Mathematisches Forschungsinstitut Oberwolfach

Report No. 35/2011

DOI: 10.4171/OWR/2011/35

Explicit Methods in Number Theory

Organised by
Karim Belabas, Talence
Hendrik W. Lenstra, Leiden
Don B. Zagier, Bonn

July 17th – July 23rd, 2011

Abstract. These notes contain extended abstracts on the topic of explicit methods in number theory. The range of topics includes the Sato-Tate conjecure, Langlands programme, function fields, L-functions and many other topics.

Mathematics Subject Classification (2000): 11xx, 12xx, 13xx, 14xx.

Introduction by the Organisers

The workshop Explicit Methods in Number Theory was organised by Karim Belabas (Talence), Hendrik W. Lenstra (Leiden), and Don B. Zagier (Bonn), and it took place July 17–23, 2011. Six previous workshops on the topic had been held in 1999, 2001, 2003, 2005, 2007 and 2009. The goal of the meeting was to present new methods and results on concrete aspects of number theory. In several cases, this included algorithmic and experimental work, but the emphasis was on the implications for number theory. There were two 'mini-series' of three hours highlighting important recent developments: one by Frank Calegari, on reciprocity in the Langlands programme and how to compute spaces of automorphic forms of arithmetic interest; and one by Manjul Bhargava on monogenic cubic fields and their applications to the average rank of rational elliptic curves. Two longer talks were split among three lecturers each: on the Sato-Tate conjecture and on the densities of discriminants of cubic fields (numerical testing and proof of the so-called Roberts's conjecture). Some other themes were:

- Modular curves
- Function fields

- L-functions
- Cohen-Lenstra heuristics.

In addition to the lectures, there were two scheduled social activities. On Wednesday afternoon there was a hike. Due to bad weather only a small group of people participated and walked to Oberwolfach-Kirche, where they had a drink and enjoyed the Black Forest cake. After that they went to MiMa, Museum for Minerals and Mathematics Oberwolfach, and enjoyed the exhibition and they walked back 'home', to arrive just in time for dinner. On Thursday a problem session was organized after the evening meal, at 8pm. After an initial announcement 2 days earlier, problems had been collected from participants by Peter Stevenhagen (Leiden), who acted as chairman during the session, and rewarded each presenter of a problem with a glass of wine. The maximum presentation time for a problem was 5 minutes. The initial list of presenters of problems counted 9 participants, and several others decided to join in during the session. For some problems, partial solutions were obtained. The problem session lasted about an hour.

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 56 participants from a variety of backgrounds, including some young researchers with an OWLG-grant. There were 36 talks of various lengths, and ample time was allotted to informal collaboration.

Workshop: Explicit Methods in Number Theory

Table of Contents

Abstracts

L-Functions of Hypergeometric Motives

Henri Cohen
(joint work with Fernando Rodriguez-Villegas)

Let $(\alpha_j)_{1\le j\le r}$ and $(\beta_j)_{1\le j\le r}$ be two disjoint sets of equal cardinality of *rational numbers*. We make the *hypergeometric assumption* that $\prod_j(X-e(\alpha_j))$ and $\prod_j(X-e(\beta_j))$ are products of cyclotomic polynomials, where $e(z)=e^{2\pi iz}$. Examples $(1/2,1/2,1/6,5/6)$, or $(1/5,2/5,3/5,4/5)$.

Then **theorem** due to N. Katz: there exists a family $H(\alpha,\beta;t)$ of *motives* defined for any $t\in\mathbb{P}_1(\mathbb{Q})\setminus\{0,1,\infty\}$, defined over $\mathbb{Q}$, of rank r, pure with a certain weight w. Therefore there exists a global L-function

$$L(s)=\sum_{n\ge1}\frac{a_n}{n^s}=\prod_p P_p(p^{-s})^{-1}$$

where $P_p(T)$ is a polynomial of degree at most equal to r (equal to r for $p\nmid N$ for a suitable *conductor* N), with $P(T)=\prod_{1\le i\le r}(1-\xi_iT)$ for $|\xi_i|=p^{w/2}$ for $p\nmid N$. This theorem also gives a precise recipe for the weight and the Euler factors $P_p(T)$ for $p\nmid N$, but *not* for N or $P_p(T)$ for $p\mid N$.

A conjecture due to Corti–Golyshev also gives a precise recipe for the *Hodge numbers* of this motive, hence by old theorems of Serre, gives a factor at infinity $L_\infty(s)$ as products of gamma factors. Thus conjecturally, if one sets $\Lambda(s)=N^{s/2}L_\infty(s)L(s)$ then Λ should extend to an entire function on $\mathbb{C}$ satisfying the functional equation $\Lambda(w+1-s)=\pm\Lambda(s)$ (self-dual).

The goal of this work is to understand more precisely the conductor N and the precise shape of the Euler factors $P_p(T)$ for the "bad" primes $p\mid N$. These bad primes split naturally into two classes: the *wild* primes, which are those which divide the denominator of one of the α_j or β_j, and the *tame* primes p, which are nonwild primes with $v_p(t)>0$ or $v_p(1/t)>0$ or $v_p(t-1)>0$. All other primes are good, and do not divide N.

We have experimented on hundreds of examples up to degree $r=6$: in particular, we understand completely the behavior of bad primes for the 13 examples in degree 2, which include 10 interesting families of elliptic curves (without CM), and the case $\alpha=(1/5,2/5,3/5,4/5)$, $\beta=(0,0,0,0)$ corresponding to the mirror of the Calabi–Yau quintic

$$x_0^5+x_1^5+x_2^5+x_3^5+x_4^5-5t\,x_0x_1x_2x_3x_4=0\,.$$

In all generality, we have a good (although not absolutely complete) understanding of the behavior of the *tame* primes. On the other hand, the behavior of the wild primes is much more mysterious.

See `http://www.math.u-bordeaux1.fr/~cohen/ow.pdf` for the slides of the talk.

Jet list decoding

Daniel J. Bernstein

There is a classic algorithm that uses LLL to quickly find all divisors of N in an interval $[A-H, A+H]$, provided that H is not too large compared to the smallest possible divisor $A-H$. Specifically, the algorithm handles $H \approx N^{\theta^2}$ in polynomial time if $A - H = N^\theta$.

This algorithm has been generalized in many ways, but the following direction of generalization appears to be new: one can use LLL to quickly find all $t \in \{-H, \ldots, -1, 0, 1, \ldots, H\}$ such that the Gaussian integer $A_0 + A_1 i + (B_0 + B_1 i)t \in \mathbf{Z}[i]/(i^2+1)$ divides $N_0 + N_1 i$, under suitable nondegeneracy assumptions. To reduce this to a previously solved problem, simply multiply by the conjugate of the divisor and extract the coefficient of i, concluding that $\gcd\{A_0N_1 - A_1N_0 + (B_0N_1 - B_1N_0)t, N_0^2 + N_1^2\}$ has a large divisor, namely $(A_0 + B_0t)^2 + (A_1 + B_1t)^2$.

The same technique finds all $t \in \{-H, \ldots, -1, 0, 1, \ldots, H\}$ such that a 1-jet $A_0 + A_1\epsilon + (B_0 + B_1\epsilon)t \in \mathbf{Z}[\epsilon]/\epsilon^2$ divides $N_0 + N_1\epsilon$. Compared to searching for a divisor $A_0 + B_0t$ of N_0, the new algorithm doubles the number of digits in H.

A few years ago I introduced a very fast list-decoding algorithm for classical irreducible binary Goppa codes. The jet-divisor idea (with the affine t line replaced by the projective t line, and with $\mathbf{Q}$ replaced by the rational function field $\mathbf{F}_2(x)$) is directly applicable here, and produces a very fast list-decoding algorithm that should decode approximately twice as many extra errors for the same codes.

Don Zagier adds that the 1-jet R-algebra $R[\epsilon]/\epsilon^2$, being generated by 2 elements as an R-module, should obviously be called a jet plane.

The radical root and the integral closure

Michiel Kosters
(joint work with Hendrik W. Lenstra)

This talk consists of two parts. In the first part, we let $(R, \mathfrak{m})$ be a zero-dimensional principal ideal ring. For example one can take $R = \mathbb{Z}/p^i\mathbb{Z}$ where $i \in \mathbb{Z}_{\geq 1}$. Let M be a finitely generated R-module and let N be an R-module such that $N \cong_R R$. We consider a non-degenerate symmetric R-bilinear form $\varphi : M \times M \to N$. We define the radical root of φ as

$$\mathrm{rr}(M, \varphi) = \bigcap_{L \subseteq M : \mathfrak{m}L^\perp \subseteq L \subseteq L^\perp} L \subseteq M.$$

Under the assumption that $\mathrm{char}(R/\mathfrak{m}) \neq 2$, we give a list of options for $\mathrm{rr}(M, \varphi)$, and we remark that this option depends on the anisotropy of certain symmetric bilinear forms on $R/\mathfrak{m}$.

In the second part we explain why this radical root is useful in algebraic number theory. For simplicity we let $(Z, \mathfrak{p})$ be a complete discrete valuation ring with quotient field Q, instead of working over a Dedekind domain. Now consider an order A over Z (A is a Z-algebra which is free of finite rank as Z-module). One

of the main algorithmic problems is to find the integral closure $\overline{A}$ of A in its total quotient ring $Q(A)$. We define the trace dual of A as $A^\dagger = \{x \in Q(A) : \mathrm{Tr}_{Q(A)/Q}(xA) \subseteq Z\}$ and let $B = A^\dagger/A$, a finitely generated torsion Z-module. For some $i \in \mathbb{Z}_{\geq 1}$ we obtain a non-degenerate symmetric $Z/\mathfrak{p}^i$-bilinear form $\varphi : B \times B \to \mathfrak{p}^{-i}Z/Z$. This is precisely a form as discussed in the first part. Under some technical assumptions, namely if $\mathrm{char}(Z/\mathfrak{p}) = 0$ or if $\mathrm{char}(Z/\mathfrak{p}) > \dim_{Z/\mathfrak{p}}(B/\mathfrak{p}B)$, we can show that $\mathrm{rr}(A^\dagger/A, \varphi) \subseteq \overline{A}/A$. This already shows that if $\mathrm{rr}(A^\dagger/A, \varphi) \neq 0$, we find a piece of $\overline{A}$ which is strictly larger than A. A priori the lift of $\mathrm{rr}(A^\dagger/A, \varphi)$ under the map $A^\dagger \to A^\dagger/A$ is just a Z-module. It turns out that this Z-module is in fact a ring in a special case. During this lecture we discuss the proof of this special case.

References

[1] M. Kosters, *Anisotropy and the integral closure*, Universiteit Leiden (2010)

$A(1)$ and the dilogarithm

Fernando Rodriguez Villegas

I gave a talk on this subject at an earlier Oberwolfach meeting *Representation theory of quiver and finite dimensional algebras*. At the present *Explicit methods in number theory* workshop I emphasized more the connection to asymptotics of certain q-series at $q = 1$ and the dilogarithm and this report will reflect that.

Before he had a proof of a now famous identity

$$\sum_{\mathbf{n}\geq 0} \frac{q^{n^2}}{(q)_n} = \prod_{k\geq 1}(1-q^k)^{-1}, \qquad k \equiv \pm 1 \bmod 5,$$

Ramanujan tested it by studying the asymptotics of the logarithm of each side for $q = e^{-t}$ with t approaching 0. The equality of the leading terms in t amounts to the following identity due to Landen

$$L\left(\frac{3-\sqrt{5}}{2}\right) = \frac{\pi^2}{15},$$

where L denotes the Rogers dilogarithm.

