Mathematisches Forschungsinstitut Oberwolfach

Report No. 34/2018

DOI: 10.4171/OWR/2018/34

Explicit Methods in Number Theory

Organised by
Karim Belabas, Bordeaux
Bjorn Poonen, Cambridge MA
Fernando Rodriguez Villegas, Trieste

22 July – 28 July 2018

Abstract. The aim of the series of Oberwolfach meetings on 'Explicit methods in number theory' is to bring 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 meeting provides a forum for presenting new methods and results on concrete aspects of number theory. Considerable attention is paid to computational issues, but the emphasis is on aspects that are of interest to the pure mathematician. In this respect the meetings differ from virtually all other computationally oriented meetings in number theory (most notably the ANTS series), which have a tendency to place actual implementations, numerical results, and cryptographic implications in the foreground.
The 2018 meeting featured a mini-course on nonabelian Chabauty theory, so several of the talks were on this topic; the other talks covered a broad range of topics in number theory.

Mathematics Subject Classification (2010): 11xx.

Introduction by the Organisers

The workshop Explicit Methods in Number Theory was organised by Karim Belabas (Talence), Bjorn Poonen (Cambridge, MA), and Fernando Rodriguez Villegas (Trieste), and it took place July 22–28, 2018. Nine previous workshops on the topic had been held since 1999. The 2018 instance of the workshop featured a mini-course on nonabelian Chabauty theory, because of the potential for advances in this field that became apparent in recent years.

The non-abelian Chabauty program is aimed at determining the rational and integral points on curves over number fields. It is a conjectural approach and though the initial theoretical ideas were put forth by Minhyong Kim over a decade ago, it was unclear for a long time whether they could ever be made practical enough to solve problems that were inaccessible by other methods. But in the last few years, new theoretical and computational methods have been developed (largely by junior mathematicians) which have begun to bear fruit — we note in particular the recent articles *Computing integral points on hyperelliptic curves using quadratic Chabauty* by Amnon Besser, Jennifer Balakrishnan, Jan Steffen Müller and *Quadratic Chabauty and rational points I: p-adic heights* by Jennifer Balakrishnan and Netan Dogra (with an appendix by Müller), the second of which determines $X(\mathbb{Q})$ for a curve X for which the rank condition necessary for the classical Chabauty method fails.

The workshop brought such works to the attention of experts in explicit arithmetic geometry who might be able to contribute ideas towards the project. The mini-course on the non-abelian Chabauty method consisted of the following talks:

- *Explicit aspects of the Chabauty–Kim method* by Jennifer S. Balakrishnan;
- *p-adic heights and integral points on curves* by Amnon Besser;
- *Mixed Tate motives and the S-unit equation* by David Corwin;
- *Overview of the Chabauty–Kim method* by Ishai Dan-Cohen; and
- *p-adic heights and rational points on curves* by Netan Dogra.

Two other talks presented alternative p-adic approaches to rational points:

- Bas Edixhoven presented a geometric approach to the first non-abelian level of the Chabauty–Kim approach, involving the Poincaré torsor; and
- Brian Lawrence reported on joint work with Akshay Venkatesh using a p-adic period map and p-adic Hodge theory.

As always in Oberwolfach, the atmosphere was lively and active, providing an ideal environment for the exchange of ideas and productive discussions. The meeting was well-attended, with 53 participants from a variety of backgrounds and seniority. There were 27 talks of various lengths, and ample time was allotted to informal collaboration.

The remaining abstracts included here cover the following areas:

- Arithmetic statistics: Levent Alpoge on the average number of rational points on genus 2 curves, Will Sawin on Cohen–Lenstra heuristics, and Jiuya Wang on Malle's conjecture.
- Modularity: Frank Calegari on modularity of abelian surfaces, Henri Cohen on modular forms in PARI/GP, John Cremona on using Bianchi newforms to understand elliptic curves of prime conductor over certain quadratic fields, Paul Gunnells on Siegel modular forms, Adam Logan on modular Calabi-Yau 5-folds, Bianca Viray on low-degree points on modular curves, and David Zureick-Brown on rational points on modular curves associated to nonstandard congruence subgroups.

- Characteristic p geometry: Rachel Pries on unlikely intersections between the Torelli locus and Newton polygon strata in the moduli space of principally polarized abelian varieties.
- Integral models of curves: Tim Dokchitser on an almost purely combinatorial approach to understanding regular models of curves, Elisa Lorenzo García on models of nonhyperelliptic curves whose special fiber is hyperelliptic, and Stefan Wewers on a new software project for calculations with models of curves.
- Endomorphisms and isogenies of abelian varieties: E. Victor Flynn on explicit formulas for abelian surfaces with real multiplication by $\sqrt{3}$, John Voight on computing endomorphism rings, and Isabel Vogt on the failure of a local-global principle for the existence of isogenies between elliptic curves.
- Analytic number theory: Michael Bennett on counting primes in an arithmetic progression, and Mark Watkins on two new analytic approaches to the solution to the class number 1 problem.

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: Explicit Methods in Number Theory

Table of Contents

Levent Alpoge
The average number of rational points on genus two curves over $\mathbb{Q}$ is bounded 2039

Jennifer S. Balakrishnan
Explicit aspects of the Chabauty-Kim method 2040

Amnon Besser
p-adic heights and integral points on curves 2043

Michael A. Bennett (joint with Greg Martin, Kevin O'Bryant, and Andrew Rechnitzer)
Explicit bounds for primes in arithmetic progressions 2043

Frank Calegari (joint with George Boxer, Toby Gee, and Vincent Pilloni)
Modularity of abelian surfaces 2045

David Corwin (joint with Ishai Dan-Cohen)
Mixed Tate Motives and the S-Unit Equation 2045

Henri Cohen (joint with Karim Belabas)
The modular forms package in PARI/GP 2045

John Cremona (joint with Ariel Pacetti)
On elliptic curves of prime conductor over imaginary quadratic fields of class number one 2046

Ishai Dan-Cohen
Overview of the Chabauty-Kim method 2046

Netan Dogra
p-adic heights and rational points on curves 2046

Tim Dokchitser
Regular models of curves 2047

Bas Edixhoven
Quadratic Chabauty and the Poincaré torsor 2047

E. Victor Flynn (joint with Nils Bruin, and Ari Shnidman)
Abelian Surfaces with Multiplication by $\sqrt{3}$. 2050

Elisa Lorenzo García (joint with Reynald Lercier, Qing Liu, and Christophe Ritzenthaler)
Hyperelliptic reduction of plane quartic curves 2052

Paul E. Gunnells (joint with Mathieu Dutour Sikirić)
Computing Hecke operators on Siegel modular forms 2052

Brian Lawrence (joint with Akshay Venkatesh)
Diophantine Problems and a p-adic Period Map 2055

Adam Logan
Three modular fivefolds of level 8 2057

Rachel Pries (joint with Wanlin Li, Elena Mantovan, and Yunqing Tang)
Special Shimura varieties and Newton polygons of cyclic covers of the projective line 2059

Will Sawin (joint with Jacob Tsimerman, and Michael Lipnowski)
New invariants on class groups and Cohen-Lenstra heuristics in the presence of roots of unity 2060

Bianca Viray (joint with Abbey Bourdon, Özlem Ejder, Yuan Liu, Frances Odumodu)
On the level of modular curves that give rise to sporadic j-invariants . . . 2061

Isabel Vogt
A local-global principle for isogenies of composite degree 2062

John Voight (joint with Edgar Costa, Nicolas Mascot, and Jeroen Sijsling)
Rigorous computation of the endomorphism ring of a Jacobian 2062

Jiuya Wang (joint with Robert J. Lemke Oliver, and Melanie Matchett Wood)
Inductive Methods for Proving Malle's Conjecture 2064

Mark Watkins
Two new proofs of class number one 2066

Stefan Wewers (joint with Julian Ruth)
MCLF: a toolbox for computations with Models of Curves over Local Fields 2071

David Zureick-Brown
Progress on Mazur's "Program B" 2071

Abstracts

The average number of rational points on genus two curves over $\mathbb{Q}$ is bounded

Levent Alpoge

Let $f \in \mathbb{Z}[x]$ be such that $\Delta_f := \mathrm{disc}(f) \neq 0$. Let $C_f : y^2 = f(x)$. Let

$$\mathcal{F}_{\mathrm{univ}} := \{f \in \mathbb{Z}[x] : \Delta_f \neq 0, f(x) = x^5 + a_2x^3 + \cdots + a_5 \text{ s.t. } n^{2i} | a_i \forall i \implies n = \pm 1\}.$$

Then $\mathcal{F}_{\mathrm{univ}}$ is the "universal family" of genus two curves over $\mathbb{Q}$ with a marked rational Weierstrass point. Let, for $f \in \mathcal{F}_{\mathrm{univ}}$,

$$H(f) := \max_i |a_i|^{\frac{1}{i}},$$

where $f(x) =: x^5 + a_2x^3 + \cdots + a_5$. We prove that

$$\limsup_{X \to \infty} \frac{\sum_{f \in \mathcal{F}_{\mathrm{univ}} : H(f) \leq X} \#|C_f(\mathbb{Q})|}{\sum_{f \in \mathcal{F}_{\mathrm{univ}} : H(f) \leq X} 1} < \infty.$$

The techniques include sphere packing bounds in high dimensions, gap principles, and Vojta's proof of the Mordell conjecture.

References

[1] Henry Frederick Baker. *An introduction to the theory of multiply periodic functions*. Cambridge University Press, Cambridge, 1907. Digitized in 2007, original from Cabot Library at Harvard University.

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

[3] Oskar Bolza. Darstellung der rationalen ganzen Invarianten der Binärform sechsten Grades durch die Nullwerthe der zugehörigen ϑ-Functionen. *Math. Ann.*, 30(4):478–495, 1887.

[4] Enrico Bombieri. The Mordell conjecture revisited. *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)*, 17(4):615–640, 1990.

[5] J. W. S. Cassels and E. V. Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus 2*, volume 230 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1996.

[6] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[7] Victor Flynn. My Genus 2 Site. https://people.maths.ox.ac.uk/flynn/genus2/. Accessed: 2018-01-22.

[8] David Grant. Formal groups in genus two. *J. Reine Angew. Math.*, 411:96–121, 1990.

[9] H. A. Helfgott and A. Venkatesh. Integral points on elliptic curves and 3-torsion in class groups. *J. Amer. Math. Soc.*, 19(3):527–550, 2006.

[10] Jun-ichi Igusa. Modular forms and projective invariants. *Amer. J. Math.*, 89:817–855, 1967.

[11] G. A. Kabatjanskiĭ and V. I. Levenšteĭn . Bounds for packings on the sphere and in space. *Problemy Peredači Informacii*, 14(1):3–25, 1978.

[12] Helmut Klingen. *Introductory lectures on Siegel modular forms*, volume 20 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1990.

[13] David Mumford. *Tata lectures on theta. II*, volume 43 of *Progress in Mathematics*. Birkhäuser Boston, Inc., Boston, MA, 1984. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura.
[14] Fabien Pazuki. Minoration de la hauteur de Néron-Tate sur les surfaces abéliennes. *Manuscripta Math.*, 142(1-2):61–99, 2013.
[15] Bjorn Poonen and Michael Stoll. Most odd degree hyperelliptic curves have only one rational point. *Ann. of Math. (2)*, 180(3):1137–1166, 2014.
[16] B. Riemann. Ueber das Verschwinden der ϑ-Functionen. *J. Reine Angew. Math.*, 65:161–172, 1866.
[17] Jacques Sesiano. *Books IV to VII of Diophantus' Arithmetica in the Arabic translation attributed to Qus?ā ibn Lūqā*, volume 3 of *Sources in the History of Mathematics and Physical Sciences*. Springer-Verlag, New York, 1982.
[18] Arul Shankar and Xiaoheng Wang. Rational points on hyperelliptic curves having a marked non-Weierstrass point. *Compos. Math.*, 154(1):188–222, 2018.
[19] Michael Stoll. On the height constant for curves of genus two. *Acta Arith.*, 90(2):183–201, 1999.
[20] Michael Stoll. On the height constant for curves of genus two. II. *Acta Arith.*, 104(2):165–182, 2002.
[21] Michael Stoll. An explicit theory of heights for hyperelliptic jacobians of genus three, 2017.
[22] Marco Streng. Computing Igusa class polynomials. *Math. Comp.*, 83(285):275–309, 2014.
[23] Joseph Loebach Wetherell. *Bounding the number of rational points on certain curves of high rank*. ProQuest LLC, Ann Arbor, MI, 1997. Thesis (Ph.D.)–University of California, Berkeley.
[24] Kentaro Yoshitomi. On height functions on Jacobian surfaces. *Manuscripta Math.*, 96(1):37–66, 1998.

Explicit aspects of the Chabauty-Kim method

Jennifer S. Balakrishnan

The aim of the *Chabauty–Kim method* is to compute rational points on a hyperbolic curve $X/\mathbb{Q}$ via a sequence of sets of p-adic points

$$X(\mathbb{Q}_p)_1 \supset X(\mathbb{Q}_p)_2 \supset \cdots \supset X(\mathbb{Q}_p)_n, \tag{1}$$

where each set $X(\mathbb{Q}_p)_k$ contains the set of rational points $X(\mathbb{Q})$. In particular, one would like to show that, for a given curve $X/\mathbb{Q}$, there is a computable depth ℓ at which the set $X(\mathbb{Q}_p)_\ell$ is finite. Moreover, one would like to compute the set $X(\mathbb{Q}_p)_\ell$, which is described by ℓ-fold iterated Coleman integrals.

For instance, when $X/\mathbb{Q}$ is a smooth projective curve of genus g with Jacobian having Mordell–Weil rank less than g, the set $X(\mathbb{Q}_p)_1$ is known to be finite and explicitly computable, by the work of Chabauty [Cha41] and Coleman [Col85a]. This is known as the *Chabauty–Coleman method* and gives rise to a technique that works well in practice for computing rational points on curves.

In a series of landmark papers [Kim09, Kim05, KT08, Kim10], Kim proposed that $X(\mathbb{Q}_p)_1$ can be further refined by studying *Selmer varieties*, giving rise to (1). In particular, the Chabauty–Kim method conjecturally extends the Chabauty–Coleman method to curves with Jacobians having larger Mordell-Weil rank.

Here we describe some computational tools that make it possible to carry out the Chabauty–Kim method for certain classes of curves, as well as some recent examples where the method has been used to solve new Diophantine equations.

