515, 1984.
[6] D.R. Heath-Brown. The size of Selmer groups for the congruent number problem, II. *Invent. Math.* 118:331-370, 1994.
[7] P. Koymans and C. Pagano. Higher genus theory. *arXiv preprint*, 1909.13871.
[8] P. Koymans and C. Pagano. Higher Rédei reciprocity and integral points on conics. *arXiv preprint*, 2005.14157.
[9] A. Smith. Governing fields and statistics for 4-Selmer groups, 8-class groups. *arXiv preprint*, 1607.07860.
[10] A. Smith. 2^∞-Selmer Groups, 2^∞-class groups, and Goldfeld's conjecture. *arXiv preprint*, 1702.02325v2.
[11] P. Stevenhagen. The number of real quadratic fields having units of negative norm. *Experiment. Math.* 2:121-136, 1993.

Abelian varieties over $\mathbb{F}_2$ of prescribed order

Kiran S. Kedlaya

We study the question: under what conditions, and in what ways, can a given positive integer m occur as the order of the group of $\mathbb{F}_q$-rational points of an abelian variety A over $\mathbb{F}_q$? Recall that this order equals $P(1)$ where P is the Weil polynomial associated to A (the characteristic polynomial of Frobenius on the ℓ-adic Tate module for any prime $\ell \nmid q$); by this plus the Honda–Tate theorem, we can answer the original question via existence/nonexistence results about Weil polynomials.

Using this point of view (and building on [2]), Howe–Kedlaya [3] recently showed that every positive integer occurs as the order of some (ordinary) abelian variety over $\mathbb{F}_2$. This work was then extended by van Bommel et al. [1] to show that for fixed q, every sufficiently large positive integer (in a sense depending on q) occurs as the order of some (ordinary, geometrically simple, principally polarizable) abelian variety over $\mathbb{F}_2$.

We now restrict to simple abelian varieties, corresponding to irreducible Weil polynomials. By refining the Weil bound (e.g., see [4]), one can show that for $q > 2$, the number of simple abelian varieties over $\mathbb{F}_2$ of any fixed order is finite. However, it has been known since work of Madan–Pal from the 1970s [6] that over $\mathbb{F}_2$ there exist infinitely many simple abelian varieties of order 1.

In response to a question of Kadets, we show in [5] that for every positive integer m, there exist infinitely many simple abelian varieties over $\mathbb{F}_2$ of order m. The basic approach is constructive: we introduce a modification of the Madan–Pal construction that, given a monic integer polynomial $Q(z) = \sum_{i=0}^k a_i z^i$ with

$Q(2) = m$ with all complex roots in the disc $|z| \leq \sqrt{2}$, produces a sequence of Weil polynomials corresponding to abelian varieties of order m. However, it is not immediately clear how to add the simplicitly condition to this construction. We do this by choosing the a_i so that some of the resulting Weil polynomials are nearly irreducible over $\mathbb{Q}_2$. For m even we can nearly always do this using the nonadjacent binary representation (i.e., $a_i \in \{0, \pm 1\}$ and no two consecutive a_i are nonzero); for m odd we need a more restricted choice of the a_i, whose existence is established by a short computer calculation.

References

[1] Raymond van Bommel, Edgar Costa, Wanlin Li, Bjorn Poonen, and Alexander Smith, Abelian varieties of prescribed order over finite fields, arXiv:2106.13651v1 (2021).

[2] S.A. DiPippo and E.W. Howe, Real polynomials with all roots on the unit circle and abelian varieties over finite fields, *J. Number Theory* **73** (1998), no. 2, 426–450.

[3] E.W. Howe and K.S. Kedlaya, Every positive integer is the order of an ordinary abelian variety over $\mathbb{F}_2$, arXiv:2103.16530v3 (2021); to appear in *Research in Number Theory*.

[4] B. Kadets, Estimates for the number of rational points on simple abelian varieties over finite fields, *Math. Z.* **297** (2021), 465–473.

[5] K.S. Kedlaya, Abelian varieties over $\mathbb{F}_2$ of prescribed order, arXiv:2107.12453v1 (2021).

[6] M.L. Madan and S. Pal, Abelian varieties and a conjecture of R. M. Robinson, *J. reine angew. Math.* **291** (1977), 78–91.

The Second Moment of the Size of the 2-Selmer Group of Elliptic Curves

Ashvin A Swaminathan

(joint work with Manjul Bhargava and Arul Shankar)

Recall that for an elliptic curve $E/\mathbb{Q}$ and a prime p, the p-Selmer group $\mathrm{Sel}_p(E)$ parametrizes isomorphism classes of locally soluble p-coverings of E. A key objective in arithmetic statistics is to determine the distribution of $\mathrm{Sel}_p(E)$ as E varies among all elliptic curves over $\mathbb{Q}$. We have the following beautiful conjecture about this distribution due to Poonen and Rains:

Conjecture 1 ([4, Conjecture 1.1(c)])**.** *Let p be prime. When elliptic curves $E/\mathbb{Q}$ are ordered by height, the m^{th} moment of the size of* $\mathrm{Sel}_p(E)$ *is* $\prod_{i=1}^{m}(p^i + 1)$.

In the series of papers [1–3], Bhargava and Shankar develop a general technique for counting integral orbits of coregular representations and use it to verify the conjecture when $m = 1$ and $n \in \{2, 3, 5\}$. The purpose of this talk is to discuss the particularly difficult case where $m = n = 2$. Our main result is as follows:

Theorem 2. *When elliptic curves over $\mathbb{Q}$ are ordered by height, the second moment of the size of the 2-Selmer group is at most* 15.