The asymptotics of this type of series has been studied extensively. For example, they play an important role in conformal field theory (see for example, [4, 6]). There are several approaches to study these asymptotics (see [5], [6], and [10]). The main feature is that their leading term appears as a sum of values of the dilogarithm function. In this talk I presented another instance where these asymptotics play a role. Namely, in obtaining a formula for the value at $q = 1$ of the A-polynomial of an arbitrary quiver.

A quiver is simply a finite directed graph. A representation of a quiver is an assignment of finite dimensional vector spaces to the vertices and linear maps between them to the arrows. The A-polynomial $A(q)$ of a quiver Γ counts the

number of absolutely indecomposable representations of Γ over the field $\mathbb{F}_q$ with a given dimension vector.

One one hand, by our joint work [2] with Hausel and Letellier, we expect the value $A(1)$ to be the middle Betti number of an associated character variety. On the other, it is tempting to interpret $A(1)$ as counting certain simpler combinatorial objects resulting from letting the field size q become 1. Our main formula (2) might shed light on these questions. See [9] for the full version.

I concentrate on the following example. Let S_g be the quiver consisting of one vertex and g loops and let $A_n^g(q)$ be the A-polynomial for dimension n. We define a priori rational functions $A_\lambda(q)$ indexed by partitions λ which give a decomposition

$$A_n(q) = \sum_{|\lambda|=n} A_\lambda(q)$$

of the A-polynomial of S_g.

Computations suggest that for $g > 0$, which we assume from now on, $A_\lambda(q)$ is in fact a polynomial in q with non-negative integer coefficients. For example, for $g = 2$ and $n = 3$ we obtain

$$A_{(1,1,1)}(q) = q^{10} + q^8 + q^7, \quad A_{(2,1)} = q^6 + q^5, \quad A_{(3)} = q^4$$

with sum

$$A_3(q) = q^{10} + q^8 + q^7 + q^6 + q^5 + q^4$$

The main result given below (2) is a sort of fermionic-type formula. In fact, the kind of analysis used to prove it appears prominently in the (extensive) physics literature under the heading of Q-systems, originating from the work of Kirillov–Reshetikhin on representation theory and the combinatorics of the Bethe Ansatz. The basic application of Lagrange's inversion we use can be found for example in [4]. We preferred to rederive the results we needed from scratch.

The starting point for the proof of (2) is the formula of Hua for the A-polynomial. Truncating the sum for the S_g quiver to partitions with parts at most N leads to a series of the following form

$$\sum_{m=(m_1,\ldots,m_N)} \frac{q^{(g-1)^t m \mathcal{H}_N m}}{\prod_{i=1}^N (q^{-1})_{m_i}} T^{\sum_i i m_i} \tag{1}$$

where $m_i \in \mathbb{Z}_{\geq 0}$ and $\mathcal{H}_N := (\min(i,j))\,, i,j = 1,2,\ldots,N$. This is a q-series of the kind we alluded to above for which we obtain an expression for the leading term as q tends to 1 in terms of the dilogarithm. On the other hand, by Hua's formula this leading term can also be expressed in terms of $A_n^g(1)$. After some work, combining these two expressions yields a proof of (2).

Theorem 1. *For any non-zero partition λ we have*

$$A_\lambda(1) = \frac{1}{\rho} \sum_{d|m} \frac{\mu(d)}{d^2} \frac{1}{P_1(m/d) P_N(m/d)} \prod_{i \geq 1} \binom{\rho P_i(m/d) - 1 + m_i/d}{m_i/d} \tag{2}$$

where $\lambda = (1^{m_1}2^{m_2}\cdots N^{m_N})$ *with* $N = \lambda_1$*, the largest part of* λ*,*

$$P_i(m) := \sum_{j\geq 1} \min(i,j)\, m_j, \qquad m := (m_1, m_2, \ldots), \quad \rho =: 2g-2,$$

and μ *is the Möbius function of number theory.*

The case $\lambda = (1^n)$ was previously proved by Reineke [7] by different methods. By the conjectures of [1] the number $A_n(1) = \sum_{|\lambda|=n} A_\lambda(1)$ should equal the dimension of the middle dimensional cohomology group of the character variety $\mathcal{M}_n$ studied there. A refined version of this conjecture states that $A_\lambda(1)$ is the number of connected components of type λ of a natural $\mathbb{C}^\times$ action on the moduli space of Higgs bundles, which is diffeomorphic to $\mathcal{M}_n$. A proof of this conjecture for $\lambda = (1^n)$ was recently given by Reineke [8, Theorem 7.1]. The refined conjecture originates in [1, Remark 4.4.6] and was in fact the motivation to construct the truncated polynomials $A_\lambda(q)$ studied here.

There are some difficulties but I expect that a similar analysis can be carried out for an arbitrary quiver.

References

[1] T. Hausel and F. Rodriguez Villegas, with an appendix by N. Katz *Mixed Hodge polynomials of character varieties*, arXiv:0612668 Invent. Math. **174** 555–624(2008).

[2] T. Hausel, E. Letellier and F. Rodriguez Villegas *Arithmetic harmonic analysis on character and quiver varieties* arXiv:0810.2076 (to appear in Duke Math. J.)

[3] G. Helleloid and F. Rodriguez Villegas: *Counting Quiver Representations over Finite Fields Via Graph Enumeration*, math.RT/0810.2127, J. of Alg. 322 (2009) 1689–1704.

[4] A. Kuniba, T. Nakanishi and Z. Tsuboi: *The canonical solutions of the Q-systems and the Kirillov-Reshetikhin conjecture* Comm. Math. Phys. **227** (2002) 155–190

[5] R. Mcintosh: *Asymptotic transformations of q-series* Can. J. Math. **50** (1998) 412–425

[6] W. Nahm: *Conformal field theory and torsion elements of the Bloch group* Frontiers in number theory, physics, and geometry. II, 67–132, Springer, Berlin, 2007

[7] M. Reineke: *Cohomology of quiver moduli, functional equations, and integrality of Donaldson–Thomas type invariants* (to appear in Comp. Math.) arXiv:0903.0261

[8] M. Reineke: *Degenerate cohomological Hall algebra and quantized Donaldson–Thomas invariants for m-loop quivers* arXiv:1102.3978

[9] F. Rodriguez Villegas: *A refinement of the A-polynomial of quivers* arXiv:1102.5308

[10] D. Zagier: *The dilogarithm function* Frontiers in number theory, physics, and geometry. II, 3–65, Springer, Berlin, 2007

Reciprocity in the Langlands Programme

Frank Calegari

1. Introduction

The "reciprocity" conjecture in the Langlands programme broadly posits a bijection between two classes of objects:

$$\{\textit{geometric}\text{ Galois representations }\rho\} \leftrightsquigarrow \{\textit{algebraic}\text{ automorphic representations }\pi\}$$

This correspondence should roughly be seen as a generalization of the following two theorems:

(1) Cuspidal modular eigenforms give rise to Galois representations (Shimura, Deligne),
(2) Semistable Elliptic curves over $\mathbb{Q}$ are modular (Wiles, Taylor–Wiles).

More classically, class field theory gives a correspondence between cyclic extensions of a number field K and characters of the idele class group. The goal of these three lectures will be to discuss:

(1) The main properties of geometric Galois representations,
(2) The basic properties of algebraic automorphic representations and their incarnations.
(3) Methods for computing spaces of automorphic forms of arithmetic interest, including:
    (a) Computations on algebraic varieties
    (b) Computations on finite sets
    (c) Computations on manifolds
(4) Phenomenology: To what extent does the special case of modular forms mirror the general picture, and to what extent does it look quite different?
(5) Variations: What happens when we consider Galois representations with images in finite fields, or over complete local Noetherian rings with finite residue field?
(6) Applications: What can one say about even Galois representations:

$$\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)?$$

For space reasons, this write up will only contain some discussion of the last point.

2. An Example: Even Galois Representations

Let $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ be an even Galois representation. What does the arithmetic Langlands programme say about such representations? There are two natural classes of arithmetic quotients of symmetric spaces where we may look to find Hecke eigenclasses which are related to $\overline{\rho}$.

(1) Choose an auxiliary imaginary quadratic field $E/\mathbb{Q}$, and then consider the restriction $\overline{\rho} : G_E \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$. Then, conjecturally, $\overline{\rho}$ should give rise to a class in $H_1(X(\Gamma), \mathscr{L}/p)$ for an appropriate local system $\mathscr{L}$.
(2) Choose an auxiliary imaginary quadratic field $E/\mathbb{Q}$, and consider the Galois representation: $\overline{\varrho} = \mathrm{Sym}^2(\overline{\rho}) \det(\overline{\rho})^{-1} : G_E \to \mathrm{GL}_3(\overline{\mathbb{F}}_p)$. The representation ϱ is conjugate self dual, and also odd (in the sense of Clozel–Harris–Taylor), and thus if $X(\Gamma)$ is the finite set corresponding to an appropriate arithmetic quotient for the group $U(3)$, then ϱ conjecturally gives rise to a class in $H^0(X(\Gamma), \mathscr{L}/p)$. Since H^0 of a point is torsion free, it also gives rise to a class in $H^0(X(\Gamma), \mathscr{L})$. The existence of Galois representations is known in this case.

In light of this correspondence, we might ask ourselves the following: what is the smallest absolutely irreducible even continuous even Galois representation:

$$\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

unramified at all places of $\mathbb{Q}$ except p? In particular, since we insist that $\overline{\rho}$ is unramified at infinity, the representation $\overline{\rho}$ is even. It is known that no such representation exists when $p \leq 7$ (for $p = 2$ this is a well known result of Tate [4], for other small p see Theorem 1 of [2]). The generalized version of Serre's conjecture predicts that there are only finitely many such representations for each p. There are two plausible measures by which we can define "smallest." One measure is to ask for the smallest prime p such that there exists such a representation $\overline{\rho}$. A second plausible parameter is the Serre weight $k := k(\overline{\rho})$, which is an integer $2 \leq k \leq p^2 - 1$. After twisting, we may assume that k actually satisfies the inequality $2 \leq k \leq p+1$. We might also ask for the smallest k such that there exists a representation $\overline{\rho}$ with $k(\overline{\rho}) = k$. We make some progress on both questions, mostly in the direction of giving lower bounds. Unfortunately, we are not able to find any Galois representations $\overline{\rho}$ as above with image containing $\mathrm{SL}_2(\mathbb{F}_p)$. We do, at least, find "evidence" of representations $\overline{\rho}$ with solvable image, which (as such representations can be found directly) lends some confidence that our method is sound. The Heuristics metioned Akshay's lecture suggest that the number of such representations with image containing $\mathrm{SL}_2(\mathbb{F}_p)$ for $p < x$ is (approximately) $\log(\log(x))$. Unfortunately, this function is well known to be constant, and the range in which we are computing it seems to be zero.

2.1. **Unitary Groups $U(3)$.** David Loeffer wrote some programs to compute automorphic forms for the unitary group $U(3)$ which splits over $E = \mathbb{Q}(\sqrt{-7})$. Given $\overline{\rho}$ and $\overline{\varrho}$, one has to compute all the forms on $U(3)$ and level 1 for local systems of weight "$\leq p$". Given a form π, one can compute the Hecke operators, and then check:

(1) Is $a_{\mathfrak{q}} \equiv a_{\mathfrak{q}^c} \mod \varpi$ for all split $\mathfrak{q}$ and some prime p?
(2) If so, is the representation a twist of a representation of the form $\mathrm{Sym}^2(\overline{\rho})$ for some $\overline{\rho}$ defined over $G_{\mathbb{Q}}$.
(3) If $\overline{\varrho}$ *is* of this form, is the corresponding representation $\overline{\rho}$ even?