As alluded to above, one technique that plays a key role in the method is an algorithm for numerical *iterated Coleman integration*. Coleman [Col82, Col85b] developed a p-adic theory of line integration based on Dwork's principle of *analytic continuation along Frobenius*; this is now known as Coleman integration. Coleman [Col82], Coleman and de Shalit [CdS88], and Besser [Bes02] defined iterated Coleman integrals

$$\int_P^Q \xi_n \cdots \xi_1,$$

which behave formally like iterated path integrals

$$\int_0^1 \int_0^{t_1} \cdots \int_0^{t_{n-1}} f_n(t_n) \cdots f_1(t_1)\, dt_n \cdots dt_1.$$

Besser and de Jeu [BdJ08] were the first to give an algorithm to compute iterated Coleman integrals, in the case of $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$. These integrals are defined by the p-adic differential equations

$$\begin{aligned} \mathrm{Li}_0(z) &= \frac{z}{1-z} \\ d\,\mathrm{Li}_{n+1}(z) &= \mathrm{Li}_n(z)\frac{dz}{z}, n \geq 0. \end{aligned}$$

Dan-Cohen and Wewers [DCW15, DCW16] used the Besser–de Jeu algorithm in a number of cases for computing S-integral points on $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ using the Chabauty–Kim method.

The author, in joint work with Bradshaw and Kedlaya [BBK10], gave an algorithm for computing single Coleman integrals on hyperelliptic curves. This was extended in two directions, first in [Bal13] to iterated Coleman integrals on hyperelliptic curves, and more recently, in joint work with Tuitman [BT17], to single integrals on smooth curves. The key step in all of these algorithms is to compute the action of Frobenius on a p-adic cohomology group and use this to relate integrals pulled back by Frobenius to other simpler integrals that can be computed without Frobenius. Taking $\{\omega_0, \ldots, \omega_{2g-1}\}$ a basis for $H^1_{\mathrm{dR}}(X_{\mathbb{Q}_p})$, one computes the action of p-power Frobenius F_p as

$$F_p^*(\omega_i) = df_i + \sum_{j=0}^{2g-1} \Phi_{ij}\omega_j,$$

then uses properties of the Coleman integral to deduce the values of integrals on basis differentials between points P, Q where the f_i converge:

$$\sum_{j=1}^{2g} (\Phi - I)_{ij} \left(\int_P^Q \omega_j \right) = f_i(P) - f_i(Q) - \int_P^{F_p(P)} \omega_i - \int_{F_p(Q)}^Q \omega_i.$$

These Coleman integration algorithms are used in work of the author with Besser and Müller [BBM16] in computing integral points on affine models of hyperelliptic curves having Jacobians with Mordell-Weil rank equal to genus, as well as work of the author with Dogra, Müller, Tuitman, and Vonk [BDM$^+$17], to compute rational points on $X_s(13)$, the split Cartan curve of level 13. The curve $X_s(13)$ is of interest as the last remaining split Cartan case of Serre's uniformity problem, after the work of Bilu–Parent–Rebolledo [BPR13]. It has genus 3, and its Jacobian has rank 3. As such, it was not amenable to standard techniques for computing rational points.

We compute $X_s(13)(\mathbb{Q})$ using *quadratic Chabauty*, i.e., functions vanishing on $X(\mathbb{Q}_p)_2$. Given a curve $X/\mathbb{Q}$, one computes a quadratic Chabauty function (QCF) by associating to points $x \in X(\mathbb{Q})$ certain p-adic Galois representations $A(x)$, and then computing their p-adic heights $h(A(x))$ [Nek93]. This representation depends on a choice of "nice" correspondence on X, which exists when the rank of the Néron-Severi group of the Jacobian of X is larger than 1. Moreover, the global p-adic height can be written as $h = \sum h_v$, a finite sum of local heights h_v. When X has everywhere potentially good reduction, the local height contributions away from p are trivial. The local height h_p can be computed using p-adic Hodge theory, using an explicit description of $D_{cris}(A(x))$ as a filtered ϕ-module.

In the case of $X = X_s(13)$, the rank of the Néron-Severi group of its Jacobian is 3; moreover, X has everywhere potentially good reduction. This allows us to compute two different QCFs, and we find that $X_s(13)(\mathbb{Q})$ consists of precisely seven points.

References

[Bal13] J. S. Balakrishnan, *Iterated Coleman integration for hyperelliptic curves*, ANTS-X: Proceedings of the Tenth Algorithmic Number Theory Symposium (E. W. Howe and K. S. Kedlaya, eds.), Open Book Series, vol. 1, Mathematical Sciences Publishers, 2013, pp. 41–61.

[BBK10] J. S. Balakrishnan, R. W. Bradshaw, and K. S. Kedlaya, *Explicit Coleman integration for hyperelliptic curves*, Algorithmic Number Theory (G. Hanrot, F. Morain, and E. Thomé, eds.), Lecture Notes in Computer Science, vol. 6197, Springer, 2010, pp. 16–31.

[BBM16] Jennifer S. Balakrishnan, Amnon Besser, and J. Steffen Müller, *Quadratic Chabauty: p-adic heights and integral points on hyperelliptic curves*, J. Reine Angew. Math. **720** (2016), 51–79.

[BdJ08] A. Besser and R. de Jeu, Li$^{(p)}$*-service? An algorithm for computing p-adic polylogarithms*, Math. Comp. **77** (2008), no. 262, 1105–1134.

[BDM$^+$17] J. S. Balakrishnan, N. Dogra, J. S. Muller, J. Tuitman, and J. Vonk, *Explicit Chabauty-Kim for the split Cartan modular curve of level 13*, arXiv preprint arXiv:1711.05846 (2017).

[Bes02] A. Besser, *Coleman integration using the Tannakian formalism*, Math. Ann. **322** (2002), 19–48.

[BPR13] Y. Bilu, P. Parent, and M. Rebolledo, *Rational points on $X_0^+(p^r)$*, Ann. Inst. Fourier **63** (2013), no. 3, 957–984.

[BT17] Jennifer S. Balakrishnan and Jan Tuitman, *Explicit Coleman integration for curves*, arXiv preprint 1710.01673 (2017).

[CdS88] R. F. Coleman and E. de Shalit, *p-adic regulators on curves and special values of p-adic L-functions*, Invent. Math. **93** (1988), no. 2, 239–266.
[Cha41] C. Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, C. R. Acad. Sci. Paris **212** (1941), 882–885.
[Col82] R. F. Coleman, *Dilogarithms, regulators and p-adic L-functions*, Invent. Math. **69** (1982), no. 2, 171–208.
[Col85a] ———, *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765–770.
[Col85b] ———, *Torsion points on curves and p-adic abelian integrals*, Ann. of Math. (2) **121** (1985), no. 1, 111–168.
[DCW15] Ishai Dan-Cohen and Stefan Wewers, *Explicit Chabauty-Kim theory for the thrice punctured line in depth 2*, Proc. Lond. Math. Soc. (3) **110** (2015), no. 1, 133–171. MR 3299602
[DCW16] ———, *Mixed Tate motives and the unit equation*, Int. Math. Res. Not. IMRN (2016), no. 17, 5291–5354.
[Kim05] M. Kim, *The motivic fundamental group of* $\mathbf{P}^1 \setminus \{0, 1, \infty\}$ *and the theorem of Siegel*, Invent. Math. **161** (2005), no. 3, 629–656.
[Kim09] ———, *The unipotent Albanese map and Selmer varieties for curves*, Publ. Res. Inst. Math. Sci. **45** (2009), no. 1, 89–133.
[Kim10] ———, *Massey products for elliptic curves of rank 1*, J. Amer. Math. Soc. **23** (2010), 725–747.
[KT08] M. Kim and A. Tamagawa, *The l-component of the unipotent Albanese map*, Math. Ann. **340** (2008), no. 1, 223–235.
[Nek93] J. Nekovář, *On p-adic height pairings*, Séminaire de Théorie des Nombres, Paris, 1990–91, Birkhäuser Boston, Boston, MA, 1993, pp. 127–202.

p-adic heights and integral points on curves

Amnon Besser

We survey quadratic Chabauty, which is a method for getting a Coleman function on $X(\mathbb{Q}_p)$ that vanishes on all the integral points of X, assuming that the rank of the rational points on the Jacobian of X is the same as the genus of X. The method uses p-adic heights, and we explain these in general using work of Nekovar.[1]

Explicit bounds for primes in arithmetic progressions

Michael A. Bennett
(joint work with Greg Martin, Kevin O'Bryant, and Andrew Rechnitzer)

We derive explicit upper bounds for various counting functions for primes in arithmetic progressions. By way of example, if q and a are integers with $\gcd(a, q) = 1$ and $3 \leq q \leq 10^5$, and $\theta(x; q, a)$ denotes the sum of the logarithms of the primes $p \equiv a \mod q$ with $p \leq x$, we show that

$$\left|\theta(x; q, a) - x/\phi(q)\right| < \frac{1}{160} \frac{x}{\log x}$$

for all $x \geq 8 \cdot 10^9$, with significantly sharper constants obtained for individual moduli q. We establish inequalities of the same shape for the other standard

[1]Compiled by the reporter from the hand-written abstract at Oberwolfach

prime-counting functions $\pi(x;q,a)$ and $\psi(x;q,a)$, as well as inequalities for the nth prime congruent to $a \mod q$ when $q \leq 1200$. For moduli $q > 10^5$, we find even stronger explicit inequalities, but only for much larger values of x. Along the way, we also derive an improved explicit lower bound for $L(1,\chi)$ for quadratic characters χ, and an improved explicit upper bound for exceptional zeros.

The current literature naturally enough contains a number of explicit bounds for primes in arithmetic progression. Rather surprisingly, the great majority of these have the property that, unlike ours, their error terms are the same order of magnitude as their main terms, i.e. they are of "Chebyshev" type and do not actually imply the Prime Number Theorem for Arithmetic Progressions. Deriving good approximations for the classical functions counting primes in arithmetic progressions $\psi(x;q,a)$, $\theta(x;q,a)$, and $\pi(x;q,a)$ depends upon understanding the distribution of the zeros of Dirichlet L-functions. As is traditional in this subject, our approach takes as a starting point von Mangoldt's formula, and hence we are led to initially derive bounds for $\psi(x;q,a)$, from which our estimates for $\theta(x;q,a)$ and $\pi(x;q,a)$ follow. The fundamental arguments providing the connection between zeros of Dirichlet L-functions and explicit bounds for error terms in prime counting functions derive from classic work of Rosser and Schoenfeld [7], as extended by McCurley [3], and subsequently by Ramaré and Rumely [6] and Dusart [1]. The main ingredients involved include explicit zero-free regions for Dirichlet L-functions by Kadiri [2] and McCurley [4], explicit estimates for the zero-counting function for Dirichlet L-functions by Trudgian [8], and the results of large-scale computations of Platt [5], all of which we cite from the literature. Other necessary results include lower bounds for $L(1,\chi)$ for quadratic characters χ, upper bounds for exceptional zeros of L-functions with associated character χ, and explicit inequalities for $b(\chi)$, the constant term in the Laurent expansion of $\frac{L'}{L}(s,\chi)$ at $s=0$

References

[1] P. Dusart. Estimates of $\theta(x;k,l)$ for large values of x. *Math. Comp.* **71** (2002), no. 239, 1137–1168.

[2] H. Kadiri. Explicit zero-free regions for Dirichlet L-functions. *Mathematika* **64** (2018), no. 2, 445–474.

[3] K. S. McCurley. Explicit estimates for the error term in the prime number theorem for arithmetic progressions. *Math. Comp.* **42** (1984), no. 165, 265–285.

[4] K. S. McCurley. Explicit zero-free regions for Dirichlet L-functions. *J. Number Theory* **19** (1984), no. 1, 7–32.

[5] D. J. Platt. Numerical computations concerning the GRH. *Math. Comp.* **85** (2016), no. 302, 3009–3027.

[6] O. Ramaré and R. Rumely. Primes in arithmetic progressions. *Math. Comp.* **65** (1996), 397–425.

[7] J. B. Rosser and L. Schoenfeld. Approximate formulas for some functions of prime numbers. *Ill. J. Math.* **6** (1962), 64–94.

[8] T. Trudgian. An improved upper bound for the error term in the zero-counting formulae for Dirichlet L-functions and Dedekind zeta-functions. *Math. Comp.* **84** (2015), 1439–1450.

Modularity of abelian surfaces

Frank Calegari
(joint work with George Boxer, Toby Gee, and Vincent Pilloni)

I shall discuss some recent progress in modularity lifting [1]. Some applications include a proof of the Hasse–Weil conjecture for genus two curves $X/\mathbf{Q}$, and the potential modularity of abelian surfaces over totally real fields.

References

[1] G. Boxer, F. Calegari, T. Gee, V. Pilloni, *Abelian Surfaces over totally real fields are Potentially Modular*, preprint.

Mixed Tate Motives and the S-Unit Equation

David Corwin
(joint work with Ishai Dan-Cohen)

We describe work by the speaker and Ishai Dan-Cohen, building on similar work of Brown, Dan-Cohen, and Wewers, that computes with Kim's method in the case of the S-unit equation, geometrically the projective line minus three points. For computational purposes, it is best to replace an abstract Galois group by a Tannakian Galois group, whose category of representations is equivalent (up to extension of scalars) to the relevant category of Galois representations. Being an algebraic group, this Tannakian Galois group is described by its Hopf algebra of regular functions, and this Hopf algebra in fact has the structure of a graded Hopf algebra. The Hopf algebra can then be abstractly described as a graded Hopf algebra via the rational algebraic K-theory of the S-integers (which correspond to the Ext groups in this category of representations). At the same time, one may define explicit elements of this Hopf algebra as motivic versions of special values of polylogarithms. In the end, most of the explicit computations have to do with computing coproducts of these motivic special values to relate them to the abstract description of the Hopf algebra.

The modular forms package in PARI/GP

Henri Cohen
(joint work with Karim Belabas)

We present the Modular Forms package in the PARI/GP system, which computes spaces of classical modular forms $M_k(\Gamma_0(N), \chi)$, $k \in \frac{1}{2}\mathbb{Z}$, and standard subspaces. Contrary to most existing implementations, which use modular symbols, the package relies on trace formulas for integral $k > 1$. The cases $k = 1$, respectively k half-integral, are treated by multiplying by an appropriate fixed Eisenstein series of weight 1, respectively a theta series of weight $\frac{1}{2}$, and working in the larger space of integral weight $k + 1$, respectively $k + \frac{1}{2}$.