In fact, we prove that Theorem 2 holds for any subfamily of elliptic curves defined by very general infinite sets of congruence conditions, and further that the bound of 15 is tight if one assumes a certain plausible tail estimate.

A key ingredient in the proof of Theorem 2 is the computation of the average size of the 2-Selmer group of the Jacobian of locally soluble genus-1 curves:

Theorem 3. *When locally soluble genus-*1 *curves over* $\mathbb{Q}$ *are ordered by height, the average size of the* 2*-Selmer group of the Jacobian is at most* 6*.*

We also prove the following generalization of Theorem 3 to even-degree hyperelliptic curves of arbitrary genus:

Theorem 4. *When hyperelliptic curves* (*resp., locally soluble hyperelliptic curves*) *over* $\mathbb{Q}$ *of degree* $n \equiv 2 \pmod 4$ (*resp.,* $n \equiv 0 \pmod 4$) *with squarefree discriminant are ordered by height, the average size of the* 2*-Selmer group of the Jacobian is at most* 6*.*

To prove Theorems 2–4, we apply an enhanced version of the parametrize-and-count strategy developed by Bhargava and Shankar. This strategy consists of two pieces: an algebraic piece, in which one parametrizes the objects of interest in terms of rational orbits of a certain coregular representation and constructs integral representatives for these orbits; and an analytic piece, in which one combines geometry-of-numbers and sieve techniques to count these integral representatives.

On the algebraic side, a serious obstacle to parametrizing 2-Selmer groups of non-monic hyperelliptic curves is that these curves are often insoluble. To deal with this, we take a hyperelliptic curve of the form $C\colon z^2 = f(x,y)$, where f has even degree n and leading coefficient $f_0 \neq 0$, and we simply manufacture a $\mathbb{Q}$-rational point by replacing C with the curve $C'\colon z^2 = f^{\mathrm{mon}}(x,y) := f_0^{-1} \times f(x, f_0 y)$. The monic (hence, soluble) curve C' is a twist of C by $\mathbb{Q}(\sqrt{f_0})$, and so the elements of $\mathrm{Sel}_2(\mathrm{Jac}(C))$ can be realized as certain 2-coverings of $\mathrm{Jac}(C')$. This leads to the following key orbit construction:

Theorem 5. *Let* $\mathcal{A} := \sum_{i=0}^{n} x_i y_{n-i}$*, let* f *be a separable binary form of even degree* n *over* $\mathbb{Z}$*, and suppose* $C\colon z^2 = f(x,y)$ *is locally soluble if* $n \equiv 0 \pmod 4$*. For some integer* $\kappa := \kappa(n) \geq 1$*, there is a natural injective map of sets taking elements of* $\mathrm{Sel}_2(\mathrm{Jac}(C))$ *to* $(\mathrm{SL}_n/\mu_2)(\mathbb{Z})$*-orbits of pairs* $(\mathcal{A}, B)$ *of* n*-ary quadratic forms over* $\mathbb{Z}$ *such that* $\det(x\mathcal{A} + yB) = f^{\mathrm{mon}}(x, \kappa y)$*.*

With notation as in Theorem 5, let R_f be the ring of global sections of the subscheme of $\mathbb{P}^1_{\mathbb{Z}}$ cut out by f. To prove Theorem 5, we first prove that elements of $\mathrm{Sel}_2(\mathrm{Jac}(C))$ correspond to square roots of the ideal class of the inverse different of R_f. We then apply the following (loosely stated) parametrization result:

Theorem 6 (S., [5, Theorem 1])**.** *Square roots of the class of the inverse different of* R_f *naturally give rise to certain* $\mathrm{SL}_n^{\pm}(\mathbb{Z})$*-orbits of pairs* (A, B) *of* n*-ary quadratic forms over* $\mathbb{Z}$ *such that* $\det(xA + yB) = \pm f^{\mathrm{mon}}(x,y)$*.*

A key feature of the orbit construction in Theorem 6 is that, at least when $n = 4$ or when f has squarefree discriminant, the image is defined by certain congruence conditions modulo the leading coefficient f_0 of f, and not some higher power thereof. An n-ary quadratic form B satisfying these congruence conditions is said to be *special at* f_0. When f_0 is squarefree or when f has squarefree discriminant,

the condition of being special at f_0 is beautifully explicit: namely, B must have rank ≤ 1 modulo f_0.

Combining Theorem 5 with the orbit-counting techniques developed by Bhargava and Shankar immediately yields the following result for families of hyperelliptic curves with fixed nonzero leading coefficient:

Theorem 7. *When hyperelliptic curves (resp., locally soluble hyperelliptic curves) over $\mathbb{Q}$ of degree $n \equiv 2 \pmod 4$ (resp., $n \equiv 0 \pmod 4$) with fixed nonzero leading coefficient are ordered by height, the average size of the 2-Selmer group of the Jacobian is at most 6.*

Having established the parametrization, we must then estimate the number of orbits having bounded height that arise from 2-Selmer elements. The key difficulty here is that we must count orbits for a group acting on a family of increasingly sparse subsets of a lattice. Indeed, taking $n = 4$ for simplicity and fixing a leading coefficient $f_0 \neq 0$, observe that the set $\{f^{\mathrm{mon}} : f(x, y) = f_0x^4 + \cdots\}$ has density f_0^{-6} in the set of all monic binary quartic forms. Hence, we expect the set of pairs $(\mathcal{A}, B)$ such that $\det(x\mathcal{A} + yB) = f^{\mathrm{mon}}(x, y)$ for some $f(x, y) = f_0x^4 + \cdots$ to also have density around f_0^{-6} in the set of all $(\mathcal{A}, B)$.