These computations were carried out for $p \leq 11$, and no irreducible even representations $\overline{\rho}$ were found.

2.2. **Imaginary Quadratic Fields.** Let E denote an imaginary quadratic field. For convenience let us also assume that E has class number one — since the only fields for which any computations were done were for $E = \mathbb{Q}(\sqrt{-2})$ and $E = \mathbb{Q}(\sqrt{-11})$, this is not a restriction. Our computations rely on the following conjecture (which can be made much more precise):

Conjecture 1. *Serre's conjecture for imaginary quadratic fields E of class number one is true for representations $\overline{\rho} : G_E \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ of level $N(\overline{\rho}) = 1$.*

Given an even absolutely irreducible Galois representation $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$, the restriction of $\overline{\rho}$ to G_E is also absolutely irreducible (the only representations which become reducible are those dihedral representations coming from characters of the class group of E, which can be determined in advance), and thus corresponds (via Conjecture 1) to a cohomology class for $\mathrm{GL}_2(\mathcal{OL}_E)$. We shall be interested in computing the following quantity:

$$\dim H_1(\mathrm{GL}_2(\mathcal{OL}_E), \mathscr{L} \otimes \mathbb{F}_p) - \dim H_1(\mathrm{GL}_2(\mathcal{OL}_E), \mathscr{L} \otimes \mathbb{C})^{BC},$$

where $\mathscr{L}$ is the local system corresponding to the representation $\mathrm{Sym}^{k-2} \otimes \overline{\mathrm{Sym}^{k-2}}$, and BC denotes the subspace of forms which are either CM or arise from base change from $\mathrm{GL}(2)/\mathbb{Q}$. If $\overline{\rho}$ has Serre weight k, then the first cohomology group will have larger dimension than the second. Hence, if we compute the quantity above and it is non-zero, this indicates that there exists a possible $\overline{\rho}$. Moreover, if we compute this quantity for *different* fields E and still obtain a non-zero value, this gives strong evidence for the existence of $\overline{\rho}$. (Conversely, if we compute for some field E and find that the quantity above is zero, then $\overline{\rho}$ can not exist, assuming our conjectures). It is the case that in the range of any computation that we do that $\dim H_1(\mathscr{L} \otimes \mathbb{C})^{BC} = \dim H_1(\mathscr{L} \otimes \mathbb{C})$. Hence, when we are able to compute $H_1(\mathscr{L})$ integrally, we can determine when the quantity above is zero for a fixed k and all p simultaneously, namely, the exponents of the torsion subgroup of $H_1(\mathscr{L})$. (If $\dim H_1(\mathscr{L} \otimes \mathbb{C})^{BC} < \dim H_1(\mathscr{L} \otimes \mathbb{C})$, we would need to do some extra computations with Hecke operators to determine the finite set of possible p.)

3. The results

In the range of our computations, we find exactly one irreducible representation $\overline{\rho}$ up to twist. Namely, a representation

$$G_{\mathbb{Q}} \to \mathrm{Gal}(E/\mathbb{Q}) \simeq \widetilde{A_4} \to \mathrm{GL}_2(\mathbb{F}_{163}),$$

corresponding to a lift of the even A_4-extension of $\mathbb{Q}$ ramified only at 163. The determinant of this extension is (one of the) characters of $\mathbb{Q}(\zeta_{163})$ of order 3, which are all conjugate to $\omega^{(163-1)/3} = \omega^{55-1}$. Thus this representation corresponds to $(p, k) = (163, 55)$. Our computations are generally for the field $\mathbb{Q} = \mathbb{Q}(\sqrt{-2})$. The entry in column (p, k) denotes the quantity indicated above. We make some specific remarks on the tables (all modulo Conjecture 1):

- If $k > p + 1$, the quantity is greyed out, because any $\overline{\rho}$ is twist equivalent to a representation with $k(\overline{\rho}) \leq p + 1$.
- We only list what happens for odd k. If $\overline{\rho}$ has $k(\overline{\rho}) = k$, then $\det(\overline{\rho}) = \omega^{k-1}$ which is only even if k is odd (at least when p is odd. When $p = 2$, one can appeal to [4].)
- The green squares correspond to weights for which the non-existence of $\overline{\rho}$ is known, whereas magenta squares correspond to weights in which a similar conclusion is known modulo GRH. (See [2]).

- The yellow squares denote pairs (p, k) for which the computation above yields a non-zero quantity for $K = \mathbb{Q}(\sqrt{-2})$, but such that the same computation for the field $K = \mathbb{Q}(\sqrt{-11})$ yields the result zero. In particular, for yellow squares, there are no even representations $\overline{\rho}$ (assuming Conjecture 1.)
- The reason that all the non-zero squares are even is explained by "doubling"; see [1].
- The blue squares are the squares for which our quantity is non-zero for *both* $K = \mathbb{Q}(\sqrt{-2})$ and $K = \mathbb{Q}(\sqrt{-11})$. They are the "money" squares, which could plausibly correspond to even Galois representations. Sadly, the only blue square corresponds to $(p, k) = (163, 55)$.
- If $k \leq 21$, the results are in agreement with Şengün's integral computations for $K = \mathbb{Q}(\sqrt{-2})$, which were computed using another method (see [3]).
- If $k \leq 32$, the integral cohomology for $K = \mathbb{Q}(\sqrt{-1})$ was computed by Şengün [3]. (There is a conflict of notation here — our $\mathscr{L}$ in weight k corresponds to Şengün's $M_{k-2,k-2}$.) If follows from those computations that the only possible even $\overline{\rho}$ of weight $k(\overline{\rho}) = k \leq 32$ must occur with $(p, k) = (89, 31)$. Yet the corresponding computation with $K = \mathbb{Q}(\sqrt{-2})$ yields zero.

We can summarize the results of our computation as follows: We have:

Theorem 2. *Let $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ be an absolutely irreducible continuous even Galois representation of Serre level $N(\overline{\rho}) = 1$ and of Serre weight $k = k(\overline{\rho})$. Then k is odd, moreover, assuming Conjecture 1:*

(1) *The prime p is at least 79.*
(2) *The weight k is at least 33.*
(3) *If $k < 54$, then $p > 1000$.*
(4) *If $k = 55$, then p is either > 200, or $p = 163$. Moreover, if $k = 55$ and $p = 163$, then $\overline{\rho}$ is the unique representation with projective image A_4.*
(5) *If $k \in \{57, \ldots, 69\}$, then either $p > 200$ or (p, k) corresponds to a red square in Table 3.*

Heuristics indicate that there may exist perhaps one $p < 1000000$ such that there exists an even representation $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ unramified outside p with image containing $\mathrm{SL}_2(\mathbb{F}_p)$.

References

[1] F. Calegari, A. Venkatesh, *A Torsion Jacquet–Langlands conejcture*, preprint.
[2] H. Moon, Y. Taguchi, *Refinement of Tate's discriminant bound and non-existence theorems for mod p Galois representations*, *Documenta Mathematica*, 2003, pp. 641–654.
[3] M. Şengün, *On the integral cohomology of Bianchi groups*, To appear in *Experimental Mathematics*.
[4] J. Tate, *The non-existence of certain Galois extensions of* **Q** *unramified outside* 2, In *Arithmetic geometry (Tempe, AZ, 1993)*, Providence, RI, 1994, pp. 153–156.

Prime p \ Serre weight k	3	5	7	9	11	13	15	17	19	21	23	25	27
3	0												
5	0	0											
7	0	0	0										
11	0	0	0	0	0								
13	0	0	0	0	0	0							
17	0	0	0	0	0	0	0	0					
19	0	0	0	0	0	0	0	0	0				
23	0	0	0	0	0	0	0	0	0	0	0		
29	0	0	0	0	0	0	0	0	0	0	0	0	0
31	0	0	0	0	0	0	0	0	0	0	0	0	0
37	0	0	0	0	0	0	0	0	0	0	0	0	0
41	0	0	0	0	0	0	0	0	0	0	0	0	0
43	0	0	0	0	0	0	0	0	0	0	0	0	0
47	0	0	0	0	0	0	0	0	0	0	0	0	0
53	0	0	0	0	0	0	0	0	0	0	0	0	0
59	0	0	0	0	0	0	0	0	0	0	0	0	0
61	0	0	0	0	0	0	0	0	0	0	0	0	0
67	0	0	0	0	0	0	0	0	0	0	0	0	0
71	0	0	0	0	0	0	0	0	0	0	0	0	2
73	0	0	0	0	0	0	0	0	0	0	0	0	0
79	0	0	0	0	0	0	0	0	0	0	0	0	0
83	0	0	0	0	0	0	0	0	0	0	0	0	0
89	0	0	0	0	0	0	0	0	0	0	0	0	0
97	0	0	0	0	0	0	0	0	0	0	0	0	0
101	0	0	0	0	0	0	0	0	0	0	0	0	0
103	0	0	0	0	0	0	0	0	2	0	0	0	0
107	0	0	0	0	0	0	0	0	0	0	0	0	0
109	0	0	0	0	0	0	0	0	0	0	0	0	0
113	0	0	0	0	0	0	0	0	0	0	0	0	0
127	0	0	0	0	0	0	0	0	0	0	0	0	0
131	0	0	0	0	0	0	0	0	0	0	0	0	0
137	0	0	0	0	0	0	0	0	0	0	0	0	0
139	0	0	0	0	0	0	0	0	0	0	0	0	0
149	0	0	0	0	0	0	0	0	0	0	0	0	0
151	0	0	0	0	0	0	0	0	0	0	0	0	0
157	0	0	0	0	0	0	0	0	0	0	0	0	0
163	0	0	0	0	0	0	0	0	0	0	0	0	0
167	0	0	0	0	0	0	0	0	0	0	0	0	0
173	0	0	0	0	0	0	0	0	0	0	0	0	0
179	0	0	0	0	0	0	0	0	0	0	0	0	0
181	0	0	0	0	0	0	0	0	0	0	0	0	0
191	0	0	0	0	0	0	0	0	0	0	0	0	0
193	0	0	0	0	0	0	0	0	0	0	0	0	0
197	0	0	0	0	0	0	0	0	0	0	0	0	0
199	0	0	0	0	0	0	0	0	0	0	0	0	0

TABLE 1. $\overline{\rho} : G_{\mathbb{Q}(\sqrt{-2})}$ of odd Serre weight $p \leq k+1$ not coming from modular representations over $\mathbb{Q}$

Prime p \ Serre weight k	29	31	33	35	37	39	41	43	45	47	49	51	53
29	0												
31	0	0											
37	0	0	0	2	0								
41	0	0	0	0	0	0	0						
43	0	0	0	0	0	0	0	0					
47	0	0	0	0	0	0	0	0	0	0			
53	0	0	0	0	0	0	0	0	0	0	2	0	0
59	0	0	0	0	0	0	0	0	0	0	0	0	0
61	0	0	0	0	0	0	0	0	0	0	0	0	0
67	0	0	0	0	0	0	0	0	0	0	0	0	0
71	0	0	0	0	6	0	0	0	0	0	0	0	0
73	0	0	0	0	0	0	0	0	0	0	0	0	0
79	0	0	0	0	0	0	0	0	0	0	0	0	0
83	0	0	0	0	0	0	0	0	0	0	0	0	0
89	0	0	0	0	0	0	0	0	0	0	0	0	0
97	0	0	0	0	0	0	0	0	0	0	0	0	0
101	0	0	0	0	0	0	0	0	0	0	0	0	0
103	0	0	0	2	0	0	0	0	0	0	0	0	0
107	0	0	0	0	0	0	0	0	0	0	0	0	0
109	0	0	0	0	0	0	0	0	0	0	0	0	0
113	0	2	0	0	0	0	0	0	0	0	0	0	0
127	0	0	0	0	0	0	0	0	0	0	0	0	0
131	0	0	0	0	0	0	0	0	0	0	0	0	0
137	0	0	0	0	0	0	0	0	0	0	0	0	0
139	0	0	0	0	0	0	0	0	0	0	0	0	0
149	0	0	0	0	0	0	0	0	0	0	0	0	0
151	0	0	0	0	0	0	0	0	0	0	0	0	0
157	0	0	0	0	0	0	0	0	0	0	0	0	0
163	0	0	0	0	0	0	0	0	0	0	0	0	0
167	0	0	0	0	0	0	0	0	0	0	0	0	0
173	0	0	0	0	0	0	0	0	0	0	0	0	0
179	0	0	0	0	0	0	0	0	0	0	0	0	0
181	0	0	0	0	0	0	0	0	0	0	0	0	0
191	0	0	0	0	0	0	0	0	0	0	0	0	0
193	0	0	0	0	0	0	0	0	0	0	0	0	0
197	0	0	0	0	0	0	0	0	0	0	0	0	0
199	0	0	0	0	0	0	0	0	0	0	0	0	0