Once the space is generated together with a fixed basis, a basic class of functions involves nothing more than linear algebra over cyclotomic fields: e.g., Hecke operators or splitting the new space. The rest of the package relies on an explicit rewriting of a given basis in terms of products of the Eisenstein series. This in particular allows one to recoved the Fourier coefficients of $f|\gamma$ for arbitrary $\gamma \in \mathrm{PSL}_2(\mathbb{Z})$, hence to evaluate forms at arbitrary points in $\mathfrak{h}$ or to evaluate Petersson scalar products, including weight 1 and half-integral weight.[2]

On elliptic curves of prime conductor over imaginary quadratic fields of class number one

John Cremona
(joint work with Ariel Pacetti)

We extend from $\mathbb{Q}$ to each of the nine imaginary quadratic fields of class number one a result of Serre (1987) and Mestre-Oesterlé (1989), namely that every isogeny class of elliptic curves over $\mathbb{Q}$ of prime conductor p contains a curve of minimal discriminant $\pm p$. For four of the nine fields the theorem holds with no essential change, while for the other five fields (those in which 2 is inert) the isogeny class contains a curve whose minimal discriminant has valuation 1 or 2. The proof is conditional, and relies on the curves in question being modular (in the sense of being attached to suitable Bianchi newforms) together with a certain level-lowering conjecture for Bianchi newforms.[3]

Overview of the Chabauty-Kim method

Ishai Dan-Cohen

I will discuss (in brief outline) the Bloch-Kato exponential, the unipotent fundamental group, Olsson's nonabelian p-adic Hodge theory, and Kim's Selmer varieties and their use in bounding sets of integral points on hyperbolic curves.[4]

p-adic heights and rational points on curves

Netan Dogra

In this talk we explain some situations in which one can compute finite sets of p-adic points of a curve over $\mathbb{Q}$ containing the set of rational points under certain conditions on the Mordell-Weil rank and Picard number of the Jacobian. The finite sets are described in terms of Nekovar p-adic heights.[5]

[2]Compiled by the reporter from the hand-written abstract at Oberwolfach
[3]Compiled by the reporter from the hand-written abstract at Oberwolfach
[4]Compiled by the reporter from the hand-written abstract at Oberwolfach
[5]Compiled by the reporter from the hand-written abstract at Oberwolfach

Regular models of curves

Tim Dokchitser

In this talk I explained how to construct regular models and study invariants of arithmetic surfaces using a toric resolution derived from the defining equation.

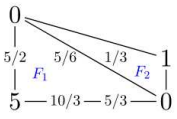
Say K is a field with a discrete valuation v_K and residue field k, and C/K is a smooth projective curve specified by an affine equation $f(x,y)=0$. It turns out that the Newton polytope Δ_v of f with respect to v_K, under a 'generic' condition called Δ_v-regularity, determines explicitly

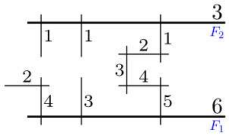
— the minimal regular normal crossings model of C over O_K;
— whether C and $\operatorname{Jac} C$ have good, semistable and tame reduction;
— the action of $\mathrm{Gal}(\bar{K}/K)$ on $H^1_{\text{ét}}(C_{\bar{K}},\mathbb{Q}_l)$ when C is tamely ramified, and the action on its wild inertia invariants in general, for $l \neq \operatorname{char} k$;
— a basis of global sections of the relative dualising sheaf;
— the reduction map on points from the generic to the special fibre.

A regular model is usually constructed by starting with any model over O_K, and repeatedly blowing up at points and components of the special fibre and taking normalisations. In effect, the toric resolution replaces repeated blow-ups along coordinate axes, and for Δ_v-regular curves one such resolution is enough to get a good model.

For example, say $\pi \in K$ is a uniformiser, and take a curve (left)

$$C\colon\ y^2+\pi x^3 y+x^3+\pi^5=0$$





Its Newton polygon Δ_v is in the middle. Elementary numerology determines the shape of the special fibre of the regular model of C over O_K with normal crossings (right). We refer the reader to [1], and Magma implementation [2].

References

[1] T. Dokchitser, Models of curves over DVRs, preprint, June 2018, arXiv: 1807.00025.
[2] `https://people.maths.bris.ac.uk/~matyd/newton/`

Quadratic Chabauty and the Poincaré torsor

Bas Edixhoven

In the workshop a minicourse was given on the Chabauty-Kim method, and in particular on the recent advances in "quadratic Chabauty." *This* talk concerned a recent development in a joint project of Guido Lido (a PhD student of René Schoof) and me that started only a few months before the workshop. The aim of that project is to replace everything in quadratic Chabauty by "good old-fashioned" geometry over $\mathbb{Z}$ and over $\mathbb{Z}/p^2\mathbb{Z}$, not to prove or reprove general finiteness results, but to find $C(\mathbb{Q})$ for specific curves C over $\mathbb{Q}$.

Below I briefly describe how we intend to do this. Handwritten notes of the talk can be found in [1]. A good reference for what we mean by "good old-fashioned" geometry is [2].

The idea behind this project is very simple: if the Mordell-Weil rank is too high for ordinary Chabauty, that is, higher than the dimension of the ambient group, then try to increase the ambient dimension accordingly, while keeping the dimension of the p-adic closure of the set of rational points the same. In our project, the ambient variety is not a group, but has a quadratic structure coming from biextensions, and one has to work over $\mathbb{Z}$ because $\mathbb{Q}^\times$ is too big, while $\mathbb{Z}^\times$ is small.

The insight that the Poincaré torsor plays an important role in quadratic Chabauty came from my work, joint with Daniel Bertrand, where we heavily use that, as a complex variety, the Poincaré torsor is the moduli space of mixed $\mathbb{Z}$-Hodge structures of weights -2, -1 and 0, with $\mathbb{Z}(1)$ in weight -2, $\mathrm{H}_1(C(\mathbb{C}),\mathbb{Z})$ in the middle, and $\mathbb{Z}(0)$ in weight 0, that correspond precisely to the kind of p-adic Galois representations occuring in quadratic Chabauty. Of course, Deligne's 1-motives give the algebraic description of the Poincaré torsor as a moduli space.

Let C be a curve over $\mathbb{Z}$, proper, regular, flat, with geometrically connected fibers, of genus $g \geq 2$, smooth over $\mathbb{Z}[1/n]$ ($n \geq 1$), and let J be the Néron model over $\mathbb{Z}$ of the jacobian of $X_\mathbb{Q}$. Then we have the Poincaré bundle $B_\mathbb{Q}$ on $J_\mathbb{Q} \times J^\vee_\mathbb{Q}$, trivialised on the union of the zero sections over $J_\mathbb{Q}$ and $J^\vee_\mathbb{Q}$. The Poincaré torsor is then the $\mathbb{G}_\mathrm{m}$-torsor $P_\mathbb{Q} = \mathrm{Isom}(\mathcal{O}, B_\mathbb{Q})$ (trivial locally for the Zariski topology) on $J_\mathbb{Q} \times J^\vee_\mathbb{Q}$. It has a unique *biextension structure* coming from the theorem of the square, or, equivalently, from the interpretation of $J^\vee_\mathbb{Q}$ as the base space for the universal extension of $J_\mathbb{Q}$ by $\mathbb{G}_\mathrm{m}$.

We let $J^{\vee,0}$ be the fiberwise connected component of the Néron model of $J^\vee_\mathbb{Q}$, and let $\Phi := J^\vee/J^{\vee,0}$; hence Φ is a finite groupscheme over $\mathbb{Z}$, supported on $\mathbb{Z}/n\mathbb{Z}$. We let m be the smallest positive integer that annihilates all the groups $\Phi(\overline{\mathbb{F}}_p)$ with p dividing n. Then $P_\mathbb{Q}$, with its biextension structure, extends uniquely to a $\mathbb{G}_\mathrm{m}$-torsor P on $J \times J^{\vee,0}$.

Our next assumption is that we have a $b \in C(\mathbb{Q}) = C^{\mathrm{sm}}(\mathbb{Z})$. That gives us an immersion $j_b \colon C^{\mathrm{sm}} \to J$, sending $P \mapsto [P - b]$. Picard functoriality applied to j_b gives $j_b^* = -\lambda^{-1} \colon J^\vee_\mathbb{Q} \to J_\mathbb{Q}$, with λ the canonical principal polarisation. Let $\mathrm{NS}_{J_\mathbb{Q}/\mathbb{Q}}$ be the $\mathbb{Q}$-group scheme $\mathrm{Pic}_{J_\mathbb{Q}/\mathbb{Q}}/J^\vee_\mathbb{Q}$. Then $\ker(j_b^* \colon \mathrm{Pic}(J_\mathbb{Q}) \to \mathrm{Pic}(C_\mathbb{Q}))$ is equal to the kernel of $j_b^* \colon \mathrm{NS}_{J_\mathbb{Q}/\mathbb{Q}}(\mathbb{Q}) \to \mathbb{Z}$. Note that $\mathrm{NS}_{J_\mathbb{Q}/\mathbb{Q}}(\mathbb{Q}) = \mathrm{End}(J_\mathbb{Q})^+$, the ring of symmetric endomorphisms of $J_\mathbb{Q}$; as a $\mathbb{Z}$-module it is free of finite rank, and we denote that rank by ρ. Then $\ker(j_b^* \colon \mathrm{Pic}(J_\mathbb{Q}) \to \mathrm{Pic}(C_\mathbb{Q}))$ is free of rank $\rho - 1$. And note that the map $j_b^* \colon \mathrm{End}(J_\mathbb{Q})^+ \to \mathbb{Z}$ is the trace map (trace on $\mathrm{H}_1(J(\mathbb{C}),\mathbb{Z})$).

Let $\mathcal{L}_1, \ldots, \mathcal{L}_{\rho-1}$ be a $\mathbb{Z}$-basis of the kernel of $j_b^* \colon \mathrm{Pic}(J_\mathbb{Q}) \to \mathrm{Pic}(C_\mathbb{Q})$, with each $\mathcal{L}_i$ rigidified at 0. For each line bundle $\mathcal{L}$ on $J_\mathbb{Q}$, we have the usual morphism $\varphi_\mathcal{L} \colon J_\mathbb{Q} \to J^\vee_\mathbb{Q}$, sending a point x to $\mathrm{tr}_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$, and

$$\mathcal{L}^{\otimes 2} = \mathcal{L} \otimes (-\mathrm{id}^*\mathcal{L}^{-1}) \otimes \mathcal{L} \otimes (-\mathrm{id}^*\mathcal{L})\,.$$

Here, $\mathcal{L} \otimes (-\mathrm{id}^* \mathcal{L}^{-1})$ corresponds to a point c in $J^\vee_{\mathbb{Q}}(\mathbb{Q})$, and

$$\mathcal{L} \otimes (-\mathrm{id}^* \mathcal{L}) = (\mathrm{id}, \varphi_{\mathcal{L}})^* B_{\mathbb{Q}} \,.$$

Then we have (assuming that $\mathcal{L}$ is rigidified at 0)

$$\mathcal{L}^{\otimes 2} = (\mathrm{id}, f_{\mathcal{L}})^* B_{\mathbb{Q}} \,, \quad \text{with} \quad f_{\mathcal{L}} = \mathrm{tr}_c \circ \varphi_{\mathcal{L}} \colon J_{\mathbb{Q}} \to J^\vee_{\mathbb{Q}} \,.$$

The fact that, for each i, $\mathcal{L}_i^{\otimes 2}$ becomes trivial on $C_{\mathbb{Q}}$ after pullback by j_b means that the immersion $j_b \colon C_{\mathbb{Q}} \to J_{\mathbb{Q}}$ lifts to the $\mathbb{G}_{\mathrm{m}}^{\rho-1}$-torsor $P'_{\mathbb{Q}}$ on $J_{\mathbb{Q}}$ obained from $P_{\mathbb{Q}}^{\rho-1}$ via pullback as follows by the morphism $(\mathrm{id}, f_{\mathcal{L}_1}, \ldots, f_{\mathcal{L}_{\rho-1}}) \colon J_{\mathbb{Q}} \to J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\vee,\rho-1}$

$$\begin{array}{ccccc} & & P'_{\mathbb{Q}} & \longrightarrow & P_{\mathbb{Q}}^{\rho-1} \\ & \overset{\widetilde{j_b}}{\nearrow} & \downarrow & & \downarrow \\ C_{\mathbb{Q}} & \xrightarrow[j_b]{} & J_{\mathbb{Q}} & \longrightarrow & J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\vee,\rho-1} \end{array}$$

The next step is to extend the geometry over $\mathbb{Z}$. Each $f_{\mathcal{L}_i}$ extends to $f_{\mathcal{L}_i} \colon J \to J^\vee$, and by definition of m, we have

$$m \cdot f_{\mathcal{L}_i} \colon J \to J^{\vee,0} \,.$$

For each i we have $(\mathrm{id}, m \cdot f_{\mathcal{L}_i})^* B_{\mathbb{Q}} = \mathcal{L}_i^{\otimes 2m}$. The morphism j_b extends uniquely to $j_b \colon C^{\mathrm{sm}} \to J$. The line bundle $j_b^* (\mathrm{id}, m \cdot f_{\mathcal{L}_i})^* B$ on C^{sm} is trivialisable on $C_{\mathbb{Q}}$, hence trivialisable (uniquely up to a sign) on any of the finitely many open subschemes U of C^{sm} obtained by removing all but 1 of the irreducible components of each of the reducible fibres of C^{sm}. Note that every element of $C(\mathbb{Q})$ extends uniquely to an element of a $U(\mathbb{Z})$ for a unique U. For such a U, we have the morphism

$$(\mathrm{id}, m f_{\mathcal{L}_1}, \ldots, m f_{\mathcal{L}_{\rho-1}}) \colon J \to J \times_{\mathbb{Z}} J^{\vee,0,\rho-1}$$

and the diagram

$$\begin{array}{ccccc} & & P'' & \longrightarrow & P^{\rho-1} \\ & \overset{\widetilde{j_b}}{\nearrow} & \downarrow & & \downarrow \\ U & \xrightarrow[j_b]{} & J & \longrightarrow & J \times_{\mathbb{Z}} J^{\vee,0,\rho-1} \end{array}$$

The map $P''(\mathbb{Z}) \to J(\mathbb{Z})$ is a $(\pm 1)^{\rho-1}$-torsor. Optimistically, we therefore expect that for each prime p the closure of $P''(\mathbb{Z})$ in $P''(\mathbb{Z}_p)$ is a p-adic manifold of dimension at most $r := \mathrm{rank}(J(\mathbb{Z}))$, meeting $C(\mathbb{Z}_p)$ in only finitely many points. What we intend to do next is to state and prove a theorem that, for p a prime of good reduction and for each $x \in C(\mathbb{F}_p)$, gives sufficient conditions, that one can check with a computer, in terms of the set $P''(\mathbb{Z}/p^2\mathbb{Z})_x$ of the $\mathbb{Z}/p^2\mathbb{Z}$-valued points of P'' that reduce to $\widetilde{j_b}(x)$ in $P''(\mathbb{F}_p)$ for concluding that the list of known elements of $C(\mathbb{Q})$ is all of it, and to carry this out for as many curves as we can. We also intend to clarify how our approach relates to the usual one. We expect that, choosing analytic coordinates on $P^{\rho-1}$ that correspond to the logarithm of

the biextension, the closure of $P''(\mathbb{Z})$ is described by the functions that are used in the usual approach.