The leading coefficient f_0 of f grows with the height of f. Concretely, if f has height X, then the coefficients $f_0, \ldots, f_4$ of f satisfy the following bounds:

$$|f_0| \ll \frac{X}{t^4}, \quad |f_1| \ll \frac{X}{t^2}, \quad |f_2| \ll X, \quad |f_3| \ll t^2X, \quad |f_4| \ll t^4X,$$

where $t \geq \sqrt[4]{3}/\sqrt{2}$ is necessarily $\ll X^{1/4}$, for otherwise f_0 is forced to be 0. For simplicity, we assume in what follows that $t = 1$ (the number of points when t is large is negligible, and the proof for small $t \neq 1$ is nearly identical). Then the monicization f^{mon} has coefficients 1, f_1, f_0f_2, $f_0^2f_3$, $f_0^3f_4$, which satisfy the bounds

$$|f_1| \ll X, \quad |f_0f_2| \ll X^2, \quad |f_0^2f_3| \ll X^3, \quad |f_0^3f_4| \ll X^4.$$

Therefore, any lift $(\mathcal{A}, B)$ such that $\det(x\mathcal{A}+yB) = f^{\mathrm{mon}}(x, y)$ has an $(\mathrm{SL}_4/\mu_2)(\mathbb{Z})$-translate of the form $(\mathcal{A}, B')$ such that the coefficients b'_{ij} of B' are all bounded by some constant times X, multiplied by some cuspidal coefficients that are easily bounded. Furthermore, the element B', like f, satisfies congruence conditions having density approximately f_0^{-6} (this density is exact when f_0 is squarefree).

Our task is now to determine, for each nonzero $f_0 \ll X$, an asymptotic for the number of $(\mathrm{SL}_4/\mu_2)(\mathbb{Z})$-orbits on pairs of the form $(\mathcal{A}, B)$, where the height of B is bounded by X and B is special at f_0. We must then sum this asymptotic over f_0. Heuristically, the total sum is given by

$$\asymp \sum_{f_0 \ll X} f_0^{-6}X^{10} \asymp X^5,$$

which is exactly what we expect. However, there are several difficulties in turning this heuristic into a proof. For instance, we need to keep precise control over the error dependence on both X and f_0, particularly when f_0 is around the size of X. We achieve this for squarefree f_0 using twisted Poisson summation together with a computation of the Fourier coefficients of the set of points special at f_0 (this

shows that special points are equidistributed modulo f_0). These equidistribution methods are less readily available when f_0 is not squarefree, since the notion of specialness is rather more complicated in this case. A related issue is that the fundamental domains in which we count points are quite skewed when f_0 is small relative to X. For forms f with leading coefficient f_0, where f_0 has large powerful part or is small relative to X, we simply bound the number of lifts; this suffices because such f_0 appear rarely and hence contribute negligibly to the total.

References

[1] M. Bhargava and A. Shankar. The average size of the 5-selmer group of elliptic curves is 6, and the average rank is less than 1. *arXiv preprint arXiv:1312.7859*, 2013.

[2] M. Bhargava and A. Shankar. Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. *Ann. of Math. (2)*, 181(1):191–242, 2015.

[3] M. Bhargava and A. Shankar. Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. *Ann. of Math. (2)*, 181(2):587–621, 2015.

[4] B. Poonen and E. Rains. Random maximal isotropic subspaces and Selmer groups. *J. Amer. Math. Soc.*, 25(1):245–269, 2012.

[5] A. Swaminathan. Average 2-torsion in class groups of rings associated to binary n-ic forms. *arXiv preprint arXiv:2011.13578*, 2020.

Distributions of unramified extensions of global fields

Melanie Matchett Wood

(joint work with Yuan Liu and David Zureick-Brown)

This talk presents the work in [LWZ19]. Every number field K has a maximal unramified extension K^{un}, with Galois group $\mathrm{Gal}(K^{un}/K)$ (whose abelianization is the class group of K). Cohen, Lenstra, and Martinet [CL84, CM90] have given conjectures of the distribution of the class groups of number fields, and it is natural to ask then about the distribution $\mathrm{Gal}(K^{un}/K)$.

For this work, we fix a finite group Γ and consider the family of totally real (split completely at infinity) Γ extensions of $\mathbb{Q}$ or $\mathbb{F}_q(t)$, ordered by the norm of the radical of their discriminant. We prove some results about the structure of $\mathrm{Gal}(K^{un}/K)$ that motivate us to give a conjecture about the distribution of $\mathrm{Gal}(K^{un}/K)$ in our considered family, which we also conjecture in the function field analog, where we can prove a result towards our conjectures.