TABLE 2. $\overline{\rho} : G_{\mathbb{Q}(\sqrt{-2})}$ of odd Serre weight $p \leq k+1$ not coming from modular representations over $\mathbb{Q}$

	Serre weight k												
	29	31	33	35	37	39	41	43	45	47	49	51	53
211	0	0	0	0	0	0	0	0	0	0	0	0	0
223	0	0	0	0	0	2	0	0	0	0	0	0	0
227	0	0	0	0	0	0	0	0	0	0	0	0	0
229	0	0	0	0	0	0	0	0	0	0	0	0	0
233	0	0	0	0	0	0	0	0	0	0	0	0	0
239	0	0	0	0	0	0	0	0	0	0	0	0	0
241	0	0	0	0	0	0	0	0	0	0	0	0	0
251	0	0	0	0	0	0	0	0	0	0	0	0	0
257	0	0	0	0	0	0	0	0	0	0	0	0	0
263	0	0	0	0	0	0	0	0	0	0	0	0	0
269	0	0	0	0	0	0	0	0	0	0	0	0	0
271	0	0	0	0	0	0	0	0	0	0	0	0	0
277	0	0	0	0	0	0	0	0	0	0	0	0	0
281	0	0	0	0	0	0	0	0	0	0	0	0	0
283	0	0	0	0	0	0	0	0	0	0	0	0	0
293	0	0	0	0	0	0	0	0	0	0	0	0	0
307	0	0	0	0	0	0	0	0	0	0	0	0	0
311	0	0	0	0	0	0	0	0	0	0	0	0	0
313	0	0	0	0	0	0	0	0	0	0	0	0	0
317	0	0	0	0	0	0	0	0	0	0	0	0	0
331	0	0	0	0	0	0	0	0	0	0	0	0	0
337	0	0	0	0	0	0	0	0	0	0	0	0	0
347	0	0	0	0	0	0	0	0	0	0	0	0	0
349	0	0	0	0	0	0	0	0	0	0	0	0	0
353	0	0	0	0	0	0	0	0	0	0	0		
⋱													
523	0	0	0	0	0	0	0	2	0	0	0		
⋱													
599	0	0	2	0	0	0	0	0	0	0	0		
⋱													
643	0	0	0	0	0	0	0	0	0	0	2		
⋱													
701	0	0	0	0	0	0	2	0	0	0	0		
⋱													
743	0	0	0	0	0	0	0	0	0	2	0		
⋱													
983	0	0	0	0	0	0	0	0	0	0	0		

TABLE 3. $\overline{\rho} : G_{\mathbb{Q}(\sqrt{-2})}$ of odd Serre weight $p \leq k+1$ not coming from modular representations over $\mathbb{Q}$

Prime p \ Serre weight k	55	57	59	61	63	65	67	69	71	73	75	77	79
59	0	0	0										
61	0	0	0	0									
67	0	0	0	0	0	0	0						
71	0	0	0	0	0	0	0	0	0				
73	0	0	0	0	0	0	0	0	0	0			
79	0	0	0	0	0	0	0	0					
83	0	0	2	0	0	0							
89	0	0	0	0	0	0							
97	0	0	0	0	0	2	0						
101	0	0	0	0	0	0	0						
103	0	0	0	0	0	0							
107	0	0	0	0									
109	0	0	0	0									
113	0	0	0	0									
127	0												
131	0	0	0	0									
137	0												
139	0												
149	0												
151	0	0	0	0									
157	0	0	0	0									
163	2	0	0	0									
167	0												
173	0												
179	0	0	0	0									
181	0	0	0										
191	0	0	0										
193	0	0	0	0									
197	0	0	0										
199	0												

TABLE 4. $\overline{\rho} : G_{\mathbb{Q}(\sqrt{-2})}$ of odd Serre weight $p \leq k+1$ not coming from modular representations over $\mathbb{Q}$

Mahler measures and q-series

Anton Mellit

In the paper [1] the following (conjectural) identity was mentioned:

$$(*) \qquad m(x+\frac{1}{x}+y+\frac{1}{y}-\sqrt{-4}) \doteq L'_{E/\mathbb{Q}}(0).$$

Here E is the elliptic curve defined by equation

$$x-\frac{1}{x}+y-\frac{1}{y}=2$$

and m denotes the Mahler measure, for $P \in \mathbb{C}[x,y]$

$$m(P)=(2\pi i)^{-2}\int_{|x|=|y|=1}\log|P(x,y)|\frac{dx}{x}\frac{dy}{y}.$$

The elliptic curve E has conductor 40 and there is a corresponding modular form on $\Gamma_0(40)$

$$f(q)=q+q^5-4q^7-3q^9+4q^{11}-2q^{13}+2q^{17}+4q^{19}+\cdots,$$

whose L-function is the L-function of E. There is a corresponding modular parametrization $\pi : X_0(40) \to E$. The variables x and y can be viewed as functions on E and $\{x,y\}$ is an element of $K_2(\mathbf{C}(E))$, whose regulator is $m(P)$ (see [2]).

By a theorem of Beilinson, if an algebraic curve has modular parametrization and g_1, g_2 are functions on the curve which are also modular units, then the regulator of $\{g_1,g_2\}$ can be expressed in terms of L-functions of modular forms. However, in our case, x and y are not modular units with respect to π.

I was trying to find a different modular parametrization of E by looking at different congruence subgroups which are "close" to $\Gamma_0(40)$, for which x and y are modular units. If such a parametrization exists, then the identity $(*)$ is proved by Beilinson's theorem. However, this analysis of different groups, whether they parametrize E or not and whether x and y become modular units was quite difficult. Then I discovered a "trick" which simplifies this task a lot. This is what I am going to present.

Looking on the problem from a different angle, we just need to find two q-series $x(q)$ and $y(q)$ which satisfy the following conditions:

(1) $x(q)-\frac{1}{x(q)}+y(q)-\frac{1}{y(q)}=2$,
(2) $\frac{y(q)}{x(q)(y(q)^2+1)}q\frac{d}{dq}y(q)=kf(q)$,
(3) $x(q)$ and $y(q)$ are modular units for some congruence subgroup.

The second condition must be satisfied for some $k \in \mathbb{Q}$ and is coming from the fact that the pullback of the holomorphic differential form from E must be proportional to $f(q)\frac{dq}{q}$.

We can see now that for fixed k equations (1) and (2) have a unique solution $(x_k(q),\, y_k(q))$ such that x_k and y_k both have a simple pole at $q=0$, and, say the residue of x is positive. Condition (3) can be easily checked in practice simply by

looking at the coefficients of the q-expansions: they must be small integer numbers. In fact, in our example we quickly find that for $k = 1$

$$x_1(q) = q^{-1} + 1 - q^2 - q^3 + q^5 + q^8 + q^9 + q^{10} - 2q^{12} - q^{13} + \cdots,$$
$$y_1(q) = -q^{-1} + 1 - q^2 + q^3 - q^5 + q^8 - q^9 + q^{10} - 2q^{12} + q^{13} + \cdots.$$

After a little more work we can identify x_1 and y_1 in terms of "known" modular forms. Put

$$\lambda(q) = q^{\frac{1}{5}} \prod_{n=1}^{\infty} \frac{(1-q^{5n-1})(1-q^{5n-4})}{(1-q^{5n-2})(1-q^{5n-3})},$$

which is a modular unit on $\Gamma(5)$. Then we can easily see that

$$x_1(q) := \frac{\lambda(q^4)}{\lambda(q)\lambda(q^8)},$$
$$y_1(q) := -\frac{\lambda(q)\lambda(q^2)}{\lambda(q^8)},$$

Beilinson's theorem applies in this case, and (*) can be proved.

References

[1] Harada, S., *Hasse-Weil zeta function of absolutely irreducible SL_2-representations of the figure 8 knot group*, Proc. Amer. Math. Soc. **139** (2011), 3115–3125.

[2] Villegas, F.Rodriguez, *Modular Mahler measures. I* Topics in number theory (University Park, PA, 1997), 17–48, Math. Appl., 467, Kluwer Acad. Publ., Dordrecht, 1999.

Monogenic cubic fields and elliptic curves

Manjul Bhargava
(joint work with Arul Shankar)

We determine the mean number of 2-torsion elements in the class groups of *monogenic* maximal cubic orders. We similarly determine the mean number of 2-torsion elements in the class groups of maximal cubic orders having a monogenic subring of bounded index. Surprisingly, we find that these mean values are different! This demonstrates that, on average, the monogenicity of a ring has a direct altering effect on the behavior of the class group.

We make use of the above results to prove that the average rank of elliptic curves, when ordered by their heights, is bounded. In particular, we prove that when elliptic curves are ordered by height, the mean size of the 2-Selmer group is 3.

The above results are obtained via a determination of the asymptotic number of binary quartic forms having bounded invariants; this extends, to the quartic case, the classical results of Gauss [8] and Davenport [5] in the quadratic and cubic cases, respectively. Using some natural extensions of correspondences of Birch and Swinnerton-Dyer [3] and of Wood [10], we are then able to deduce the above-mentioned results on monogenic cubic fields and 2-Selmer groups of elliptic curves.

Our techniques in the above determinations are quite general, and may be applied to counting integer orbits in other representations of algebraic groups. As further examples of the application of these methods, we similarly count integral orbits having bounded invariants in the spaces of (a) ternary cubic forms, (b) pairs of quaternary quadratic forms, and (c) quintuples of quinary alternating 2-forms. By combining the resulting asymptotic counting theorems with the correspondences of Cremona, Fisher, and Stoll [4] and Fisher [7], we are then able to obtain also the mean sizes of the 3-, 4-, and 5-Selmer groups of elliptic curves; these mean sizes are found to be 4, 7, and 6 respecitvely.

Finally, by studying root numbers in relation to the above results, and then applying the recent results of Dokchitser–Dokchitser [6] and of Skinner–Urban [9], we are able to deduce that a positive proportion of elliptic curves have rank 0 and also analytic rank 0. In particular, a positive proportion of elliptic curves satisfy the BSD rank conjecture.

References

[1] M. Bhargava and A. Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, `arXiv:1006.1002v2`.

[2] M. Bhargava and A. Shankar, *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank* 0, `arXiv:1007.0052v1`.

[3] B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves I*, J. Reine Angew. Math. **212** 1963 7–25.

[4] J. Cremona, T. Fisher, and M. Stoll, *Minimisation and reduction of* 2*-,* 3*- and* 4*-coverings of elliptic curves*, Journal of Algebra Number Theory **4** (2010), no. 6, 763–820.