We (Bas and Guido) thank Netan Dogra, Steffen Müller and Jennifer Balakrishnan for the encouraging discussions we had with them in Leiden, Groningen and Oberwolfach.

References

[1] S.J. Edixhoven, *Quadratic Chabauty and the Poincaré torsor*, Scan of handwritten notes of a talk at Oberwolfach, July 27, 2018.
`http://pub.math.leidenuniv.nl/~edixhovensj/talks/2018/2018_07_27_Oberwolfach.pdf`

[2] L. Moret-Bailly, *Métriques permises.* Séminaire sur les pinceaux arithmétiques: la conjecture de Mordell. (Paris, 1983/84). Astérisque No. 127 (1985), 29–87.

Abelian Surfaces with Multiplication by $\sqrt{3}$.

E. Victor Flynn
(joint work with Nils Bruin, and Ari Shnidman)

We first recall the following result (Theorem 6 in [2]), parametrising curves C of genus 2 whose Jacobians J admit a $(3,3)$-isogeny.

Theorem 1. *Let k be a field of characteristic different from $2,3$ and suppose that (C,T_1,T_2) consists of a genus 2 curve C over k and $T_1,T_2 \in \mathrm{Pic}(\mathcal{C}/k)[3]$ such that $\#\langle T_1,T_2\rangle = 9$ and $e_3(T_1,T_2)=1$, where e_3 is the non-degenerate, bilinear, alternating* Weil pairing $e_3\colon J[3]\times J[3]\to\mu_3$, *and where μ_3 is the group scheme representing the cube roots of unity. If the specified data is sufficiently general then (C,T_1,T_2) is isomorphic to a suitable specialization of r,s,t in the family described by the following data.*

$$\begin{aligned} H_1 &= x^2+rx+t \\ \lambda_1 &= 4s \\ G_1 &= (s-st-1)x^3+3s(r-t)x^2+3sr(r-t)x-st^2+sr^3+t \end{aligned}$$

$$\begin{aligned} H_2 &= x^2+x+r \\ \lambda_2 &= 4st \\ G_2 &= (s-st+1)x^3+3s(r-t)x^2+3sr(r-t)x-st^2+sr^3-t. \end{aligned}$$

Here $\mathcal{C}_{rst}\colon y^2=F_{rst}(x)=G_i^2+\lambda_i H_i^3$, with Jacobian $\mathcal{J}_{rst}$, and $T_i=[\{H_i(x)=0, y-G_i(x)=0\}-\kappa]$ for $i=1,2$, where κ is a canonical divisor.

If we let Σ denote $\langle T_1,T_2\rangle$, then $\mathcal{J}_{rst}/\Sigma$ is the Jacobian of a similar curve, as described in the following result (which is Theorem 10 in [2]).

Theorem 2. *Let $\mathcal{C}_{rst}$ be as described by Theorem 1. Then $\widetilde{\mathcal{J}}_{rst}=\mathcal{J}_{rst}/\Sigma$ is the Jacobian of the genus 2 curve*

$$\widetilde{\mathcal{C}}_{rst}\colon\ -3y^2=\widetilde{G}_4^2+\tilde{\lambda}_4\widetilde{H}_4^3,$$

with

$$\begin{aligned}\widetilde{G}_4 &= \Delta\left((s-st-1)x^3+3s(r-t)x^2+3rs(r-t)x+(r^3s-st^2-t)\right),\\ \widetilde{H}_4 &= (r-1)(rs-st-1)x^2+(r^3s-2r^2s+rst+r-st^2+st-t)x\\ &\quad -(r^2-t)(rs-st-1),\\ \tilde{\lambda}_4 &= 4\Delta st,\end{aligned}$$

where

(2)

$$\begin{aligned}\Delta = {} & r^6s^2-6r^4s^2t-3r^4s+2r^3s^2t^2+2r^3s^2t+3r^3st+r^3s+r^3+9r^2s^2t^2+6r^2st\\ & -6rs^2t^3-6rs^2t^2-9rst^2-3rst-3rt+s^2t^4+2s^2t^3+s^2t^2+2st^3\\ & +3st^2+t^2+t.\end{aligned}$$

If we adopt the notation, for any $C : y^2 = F(x)$, that $C^{(d)} : dy^2 = F(x)$ is the quadratic twist by d, then we find that the above $\widetilde{\mathcal{C}}_{rst}^{(-3)}$ is of the form $\mathcal{C}_{r's't'}$, as described in the below result (which is Lemma 11 of [2]).

Lemma 1. *Let $\mathcal{C}_{rst}$ be as in Theorem 1, let $\widetilde{\mathcal{C}}_{rst}$ be as in Theorem 2, and let $\widetilde{\mathcal{C}}_{rst}^{(-3)}$ be the quadratic twist of $\widetilde{\mathcal{C}}_{rst}$ by -3. Define ψ_0 by*

$$\psi_0(r,s,t)=\Big(\frac{-s(r-1)(r^2-t)(\delta_5-r)}{(rs-st-1)^2\delta_4},\ \frac{(rs-st-1)^3\delta_4^2}{st(r-1)^3\Delta},\ \frac{s^2(r-1)^3(r^2-t)^3}{(rs-st-1)^3\delta_4^2}\Big),$$

where $\delta_4 = r^3-3rt+t^2+t$ and $\delta_5 = r^3s-3rst+st^2+st+t$. Then $\mathcal{C}_{r's't'}$ is birationally equivalent to $\widetilde{\mathcal{C}}_{rst}^{(-3)}$, where $(r',s',t')=\psi_0(r,s,t)$. Furthermore, as a rational map we have $\psi_0(\psi_0(r,s,t))=(r,s,t)$. The $\Sigma^{(-3)}$ level structure induced on $\widetilde{\mathcal{J}}_{rst}$ determines the kernel of the dual isogeny $\widetilde{\mathcal{J}}_{rst}\to\mathcal{J}_{rst}$

We note that, using the above formulas, we find that $\widetilde{\mathcal{C}}_{rst}^{(-3)}$ is birationally equivalent over k to $\mathcal{C}_{rst}$ when $g(r,s,t)=0$, where

(3)

$$\begin{aligned}g(r,s,t) = {} & r^6s^2t+r^6s^2-3r^5s^2t-3r^4s^2t^2+r^3s^2t^3+r^6s-3r^4s^2t+12r^3s^2t^2\\ & -3r^2s^2t^3-3r^5s-3r^4st+r^3s^2t+2r^3st^2-3r^2s^2t^2-3rs^2t^3+s^2t^4\\ & +12r^3st-6r^2st^2+s^2t^3+r^3t-3r^2st-3rst^2+2st^3+r^3\\ & -3r^2t+st^2+t^2.\end{aligned}$$

It can be checked that $g(r,s,t)=0$ is geometrically a rational surface.

In this work, we find a change in parameters from r,s,t to u,v,w to obtain a parametrisation $\mathcal{C}_{uvw}$ for which $\mathcal{J}_{uvw}[3]$ has a subgroup of the form $\mathbb{Z}/3\times\mu_3$. That is to say: $\mathcal{C}_{uvw} : y^2 = G_a^2+\lambda_a H_a^3 = -3G_b^2+\lambda_b H_b^3$. We use this to obtain $h(u,v,w)$ with the property that $\mathcal{J}_{uvw}$ has real multiplication by $\sqrt{3}$ over k when $h(u,v,w)=0$, and show this also to be a rational surface. This results in the parametrisation over k of a family for which $\mathcal{J}_{uvw}$ has real multiplication by $\sqrt{3}$ over k.

We also described work in progress, aiming to generalise ideas in [1] and aiming to show that, for a large subset of this family there are many quadratic twists with nontrivial 3-part of the Tate-Shafarevich group.

References

[1] M. Bhargava, Z. Klagsbrun, R. Lemke Oliver, and A. Shnidman. *On the proportion of twists with non-trivial Tate-Shaferevich groups in quadratic twist families*, preprint (2018).
[2] N. Bruin, E.V. Flynn and D. Testa. *Descent via* $(3,3)$*-isogeny on Jacobians of genus* 2 *curves.* Acta Arith. **165** (2014), 201–223.

Hyperelliptic reduction of plane quartic curves

Elisa Lorenzo García
(joint work with Reynald Lercier, Qing Liu, and Christophe Ritzenthaler)

Let $C: F(x,y,z)=0$ be a plane quartic curve defined over a number field K. Let $\mathfrak{p}$ be a prime dividing its discriminant. What can we say about the prime $\mathfrak{p}$? For sure the model given by $F=0$ has bad reduction. But is $\mathfrak{p}$ a prime of geometrically bad reduction? And if it is not, how can we decide if we have potentially good non-hyperelliptic reduction or potentially good hyperelliptic reduction?

In this joint work, we answer these questions and we characterize the reduction type. Among the different characterizations, we get a very convenient one in terms on the Dixmier-Ohno invariants of the curve C. We also provide, in the potentially good (hyperelliptic or non-hyperelliptic) reduction case, a explicit description of the special fiber of the semi-stable model.

Computing Hecke operators on Siegel modular forms

Paul E. Gunnells
(joint work with Mathieu Dutour Sikirić)

Let $G=\mathrm{Sp}_4(\mathbb{R})$ be the Lie group of 4×4 symplectic matrices and let $K=\mathrm{U}(2)$ be a maximal compact subgroup. The symmetric space $\mathfrak{H}_2=G/K$ can be identified with the Siegel upper halfspace of degree 2 (the space of 2×2 symmetric complex matrices with positive-definite imaginary part). Let $\Gamma\subset\mathrm{Sp}_4(\mathbb{Z})$ be a level N congruence subgroup. The locally symmetric space $\Gamma\backslash\mathfrak{H}_2$ is a Siegel modular threefold, and is a moduli space of abelian surfaces with level structure related to Γ.

Our main goal is explicitly computing the cohomology spaces $H^*(\Gamma\backslash\mathfrak{H}_2,\mathbb{C})$, or more generally $H^*(\Gamma\backslash\mathfrak{H}_2,\mathcal{M})$, where $\mathcal{M}$ ranges over certain complex local systems on the threefold. We are especially interested in $H^3(\Gamma\backslash\mathfrak{H}_2,\mathcal{M})$, which is known to be computable in terms of certain (vector-valued) Siegel modular forms. Furthermore, we want to understand H^3 not just as a vector space, but as a Hecke module. More precisely, for each prime $p\nmid N$ there are two Hecke operators $T_{p,1},T_{p,2}$ acting on the cohomology, and we want to understand the decomposition

into eigenspaces. Such computations are essential to understand the arithmetic nature of the cohomology. Our eventual application will be to test conjectures of Harder, which uses the critical values of certain L-functions to predict congruences between vector-valued Siegel modular forms and elliptic modular forms. For more details about Siegel modular forms, their relations with cohomology, the Hecke operators, and Harder's conjectures, we refer to [Har08, vdG08].

Before describing our techniques, we give a selected overview of prior related work. Poor–Yuen [PY15], in their computational investigation of Brumer–Kramer's paramodular conjecture—which predicts that the L-functions of certain abelian surfaces should agree with the spinor L-functions of certain Siegel modular forms of paramodular type—computed weight 2 and 3 Siegel paramodular forms of prime levels < 600 along with the Hecke operators. We remark that the weight 2 forms are not cohomological, in that they cannot appear in the cohomology of the Siegel modular variety. Their techniques use theta series and the product structure on Siegel modular forms in an essential way. Cunningham–Dembélé [CD09] use the technique of algebraic modular forms. In particular they take a real quadratic field F, a quaternion algebra B/F ramified only at the two real places, and then use the Jacquet–Langlands correspondence to pass from automorphic forms on the group of unitary similitudes $\mathrm{GU}_2(B)$ to the forms on the group of symplectic similitudes $\mathrm{GSp}_4(F)$. Finally, Faber–van der Geer [FvdG04a, FvdG04b] treated the case of full level ($N = 1$) by using the moduli space interpretation of $\mathrm{Sp}_4(\mathbb{Z})\backslash\mathfrak{H}_2$. In particular they made lists of $\mathbb{F}_q$-isomorphism classes of genus two curves with their automorphisms, and used this data to compute the traces of the Hecke operators on the cohomology of the Siegel modular threefold. This enabled them to provide convincing evidence for Harder's conjectures in many cases [vdG08].

We now turn to our techniques. Our work uses tools similar to those found in modular symbols calculations [Cre97, Man72]. In particular, (i) we compute cohomology using an explicit finite cell complex that comes from considering an infinite cell complex with Γ-action; and (ii) the Hecke operators do not act on the cells of the complex, but we have an algorithm that allows us to write the Hecke image of any cycle in terms of cycles supported on the complex.

First we consider the complex. We use the reduction theory for $\mathrm{Sp}_4(\mathbb{R})$ due to McConnell–MacPherson [MM93]. This constructs a $\mathrm{Sp}_4(\mathbb{Z})$-equivariant cell decomposition of the symmetric space $\mathfrak{H}_2$ using Voronoi's explicit reduction for positive-definite real quadratic forms. The data indexing the cells, which are lists of primitive integral vectors in $\mathbb{Z}^4$, can be found in [MM93, MM89]. We remark that the top-dimensional cells in this complex are *not* fundamental domains for the action of $\mathrm{Sp}_4(\mathbb{Z})$ on $\mathfrak{H}_2$, but are not far from it: the action of $\mathrm{Sp}_4(\mathbb{Z})$ on the cells has only finite stabilizers, and one can use the knowledge of the boundary maps and the stabilizers to compute the cohomology of $\Gamma\backslash\mathfrak{H}_2$ with coefficients in the local systems $\mathcal{M}$. Moreover, the stabilizer subgroups themselves can easily be computed from the data in [MM93, MM89]. The picture the reader should keep in mind is the Farey tessellation in the elliptic modular case. The upper half

plane $\mathfrak{H}_1$ can be $\Gamma' = \mathrm{SL}_2(\mathbb{Z})$-equivariantly tessellated by the Γ' orbit of the ideal triangle Δ with vertices at $0, 1, \infty$. The triangle Δ is not a fundamental domain for Γ', but a subdivision of Δ into three smaller triangles is.