Let $K^{\#}$ be the maximal unramified extension of K that is split completely at all places of K above ∞ and of order relatively prime to $|\Gamma|$ and the order of the roots of unity in our base field ($\mathbb{Q}$ or $\mathbb{F}_q(t)$), and also prime to q in the latter case. A Γ-*group* is a profinite group with a continuous action of Γ. A Γ-group G is *admissible* if it is Γ-generated topologically by the elements $\{g^{-1}\gamma(g)|g \in G, \gamma \in \Gamma\}$ and is of order prime to $|\Gamma|$. We show that $\mathrm{Gal}(K^{\#}/K)$ is an admissible Γ-group. We construct a group $\mathbb{F}_n$, *the free admissible* Γ*-group on* n *generators*, by taking the subgroup of the free profinite Γ-group on γx_i (for $\gamma \in \Gamma$ and $1 \leq i \leq n$) generated by elements of the form $g^{-1}\gamma(g)$. Further, we will see that $\mathrm{Gal}(K^{\#}/K)$ has what

we call *Property E*, i.e. for every prime p and every non-split central extension of Γ-groups

$$1 \to \mathbb{Z}/p\mathbb{Z} \to \widetilde{G} \to G \to 1, \tag{1}$$

(where $\mathbb{Z}/p\mathbb{Z}$ has trivial Γ-action), any Γ-equivariant surjection $\mathrm{Gal}(K^{\#}/K) \to G$ lifts to a Γ-equivariant surjection $\mathrm{Gal}(K^{\#}/K) \to \widetilde{G}$ (as long as p is one of the primes that could possibly divide $\mathrm{Gal}(K^{\#}/K)$ by definition). We show that a quotient of $\mathbb{F}_n$ has Property E if and only if it is $\mathbb{F}_n/[r^{-1}\gamma(r)]_{r\in S,\gamma\in\Gamma}$ for some S. We thus define a random group $X_{\Gamma,n} := \mathbb{F}_n/[r^{-1}\gamma(r)]_{r\in S,\gamma\in\Gamma}$, where S is random from Haar measure on $\mathbb{F}_n^{n+1}$. We prove that these groups approach a limiting distribution as $n \to \infty$, and conjecture that this is the distribution of $\mathrm{Gal}(K^{\#}/K)$ for our families.

We give theorems in the function field case (as the size of the finite field goes to infinity) that support these new conjectures. We let D_K denote the norm of the radical of the ideal $\mathrm{Disc}(K/\mathbb{F}_q(t))$. Let $E_\Gamma(D, \mathbb{F}_q(t))$ be the set of isomorphism classes of totally real Γ-extensions of $\mathbb{F}_q(t)$ with $D_K = D$. We then have the following theorem giving the moments of the distribution in a certain limit, and moreover we show that our conjectured distribution has these same moments.

Theorem 1. *Let Γ be a finite group and H be a finite admissible Γ-group. Then,*

$$\lim_{N\to\infty} \lim_{\substack{q\to\infty \\ (q,|\Gamma||H|)=1 \\ (q-1,|H|)=1}} \frac{\sum_{n\le N}\sum_{K\in E_\Gamma(q^n,\mathbb{F}_q(t))} |\operatorname{Sur}_\Gamma(\mathrm{Gal}(K^{\#}/K), H)|}{\sum_{n\le N}|E_\Gamma(q^n,\mathbb{F}_q(t))|}$$
$$= \int_X |\operatorname{Sur}_\Gamma(X,H)| d\mu_\Gamma(X) = [H : H^\Gamma]^{-1},$$

where in the limit q is always a prime power.

In particular, our distributions abelianize to the Cohen-Lenstra-Martinet distributions for class groups, and so our function field theorems prove (suitably modified) versions of the Cohen-Lenstra-Martinet heuristics over function fields as the size of the finite field goes to infinity. In particular, using the results of W. Wang and the second author [WW21, Theorem 6.2, Proposition 6.6, Theorem 6.11] that the conjectured distribution of Cohen, Lenstra, and Martinet has these same moments and that the moments determine a unique distribution, we have the following corollary.

Corollary 2. *Let $p \nmid |\Gamma|$ be a prime and A a finite Γ-module of order a power of p such that $A^\Gamma = 1$. Then*

$$\lim_{N\to\infty} \lim_{\substack{q\to\infty \\ (q,|\Gamma|p)=1 \\ (q-1,p)=1}} \frac{\sum_{n\le N}|\{K \in E_\Gamma(q^n,\mathbb{F}_q(t))|\mathrm{Cl}_{\mathcal{O}_K}[p^\infty] \simeq A\}|}{\sum_{n\le N}|E_\Gamma(q^n,\mathbb{F}_q(t))|} = \frac{c}{|A||\operatorname{Aut}_\Gamma(A)|},$$

where c is a constant only depends on Γ and p, and $\mathcal{O}_K$ is the integral closure of $\mathbb{F}_q[t]$ in K.

Using the work of Sawin [Saw20] on the non-abelian moment problem, one has an analogous corollary for $\mathrm{Gal}(K^{\#}/K)$.

References

[CL84] Henri Cohen and Hendrik W. Lenstra, Jr. Heuristics on class groups of number fields. In *Number Theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, volume 1068 of *Lecture Notes in Math.*, pages 33–62. Springer, Berlin, 1984.

[CM90] Henri Cohen and Jacques Martinet. étude heuristique des groupes de classes des corps de nombres. *Journal für die Reine und Angewandte Mathematik*, 404:39–76, 1990.

[LWZ19] Yuan Liu, Melanie Matchett Wood, and David Zureick-Brown. A predicted distribution for Galois groups of maximal unramified extensions. *arXiv:1907.05002 [math]*, July 2019.

[Saw20] Will Sawin. Identifying measures on non-abelian groups and modules by their moments via reduction to a local problem. *arXiv:2006.04934 [math]*, June 2020.

[WW21] Weitong Wang and Melanie Matchett Wood. Moments and interpretations of the Cohen–Lenstra–Martinet heuristics. *Commentarii Mathematici Helvetici*, 96(2):339–387, June 2021.