[5] H. Davenport, *On the class-number of binary cubic forms I and II*, J. London Math. Soc. **26** (1951), 183–198.

[6] T. Dokchitser and V. Dokchitser, *On the Birch–Swinnerton-Dyer quotients modulo squares*, preprint.

[7] T. Fisher, *The invariants of a genus one curve*, Proc. Lond. Math. Soc. (3) **97** (2008), 753–782.

[8] C. F. Gauss, *Disquisitiones Arithmeticae*, 1801.

[9] C. Skinner and E. Urban, *The Iwasawa main conjectures for* GL_2, preprint.

[10] M. Wood, Moduli spaces for rings and ideals, Ph.D. Thesis, Princeton University, June 2009.

How many conjugacy classes does one need to tell a finite group apart from its subgroups?

Emmanuel Kowalski

(joint work with David Zywina)

Suppose one is given a finite Galois extension $K/\mathbf{Q}$, and one is told of an injective homomorphism $i : \mathrm{Gal}(K/\mathbf{Q}) \to G$ for some fixed finite group G. For some reason, one suspects (or hopes) that i is in fact an isomorphism. The question is: how can one check that this is indeed the case?

Example. The following general motivating example is considered in joint papers with F. Jouve and D. Zywina [1, 2]. Consider a split semisimple algebraic group $\mathbf{G}/\mathbf{Q}$, with a faithful $\mathbf{Q}$-representation $\mathbf{G} \to \mathrm{GL}_m$ for some $m \geq 1$. For

a (regular semisimple) element $g \in \mathbf{G}(\mathbf{Q})$, let $K_g/\mathbf{Q}$ be the splitting field of the characteristic polynomial $\det(T - \rho(g)) \in \mathbf{Q}[T]$. One can construct an embedding of $\mathrm{Gal}(K_g/\mathbf{Q})$ into the Weyl group $W(\mathbf{G})$ of $\mathbf{G}$, and one can prove that, in some natural sense, this Galois group is exactly the Weyl group for "most" elements g.

One method to answer the general question above is based on the following facts: (1) for any prime p which is unramified in K, the Frobenius at p, say Fr_p, gives a *conjugacy class* in the Galois group, and hence (via i) in G; (2) moreover, all conjugacy classes which intersect the image of i appear for some p (by the Chebotarev density theorem); (3) a result of Jordan states that, for any finite group G, no *proper* subgroup H intersects every conjugacy class of G.

Thus, if we enumerate the successive Frobenius conjugacy classes, and we "see" at some point that no proper subgroup $H \subset G$ is compatible with those, we can conclude that i is surjective. Conversely, if i is surjective, we know that this algorithm will terminate.

Example. In [1], this is applied to a specific $K/\mathbf{Q}$ with $G = W(E_8)$, the Weyl group of the exceptional algebraic group E_8 (constructed as in the previous example). It is found that the first two unramified Frobenius classes Fr_7 and Fr_{11} are enough to show that the Galois group is $W(E_8)$.

We then ask: in general, how many conjugacy classes should one expect to require before reaching the conclusion (when i is indeed surjective)? Since each conjugacy class $c \in G^\sharp$ appears as a Frobenius with proportion roughly $|c|/|G|$ when we enumerate primes in order, it is natural to use the following probabilistic model to get a rough insight into this question.

Consider the space Ω of sequences $\boldsymbol{g} = (g_k)_{k \geq 1}$ with $g_k \in G$ for all k, with the probability Haar measure μ on Ω. With respect to this measure, the components g_k are independent and uniformly distributed on G. Define a "waiting time"

$$\tau(\boldsymbol{g}) = \min\{k \geq 1 \mid (g_1^\sharp, \ldots, g_k^\sharp) \text{ generate} G\} \in [0, +\infty]$$

were $g^\sharp$ is the conjugacy class of an element g, and we say that a tuple of conjugacy classes generates G if, for *any* choice of elements $h_k \in g_k^\sharp$, the tuple $(h_1, \ldots, h_k)$ generates G.

The *Chebotarev invariant* $c(G)$ is defined to be

$$c(G) = \int_\Omega \tau(\boldsymbol{g}) d\mu(\boldsymbol{g}),$$

and the secondary invariant is the second moment

$$c_2(G) = \int_\Omega \tau(\boldsymbol{g})^2 d\mu(\boldsymbol{g}).$$

Here are some results concerning the properties of these invariants of finite groups:

– One can write an "explicit" formula, which is useful for numerical experiments for groups with few conjugacy classes of maximal subgroups: we have

$$c(G) = \sum_{\substack{I \subset \max(G) \\ I \neq \emptyset}} \frac{(-1)^{|I|+1}}{1 - \nu(\mathcal{H}_I^\sharp)},$$

and

$$c_2(G) = \sum_{\substack{I \subset \max(G) \\ I \neq \emptyset}} \frac{(-1)^{|I|}}{1 - \nu(\mathcal{H}_I^\sharp)} \Big(1 - \frac{2}{1 - \nu(\mathcal{H}_I^\sharp)}\Big),$$

where $\max(G)$ is the set of conjugacy classes of maximal subgroups of G, $\mathcal{H}_I^\sharp$ is – for $I \subset \max(G)$ – the set of conjugacy classes in G which intersect *every* $H \in I$, and for any set A of conjugacy classes, $\nu(A) = \sum_{c \in A} |c|/|G|$. These formulas are obtained by inclusion-exclusion type methods.

– Using such formulas, one shows for instance that if $G_n = \mathbf{Z}/n\mathbf{Z}$ is a finite cyclic group, we have

$$c(G_n) \leq \limsup_{k \to +\infty} c(G_k) = 2 + \sum_{j \geq 2} (1 - \zeta(j)^{-1}),$$

and is therefore bounded. This is of some interest because a "naive" upper-bound for $c(G_n)$ would be

$$c(G_n) \leq \sum_{p|n} \frac{1}{p},$$

which can be of size $\log\log\log n$ for certain integers n, and in particular is not bounded.

– Similarly, using delicate results of Luczak and Pyber, one can show that $c(\mathfrak{S}_n)$ and $c_2(\mathfrak{S}_n)$ are bounded for $n \geq 1$.

– A "worse-type" behavior is given by the solvable groups

$$H_q = \Big\{ \begin{pmatrix} a & t \\ 0 & 1 \end{pmatrix} \mid a \in \mathbf{F}_q^\times, \quad t \in \mathbf{F}_q \Big\},$$

for which $c(H_q) \sim q \sim \sqrt{|H_q|}$, $c_2(H_q) \sim q(2q-1)$, as $q \to +\infty$. Indeed, Kantor, Lubotzky and Shalev [3] have shown, using sophisticated results concerning finite groups, that one has

$$c(G) \ll \sqrt{|G|}\sqrt{\log|G|},$$

for any finite group G.

– Numerical data could be obtained for a number of interesting (close to simple) finite groups. For instance, for the Weyl group of E_8, of order 696729600, one has

$$c(W(E_8)) = 4.194248\ldots, \qquad c_2(W(E_8)) = 20.79438\ldots,$$

and for the Rubik's Cube group, of order 43252003274489856000, we obtain

$$c(G) = 5.668645\ldots, \qquad c_2(G) = 36.78701\ldots.$$

These computations were performed using the MAGMA software [5].

More results, examples and remarks can be found in the paper [4] (the arXiv version of which is more complete than the soon-to-appear published one).

References

[1] F. Jouve, E. Kowalski and D. Zywina, *An explicit integral polynomial whose splitting field has Galois group $W(E_8)$*, J. Th. Nombres Bordeaux 20 (2008), 761–782.

[2] F. Jouve, E. Kowalski and D. Zywina, *Splitting fields of characteristic polynomials of random elements in arithmetic groups*, to appear in Israel J. of Math.

[3] W.M. Kantor, A. Lubotzky and A. Shalev: *Invariable generation and the Chebotarev invariant of a finite group*, preprint (2010).

[4] E. Kowalski and D. Zywina, *The Chebotarev invariant of a finite group*, to appear in Experimental Math.; `arXiv:1008.4909`.

[5] W. Bosma, J. Cannon and C. Playoust: *The Magma algebra system, I. The user language* J. Symbolic Comput., 24 (1997), 235–265; also `http://magma.maths.usyd.edu.au/magma/`

On the integral cohomology of Bianchi groups

Mehmet Haluk Şengün

Bianchi groups are groups of the form $\mathrm{SL}_2(\mathcal{O})$ where $\mathcal{O}$ is the ring of integers of an imaginary quadratic field K. They arise naturally in the study of hyperbolic 3-manifolds and of certain generalizations of the classical modular forms (called Bianchi modular forms) for which they assume the role of the classical modular group $\mathrm{SL}_2(\mathbb{Z})$.

Let Γ be a congruence subgroup of a Bianchi group G. Let $\mathbb{E}$ be a Γ-invariant lattice in a finite dimensional irreducible complex representation of the real Lie group $\mathrm{SL}_2(\mathbb{C})$. It is known since the first computations of Fritz Grunewald in 1981 that first homology of Γ with coefficients in $\mathbb{E}$ can have torsion that cannot be explained by the torsion elements of Γ. In fact, recent computations in [2] show that the prime divisors of the size of torsion are very sporadic and can get to astronomical sizes. Nevertheless, computations in [2], following recent work of Bergeron and Venkatesh [1], strongly suggest the following conjecture is true.

Conjecture Let G be a Bianchi group. Let $\mathbb{H}$ denote the hyperbolic 3-space. Then

$$\lim_{N\mathfrak{p}\to\infty} \frac{\log |H_1(\Gamma_0(\mathfrak{p}),\mathbb{Z})_{tor}|}{\mathrm{vol}(\Gamma_0(\mathfrak{p})\backslash\mathbb{H})} = \frac{1}{6\pi}$$

where the limit is taken over prime ideals $\mathfrak{p}$ of residue degree one.

From the perspective of Langlands' Programme, it is interesting to understand connections of these torsion classes and 2-dimensional mod p Galois representations. The following explicit example may be an instance of a bigger phenomenon.

The polynomial $x^8 - x^7 - 44x^6 + 43x^5 + 442x^4 - 32x^3 - 1311x^2 - 1156x - 241$ has Galois group $\hat{A}_4$, which has an embedding into $\mathrm{GL}_2(\mathbb{Z}[\zeta_3])$. The arising Artin

representation of $G_{\mathbb{Q}}$ has conductor 163^2 and it is even. We reduce the image mod 163 and then resrict it to $G_{\mathbb{Q}(i)}$ to get

$$\rho_K : G_{\mathbb{Q}(i)} \to \mathrm{GL}_2(\mathbb{F}_{163})$$

with trivial conductor. We compute the cohomology spaces $H^2(\mathrm{GL}_2(\mathbb{Z}[i]), \mathbb{E}(\mathbb{F}_{163}))$ and find a matching eigenvalue system Ψ for the weights

$$\mathbb{E}^{27,27}_{53,53}(\mathbb{F}_{163}) \text{ and } \mathbb{E}^{135,135}_{107,107}(\mathbb{F}_{163}).$$

Further considerations show that the eigenvalue system Ψ is not the reduction of an eigenvalue system that is captured in the complex cohomology with the same level and weight. This means that there is a 163-torsion class that is responsible for Ψ.

References

[1] N. Bergeron, A. Venkatesh. *The asymptotic growth of torsion homology for arithmetic groups.* 2010. preprint.

[2] M.H. Sengun. *On the integral cohomology of Bianchi groups.* Experimental Mathematics, 2011. to appear.

[3] M.H. Sengun. *On the torsion homology of non-arithmetic hyperbolic tetrahedral groups.* International Journal of Number Theory, 2011. to appear.