Next we consider the Hecke operators. For simplicity we discuss how the algorithm computes on H^4, which is considerably simpler than H^3. We also discussing only the case of trivial coefficients, so that we can focus on the geometry of the problem. This is the direct analogue of the classical modular symbols case for $\mathrm{SL}_2(\mathbb{Z})$; our techniques now are already significantly different from the usual modular symbol algorithm (continued fractions), which was worked out for the symplectic group in [Gun00].

Let $x_0 \in \mathfrak{H}_2$ be the basepoint corresponding to the maximal compact subgroup K, and let T be the standard maximal torus in $\mathrm{Sp}_4(\mathbb{R})$. The orbit $T \cdot x_0$ is a 2-dimensional subset in $\mathfrak{H}_2$, and by duality represents a cohomology class in $H^4(\Gamma\backslash\mathfrak{H}_2; \mathbb{C})$. Under a Hecke operator, the orbit $T \cdot x_0$ is taken to a finite set of orbits $\{T_i \cdot y_i\}$, where each T_i is now a rational conjugate of T and y_i is some other point in $\mathfrak{H}_2$. We must find a homology between each of these new subsets and cycles supported on $\mathrm{Sp}_4(\mathbb{Z})$-translates of $T \cdot x_0$, because it is these translates that form the 2-cells of our cell complex.

To do this, we work in a certain Satake (partial) compactification $\mathfrak{H}_2^*$ of $\mathfrak{H}_2$ [BJ06]. This enlarges $\mathfrak{H}_2$ by adjoining copies of the upper half plane $\mathfrak{H}_1$ and points at infinity, much in the same way that the upper half plane is enlarged by adding cusps. Indeed, the construction is hereditary, in that the single points we add to $\mathfrak{H}_2$ are actually the cusps of the upper half planes we add at infinity. The cell decomposition of $\mathfrak{H}_2$ extends to $\mathfrak{H}_2^*$, and on the boundary components one sees the Farey tessellation. Let O be a Hecke image $T_i \cdot y_i$ and let $\bar{O}$ be its closure in $\mathfrak{H}_2^*$. Then the "edges" $\partial O := \bar{O} \smallsetminus O$ appear in certain boundary components as ideal geodesics going from cusp to cusp, and cutting across the edges of the Farey tessellation. As a first step in finding a cellular representative for the class of $\bar{O}$, we "fix" the edges of ∂O: we apply the classical modular symbol algorithm for $\mathrm{SL}_2(\mathbb{Z})$ to first write the boundary ∂O as a 1-cycle $\eta = \sum n_i \gamma_i$, where the γ_i are edges in the boundary tessellation.

Next we must fill in the 1-cycle: we must find a 2-chain ξ supported on the cells of our complex such that $\partial\xi = \eta$. Such a 2-chain is exactly our representative for the class of our Hecke image. To do this, we simply take a large set of top-dimensional cells $C_1, \ldots, C_k$ that covers $\bar{O}$ and the support of η. We then attempt to solve the equation $(*)$ $\partial\xi = \eta$ with a 2-cycle supported on the 2-faces of the C_i.

Any such solution is exactly what we need, as it gives a representative for the class of our Hecke image supported on the complex. Moreover, we are guaranteed to succeed: *if we have sufficiently many C_i, we know that a solution exists.* Note that there is no complicated geometry needed to find ξ as in [Gun00]; it is simply a problem in numerical linear algebra. We take many C_i and try to solve $(*)$; if we are unsuccessful, we add more top cells and try again. Eventually we will succeed.

We remark that for practical computations it is not enough to simply solve $(*)$. We need to find a solution to $(*)$ supported on as few 2-cells as possible. This can

be done using a tool from applied mathematics, namely *compressed sensing*. Compressed sensing is a signal processing technique for acquiring and reconstructing a signal by finding solutions to underdetermined linear systems. The underlying problem of finding sparse solutions of linear systems is called *basis pursuit*; in our application we solve this problem using the approximate message passing algorithm proposed in [DMM09].

References

[BJ06] Armand Borel and Lizhen Ji, *Compactifications of symmetric and locally symmetric spaces*, Mathematics: Theory & Applications, Birkhäuser Boston, Inc., Boston, MA, 2006. MR 2189882

[CD09] Clifton Cunningham and Lassina Dembélé, *Computing genus-2 Hilbert-Siegel modular forms over $\mathbb{Q}(\sqrt{5})$ via the Jacquet-Langlands correspondence*, Experiment. Math. **18** (2009), no. 3, 337–345. MR 2555703

[Cre97] J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997. MR 1628193

[DMM09] David L. Donoho, Arian Maleki, and Andrea Montanari, *Message-passing algorithms for compressed sensing*, Proceedings of the National Academy of Sciences **106** (2009), no. 45, 18914–18919.

[FvdG04a] Carel Faber and Gerard van der Geer, *Sur la cohomologie des systèmes locaux sur les espaces de modules des courbes de genre 2 et des surfaces abéliennes. I*, C. R. Math. Acad. Sci. Paris **338** (2004), no. 5, 381–384. MR 2057161

[FvdG04b] ———, *Sur la cohomologie des systèmes locaux sur les espaces de modules des courbes de genre 2 et des surfaces abéliennes. II*, C. R. Math. Acad. Sci. Paris **338** (2004), no. 6, 467–470. MR 2057727

[Gun00] Paul E. Gunnells, *Symplectic modular symbols*, Duke Math. J. **102** (2000), no. 2, 329–350. MR 1749441

[Har08] Günter Harder, *A congruence between a Siegel and an elliptic modular form*, The 1-2-3 of modular forms, Universitext, Springer, Berlin, 2008, pp. 247–262. MR 2409680

[Man72] Ju. I. Manin, *Parabolic points and zeta functions of modular curves*, Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 19–66. MR 0314846

[MM89] Robert MacPherson and Mark McConnell, *Classical projective geometry and modular varieties*, Algebraic analysis, geometry, and number theory (Baltimore, MD, 1988), Johns Hopkins Univ. Press, Baltimore, MD, 1989, pp. 237–290. MR 1463705

[MM93] ———, *Explicit reduction theory for Siegel modular threefolds*, Invent. Math. **111** (1993), no. 3, 575–625. MR 94a:32052

[PY15] Cris Poor and David S. Yuen, *Paramodular cusp forms*, Math. Comp. **84** (2015), no. 293, 1401–1438. MR 3315514

[vdG08] Gerard van der Geer, *Siegel modular forms and their applications*, The 1-2-3 of modular forms, Universitext, Springer, Berlin, 2008, pp. 181–245. MR 2409679

Diophantine Problems and a p-adic Period Map

Brian Lawrence

(joint work with Akshay Venkatesh)

We discuss new proofs of the S-unit theorem and Mordell's conjecture, using p-adic Hodge theory to study the global Galois representations coming from a family of varieties over a number field. The same methods also give a new result of Shafarevich type for hypersurfaces. Everything is joint work with Akshay Venkatesh.

Let K be a number field.

Theorem 1. *Let S be a finite set of places of K, and let $\mathcal{O}_{K,S}$ be the ring of S-integers of K. Then*

$$\{(a,b) \in \mathcal{O}_{K,S}^2 | a+b=1\}$$

is finite.

Theorem 2. *Let Y be a curve over K, of genus at least 2. Then $Y(K)$ is finite.*

Theorem 3. *Let Y be the moduli space of smooth hypersurfaces of dimension n and degree d in $\mathbf{P}^{n+1}$, with n and d sufficiently large. Fix S a finite set of primes of $\mathbf{Z}$. Then $Y(\mathbf{Z}[\mathbf{S^{-1}}])$ is finite.*

Here "sufficiently large" means that n is chosen first, and d is taken sufficiently large with respect to n. The condition on n and d is effective: it is an explicit bound on the Hodge numbers of the relevant hypersurfaces.

The proof has five main steps.

(1) Build a smooth proper family $X \to Y$ of varieties over Y. If (a,b) is a solution to the S-unit equation, then

$$y^2 = x(x-a)(x+b)$$

is an elliptic curve with good reduction outside S. For Mordell, we use a variant of the Kodaira–Parshin construction, which gives a family $X \to Y$ of curves over Y. In the hypersurface case we take X the universal family of hypersurfaces.

A lemma of Faltings shows that for a fixed family $X \to Y$ as above, there are only finitely many possibilities for the semisimplified Galois representation $H^1_{et}(X_y, \mathbf{Q}_p)^{ss}$, for $y \in Y(\mathbf{Z}[\mathbf{S^{-1}}])$. Our goal is to study how this Galois representation varies with y.

(2) We use p-adic Hodge theory to study the local Galois representation

$$H^1_{et}(X_y, \mathbf{Q}_p)|_{K_v} = H^1_{et}((X_y)_{K_v}, \mathbf{Q}_p)|_{K_v},$$

where v is a place of K lying above p. Under the correspondence of p-adic Hodge theory, this local representation corresponds to the de Rham cohomology of $(X_y)_{K_v}$. This de Rham cohomology is a K_v vector space, equipped with a Hodge fitration and (by crystalline cohomology) a Frobenius endomorphism. The Hodge filtration is known to vary with $y \in Y(K_v)$ by the theory of the Gauss-Manin connection.

(3) De Rham cohomology defines a v-adic analytic *period map*

$$\Phi_p : Y \to \mathfrak{h}$$

from Y to a period domain, analogous to the classical complex-analytic period map, and in fact given by the same formal power series over K. We show that Φ_p has Zariski-dense image in $\mathfrak{h}$ by a topological monodromy calculation in the complex setting.

(4) We need to translate our results about the period map to a statement about the semisimplified global Galois representation $H^1_{et}(X_y, \mathbf{Q}_p)^{ss}$. First of all, the Frobenius centralizer acts algebraically on $\mathfrak{h}$, and points in the same orbit correspond to isomorphic Galois representations. Under suitable conditions, no orbit is Zariski dense, so the period map Φ_p does not land in any single Frobenius-centralizer orbit. When Y is one-dimensional, this implies that the inverse image of any orbit under Φ_p is finite: only finitely many $y \in Y(K)$ can give rise to a single isomorphism class of Galois representation.

Faltings' finiteness lemma applies to semisimple representations. In the case when the map $X \to Y$ has dimension 1, the representations that arise are known to be semisimple by Faltings's work. Since we wish to provide an independent proof of Mordell's conjecture, we argue as follows.

Typically the local Galois representations that arise are *not* semisimple. But by considerations involving weights, we can show the following: A generic point in $\mathfrak{h}$ corresponds to a local Galois representation, no subrepresentation of which can come from a global representation arising from geometry. Therefore, there is a proper Zariski-closed subset $Z \subseteq \mathfrak{h}$ such that, if $y \in Y(K)$ is such that $\Phi(y) \notin Z$, then the corresponding Galois representation is simple.

When Y is one-dimensional, this implies that all but finitely many points $y \in Y(K)$ give rise to simple global Galois representations. This proves the S-unit theorem and Mordell's conjecture.

(5) When $\dim Y > 1$, the inverse image $\Phi^{-1}(Z)$ of a Zariski-closed subset of $\mathfrak{h}$ need not be a finite set. *A priori*, it could be an arbitrary closed subset for the p-adic analytic topology on $Y(K_v)$. A recent transcendence result of Bakker and Tsimerman guarantees that $\Phi^{-1}(Z)$ lies inside a proper algebraic subset of Y, under suitable dimension conditions. This is enough to deduce Theorem 3.

Three modular fivefolds of level 8

Adam Logan

We will say that a variety $V/\mathbb{Q}$ is *modular* if there is a formula valid for all but finitely many p that expresses the number of points of V over F_p in terms of powers of p, Artin symbols at p, and the pth coefficients of Hecke eigenforms. The eigenforms involved are said to be *realized* by V; if only one is needed, it is *strongly realized* by V. The most famous theorem on modularity and realization is due to Eichler-Shimura, Wiles, Taylor-Wiles, et al., and can be stated as follows:

Theorem. Every eigenform of weight 2 with rational coefficients is strongly realized by an elliptic curve over $\mathbb{Q}$. Conversely, every elliptic curve over $\mathbb{Q}$ strongly realizes an eigenform of weight 2.

Elkies and Schütt proved a similar result [3, Theorem 1] relating eigenforms of weight 3 and certain K3 surfaces. The flavour is quite different, however; there

are only finitely many eigenforms of weight 3 up to quadratic twist, since by a result of Schütt they arise from imaginary quadratic fields whose class group has exponent dividing 2. There has also been extensive work on eigenforms of weight 4 and rigid Calabi-Yau threefolds (see [5] for the state of the art in 2005) but it is not clear whether to expect finitely many or infinitely many such eigenforms up to twist, nor whether they can all be strongly realized on a Calabi-Yau threefold. Dieulefait-Manoharmayum and Gouvêa-Yui have shown that every rigid Calabi-Yau threefold over $\mathbb{Q}$ strongly realizes a rational eigenform of weight 4.

Beyond dimension 3, little is known about modularity; there are a few general constructions (notably that of Kuga-Sato, considering the $k-1$-fold fibre product of the universal curve over $E_0(N)$, when $\dim S(N,k) = 1$) and almost no examples beyond these. Using a criterion of Cynk and Hulek [2, Proposition 5.6] for the existence of a crepant resolution of a singular double cover, I searched for collections of 12 hyperplanes in $\mathbb{P}^5$ such that the double cover branched along their union is a candidate to have a rigid Calabi-Yau resolution. I found several interesting examples of level 8:

(1) The fivefold defined by $t^2 = \prod_{i=0}^{5} x_i(x_i + x_{i+1})$ is modular of level 8. It does not satisfy the Cynk-Hulek criterion, but it is close enough to doing so that the existence of a crepant resolution can be proved (details will appear in [4]). It admits a map to $\mathbb{P}^1$ whose general fibre is of the form $(K \times K^\sigma)/\pm 1$, where K is a K3 surface isogenous to the Kummer surface of $E \times E$, where E is defined by $y^2 = x(x-1)(x-\lambda)$ and σ indicates a quadratic twist. So the number of points on it is related to hypergeometric functions over finite fields; modularity can then be proved as an application of results of Frechette-Ono-Papanikolas.