Presentations of Galois groups of maximal extensions with restricted ramification

Yuan Liu

In the previous work with Wood and Zureick-Brown [4], we construct a random group model, which extends the Cohen–Lenstra heuristics and provides a predicted distribution for a canonical quotient $\mathrm{Gal}(K^{\#}/K)$ of Galois groups of maximal unramified extensions of K as K ranges over totally real Γ-extensions of $Q = \mathbb{Q}$ or $\mathbb{F}_q(t)$. Let $K^{\#}$ denote the maximal unramified extension of K that is split completely at places of K over infinity and of order relatively prime to the number of roots of unity in Q, the size of Γ, and char$Q$. Using the notation of pro-$\mathcal{C}$ completions and free admissible group $\mathcal{F}_n$ defined in [4], our conjecture implies a surprising phenomenon of the structure of $\mathrm{Gal}(K^{\#}/K)$ that was not known before: for any finite set $\mathcal{C}$ of finite Γ-groups, the followings happen to K with probability 1

(1) the pro-$\mathcal{C}$ completion $\mathrm{Gal}(K^{\#}/K)^{\mathcal{C}}$ of the Galois group $\mathrm{Gal}(K^{\#}/K)$ is a finite group, and moreover
(2) there exists some finite n such that $\mathrm{Gal}(K^{\#}/K)^{\mathcal{C}}$ is the quotient of $\mathcal{F}_n^{\mathcal{C}}$ by $[r^{-1}\gamma(r)]_{r\in T,\gamma\in\Gamma}$ for some subset T of $\mathcal{F}_n^{\mathcal{C}}$ of cardinality $n+1$, where the symbol $[r^{-1}\gamma(r)]_{r\in T,\gamma\in\Gamma}$ denotes the Γ-closed normal subgroup of $\mathcal{F}_n^{\mathcal{C}}$ generated by $r\gamma^{-1}(r)$ for all $r \in T$ and $\gamma \in \Gamma$.

The statement in (2) is a very strong condition on $\mathrm{Gal}(K^{\#}/K)$ because it implies that the deficiency (i.e. the difference between the minimal number of generators and the minimal number of relations) of $\mathrm{Gal}(K^{\#}/K)$ has a bound depending only on the order of Γ, if $\mathrm{Gal}(K^{\#}/K)$ is finitely generated.

In [2], we show that the conditions (1) and (2) both hold for all totally real Γ-extensions K/Q, which strongly supports that the random group model in [4] is the right object to study.

Theorem 1. [2] *Let Γ, Q, $\mathcal{C}$ be as described as above. Then for a Galois extension K/Q with Galois group Γ that is split completely over ∞, we have the following isomorphism of Γ-groups*

$$Gal(K^{\#}/K)^{\mathcal{C}} \simeq {\mathcal{F}_n^{\mathcal{C}}}\big/{[r^{-1}\gamma(r)]_{r\in T,\gamma\in\Gamma}}$$

for sufficiently large positive integer n and some set T consisting of $n+1$ elements of $\mathcal{F}_n^{\mathcal{C}}$.

The proof of the theorem is inspired by work [1] of Koch, which studies the minimal numbers of generators and relations for the p-class tower group of a global field, and by the work [3] of Lubotzky, which establishes a method using group cohomology to study the deficiency of finitely generated profinite groups. Explicitly, we first prove a formula relating the deficiency to the Galois cohomology $\dim_{\mathbb{F}_p} H^2(G_S(K),A)^\Gamma - \dim_{\mathbb{F}_p} H^1(G_S(K),A)^\Gamma$ for all simple $\mathrm{Gal}(K_S/Q)$-module A, where $G_S(K)$ is the Galois group of the maximal unramified-outside-S extension of K for a finite set S of primes of K. Then we define a group $\text{Б}_S(K,A)$, which generalizes the group $\text{Б}_S(K)$ in Koch's work, to bound the dimensions of cohomology groups.

The methods developed in [2] can apply to many other interesting situations. First of all, when $\Gamma = 1$ and $K = Q$ is a function field, Shusterman [5] showed that $G_\emptyset(K)$ admits a finite presentation in which the number of relations is exactly the same as the number of generatros (which is called a balanced presentation), and we prove the following analogous result in the number field case.

Theorem 2. [2] *Let K be a number field and S a finite set of places of K. If $G_S(K)$ is topologically generated by n elements, then it admits a finite presentation with n generators, in which the minimal number of relations is at most $[K:\mathbb{Q}]+n$.*

[2] also discusses the following two situations that are not considered in the conjecture of Liu–Wood–Zureick: 1) letting K varies among Γ-extensions of $\mathbb{Q}$ such that the decomposition subgroup at ∞ is a given $\mathbb{Z}/2\mathbb{Z}$-subgroup of Γ; and 2) allowing groups in the set $\mathcal{C}$ to contain groups of order not prime to the number of roots of unity of Q. In each of these two cases, we use our method to compute an upper bound for the deficiency of $G_\emptyset(K)$ at the pro-$\mathcal{C}$ level, and then show why the conjecture of Liu–Wood–Zureick doesn't work in these two exceptional cases. This computation of deficiencies also provides insights of how the random group model should be modified in these two cases.

References

[1] Helmut Koch, *Galois theory of p-extensions*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002. With a foreword by I. R. Shafarevich, Translated from the 1970 German original by Franz Lemmermeyer, With a postscript by the author and Lemmermeyer. MR1930372

[2] Yuan Liu, *Presentations of Galois groups of maximal extensions with restricted ramification*, arXiv:2005.07329 [math] (2020).

[3] Alexander Lubotzky, *Pro-finite presentations*, J. Algebra **242** (2001), no. 2, 672–690. MR1848964

[4] Yuan Liu, Melanie Matchett Wood, and David Zureick-Brown, *A predicted distribution for Galois groups of maximal unramified extensions*, arXiv:1907.05002 [math] (2019).
[5] Mark Shusterman, *Balanced presentations for fundamental groups of curves over finite fields*, arXiv:1811.04192 [math] (2018).