Some aspects of the Sato-Tate conjecture

Jean-Pierre Serre

The Sato-Tate conjecture is concerned with the distribution of the number of solutions mod p of a given system of equations, when p varies. The lecture was meant as an introduction to the next two, by K. Kedlaya and D. Kohel. We shall concentrate on the general aspects of the conjecture; for more details, the reader is referred to [3, Chap.8].

Using Hironaka's resolution of singularities, together with Grothendieck and Deligne's results on ℓ-adic cohomology, the question can be reduced to the following.

Let $X^i, i \in I$, be a finite family of smooth projective varieties over $\mathbf{Q}$ [1]. For each $i \in I$, let n_i be a positive integer. Choose a finite set S of primes such that the X^i have good reduction outside S; for every $p \notin S$, let us denote by $t_i(p)$ the trace of the geometric Frobenius at p, acting on the n_i-th cohomology of $X^i_{\overline{\mathbf{Q}}}$. If B^i denotes the Betti number $\dim H^{n_i}(X^i_{\overline{\mathbf{Q}}})$, Deligne's theorem shows that $f^i(p) = t_i(p)/p^{i/2}$ belongs to the interval $T^i = [-B^i, +B^i]$. If we denote by T the box $\prod_i T^i$, we then have a map

$$f : P - S \to T,$$

where P is the set of all prime numbers.

[1] Instead of $\mathbf{Q}$ one could take any finitely generated extension of $\mathbf{Q}$, for instance any number field.

The general Sato-Tate conjecture (see e.g. [2, §13]) predicts that the $f(p)$ are *equidistributed* with respect to a positive Radon measure μ on the space T. This means that, for every continuous function φ on T, we have

(*) $\quad \int_T \varphi(t)\mu(t) = \lim_{x\to\infty} \frac{1}{\pi_S(x)} \sum_{p\leqslant x} \varphi(f(p))$,

where $\pi_S(x) \sim x/\log x$ is the number of $p \in P - S$ with $p \leqslant x$. Equivalently, μ is the limit, for the weak topology, of the mean values of the Dirac measures at the points $f(p)$, for $p \leqslant x$ and $p \in P - S$. This can also be translated in terms of subsets of T, as follows : if $A \subset T$, define $N_A(x)$ as the number of $p \in P - S$ such that $f(p) \in A$ and $p \leqslant x$; assume that A is μ-quarrable, i.e. that its boundary has μ-measure 0; then

$$\lim_{x\to\infty} N_A(x)/\pi_S(x) \;=\; \mu(A).$$

The measure μ has some remarkable properties, for instance:

– It is invariant by the automorphism $(t_i) \mapsto ((-1)^{n_i} t_i)$ of T.

– If $\varphi : T \to \mathbf{R}$ is a polynomial in the t_i with coefficients in $\mathbf{Z}$, then $\int_T \varphi(t)\mu(t)$ belongs to $\mathbf{Z}$.

These properties are direct consequences of a (conjectural - but well motivated, see [2]) construction of μ in terms of compact Lie groups and characters. More precisely, there should exist a compact real Lie group K (the *Sato-Tate group*), together with:

(i) for every $p \in P - S$, an element s_p of the set Cl K of conjugacy classes of K;

(ii) for every $i \in I$ a continuous linear representation $\rho^i : K \to \mathbf{GL}_{B^i}(\mathbf{C})$.

These data should fulfill several conditions, the most important ones being:

(a) The s_p are equidistributed in Cl K with respect to the image of the normalized Haar measure of K.

(b) Tr $\rho^i(s_p) = t_i(p)$ for every $i \in I$ and every $p \in P - S$.

Conditions (a) and (b) imply the equidistribution stated at the beginning; more precisely, they show that the measure μ on T is the image of the Haar measure of K by the map $K \to T$ defined by the characters of the ρ^i.

The original Sato-Tate case ([4], [1]) is the one where I has one element, the corresponding X^i being an elliptic curve without complex multiplication and the integer n_i being chosen equal to 1, so that $B^i = 2$. In that case, the group K is $\mathbf{SU}_2(\mathbf{C})$, the space T is the interval $[-2, +2]$ and the data (i) and (ii) are defined in an obvious way. Property (b) is true by construction. The real problem is the equidistribution property (a), which was proved only recently (over $\mathbf{Q}$, and more generally over every totally real number field); see the references in [3, §8.1.5].

References

[1] D. Mumford, *Families of abelian varieties*, Algebraic Groups and Discontinuous Subgroups, AMS Proc. Symp. Pure Math. IX (1966), 347-351.

[2] J-P. Serre, *Propriétés conjecturales des groupes de Galois motiviques et des représentations ℓ-adiques*, Motives, AMS Proc. Symp. Pure Math. 55 (1994), vol.I, 377-400 (= Coll. Papers, vol. IV, №161).

[3] J-P. Serre, *Lectures on $N_X(p)$*, A.K. Peters (2011).

[4] J. Tate, *Algebraic cycles and poles of zeta functions*, Arithmetic Algebraic Geometry (Proc. Conf. Purdue Univ., 1963), Harper & Row, New York (1965), 93-110.

Sato-Tate and notions of generality

David Kohel

1. Point counting on special curves

This work was originally motivated by the need to understand the properties of RM curves with a view towards cryptography. For example, in the family considered by Tautz, Top, and Verberkmoes [3]: $\mathcal{C} : y^2 = x^5 - 5x^3 + 5x + t$, over $\mathbb{A}^1_{\mathbb{Z}} = \mathrm{Spec}(\mathbb{Z}[t])$, the fibers have Jacobians with real multiplication (RM) by the order $\mathbb{Z}[(1+\sqrt{5})/2]$. Moreover, the endomorphism $\phi = (1+\sqrt{5})/2$ is explicitly computable (K. & Smith), and with Gaudry and Smith we developed:

Theorem 1 (Gaudry, K. & Smith)**.** *There exists an algorithm for the point counting problem in a family of genus 2 curves with efficiently computable RM of class number 1, whose complexity is in* $\widetilde{O}((\log q)^5)$.

Consequently, we can compute zeta functions as efficiently as for elliptic curves (and even better — unconditionally), but can we in good faith recommend the use of such curves for cryptographic applications? With this view, we may ask:

Q1: In what way is an RM family special?

Q2: How special is the (one-dimensional) family of Tautz, Top, and Verberkmoes inside of the (two-dimensional) moduli space of genus 2 curves with RM by the order $\mathbb{Z}[(1+\sqrt{5})/2]$?

Motivation: Serre's talk [2] at AGCT in Luminy, 2011, explaining and motivating work of Kedlaya and Sutherland [1] for higher dimensional Sato–Tate conjectures (particularly $g = 2$).

2. Notions of generality

We consider the question: "What is special about special curves?". Here we distinguish certain geometric and arithmetic properties.

Geometric speciality. If $\mathcal{C} \to S$ is a family (of genus g curves), what is the induced image $S \to \mathcal{X}$ in the moduli space (in $\mathcal{M}_g$)?

Arithmetic speciality. Here we distinguish the (local) level structure and the (global or geometric) Galois distributions.

a. What level structure is fixed by the family? — Is there an exceptional N such that the Galois representation $\bar{\rho}_N : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_{2g}(\mathbb{Z}/N\mathbb{Z})$ is smaller than expected?

b. What is the image of the Galois action on the Tate module?

$$\rho_\ell : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T_\ell(J)) \cong \mathrm{GL}_{2g}(\mathbb{Z}_\ell).$$

The geometric and first arithmetic property can be easily characterized, so we investigate the latter arithmetic property in the context of the generalized Sato–Tate conjectures.

3. Sato–Tate in higher dimension

Let $C/\mathbb{F}_q$ be a curve and $\chi(T)$ its Frobenius characteristic polynomial and define the unit Frobenius characteristic polynomial by

$$\widetilde{\chi}(T) = \chi(\sqrt{q}\,T)/q^g = T^{2g} - s_1 T^{2g-1} + \cdots - s_1 T + 1 = \prod_{j=1}^{g} (T^2 - t_j T + 1).$$

We let s_i denote the symmetric sums in $\{t_j = (\alpha_j + \bar{\alpha}_j)/\sqrt{q}\}$, where α_j are the roots of $\chi(T)$; for $g = 2$ we have: $\widetilde{\chi}(T) = T^4 - s_1 T^3 + (s_2 + 2)T^2 - s_1 T + 1$.

The generalized Sato–Tate conjectures concern the distribution of each s_i for a curve over $\mathrm{Spec}(\mathbb{Z})$, as the prime q (of reduction) varies. Conjecturally the distribution is determined by the Haar measure (induced on conjugacy classes) on a compact subgroup H of USp_{2g}, with connected component H_0 of the identity.

Here we focus on the distribution μ_0 associated to the principal coset H_0 (a vast simplification), and the case $g = 2$ (see the work of Kedlaya & Sutherland [1] for the general senario). In general each conjugacy class C_i of cosets in the finite group H/H_0 contributes a distribution μ_i. We moreover simplify (experimentally and theoretically) by averaging over fibers over a base scheme, as in the example of the above family of curves $\mathcal{C}$ over $\mathrm{Spec}(\mathbb{Z}[t])$.

4. The principal Sato–Tate distributions

Among genus 2 curves with non-split Jacobians, the behaviors of a generic, RM and CM family of curves are distinguished. Restricting to the principal coset, the (expected, conjectural) 2-dimensional distributions in (s_1, s_2) are (up to a constant):

$$\textbf{Generic}: \quad \sqrt{(s_1^2 - 4s_2)(4 - s_1 + s_2)(4 + s_1 + s_2)}\, ds_1 ds_2,$$

$$\textbf{RM}: \quad \frac{\sqrt{(4 - s_1 + s_2)(4 + s_1 + s_2)}\, ds_1 ds_2}{\sqrt{(s_1^2 - 4s_2)}},$$

$$\textbf{CM}: \quad \frac{ds_1 ds_2}{\sqrt{(s_1^2 - 4s_2)(4 - s_1 + s_2)(4 + s_1 + s_2)}},$$

where the real and relative discriminants of $\widetilde{\chi}(T) = T^4 - s_1 T^3 + (s_2 + 2)T^2 - s_1 T + 1$ are $D_+ = s_1^2 - 4s_2$ and $D_- = (4 - s_1 + s_2)(4 + s_1 + s_2)$, which explains these expressions in the distributions. For each case experimental evidence (selecting random curves in a family) agrees well with these expected distributions.

References

[1] K. S. Kedlaya, A. V. Sutherland, *Hyperelliptic curves, L-polynomials, and random matrices*, `http://arxiv.org/abs/0803.4462`, 2010.

[2] J.-P. Serre, *What does the Sato-Tate conjecture mean?*, talk at *Arithmetic, Geometry and Coding Theory*, Luminy, 14–18 March 2011.
[3] W. Tautz, J. Top, and A. Verberkmoes, *Explicit hyperelliptic curves with real multiplication and permutation polynomials*, *Canad. J. Math.* 43 (1991) no. 5, 1055–1064.

Towards a precise Sato-Tate conjecture in genus 2

Kiran S. Kedlaya
(joint work with Grzegorz Banaszak, Francesc Fité, Victor Rotger, Andrew V. Sutherland)

Let A be an abelian variety of dimension g over a number field k. For each prime ideal $\mathfrak{p}$ of k at which A has good reduction, there is a polynomial $L_{\mathfrak{p}}(T) \in \mathbb{Z}[T]$ which occurs as the characteristic polynomial of Frobenius on the ℓ-adic Tate module of A for all primes ℓ. Moreover, the roots of this polynomial in $\mathbb{C}$ all have absolute value $q^{1/2}$ for q the absolute norm of $\mathfrak{p}$; we may thus renormalize by defining $\overline{L}_{\mathfrak{p}}(T) = L_{\mathfrak{p}}(q^{1/2}T)$, to obtain a polynomial over $\mathbb{R}$ whose roots all lie on the unit circle. The *Sato-Tate problem* is to determine the limiting distribution of the $\overline{L}_{\mathfrak{p}}$ for a fixed A as $\mathfrak{p}$ varies. (As usual, only prime ideals of absolute degree 1 contribute measurably to this question.)