(2) The fivefold defined by $t^2 = \prod_{i=0}^{5} x_i(x_i + x_{i+1} + x_{i+2})$ also appears to be modular of level 8, and does satisfy the Cynk-Hulek criterion. It turns out that this collection of hyperplanes has $\mathcal{S}_5$ as its automorphism group. As a result, there are only a few orbits of singularities, and it should be practical to construct the crepant resolution explicitly enough to count the points for enough small primes to prove the modularity, although I have not yet finished doing so.

(3) A third fivefold defined by a less elegant equation

$$t^2 = (x_0 - x_1)x_1x_4(x_4 - x_5)(x_1 - x_4 + x_5)(x_0 - x_1 + x_4)\times \\ x_2x_3(-x_2 + x_3)(x_3 + x_5)(x_0 - x_2)(x_0 - x_3)$$

again satisfies the Cynk-Hulek criterion and appears to be modular of level 8. Its group of symmetries is small and it would be quite painful to describe the resolution sufficiently explicitly to count the points. However, like the first example, this one admits a potentially useful fibration; in this case, the general fibre is of the form $(K \times L)/\pm 1$, where both K and L can be related to the Kummer surfaces of squares of elliptic curves, but K to the family with full level-2 structure and L to those with a single point of order 2. So the number of points can be described in terms of

hypergeometric functions over finite fields, but the formula mixes them in a way that appears to be new. It is a very interesting problem to try to prove the modularity and to prove an analogous identity of hypergeometric functions over $\mathbb{C}$.

In addition, there are examples in other levels, such as 4 (studied by Ahlgren [1]), 32, and 256. One example in level 32 is related to a form with complex multiplication and is thus particularly simple. Work on these examples is in progress.

References

[1] S. Ahlgren. *The points of a certain fivefold over finite fields and the twelfth power of the eta function.* Finite Fields and their Applications 8 (2002), 18–33.

[2] S. Cynk, K. Hulek. *Construction and examples of higher-dimensional modular Calabi-Yau manifolds.* Canad. Math. Bull. 50 (4), 2007, 486–503.

[3] N. Elkies, M. Schütt. *Modular forms and K3 surfaces.* Adv. Math. 240 (2013), 106–131.

[4] C. Ingalls and A. Logan, *On the Cynk-Hulek criterion for crepant resolutions of double covers*, to appear.

[5] C. Meyer. *A dictionary of modular threefolds.* PhD thesis, Johannes Gutenberg-Universität in Mainz, 2005. Available for download at `http://ubm.opus.hbz-nrw.de/volltexte/2005/751/pdf/diss.pdf`.

Special Shimura varieties and Newton polygons of cyclic covers of the projective line

Rachel Pries

(joint work with Wanlin Li, Elena Mantovan, and Yunqing Tang)

For $g \geq 9$, it is unexpected for the Torelli locus to intersect all Newton polygon strata in the modular space of principally polarized abelian varieties of dimension g. This means that there are symmetric Newton polygons of height $2g$ that are not expected to occur for the Jacobian of a smooth curve in characteristic p, for some p. Currently, no Newton polygons have been excluded from occurring, but it is known that some unexpected Newton polygons do occur for some p, using Artin-Schreier and complex multiplication theory. By studying Moonen's 20 special Shimura varieties, we demonstrate many more Newton polygons that occur for the Jacobians of curves. We develop an inductive method for studying the Newton polygon stratification on Hurwitz spaces for cyclic covers of the projective line. As an application, we prove that unlikely intersections occur for all g and all $p \equiv 2 \pmod 3$.[6]

[6]Compiled by the reporter from the hand-written abstract at Oberwolfach

New invariants on class groups and Cohen-Lenstra heuristics in the presence of roots of unity

Will Sawin
(joint work with Jacob Tsimerman, and Michael Lipnowski)

This talk discusses work in progress.

Let F be a number field and ℓ an odd prime. Given a "reasonable" set of extensions K/F, for instance all quadratic extensions (with specified splliting behavior at real places of F), we can ask for the distributions of the ℓ-parts of the relative class groups of K/F. Malle gave numerical evidence suggested that the answer should depend on the number of ℓ-power roots of unity within F [6]. A random matrix method to predict the correct distribution was developed by Friedman and Washington [3].

This method is best justified using the function field model. The function field $\mathbb{F}_q(T)$ contains exactly the $q-1$st root of unity. If we are interested in modeling number fields which contain μ_{ℓ^n} but not $\mu_{\ell^{n+1}}$, we should consider q with $v_\ell(q-1)=n$. A quadratic extension of $\mathbb{F}_q(T)$ corresponds to a hyperelliptic curve, say of genus g. Its class group is equal to the cokernel of $1-F$ where F is the action of Frobenius on the Tate module of its Jacobian. Here the Tate module is isomorphic to $\mathbb{Z}_\ell^{2g}$, and admits a natural symplectic form, the Weil pairing, on which F acts by a symplectic similitude, multiplying it by q. The heuristic says we should assume F is a random element in the set $GSp_{2g}^q(\mathbb{Z}_\ell)$ of symplectic similitudes with similitude character q. The predicted distribution over number fields is then the large g limit of the distribution of cokernels of such random F (which must be verified to be independent of the choice for q, except for the ℓ-adic valuation of $q-1$). In addition, the cokernel must be quotiented by a number of random elements equal to the difference in unit ranks of K and F.

This random heuristic has been verified by Achter in the suitable large q limit [1]. We will not dispute it. Instead, the flaw we wish to rectify is that it is not obvious how to compute the probability of a given group appearing in a nice way, as is possible for the original Cohen-Lenstra heuristics. For instance, Garton was only able to calculate the distribution in some special cases [4]. We fix this. Specifically, we find that the distribution becomes easier to calculate when suitable invariants are added to the class group. Moreover, by doing so we obtain slightly more information, at least conjecturally, because we obtain a distribution of the class group together with these new invariants. The first invariant was already defined by Lipnowski and Tsimerman over function fields using the Weil pairing [5], and can be transferred to number fields using the cup product in the cohomology of group schemes. I was alerted to the existence of the second product after trying to understand the Cassels-Tate pairing on the class group over function fields, but it is easier to define by using class field theory and Kummer theory to compare the class group and its dual.

Both these invariants can be defined for symplectic similitude matrices in the random matrix model. We calculate the joint distribution of the cokernel together

with these invariants in the large g limit, in particular verifying that it is independent of q. After modifying it to account for the unit group, we conjecture this as the joint distribution of these invariants over number fields. Dropping the new invariants, we have a calculation of the previously-conjectured distribution. We verify our new conjectures over function fields by using the bounds on cohomology proved by Ellenberg, Venkatesh, and Westerland [2] (up to a small error term depending on q, just as in the main result of [2]). The only subtlety is how to handle the new invariant, as how the Weil pairing relates to [2] was already described in [5]. However, it can be viewed as arising from a covering of the Hurwitz space which is itself covered by a further Hurwitz space, allowing its cohomology to be bounded. We also have numerical data consistent with the conjectures for quadratic extensions of $\mathbb{Q}(\mu_3)$.

References

[1] J. D. Achter, The distribution of class groups of function fields, J. Pure Appl. Algebra **204** (2006), 316 – 333.

[2] J. S. Ellenberg, A. Venkatesh, and C. Westerland, Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields, Annals of Mathematics **183** (2016), 729–786.

[3] E. Friedman and L. C. Washington, On the distribution of divisor class groups of a curve over a finite field, Théorie des nombres (Quebec, PQ, 1987), de Gruyter, Berlin, (1989), 227–239.

[4] D. Garton, Random matrices, the Cohen-Lenstra heuristics, and roots of unity, Algebra & Number Theory **9** (2015), 149 – 171.

[5] M. Lipnowski and J. Tsimerman, Cohen-Lenstra heuristics for étale group schemes and symplectic pairigns, arXiv:1610.09304 (2016).

[6] G. Malle, *Cohen-Lenstra heuristic and roots of unity*, J. Number Theory **128** (2008), 242–262.

[7] M. Muster, *Computing other invariants of topological spaces of dimension three*, Topology **32** (1990), 120–140.

On the level of modular curves that give rise to sporadic j-invariants

Bianca Viray

(joint work with Abbey Bourdon, Özlem Ejder, Yuan Liu, Frances Odumodu)

We study so-called *sporadic points* on $X_1(n)$, i.e. closed points such that the curve has only finitely many points of that degree or less. We show that a non-CM non-cuspidal sporadic point on $X_1(n)$ pushes down to a sporadic point on a lower level modular curve. This lower level is bounded depending on the set of non-surjective primes of the curve and on the level of an associated Galois representation. If we assume a folklore conjecture on uniform bounds on the primes for which the Galois representation is non-surjective, then we also obtain a uniform bound on this lower level.[7]

[7]Compiled by the reporter from the hand-written abstract at Oberwolfach

A local-global principle for isogenies of composite degree

Isabel Vogt

Let E be an elliptic curve over a number field K. If for almost all primes $\mathfrak{p}$ of K, the reduction $E_{\mathfrak{p}}$ has a rational cyclic isogeny of fixed degree, we ask if this forces E to have a cyclic isogeny of that degree over K. Building on work of Sutherland, Anni, and Banwait-Cremona in the case of prime degree, we prove finiteness results for exceptions to this local-global principle for cylic isogenies of arbitrary degree.[8]

Rigorous computation of the endomorphism ring of a Jacobian

John Voight

(joint work with Edgar Costa, Nicolas Mascot, and Jeroen Sijsling)

We report on joint work [1]. Let F be a number field with algebraic closure F^{al}. Let X be a nice curve over F of genus $g \geq 1$, let A be its Jacobian, and A^{al} be its base change to F^{al}. Write $\mathrm{End}(A)$ for the ring of endomorphisms of A defined over F. Let X be given in bits as the vanishing set of a system of equations in projective space.

To *compute the geometric endomorphism ring* of A we mean: given as input X (over F), to compute as output a (minimal, Galois) finite extension $K \supseteq F$ with $\mathrm{End}(A_K) = \mathrm{End}(A^{\mathrm{al}})$, and a multiplication table for $\mathrm{End}(A_K)$ in a $\mathbb{Z}$-basis together with a $\mathrm{Gal}(K \mid F)$-action.

For example, the curve $X\colon y^2 = x^5 - x^4 + 4x^3 - 8x^2 + 5x - 1$ over $F = \mathbb{Q}$ has $\mathrm{End}(A^{\mathrm{al}})$ defined over $K = \mathbb{Q}(\zeta_8)$; we have $\mathrm{End}(A_K) = \mathcal{O} \subseteq B$ a maximal order in a quaternion algebra B over $\mathbb{Q}$ with discriminant $\operatorname{disc} B = 6$, and $\mathrm{End}(A)$ is generated by endomorphisms α, β satisfying

$$\alpha^2 = 3, \quad \beta^2 = -\beta + 1, \quad \alpha\beta + (1+\beta)\alpha = 3.$$

Lombardo [2, §5] has shown that the geometric endomorphism ring can be computed in principle using a day-and-night algorithm—but this algorithm would be hopelessly slow in practice. We compute the endomorphism ring by saturating a subring of endomorphisms given the endomorphism algebra, and for this purposes we work by day computing lower bounds and by night computing upper bounds on the dimension of $\mathrm{End}(A_K) \otimes \mathbb{Q}$ until these bounds meet.

For lower bounds, we proceed as follows. Following van Wamelen [3] (who worked out methods in genus 2), we compute the *numerical endomorphism ring* in the following way. First, we embed F into $\mathbb{C}$ and by numerical integration we compute a period matrix for X. Second, we find putative endomorphisms of A by computing integer matrices (with small coefficients) that preserve the lattice generated by these periods, up to the computed precision. Finally, from the tangent representation of such a putative endomorphism, we compute a correspondence on X whose graph is a divisor $Y \subset X \times X$; the divisor Y may then be rigorously

[8]Compiled by the reporter from the hand-written abstract at Oberwolfach

shown to give rise to an endomorphism $\alpha \in \mathrm{End}(A_K)$ over an extension $K \supseteq F$ by exact computation. From this computation, we can also recover the multiplication law in $\mathrm{End}(A^{\mathrm{al}})$ and its Galois action.

We say that $\alpha \in \mathrm{End}(A_K)$ is nondegenerate (with respect to an embedding $\mathrm{AJ}\colon X \hookrightarrow A$) if $\alpha(AJ(X))$ is not in the locus of indeterminancy of the Mumford map $A \to \mathrm{Sym}^g(X)$.

Theorem. *There exists a deterministic algorithm that, given input $\alpha \in \mathrm{M}_g(K)$ the tangent representation of α as above, returns as output* true *if $\alpha \in \mathrm{End}(A_K)$ is nondegenerate and* false *if either $\alpha \notin \mathrm{End}(A_K)$ or α is degenerate.*

The algorithm in this theorem happens to be quite practical.

By night, we compute upper bounds as follows. Let $A_K \sim \prod_{i=1}^t A_i^{n_i}$ be the decomposition of A_K up to isogeny as the product of pairwise nonisogenous simply abelian varieties. Let $B_i := \mathrm{End}(A_i) \otimes \mathbb{Q}$, let $L_i := Z(B_i)$ be their centers, and let $e_i^2 := \dim_{L_i} B_i$. Then

$$\dim_{\mathbb{Q}}(\mathrm{End}(A_K) \otimes \mathbb{Q}) = \sum_{i=1}^{t} e_i^2 n_i^2 [L_i : \mathbb{Q}].$$

Theorem. *If the Mumford–Tate conjecture holds for A, we can effectively compute the following quantities:*

(i) *t;*
(ii) *the multiset $\{(e_i n_i, n_i \dim A_i)\}_{i=1,\ldots,t}$; and*
(iii) *the fields L_i.*

This theorem originally had a hypothesis that was removed by contributions of Zywina and Lombardo. It works by counting points on A over finite fields and using the characteristic polynomial of Frobenius to pin down the center. This method also works quite well in practice, requiring relatively few primes before a sharp upper bound is deduced (then proven to be correct by certifying endomorphisms).

References

[1] Edgar Costa, Nicolas Mascot, Jeroen Sijsling, and John Voight, *Rigorous computation of the endomorphism ring of a Jacobian*, accepted to Math. Comp.

[2] Davide Lombardo, *Computing the geometric endomorphism ring of a genus 2 Jacobian*, 2016, `arXiv:1610.09674`.