Moments, Measures, and Non-Abelian Cohen-Lenstra

Will Sawin

This talk describes work which is part of the broad program to find the most general possible version of the Cohen-Lenstra heuristics and to prove this, as much as possible, in the function field setting. It in particular has relevance to work of Liu, Wood, and Zurieck-Brown [5] discussed in Wood's talk in this volume, allowing us to deduce a stronger statement from their main geometric result.

In their original form [2], the Cohen-Lenstra heuristics predicted the distribution of the class groups of quadratic fields, i.e. $\mathbb{Z}/2$-extensions of $\mathbb{Q}$. They were quickly generalized in a number of directions (which this abstract is too short to explain) In particular, one can, recalling the theorem of class field theory that the class group is the abelianization of the Galois group of the maximal unramified extension, attempt to predict the distribution of the Galois group of the maximal unramified extension, or some more tame quotient like its maximal pro-p quotient. This direction has been investigated by many authors, e.g. [1].

Even in the original quadratic case [2], the Cohen-Lenstra heuristics can be stated in two different ways:

(Measure) For G a finite abelian ℓ-group,

$$\lim_{X\to\infty} \frac{|\{K \text{ im. quad.} \mid \mathrm{Disc}(K) < X, \mathrm{Cl}(K)_\ell \cong G\}|}{|\{K \text{ im. quad.} \mid \mathrm{Disc}(K) < X\}|} = \frac{1}{|\mathrm{Aut}(G)|} \prod_{k=1}^{\infty} (1-\ell^{-k}).$$

(Moments) For H a finite abelian ℓ-group,

$$\lim_{X\to\infty} \frac{\sum_{\substack{K \text{ im. quad.} \\ \mathrm{Disc}(K)<X}} |\mathrm{Surj}(\mathrm{Cl}(K)_\ell, H)|}{|\{K \text{ im. quad. } \mid \mathrm{Disc}(K) < X\}|} = 1.$$

It is a theorem of Ellenberg, Venkatesh, and Westerland [3, Proposition 8.3] that (Moments) implies (Measures). This is useful, in their context, because they prove [3, Theorem 8.8] the analogue of (Moments) in the function field context in a certain limit, and therefore deduce the analogue of (Measures) statement in their limit. In attempts to generalize Cohen-Lenstra, a more general implication from Moments to Measures may be useful if we can calculate the moments in a function field limit, or more simply if we are able to guess the moments (since they have simpler formulas, they are likely to be easier to guess correctly), and then use this to find the correct formula for the measure.

Thus, it would be useful to prove that moment convergence implies measure convergence in as general a context as possible. In particular, in the non-abelian context, Liu, Wood, and Zurieck-Brown proved moment convergence [5, Theorem 1.4] (albeit in a more restrictive limit than Ellenberg, Venkatesh, and Westerland)

and conjectured measure convergence, so it would be useful to prove the implication in their setting. The main theorem of this work is exactly such a statement.

For Γ a group and S a set of primes, define a Γ-S-group to be a finite group, with an action of Γ, whose order is a product of powers of primes in S.

Theorem 1. *Let Γ be a finite group and S a finite set of primes not dividing $|\Gamma|$. Let μ be a measure on the set of isomorphism classes of finite Γ-S-groups. Let μ_t be a sequence of measures on the same set. Assume that, for each finite Γ-S-group H, we have*

$$\lim_{t\to\infty} \int |\operatorname{Surj}_\Gamma(X,H)| d\mu_t(X) = \int \operatorname{Surj}_\Gamma(X,H) d\mu(X).$$

and

$$\int \operatorname{Surj}_\Gamma(X,H) d\mu(X) = O(|H|^{O(1)})$$

Then for every finite Γ-S-group H we have

$$\lim_{t\to\infty} \mu_t(H) = \mu(H).$$

This generalizes [1, Theorem 1.4] from the p-group case and [6] (which itself generalizes [3, Proposition 8.3]) from the abelian case.

The strategy of proof is to reduce the problem to a special case where calculations can be done explicitly (and in large part were already done in [4, Equation (22)]). Specifically, noting that we have information about surjections $X \to H$ and would like to understand when X is isomorphic to H, we observe that an isomorphism is simply a surjection with trivial kernel.

We therefore define from each measure μ_t in the sequence, and our hopeful limit μ, a new measure μ_t^H or μ, where the measure of a group K is the expectation of the number of surjections from X to H with kernel K. We observe that the moments of this new measure can be calculated as linear combinations of the moments of the original measure. Furthermore, the probability of attaining H under the original measure is proportional to the probability of attaining the trivial group under the new measure, so it suffices to calculate only this probability.

Next we observe that, to test whether a group is trivial, it suffices to test whether its quotient by the intersection of all its maximal proper normal invariant subgroups is trivial, and so we can replace each group appearing by such a quotient. This quotient is a product of finite simple groups. For powers of a single finite simple group, we can express the probability that the group is trivial as a linear combination of the moments by an exact identity, showing that moment convergence implies measure convergence as long as the limits of the moments grow slowly enough that this linear combination is convergent. We can handle the case of products of finite simple groups inductively by repeating the case of powers of a single finite simple group, as long as the number of isomorphism classes of finite simple groups appearing is bounded. Using our bounds for the moments of the original measures, we obtain suitable bounds for the moments of the transformed measures, sufficient to show that the linear combination is indeed convergent.