The following recipe is suggested by Serre [8, Chapter 8]. Choose a prime ℓ, and let G_ℓ be the image of the Galois representation $G_k \to \mathrm{GSp}_{2g}(\mathbb{Q}_\ell)$ coming from the Tate module. Let $G_{\ell,1}$ be the subgroup of G_ℓ acting trivially on the one-dimensional subspace of $\wedge^2 \mathbb{Q}_\ell^{2g}$ generated by the Weil pairing. Define the *algebraic Sato-Tate group* $\mathrm{AST}_\ell(A)$ to be the Zariski closure of $G_{\ell,1}$ in GSp_{2g}. (This construction bears some resemblance to that of the Mumford-Tate group; more on this below.)

Conjecture 1 (Algebraic Sato-Tate conjecture)**.** *The group* $\mathrm{AST}_\ell(A)$ *is the base extension to* $\mathbb{Q}_\ell$ *of an algebraic subgroup* $\mathrm{AST}(A)$ *of* GSp_{2g} *defined over* $\mathbb{Q}$*, the conjugacy class of which is independent of* ℓ*.*

Now base-extend $\mathrm{AST}_\ell(A)$ along some embedding $\mathbb{Q}_\ell \to \mathbb{C}$; under Conjecture 1, the resulting group does not depend on ℓ up to conjugacy, so we will drop the subscript ℓ. Take a maximal compact subgroup to obtain the *Sato-Tate group* $\mathrm{ST}(A) \subseteq \mathrm{USp}(2g)$.

Conjecture 2 (Numerical Sato-Tate conjecture)**.** *The* $\overline{L}_{\mathfrak{p}}(T)$ *are equidistributed for the image on* $\mathbb{R}[T]$ *of the Haar measure on* $\mathrm{ST}(A)$ *under the characteristic polynomial map.*

This can be deduced from analyticity of symmetric power L-functions, as described in [7, §I.A.2].

Conjecture 2 is a classical result when A is an elliptic curve with complex multiplication, in which case $\mathrm{ST}(A)$ is either $\mathrm{SO}(2)$ (when the complex multiplication is defined over k) or the normalizer of $\mathrm{SO}(2)$ in $\mathrm{USp}(2) = \mathrm{SU}(2)$ (when it's not).

Note that the latter is not connected! This has to do with the fact that half of the primes are of supersingular reduction, and for these the trace of Frobenius is 0.

When A is an elliptic curve without complex multiplication, we have $\mathrm{ST}(A) = \mathrm{SU}(2)$. When k is totally real (and perhaps in some other cases), this case follows from new results of Taylor et al. on modularity of symmetric powers of Galois representations of GL_2-type; see for instance [3].

For $g > 1$, one generically has $\mathrm{ST}(A) = \mathrm{SU}(2g)$, in which case it seems hopeless to prove Conjecture 2. However, one can expect to prove Conjecture 2 in many exceptional cases, which raises the question of classifying these exceptions. There are more than you might expect!

1. Sato-Tate and Mumford-Tate

Despite the fact that Conjecture 2 seems intractable for any given $g > 1$, there is still room for both theoretical and empirical analysis of the situation. Let's start with a bit of the former.

Recall that the *Mumford-Tate conjecture* relates the identity component of the Zariski closure of G_ℓ with a corresponding group defined in terms of Hodge structures (the *Mumford-Tate group*). In cases when the Mumford-Tate conjecture holds, the identity component of $\mathrm{AST}_\ell(A)$ (which is stable under extension of k) is independent of ℓ. This conjecture is made difficult by the fact that the Mumford-Tate group of A is not determined in general by the $\overline{k}$-endomorphism algebra of A, as shown by Mumford's examples in dimension 4 [6].

However, if one restricts to cases where the endomorphism algebra is "large enough" compared to g (including all cases with $g \leq 3$), then one can prove the Mumford-Tate conjecture by showing that both the Mumford-Tate group and the identity component of the Zariski closure of G_ℓ are determined entirely by the constraints imposed by the presence of the endomorphisms. See for instance [1].

In such cases, one can also establish Conjecture 1 by identifying a candidate group in terms of endomorphisms and then establishing an open image property. One also obtains an identification of the component group of $\mathrm{AST}(A)$ with the Galois group of the minimal extension of k over which all endomorphisms of A are defined. The idea here is to relax the constraint imposed by endomorphisms: rather than looking for elements of $\mathrm{GSp}(2g)$ which commute with endomorphisms, we allow elements which act on endomorphisms like an element of Galois. (This is joint work in progress with Grzegorz Banaszak.)

2. Dimension 2

Let us now consider the case $g = 2$ in detail. In joint work with Francesc Fité, Victor Rotger, and Andrew Sutherland (also in progress), we have described the possible Sato-Tate groups in dimension 2.

Theorem 3. *Under Conjectures 1 and 2, there are exactly* 52 *possible groups that occur up to conjugacy as the Sate-Tate groups of abelian surfaces over number fields. Of these,* 34 *occur for abelian surfaces over* $\mathbb{Q}$.

A first approximation to this result is obtained by extracting some necessary conditions on the group $\mathrm{ST}(A)$ from its definition, and then classifying the subgroups of $\mathrm{USp}(4)$ satisfying these conditions. This is an easy exercise in group theory, but sadly it gives slightly too many groups (55 rather than 52). To get the exact list, we must relate these groups to the possibilities for the action of Galois on the endomorphism algebra; we call the latter data the *Galois type* of (A, k).

For each of the 52 possible Sato-Tate groups, we exhibit examples of Jacobians of genus 2 hyperelliptic curves for which we can numerically verify the predicted equidistribution to high numerical accuracy. See `http://math.mit.edu/~drew/` for animations illustrating some of these distributions. This calculation builds on our earlier work with Sutherland [4, 5]. It should be noted that on one hand, the theoretical classification was made much easier by the numerical evidence pointing towards the correct answer; on the other hand, however, finishing the theoretical classification led to a number of new cases missed in [4, 5]! For instance, the Sato-Tate group of the Jacobian of the curve

$$y^2 = x^6 - 5x^4 + 10x^3 - 5x^2 + 2x - 1$$

has connected component $\mathrm{SO}(2)$ and component group $S_4 \times C_2$ of order 48.

3. Next steps

It would be natural to make a corresponding analysis in dimension 3, but the results will surely be much more complicated. For instance, the number of possibilities for the connected part of the Sato-Tate group grows from 6 in dimension 2 to 15 in dimension 3. The example of dimension 2 suggests that the most cases will occur for connected part $\mathrm{SO}(2)$. This case will require analysis over the list of finite subgroups of $\mathrm{SU}(3)$.

One might also try making enough of an analysis of dimension 4 to identify the Sato-Tate distribution associated to Mumford's exceptional fourfolds. This would provide a good computational method for looking for explicit examples of such fourfolds defined over number fields.

References

[1] G. Banaszak, W. Gajda, and P. Krasoń, On the image of ℓ-adic Galois representations for abelian varieties of type I and II, *Doc. Math.* extra volume (2006), 35–75.

[2] G. Banaszak, W. Gajda, and P. Krasoń, On the image of Galois ℓ-adic representations for abelian varieties of type III, *Tohoku Math. J.* **62** (2010), 163–189.

[3] T. Barnet-Lamb, D. Geraghty, and T. Gee, *The Sato-Tate conjecture for Hilbert modular forms*, J. Amer. Math. Soc. **24** (2011), 411–469.

[4] K. Kedlaya, A. Sutherland, *Computing L-series of hyperelliptic curves*, Algorithmic Number Theory Symposium-ANTS VIII, Lecture Notes in Computer Science 5011, 312-326, 2008.

[5] K. Kedlaya, A. Sutherland, *Hyperelliptic curves, L-polynomials, and random matrices*, volume 487, 119-162, 2009.

[6] D. Mumford, A note on Shimura's paper "Discontinuous subgroups and abelian varieties", *Math. Ann.* **181**, 345-351, 1969.

[7] J.-P. Serre, *Abelian ℓ-adic representations and elliptic curves*, W.A. Benjamin Inc., 1968.

[8] J.-P. Serre, Lectures on $N_X(p)$, A.K. Peters, to appear (2011).

An exceptional isomorphism between modular curves of level 13

Burcu Baran

For a positive integer n, let $X(n)$ be the modular curve over $\mathbb{Q}$ with full level n structure. Let $\mathrm{C}_{ns}^{+}(n)$ be the normalizer of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. The corresponding modular curve $X_{\mathrm{ns}}(n)$, defined as the quotient $X(n)/\mathrm{C}_{\mathrm{ns}}^{+}(n)$, is geometrically connected over $\mathbb{Q}$. A detailed discussion of these curves is in [2].

The modular curve $X_{\mathrm{ns}}(n)$ is useful for two interesting problems. For suitably chosen n, the determination of all integral points of the non-cuspidal locus of $X_{\mathrm{ns}}(n)$ gives new solutions to the class number one problem which was solved by Baker-Heegner-Stark [1, 5, 8]. Secondly, the rational points of $X_{\mathrm{ns}}(n)$ are related to Serre's uniformity problem over $\mathbb{Q}$. This problem grew out of:

Theorem (Serre [7]). *If an elliptic curve E over $\mathbb{Q}$ does not have complex multiplication then there exists a constant $C_E > 0$ such that for every prime $p > C_E$, the mod-p Galois representation $\rho_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ is surjective.*

Serre asked if C_E can be chosen independently of E. He predicted an affirmative answer:

Serre's uniformity problem over $\mathbb{Q}$. *There is a constant $C > 0$ so that if E is an elliptic curve over $\mathbb{Q}$ without complex multiplication then $\rho_{E,p}$ is surjective for all $p > C$.*

This problem is partially solved. If $\rho_{E,p}$ is not surjective, then one of the following has to hold:

(1) The image of $\rho_{E,p}$ is contained in one of a finite list of "exceptional" subgroups;
(2) The image of $\rho_{E,p}$ is contained in a Borel subgroup;
(3) The image of $\rho_{E,p}$ is contained in the normalizer of a split Cartan subgroup;
(4) The image of $\rho_{E,p}$ is contained in the normalizer of a non-split Cartan subgroup.

Serre [7] showed that case 1 can only happen for prime $p \leq 13$ and $p \neq 7$. In [6], Mazur proves that case 2 can only occur for $p \leq 37$. A few years ago, in [3] Bilu and Parent proved that there exists a constant c so that for non-CM elliptic curves, case 3 cannot occur for $p > c$. In fact, recently Bilu, Parent, and Rebolledo [4] have shown that case 3 cannot happen for $p \geq 11$ with $p \neq 13$. The remaining and most difficult part is to exclude the possibilty that $\rho_{E,p}$ has image contained in the normalizer $\mathrm{C}_{\mathrm{ns}}^{+}(p)$ of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ for "large" p. More precisely: as the curve $X_{\mathrm{ns}}(n)$ has no $\mathbb{Q}$-rational cusps when $n > 2$, does there exist a constant c such that for every prime number $p > c$, the only $\mathbb{Q}$-points of the modular curve $X_{\mathrm{ns}}(p)$ over $\mathbb{Q}$ are CM points?