[3] Paul B. van Wamelen, *Computing with the analytic Jacobian of a genus 2 curve*, in Discovering mathematics with Magma, vol. 19 of Algorithms Comput. Math., Springer, Berlin, 2006, 117–135.

Inductive Methods for Proving Malle's Conjecture

Jiuya Wang
(joint work with Robert J. Lemke Oliver, and Melanie Matchett Wood)

1. Introduction

A natural counting question people study about number fields is:
Question: Given $G \subset S_n$, denote

$$N_k(G, X) := \{K/k \mid \mathrm{Gal}(K/k) = G, \mathrm{Disc}(K/k) < X\},$$

what is the asymptotic behavior of $N_k(G, X)$ as X goes to infinity?

Malle [Mal02, Mal04] has given a conjectural answer to this question:
Malle's Conjecture Given $G \subset S_n$ and k a number field, there exists a constant $C(G, k)$ such that

$$N_k(G, X) \sim C(G, k) X^{1/a(G)} \ln^{b(G,k)-1} X,$$

where $a(G)$ and $b(G, k)$ are both integers.

On one hand, the question is indeed natural in the sense that it is a refined question of inverse Galois problem. More interestingly, accompanied by discoveries in Malle's conjecture, it has been found to be closely related to studying class numbers, in both determining asymptotic average and point-wise upper bound.

Malle's conjecture has been verified in some cases. Aside from all abelian groups proved in [Mäk85, Wri89], a list of non-abelian groups are also proved for Malle's conjecture: $S_3(3)$ in [DH71], $D_4(4)$ in [CyDO02], $S_4(4)$ in [Bha05], $S_3(6)$ in [BW08, BF10], $S_5(5)$ in [Bha10], $C_2 \wr H$ with mild conditions on H in [Klü12] and $S_n \times A$ for $n = 3, 4, 5$ with most abelian groups in [Wan17]. There has also been counter-examples by [Klü05] where the predicted $b(k, G)$ does not hold.

A natural question one could ask is: whether we could inductively prove more examples of Malle's conjecture? In particular, current results [Klü12] and [Wan17] are some successful trials in this direction.

2. Methods

In this paper, we give a general framework to universally consider different ways of inductions. Our approach is to consider number fields constructed via taking towers. Given a base field k, and two permutation groups T and B (meaning top and bottom), we consider those number fields that are constructed by taking a T-extension L/F over a B-extension F/k. By taking such a tower of fields, many possible groups could arise for $\mathrm{Gal}(L/k)$. We fix a group G that is possible.

The first challenge is to determine, for a fixed B-extension F/k, the number of T-extensions L/F with $\mathrm{Gal}(L/k) \simeq G$ and with relative discriminant bounded $\mathrm{Disc}(L/F) < X$. We will denote this number $N_{F/k}(T, G, X)$. The key idea for this step is to use local conditions of L/F to detect $\mathrm{Gal}(L/k)$. For example, if $G = S_3(3) \wr B$ where B is an arbitrary permutation group, then given a B-extension F/k and a prime p that splits in F, if a T-extension L/F is exactly

partially ramified at one of the primes above p and is unramified at all other primes above p, then $\mathrm{Gal}(L/F) = G$. Therefore it suffices to count T-extensions with such local conditions. If counting T-extensions is *multiplicative* with respect to taking local conditions, then we could show for $G = T \wr B$ wreath product, one hundred percent of T-extensions over F has $\mathrm{Gal}(L/k) = G$. There has been extra difficulties for general permutation group T when counting T-extensions is not multiplicative. Indeed, this happens a lot. For example, if T is a general abelian group like $\mathbb{Z}/4\mathbb{Z}$. For such cases, we would need to determine a minimal subgroup E of T where counting T-extensions with a fixed T/E-quotient becomes multiplicative. For non-multiplicative abelian group T, we would heavily employ class field theory to carry out the counting.

The second challenge is to add up $N_{F/k}(T, G, X)$ over all B-extensions F. If we could do the first step, then

$$N_k(G, X) = \sum_{F, \mathrm{Disc}(F/k)^{|T|} < X} N_{F/k}(T, G, \frac{X}{\mathrm{Disc}(F/k)^{|T|}}).$$

To get an asymptotic counting of $N_k(G, X)$, we define the truncated sum at Y to be

$$N_k(G, X)_Y = \sum_{F, \mathrm{Disc}(F/k)^{|T|} < Y} N_{F/k}(T, G, \frac{X}{\mathrm{Disc}(F/k)^{|T|}}).$$

If we could show for certain integers a and b such that the following two limit process commute and converge to a positive number

$$0 < \lim_{Y \to \infty} \lim_{X \to \infty} \frac{N_k(G, X)_Y}{X^{1/a} \ln^{b-1} X} = \lim_{X \to \infty} \lim_{Y \to \infty} \frac{N_k(G, X)_Y}{X^{1/a} \ln^{b-1} X} < \infty, \tag{4}$$

then we finish proving the asymptotic main term of the distribution $N_k(G, X)$. The key input we need here is an upper bound on $N_{F/k}(T, G, X)$ uniformly depending on $\mathrm{Disc}(F/k)$.

3. Results

Firstly, we prove uniform upper bound for relative $S_3(3)$ extensions and all abelian extensions.

Lemma 1. *(1) The number of S_3-cubic extensions over k is uniformly bounded by*

$$N_k(S_3(3), X) = O(\mathrm{Disc}(k)^{t+\epsilon} X)$$

with $t = 16/9$.

(2) The number of A-extensions over k is uniformly bounded by

$$N_k(A, X) = O(\mathrm{Disc}(k)^{\epsilon} h_k(A) X^{1/a(A)} \ln^{b(k,A)-1} X).$$

where $h_k(A) = |\mathrm{Hom}(\mathrm{Cl}_K, A)|$.

Secondly, we prove Malle's conjecture or give precise main term (when Malle's conjecture does not hold) for many different groups. In particular, we reproduce

[CyDO02] and [Klü12]. As an example to show what we could prove when G is in the form of a wreath product, we prove

Theorem 2. *Given a permutation group B with $N_k(B, X) \leq O(X^u)$ where $u+t < 3$, then Malle's conjecture holds for $G = S_3 \wr B \subset S_{3|B|}$.*

Similar theorems are also obtained for all abelian T, and for more types of inductions.

Concrete Examples for Malle :

(1) $S_3 \wr S_3$, $S_3 \wr \cdots \wr S_3$
(2) $S_3 \wr G$ with G in regular representation and $|G| > 4$
(3) $S_3 \wr C_p \wr G$ with arbitrary permutation group G and big enough p

References

[BF10] K. Belabas and E. Fouvry. Discriminants cubiques et progressions arithmetiqués,. *Int. J. Number Theory*, 6(7):1491–1529, 2010.

[Bha05] M. Bhargava. The density of discriminants of quartic rings and fields. *Ann. of Math.*, 162(2):1031–1063, September 2005.

[Bha10] M. Bhargava. The density of discriminants of quintic rings and fields. *Ann. of Math. (2)*, 172(3):1559–1591, 2010.

[BW08] M. Bhargava and M. M. Wood. The density of discriminants of S_3-sextic number fields. *Proc. Amer. Math. Soc.*, 136(5):1581–1587, 2008.

[CyDO02] H. Cohen, F. Diaz y Diaz, and M. Olivier. Enumerating quartic dihedral extensions of $\mathbb{Q}$. *Compositio Math.*, 133(1):65–93, 2002.

[DH71] H. Davenport and H. Heilbronn. On the density of discriminants of cubic fields. II. *Proc. Roy. Soc. London. Ser. A*, 322(1551):405–420, 1971.

[Klü05] J. Klüners. A counter example to Malle's conjecture on the asymptotics of discriminants. *C. R. Math. Acad. Sci. Paris*, 340(6):411–414, 2005.

[Klü12] J. Klüners. The distribution of number fields with wreath products as Galois groups. *Int. J. Number Theory*, (8):845–858, 2012.

[Mäk85] S. Mäki. On the density of abelian number fields. *Ann. Acad. Sci. Fenn. Diss. Series A I. Mathematica Dissertationes*, 54(104), 1985.

[Mal02] G. Malle. On the distribution of Galois groups. *J. Number Theory*, 92(2):315–329, 2002.

[Mal04] G. Malle. On the distribution of Galois groups, II. *Experiment. Math.*, 13(2):129–135, 2004.

[Wan17] J. Wang. Malle's conjecture for $S_n \times A$ for $n = 3, 4, 5$. *arXiv: 1705.00044*, 2017.

[Wri89] D. J. Wright. Distribution of discriminants of abelian extensions. *Proc. of London Math. Soc. (3)*, 58(1):1300–1320, 1989.

Two new proofs of class number one

Mark Watkins

Gauss (1801) conjectured that there are exactly 9 imaginary quadratic fields of class number one. This was proven independently by Heegner (1952), Baker (1966), and Stark (1967). The proof of Baker used transcendence theory, while the proofs of Heegner and Stark used modular functions, eventually reducing to finding all rational points on a finite list of genus 2 curves. Later works by various authors used different modular curves to give alternate proofs in this genre.

A third type of proof was proposed by Goldfeld (1976), involving the central vanishing of the L-function of a suitable elliptic curve. Indeed, given an elliptic curve with analytic rank 3 or more (again satisfying various technical conditions), it would be possible to show that the class number diverged effectively. Moreover, the famed conjecture of Birch and Swinnerton-Dyer suggested that such an L-function should in fact exist. The (difficult) work of Gross and Zagier (1986) then showed that such a triple central vanishing of an elliptic curve L-function did indeed occur.

1

Our work herein takes an opposite point of view, desiring to prove the class number one result via the use of an elliptic curve of analytic rank 2. This is much easier to verify than analytic rank 3, requiring only a modular symbols calculation rather than the Gross-Zagier theorem.

Let $-q$ be a negative fundamental discriminant and χ its character. Given a weight 2 Hecke newform $F = \sum_n c(n)e^{2\pi inz}$ of level N with $\gcd(N,q) = 1$, we let $\Lambda(s) = (Nq/4\pi^2)^{s-1}\Gamma(s)^2 L_F(s)L_{F\chi}(s)$ be the scaled and completed product L-function for F and $F\chi$, satisfying a functional equation $\Lambda(s) = \epsilon\Lambda(2-s)$. Goldfeld's argument starts from Cauchy's residue theorem, noting that

$$\frac{\Lambda^{(l)}(1)}{l!} = \left(\int_{(2)} - \int_{(0)}\right)\frac{\Lambda(s)}{(s-1)^{l+1}}\frac{\partial s}{2\pi i} = (1+\epsilon^l)\int_{(2)}\frac{\Lambda(s)}{(s-1)^{l+1}}\frac{\partial s}{2\pi i},$$

and then expands the Dirichlet series in terms of a Mellin transform to get

$$\frac{\Lambda^{(l)}(1)}{l!} = (1+\epsilon^l)\sum_{n=1}^{\infty} c(n)R_\chi(n)W_l\Big(\frac{n}{Nq}\Big) \quad \text{with} \quad W_l(x) = \int_{(2)}\frac{\Gamma(s)^2}{(4\pi^2 x)^s}\frac{\partial s/2\pi i}{(s-1)^{l+1}},$$

while $R_\chi(n)$ is half the number of representations of n by reduced binary quadratic forms (A,B,C) of discriminant $-q$. Expanding this definition gives $\Lambda^{(l)}(1)/l!$ as

$$\frac{1+\epsilon^l}{2}\sum_{(A,B,C)}\sum\sum_{(X,Y)\neq(0,0)} c\big(AX^2+BXY+CY^2\big)W_l\Big(\frac{AX^2+BXY+CY^2}{Nq}\Big).$$

The main term comes from the $Y = 0$ contributions, which are given in terms of the symmetric square L-function for F (with Euler adjustments for $p|N$ included), while the error term can be bounded crudely for each form as $O(\sum_A 1/A)$ using nothing more than the density $1/\sqrt{q}$ of represented integers and the length Nq of the approximate functional equation, in conjunction with Deligne's bound on $c(n)$ and/or the Hasse bound for elliptic curves.

Under suitable technical conditions so that $\epsilon(F\chi) = -1$, we take $l+1 = r$ to be the analytic rank of F, and writing h for the class number the above gives

$$\frac{\Lambda^{(r-1)}(1)}{(r-1)!} = 0 = 2L^{[N]}_{S^2F}(2)\frac{(\log q)^{r-2}}{(r-2)!}\sum_A\frac{c(A)}{A} + O_F\big(h\sum_A\frac{1}{A}\big).$$

The symmetric-square evaluation at the edge of its critical strip is nonzero, and so the effective divergence of the class number then follows when taking a suitable elliptic curve of analytic rank $r = 3$, such as the -139th quadratic twist of 37b.

Perhaps initially as a curiousity, given an elliptic curve with analytic rank 2 we find that $h \gg 1$. However, a numerical computation with 446d (the first curve to meet the technical conditions regarding root number variation) obtains roughly only $h \geq 2/3$ as $q \to \infty$, indicating that more work must be done if this is to achieve a useful result.

We instead show that for n represented by the principal form there is suitable cancellation in the $c(n)$, so that when $h = 1$ the error term is negligible as $q \to \infty$.

2

We have two different methods to show such cancellation in the $c(n)$ when n is restricted to representations by the principal form.

2.1. The first method is applicable for elliptic curves with complex multiplication by $\mathbf{Q}(\sqrt{-1})$, with an example of analytic rank 2 being the 136th quadratic twist of 32a. Here we recall that $c(n)$ can be written in terms of representations of n as a sum of two squares as

$$c(n) = \theta(n) \sum_{\substack{a=-\infty \\ (4a+1)^2+(2b)^2=n}}^{\infty} \sum_{b=-\infty}^{\infty} (4a+1)(-1)^b$$

where θ is either quadratic character of conductor 136.

We then write $n = X^2 + XY + \frac{q+1}{4}Y^2$ as a representation by the principal form with $Y \geq 1$, and upon completing the square we have $4n = (2X+Y)^2 + qY^2$. This then gives the error term as a sum similar to

$$\frac{1}{q} \sum_{Y=1}^{\infty} \sum_{\substack{X \\ n=(4a+1)^2+(2b)^2 \\ 4n=(2X+Y)^2+qY^2}} \sum_{a} \sum_{b} (4a+1)(-1)^b \theta(n)\, W\Big(\frac{n}{Nq}\Big).$$

The Y-sum can be truncated at small height by the decay of the Mellin transform.