References

[1] Nigel Boston and Melanie Matchett Wood, Nonabelian Cohen-Lenstra Heuristics over Function Fields, https://arxiv.org/abs/1604.0343 (2016).

[2] H. Cohen and H. W. Lenstra, Jr. Heuristics on class groups of number fields. In *NumberTheory, Noordwijkerhout 1983*, Lecture Notes in Mathematics **1068** (1984), 33-62.

[3] Jordan S. Ellenberg, Akshay Venkatesh, and Craig Westerland. Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields. *Annals of Mathematics*, **183** (2016), 729-786.

[4] D.R. Heath-Brown, The size of the Selmer groups for the congruent number problem, II, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.538.9147&rep=rep1&type=pdf preprint version

[5] Yuan Liu, Melanie Matchett Wood, and David Zurieck-Brown, A predicted distribution for Galois groups of maximal unramified extensions, https://arxiv.org/abs/1907.05002 (2019)

[6] Weitong Wang and Melanie Matchett Wood, Moments and interpretations of the Cohen-Lenstra-Martinet heuristics, https://arxiv.org/abs/1907.11201.

[7] Will Sawin, Identifying measures on non-abelian groups and modules by their moments via reduction to a local problem, https://arxiv.org/abs/2006.04934 (2020)

Infinite unramified extensions of number fields

Farshid Hajir

(joint work with Christian Maire, Ravi Ramakrishna)

We fix the following notation:

- $p \geq 2$ fixed prime
- $K/\mathbb{Q}$ of finite degree n, signature (r_1, r_2), discriminant $\mathrm{disc}(K)$
- The root discriminant of K is $\mathrm{rd}_K := |\mathrm{disc}(K)|^{1/n}$
- $\delta = 1$ or 0 according as ζ_p in K or not
- $u = r_1 + r_2 - 1 + \delta =$ the p-rank of the unit group $\mathcal{O}_K^\times$
- $d = \dim_{\mathbb{F}_p} \mathrm{Cl}_K/\mathrm{Cl}_K^p$ the p-rank of the p-class group of K
- $K_\emptyset =$ maximal unramified p-extension of K
- $G_\emptyset = \mathrm{Gal}(K_\emptyset/K) = p$-class tower group of K

The p-class tower group, or "pro-p fundamental group" $G_\emptyset$ is a natural nonabelian generalization of the p-class group. It was originally thought that all p-class tower groups are finite. The following effective criterion, due to Golod and Shafarevich as refined by Gaschutz and Vinberg, showed that this was not the case: *If $d \geq 2 + 2\sqrt{u+1}$, then $G_\emptyset$ is infinite.*

Not much is known about the structure of infinite p-class tower groups. For example, we don't know a single example of an infinite $G_\emptyset$ for which we have a presentation. On the computational side, we mention:

Difficult Problem. Give an algorithm for computing $G_\emptyset$. [Say by giving a presentation of it as a pro-p group].

(Presumably) Less Difficult Problem. Give an algorithm for determining whether $G_\emptyset$ is finite or not.

In this talk, I discussed three theorems in the spirit of explicit methods in number theory (see [1] and [2] for more details).

Theorem A. *Suppose $d > 2 + 2\sqrt{u+1}$. Then*

(1) K admits an infinite unramified p-extension L/K in which all primes split "almost completely," (have finite residual degree). In other words, all Frobenius elements in $\mathrm{Gal}(L/K)$ *are torsion.*

(2) K admits an infinite unramified p-extension M/K such that infinitely many primes of K split completely in M/K.

Part (2) of the above theorem answers a question from Ihara's 1983 paper [3]. The analogue (with the same proof) holds in the function field case as well.

Theorem B. *For every prime $p \geq 2$, there is a (solvable) finite extension $K/\mathbb{Q}$ unramified outside $\{p, \infty\}$ such that K admits an infinite unramified p-extension. Thus, there exists a sequence of number fields of p-power discriminant with bounded root discriminant.*

Remark. To replace $\{p, \infty\}$ with $\{p\}$, [in other words, to prove this theorem in the realm of totally real fields], appears to be much more difficult. In particular, for a small prime p, it is a challenge to locate a totally real number field unramified outside p in which there are at least two primes above p.

Theorem C.

(1) There is an infinite tower of complex number fields whose root discriminants are bounded above by 78.5.

(2) There is an infinite tower of totally real number fields whose root discriminants are bounded above by 857.6.

The proofs of all three theorems are based on a variation ("cutting of towers") on the standard application of the Golod-Shafarevich criterion for infinitude of a pro-p group.

References

[1] F. Hajir, C. Maire, and R. Ramakrishna, *Cutting towers of number fields*, Ann. Math. Québec (2021); https://doi.org/10.1007/s40316-021-00156-8; arXiv:1901.04354.

[2] F. Hajir, C. Maire, and R. Ramakrishna, *Infinite class field towers of number fields of prime power discriminant*, Adv. Math. 373 (2020), 107318, 8 pp. https://doi.org/10.1016/j.aim.2020.107318; arXiv:1904.07062.

[3] Y. Ihara, *How many primes decompose completely in an infinite unramified extension of global fields?*, J. Math. Soc. Japan **35** no. 4, (1983), 693–709.

Reporter: Ross Paterson

Participants

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

Dr. Jennifer S. Balakrishnan
Department of Mathematics
Boston University
111 Cummington Street
Boston, MA 02215-2411
UNITED STATES

Prof. Dr. Alex Bartel
School of Mathematics & Statistics
University of Glasgow
University Place
Glasgow G12 8QQ
UNITED KINGDOM

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

Prof. Dr. Frits Beukers
Mathematisch Instituut
Universiteit Utrecht
P.O. Box 80.001
3508 TA Utrecht
NETHERLANDS

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

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

Dr. Shiva Chidambaram
Department of Mathematics
Massachusetts Institute of
Technology
77 Massachusetts Avenue
Cambridge, MA 02139-4307
UNITED STATES

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

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

Prof. Dr. Jean-Marc Couveignes
Institut de mathématiques de Bordeaux
Université de Bordeaux
351, cours de la Liberation
33405 Talence Cedex
FRANCE

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

Dr. Netan Dogra
Department of Mathematics
King's College London
Strand
London WC2R 2LS
UNITED KINGDOM

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

Prof. Dr. Bas Edixhoven
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
2300 RA Leiden
NETHERLANDS

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

Prof. Dr. Jordan S. Ellenberg
Department of Mathematics
University of Wisconsin-Madison
480 Lincoln Drive
Madison, WI 53706-1388
UNITED STATES

Dr. Tom Fisher
Centre for Mathematical Sciences
University of Cambridge
Wilberforce Road
Cambridge CB3 0WB
UNITED KINGDOM

Prof. Dr. Andrew J. Granville
Department of Mathematics and Statistics
University of Montreal
CP 6128, succ. Centre Ville
Montréal QC H3C 3J7
CANADA

Prof. Dr. Benedict H. Gross
Department of Mathematics
Harvard University
Science Center
One Oxford Street
Cambridge MA 02138-2901
UNITED STATES

Prof. Dr. Farshid Hajir
Office of the Provost
University of Massachusetts
Whitmore Administration Building
181 President's Drive
Amherst, MA 01003-9305
UNITED STATES

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

Prof. Dr. Wei Ho
Department of Mathematics
University of Michigan
East Hall
530 Church Street
Ann Arbor, MI 48109-1109
UNITED STATES

Dr. Borys Kadets
Department of Mathematics
University of Georgia
Athens, GA 30602
UNITED STATES

Prof. Dr. Kiran S. Kedlaya
Department of Mathematics
University of California, San Diego
9500 Gilman Drive
La Jolla, CA 92093-0112
UNITED STATES

Prof. Dr. Jürgen Klüners
Institut für Mathematik
Universität Paderborn
Warburger Strasse 100
33098 Paderborn
GERMANY

Dr. Peter Koymans
Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
GERMANY

Dr. Aaron Landesman
Department of Mathematics
Stanford University
Building 380
450 Jane Stanford Way
Stanford, CA 94305-2125
UNITED STATES

Prof. Dr. Hendrik W. Lenstra
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
2300 RA Leiden
NETHERLANDS

Dr. Wanlin Li
Centre de Recherches Mathématiques
Université de Montreal
C.P. 6128, Succ. Centre-Ville
Montréal QC H3C 3J7
CANADA

Dr. Yuan Liu
Department of Mathematics
University of Michigan
530 Church Street
Ann Arbor MI 48109-1043
UNITED STATES

Prof. Dr. Melanie Matchett Wood
Department of Mathematics
Harvard University
02138 Cambridge
UNITED STATES

Dr. Carlo Pagano
School of Mathematics and Statistics
University of Glasgow
University Place
Glasgow G12 8QQ
UNITED KINGDOM

Ross Paterson
School of Mathematics & Statistics
University of Glasgow
University Place
Glasgow G12 8QQ
UNITED KINGDOM

Prof. Dr. Bjorn Poonen
Department of Mathematics
Massachusetts Institute of Technology
77 Massachusetts Avenue, Bldg. 2-243
Cambridge, MA 02139-4307
UNITED STATES

Prof. Dr. Rachel Pries
Department of Mathematics
Colorado State University
Weber Building
Fort Collins, CO 80523-1874
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. Will Sawin
Department of Mathematics
Columbia University
2990 Broadway
New York, NY 10027
UNITED STATES

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

Dr. Emre Can Sertöz
Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
GERMANY

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

Prof. Dr. Alice Silverberg
Department of Mathematics
University of California, Irvine
Irvine, CA 92697
UNITED STATES

Dr. Alexander Smith
Department of Mathematics
MIT
77 Massachusetts Avenue
02139-4307 Cambridge, MA 02139
UNITED STATES

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

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

Ashvin A. Swaminathan
Department of Mathematics
Princeton University
Fine Hall
Washington Road
Princeton, NJ 08544-1000
UNITED STATES

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

Dr. Ha Tran
Dept. of Mathematics and Statistics
Concordia University of Edmonton
7128 Ada Blvd NW
AB Edmonton T5B 4E4
CANADA

Dr. Nicholas Triantafillou
Department of Mathematics
University of Georgia
Athens, GA 30602
UNITED STATES

Prof. Dr. Akshay Venkatesh
School of Mathematics
Institute for Advanced Study
1 Einstein Drive
Princeton, NJ 08540
UNITED STATES

Dr. Bianca Viray
Department of Mathematics
University of Washington
Padelford Hall
Box 354350
Seattle, WA 98195-4350
UNITED STATES

Prof. Dr. Isabel Vogt
Department of Mathematics
Brown University
Providence, RI 02906
UNITED STATES

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

Prof. Dr. Jose Felipe Voloch
Department of Mathematics
University of Canterbury
Private Bag 4800
Christchurch 8140
NEW ZEALAND

Anne-Edgar P. R. Wilke
Institut de Mathématiques
Université de Bordeaux
351, cours de la Libération
33405 Talence Cedex
FRANCE

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