Upon equating the n-expressions we get $4(4a+1)^2 - (2X+Y)^2 = -4(2b)^2 + qY^2$, where we can factor the left-side as tu with t and u as $2(4a+1) \pm (2X+Y)$, and switch variables from (a, X) to (t, u). Furthermore, we can then implicitly have the u-variable occur via a congruence of $-4(2b)^2 + qY^2$ modulo t. Splitting into congruence classes modulo 272, an analysis of 2-adic and 17-adic conditions leads us to consider

$$\sum_{r_b=1}^{34} \sum_{r_t=1}^{272} z(Y, r_b, r_t) \sum_{t \equiv r_t \,(16\cdot 17)} \sum_{\tilde{b}} \frac{t+u}{4}\, W\Big(\frac{n}{Nq}\Big)$$
$$-4(68\tilde{b}+2r_b)^2 + qY^2 \equiv 0 \,(t)$$

where $|z(Y, r_b, r_t)| \leq 4$, while u and n are derived from t as above.

Here we wish to show that the inner double sum over t and $\tilde{b}$ has some cancellation. Let us note that its crude bounding would be $\ll q$, coming from noting that $|t|$ and $|u|$ can be curtailed at size around $\sqrt{q}$ by the W-decay, while the expectation is that there are a constant number of $\tilde{b}$-roots of the congruence on

average. Thus (roughly) the double sum over $(t, \tilde{b})$ has $\ll \sqrt{q}$ members, each of size $\ll |t+u| \ll \sqrt{q}$.

In order to rigidify the contributions from $(t+u)/4$ and the W-term, we split t and $\tilde{b}$ into intervals of size Z (slightly smaller than $\sqrt{q}$), in practice using a smooth partition of unity on $\tilde{b}$. We are essentially left to consider for various (T, B) the expressions

$$\frac{G(T,B)}{4} \times \sum_{\substack{|t-T|<Z/2 \\ t \equiv r_t \,(272) \\ -4(68\tilde{b}+2r_b)^2+qY^2 \equiv 0 \,(t)}} \sum_{|\tilde{b}-B|<Z/2} 1,$$

where

$$G(T,B) = \left(T + \frac{qY^2 - 136^2B^2}{T}\right) W\left(\frac{1}{Nq}\left[\frac{1}{4}\Big(T - \frac{qY^2 - 136^2B^2)}{T}\Big)^2 + qY^2\right]\right)$$

is an odd function of T.

We then recall a result of Hooley (1964) regarding equi-distribution of roots of a polynomial congruence to varying moduli. Our adaptation therein then gives an equi-distribution of the roots of the congruence $-4(68\tilde{b} + 2r_b)^2 + qY^2 \equiv 0\,(t)$ as t varies, implying the above double sum over $(t, \tilde{b})$ is sufficiently well-approximated as proportional to $Z^2/|T|$. This then shows the necessary cancellation, e.g. via pairing T with $-T$.

This proof rather crucially exploits the principal form in achieving the beneficial factorization of the difference of squares into tu. More generally such a factorization is plausible when the binary quadratic form represents a square (i.e., is in the principal genus), though some consideration must be given to uniformity considerations therein.

2.2. Our second method of proof codifies various work over the last decade concerning Hecke eigenvalues over quadratic sequences. This was studied by Blomer (2008), and then Templier and Tsimerman (2010). Indeed, we can almost read the desired result from the latter, though in practice (as they go rather in a different direction) it seems better to re-derive our needed estimate from their methods.

We first note that, following Selberg (1965) and Sarnak's work (1984) with Goldfeld, the method of unfolding gives that

$$\sum_{X=-\infty}^{\infty} \frac{c(X^2+qY^2)}{(X^2+qY^2)^s} = \frac{\Gamma(s)}{(4\pi)^s} \langle P_{\tilde{s}}^{qY^2}, F\bar{\theta}\rangle$$

as an inner product involving a Poincaré series at the parameter $\tilde{s} = s - 1/4$, where here the standard θ-function is given by $\theta(z) = \sum_n e^{2\pi i n^2 z}$ and an analogous formula (involving the θ-series for the odd squares) is applicable more directly to the principal form. Here the mth Poincaré series for weight $3/2$ and congruence

subgroup $\mathbf{\Gamma}$ is defined as

$$P_s^m = \sum_{\gamma \in \mathbf{\Gamma}_\infty \backslash \mathbf{\Gamma}} \bar{\nu}(\gamma) e(m\gamma z) \Big(\frac{cz+d}{|cz+d|} \Big)^{-3/2} \mathrm{Im}(\gamma z)^s,$$

where ν is the standard θ-multiplier system.

We then use the spectral decomposition for Maass forms of level $4N$ to write

$$\langle P_{\tilde{s}}^{qY^2}, F\bar{\theta} \rangle = \sum_{j=1}^{\infty} \langle P_{\tilde{s}}^{qY^2}, \phi_j \rangle \langle \phi_j, F\bar{\theta} \rangle + \sum_{\mathfrak{a}} \int_{(\frac{1}{2})} \langle P_{\tilde{s}}^{qY^2}, E_w^{\mathfrak{a}} \rangle \langle E_w^{\mathfrak{a}}, F\bar{\theta} \rangle \frac{\partial w}{4\pi i}.$$

Considering the discrete spectrum, the first inner product can be written (again by an unfolding argument via the Poincaré series) in terms of the qY^2-th Fourier coefficient of ϕ_j, and this coefficient can in turn be bounded by a result of Duke (1988), which generalizes the bound of Iwaniec (1987) for coefficients of holomorphic forms of half-integral weight. For our application, the second inner product $\langle \phi_j, F\bar{\theta} \rangle$ can be bounded almost trivially (unlike Templier and Tsimerman who in fact show the expected exponential decay in the eigenvalue parameter), while the continuous spectrum can again be handled by Duke's result.

This proof also exploits the principal form, though in general we could perhaps work at a level depending on the minimum A, and upon taking level-uniformity into account, we should be able to obtain a result when A is smaller than some explicit (small) power of q. In any case, the main difficulty in class number problems is when the minima are of size $\sqrt{q}$, and our methods do not avail for such.

Hooley's result only saves a small power of logarithm, while the use of the Iwaniec-Duke bound saves $1/28$ in the q-exponent.

References

[1] A. Baker, *Linear forms in the logarithms of algebraic numbers*. Mathematika **13** (1966), no. 2, 204–216. http://doi.org/10.1112/S0025579300003971

[2] V. Blomer, *Sums of Hecke eigenvalues over values of quadratic polynomials*. Int. Math. Res. Not. **2008**, no. 16. http://doi.org/10.1093/imrn/rnn059

[3] W. Duke, *Hyperbolic distribution problems and half-integral weight Maass forms*. Invent. Math. **92** (1988), no. 1, 73–90. http://doi.org/10.1007/BF01393993

[4] C. F. Gauss, *Disquisitiones Arithmeticae*. (Latin) [Arithmetical investigations] (1801). From his complete works (1863): http://eudml.org/doc/202621 English translation: A. A. Clarke, *Disquisitiones Arithmeticae*, Yale Univ. Press (1965).

[5] D. Goldfeld, *The class number of quadratic fields and the conjectures of Birch and Swinnerton-Dyer*. Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **3** (1976), no. 4, 624–663. http://eudml.org/doc/83732

[6] B. H. Gross, D. B. Zagier, *Heegner points and derivatives of L-series*. Invent. Math. **84** (1986), no. 2, 225–320. http://eudml.org/doc/143341

[7] K. Heegner, *Diophantische Analysis und Modulfunktionen*. (German) [Diophantine analysis and modular functions]. Math. Z. **56** (1952), 227–253. http://eudml.org/doc/169287

[8] C. Hooley, *On the distribution of the roots of polynomial congruences*. Mathematika **11** (1964), 39–49. http://doi.org/10.1112/S0025579300003466

[9] H. Iwaniec, *Fourier coefficients of modular forms of half-integral weight*. Invent. Math. **87** (1987), 385–402. http://eudml.org/doc/143426

[10] P. Sarnak, *Additive number theory and Maass forms*. In *Number theory (New York, 1982)*, edited by D. V. Chudnovsky, G. V. Chudnovsky, H. Cohn, and M. B. Nathanson. Springer LNM **1052** (1984), 286–309. http://doi.org/10.1007/BFb0071548

[11] A. Selberg, *On the estimation of Fourier coefficients of modular forms*. Proc. Sympos. Pure Math. **8** (1965), 1–15. http://bookstore.ams.org/pspum-8

[12] H. M. Stark, *A complete determination of the complex quadratic fields of class-number one*. Michigan Math. J. **14** (1967), no. 1, 1–27. http://doi.org/10.1307/mmj/1028999653

[13] N. Templier, J. Tsimerman, *Non-split sums of coefficients of $GL(2)$-automorphic forms*. Israel J. Math. **195** (2013), no. 2, 677–723. http://doi.org/10.1007/s11856-012-0112-2

MCLF: a toolbox for computations with Models of Curves over Local Fields

Stefan Wewers

(joint work with Julian Ruth)

We present a software project, MCLR, whose general goal is to make computations with integral models of curves over local fields easy and accessible. It is written in Sage/Python and builds on Julian Ruth's implementation of valuations, following work of MacLane.

In this preliminary stage, we focus on implementing methods to compute semistable reduction of curves over p-adic fields, and use this to compute arithmetic invariants, e.g. Euler factors and the conductor.

In the talk, I demonstrated the computation of semistable reduction and conductor exponents of Picard curves.[9]

Progress on Mazur's "Program B"

David Zureick-Brown

We discuss progress on Mazur's "Program B".

Reporter: Levent Alpoge

[9]Compiled by the reporter from the hand-written abstract at Oberwolfach

Participants

Levent Alpoge
Department of Mathematics
Princeton University
Fine Hall
Washington Road
Princeton, NJ 08544-1000
UNITED STATES

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

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

Renee H. Bell
Department of Mathematics
Massachusetts Institute of Technology
77 Massachusetts Avenue
Cambridge, MA 02139-4307
UNITED STATES

Prof. Dr. Michael A. Bennett
Department of Mathematics
University of British Columbia
121-1984 Mathematics Road
Vancouver BC V6T 1Z2
CANADA

Prof. Dr. Amnon Besser
Department of Mathematics
Ben-Gurion University of the Negev
P.O.Box 653
84105 Beer-Sheva
ISRAEL

Prof. Dr. Frits Beukers
Mathematisch Instituut
Universiteit Utrecht
Budapestlaan 6
P. O. Box 80.010
3508 TA Utrecht
NETHERLANDS

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

Dr. Andrew Booker
Department of Mathematics
University of Bristol
University Walk
Bristol BS8 1TW
UNITED KINGDOM

Prof. Dr. Irene I. Bouw
Institut für Reine Mathematik
Universität Ulm
Helmholtzstrasse 18
89081 Ulm
GERMANY

Prof. Dr. Nils Bruin
Department of Mathematics and Statistics
Simon Fraser University
Burnaby BC V5A 1S6
CANADA

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

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

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

Prof. Dr. John E. Cremona
Mathematics Institute
University of Warwick
Gibbet Hill Road
Coventry CV4 7AL
UNITED KINGDOM

Dr. Ishai Dan-Cohen
Department of Mathematics
Ben-Gurion University of the Negev
84105 Beer-Sheva
ISRAEL

Dr. Netan Dogra
Department of Mathematics
Imperial College London
South Kensington Campus
London SW7 2AZ
UNITED KINGDOM

Prof. Dr. Tim Dokchitser
Department of Mathematics
University of Bristol
University Walk
Bristol BS8 1TW
UNITED KINGDOM

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

Prof. Dr. Kirsten Eisentraeger
Department of Mathematics
Pennsylvania State University
University Park, PA 16802
UNITED STATES

Dr. Tony Mack Robert Ezome Mintsa
Département de Mathématiques et Informatique
Facultés des Sciences
Université des Sciences et Techniques de Masuku
901, Quartier Mbaya
P.O. Box 943
Franceville
GABON

Prof. Dr. Eugene Victor Flynn
New College
University of Oxford
Holywell Street
Oxford OX1 3BN
UNITED KINGDOM

Prof. Dr. Paul E. Gunnells
Department of Mathematics and Statistics
University of Massachusetts
710 North Pleasant Street
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

Dr. Valentijn Karemaker
Department of Mathematics
David Rittenhouse Laboratory
University of Pennsylvania
209 South 33rd Street
Philadelphia, PA 19104-6396
UNITED STATES

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

Dr. Brian Lawrence
Department of Mathematics
Columbia University
2990 Broadway
New York, NY 10027
UNITED STATES

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

Dr. Adam Logan
Tutte Institute of Mathematics and Computation
P.O. Box 9703, Terminal
Ottawa Ontario K1G 3Z4
CANADA

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

Dr. Jan Steffen Müller
Johann Bernoulli Institute for Mathematics and Computer Science
University of Groningen
P.O. Box 407
9700 AK Groningen
NETHERLANDS

Dr. Jennifer Park
Department of Mathematics
University of Michigan
2074 East Hall
530 Church Street
Ann Arbor, MI 48109-1043
UNITED STATES

Prof. Dr. Bjorn Poonen
Department of Mathematics
Massachusetts Institute of Technology
77 Massachusetts Avenue
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. Joseph Rabinoff
School of Mathematics
Georgia Institute of Technology
Atlanta, GA 30332-0160
UNITED STATES

Dr. Danylo Radchenko
Max Planck Institut für Mathematik
Vivatsgasse 7
53111 Bonn
GERMANY

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

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

Dr. 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

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

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

Prof. Dr. Douglas Ulmer
Department of Mathematics
University of Arizona
P.O.Box 210089
Tucson AZ 85721-0089
UNITED STATES

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

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

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

Prof. Dr. Jiuya Wang
Department of Mathematics
University of Wisconsin-Madison
480 Lincoln Drive
Madison, WI 53706-1388
UNITED STATES

Dr. Mark J. Watkins
MAGMA Computer Algebra Group
School of Mathematics and Statistics
The University of Sydney
Carslaw Building (F07)
Sydney NSW 2006
AUSTRALIA

Prof. Dr. Stefan Wewers
Institut für Reine Mathematik
Universität Ulm
89069 Ulm
GERMANY

Prof. Dr. Kirsten G. Wickelgren
School of Mathematics
Georgia Institute of Technology
Skiles 227
686 Cherry Street
Atlanta, GA 30332-0160
UNITED STATES

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

Dr. David Zureick-Brown
Department of Mathematics and
Computer Science
Emory University
400, Dowman Dr.
Atlanta, GA 30322
UNITED STATES