For the curves $X_{\mathrm{ns}}(n)$ that have genus ≤ 2, there has been extensive work (see [2] for a detailed discussion). There exists only one curve $X_{\mathrm{ns}}(n)$ with genus 3 and it is the one with $n = 13$. In this talk, I will briefly explain how we obtained an equation over $\mathbb{Q}$ for this curve as a plane quartic in $\mathbb{P}^2_{\mathbb{Q}}$. Finding an equation for

the modular curves $X_{\rm ns}(n)$ is difficult, as they never have a $\mathbb{Q}$-rational cusp for $n > 2$. We use a new method resting on representation theory to overcome these difficulties. In the talk we will also explain why the equation

$$(1)\ \ (-y-z)x^3+(2y^2+zy)x^2+(-y^3+zy^2-2z^2y+z^3)x+(2z^2y^2-3z^3y)=0$$

that defines the curve $X_{\rm ns}(13)$ also defines the modular curve $X_{\rm s}(13)$ associated to the normalizer of a split Cartan subgroup of level 13. Hence, these two modular curves are isomorphic over $\mathbb{Q}$! This surprising isomorphism does not have a "modular" explanation. For instance, $X_{\rm s}(13)(\mathbb{Q})$ contains a cusp but $X_{\rm ns}(13)(\mathbb{Q})$ does not.

For $|x| < 1000$, $|y| < 1000$ and $|z| < 1000$ we searched for rational points and found seven rational points. We explicitly computed the j-line map $X_{\rm ns}(13) \to X(1)$ of degree 78 and the j-line map $X_{\rm s}(13) \to X(1)$ of degree 91. We evaluated these at the known $\mathbb{Q}$-rational points. We obtained that on $X_{\rm s}(13)$ six of the known rational points correspond to elliptic curves with CM by imaginary quadratic orders in which 13 is split and the other rational point corresponds to the unique $\mathbb{Q}$-rational cusp. We also obtained that on $X_{\rm ns}(13)$ all of the known rational points correspond to elliptic curves with CM by an imaginary quadratic order in which 13 is inert. Table 1 gives the known rational points on equation (1), the corresponding discriminants and cusp on $X_{\rm s}(13)$ and on $X_{\rm ns}(13)$. This data supports Serre's uniformity conjecture.

Table 1. Imaginary quadratic discriminants associated to the known rational points on $X_{\rm s}(13)$ and on $X_{\rm ns}(13)$.

(x,y,z) on (1)	$(0,0,1)$	$(0,1,0)$	$(0,3,2)$	$(1,0,-1)$	$(1,0,0)$	$(1,0,1)$	$(1,1,0)$
on $X_{\rm s}(13)$	-27	-12	-3	-16	-43	-4	cusp
on $X_{\rm ns}(13)$	-67	-11	-163	-7	-8	-28	-19

References

[1] Baker, A. *A remark on the class number of quadratic fields*, Bull. London Math Soc. **1** (1969), 98–102.

[2] Baran, B. *Normalizers of non-split Cartan subgroups, modular curves and the class number one problem*, Journal of Number Theory **130** issue 12 (2010), 2753–2772.

[3] Bilu, Y. and Parent, P. *Serre's uniformity conjecture in the split Cartan case*, Annals of Math, to appear.

[4] Bilu, Y., Parent, P. and Rebolledo, M. *Rational points on $X_0^+(p^r)$*, preprint.

[5] Heegner, K. *Diophantische Analysis und Modulfunktionen*, Math. Zeit. **59** (1952), 227–253.

[6] Mazur, B. *Rational isogenies of prime degree*, Inv. Math. **44** (1978), 129–162.

[7] Serre, J-P. *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Inv. Math. **15** (1972), 259–331.

[8] Stark, H.M. *On complex quadratic fields with class number equal to one*, Trans. Amer. Math. Soc. **122** (1966), 112–119.

$\mathcal{B}_4$

Herbert Gangl

Zagier's Conjecture on polylogarithms relates algebraic K-groups $K_{2n-1}(F)$ for a number field F to higher analogues of the well-known Bloch group $\mathcal{B}(F) = \mathcal{B}_2(F)$, a subquotient of $\mathbb{Z}[F]$. More precisely, the latter group $\mathcal{B}(F)$ is defined as the quotient of

$$\ker\left(\partial_2^F : \mathbb{Z}[F] \to \bigwedge^2 F^\times\right),$$

where ∂_2^F is defined on generators via $[x] \mapsto x\wedge(1-x)$ (for $x = 0, 1$ we put $\partial_2^F([x]) = 0$), by a subgroup of "universal elements" in that kernel, which essentially amounts to expressions resulting from (specialisations of) the most prominent functional equation of the dilogarithm, the famous five-term relation.
The group $\mathcal{B}(F)$ is known (via pioneering work by Bloch, completed by Suslin) to be finitely generated and isomorphic, up to tensoring with $\mathbb{Q}$, to $K_3(F)$, whose rank was determined by Borel as $r_2(F)$=number of pairs of complex embeddings of F. Moreover, there is an isomorphism relating the Borel regulator map in weight 2 for $K_3(F)$ to the Bloch-Wigner dilogarithm applied to $\mathcal{B}(F)$ and, as a consequence, relates the special value $\zeta_F(2)$ of the Dedekind zeta function at the point 2 to a determinant of dilogarithm sums with arguments in F.

Zagier [2] provided a set-up which gives a similar conjectural construction for higher K-groups $K_{2n-1}(F)$, by experimentally guessing the analogous map ∂_n^F and defining "higher Bloch groups" $\mathcal{B}_n(F)$ as subquotients of $\mathbb{Z}[F]$, which in a first approximation can be described as $\ker\partial_n^F$ divided by the subgroup of "universal elements" in that kernel (there are further—somewhat technical—inductive conditions which are needed for the correct definition). Those universal elements should correspond to functional equations of the n-logarithm function, but for $n \geq 3$ it is not known what functional equations would be sufficient to render that quotient $\mathcal{B}_n(F)$ rationally isomorphic to $K_{2n-1}(F)$. In fact, for $n > 7$ no non-trivial functional equations for the n-logarithm are known. Combining the above conjectural set-up with Borel's work, this entails as a corollary that $\zeta_F(n)$ should be expressed as a determinant of n-logarithms with arguments in F. This corollary is also often referred to as Zagier's Conjecture.

In his proof of (the corollary of) Zagier's Conjecture for $n = 3$, Goncharov [1] exhibited a new functional equation with 22 terms (plus a constant term) which is generally believed to play such a "generating" role for the definition of $\mathcal{B}_3(F)$ (in fact, the equation arises from his ingenious handling of the geometry of configurations of 6 points in $\mathbf{P}^2(\mathbb{C})$ and, following an idea of Zagier, he gave a symmetrized version of it with 840 terms), but for $n > 3$ no such candidate has been known.

In his approach to prove Zagier's Conjecture also for higher n, Goncharov developed an impressive conjectural picture, which in particular for $n = 4$ reduces the corresponding corollary above to two rather elementary conjectural combinatorial statements (concerning the existence of certain elements or maps).

One of these two conjectures concerns Goncharov's ("motivic") complex given by

$$(1)\quad G_4(F) \xrightarrow{\partial_4^{(4)}} B_3(F)\otimes F^\times \oplus B_2(F)\wedge B_2(F) \xrightarrow{\partial_4^{(3)}} B_2(F)\otimes \bigwedge^2 F^\times \xrightarrow{\partial_4^{(2)}} \bigwedge^4 F^\times .$$

Here the (much larger) groups $B_n(F)$ are given by the same relations as $\mathcal{B}_n(F)$, but with *all* generators of $\mathbb{Z}[F]$ rather than just (certain) elements in $\ker \partial_n^F$, and $G_4(F)$ is a group which is yet larger than $B_4(F)$.

Goncharov conjectured that this complex should be quasi-isomorphic to a subcomplex

$$B_4(F) \xrightarrow{\partial_4^{(4)}} B_3(F)\otimes F^\times \xrightarrow{\partial_4^{(3)}} B_2(F)\otimes \bigwedge^2 F^\times \xrightarrow{\partial_4^{(2)}} \bigwedge^4 F^\times .$$

where $\mathcal{B}_2(F)\wedge\mathcal{B}_2(F)$ has been taken out of the picture, and the group $G_4(F)$ has been replaced by (a subgroup) $B_4(F)$.

The first elementary conjecture mentioned above now introduces a certain distinguished element $\kappa(x,z)\in \mathcal{B}_3(F)\otimes F^\times \ \oplus\ \mathcal{B}_2(F)\wedge\mathcal{B}_2(F)$, whose second component, i.e. the part lying in $\mathcal{B}_2(F)\wedge\mathcal{B}_2(F)$, is a generator, say $\{x\}_2\wedge\{z\}_2$ (the notation $\{x\}_2$ simply referring to the image of the generator $[x]\in\mathbb{Z}[F]$ under the projection along the universal relations for the dilogarithm).

As the five term relation $\xi(x,y)$ lies in $\ker\partial_2^F$, the "coboundary" $\partial_4^{(3)}\big(\kappa(\xi(x,y),z)\big)$ vanishes, where $\kappa(\cdot,\cdot)$ is linearly extended in both arguments. The cohomology groups of (1) should be certain K-groups which for number fields vanish in degree ≥ 2 (i.e. except possibly in the first slot of (1)), hence Goncharov was led to the

Conjecture. (Goncharov, ∼1991, cf. also [1])
There exists a combination $S_4(x,y;z)\in\mathbb{Z}[F]$ with image $\kappa(\xi(x,y),z)$ under $\partial_4^{(4)}$.

As a corollary, Goncharov already deduced from the existence of $S_4(x,y;z)$ the existence of a functional equation for the 4-logarithm in 4 variables which should play the role of a generator of the relations in the "correct" definition of $\mathcal{B}_4(F)$.

Our result is the following: after replacing $\kappa(x,z)$ by an equivalent element $\eta(x,z)$ (with the *same second component*) arising from the iterated integral $I_{3,1}(x,z)$ (this had previously been suggested by Nicusor Dan and turned out to be more convenient for our experiments, for which we used Mathematica and Pari), we find

Theorem. *There exists a combination $\widetilde{S}_4(x,y;z)\in\mathbb{Z}[F]$ with at most 122 terms whose image under $\partial_4^{(4)}$ coincides with $\eta(\xi(x,y),z)$.*

Corollary. *There exists a functional equation in four variables for the 4-logarithm with 931 terms which gives a candidate relation for the definition of $\mathcal{B}_4(F)$.*

References

[1] A.B. Goncharov, *Polylogarithms and motivic Galois groups*, Proceedings of the AMS Research Summer Conference on Motives, Symposia in Pure Mathematics **55** (1994), 43–96.

[2] D.B. Zagier, *Polylogarithms, Dedekind zeta functions and the algebraic K-theory of a field*, Arithmetical Algebraic Geometry (Texel 1989), Progress in Mathematics **89**, Birkhäuser (1991), 391–430.

On Hilbert modular threefolds of discriminant 49

Paul E. Gunnells
(joint work with Lev Borisov)

Let F be the totally real cubic field of discriminant 49, let $\mathcal{O}$ be its ring of integers, and let $\mathfrak{p} \subset \mathcal{O}$ be the prime over 7. Let $\Gamma(\mathfrak{p}) \subset \Gamma = SL_2(\mathcal{O})$ be the principal congruence subgroup of level $\mathfrak{p}$. Then our talk presented results about the geometry of the Hilbert modular threefold $X^\circ = \Gamma(\mathfrak{p})\backslash\mathfrak{H} \times \mathfrak{H} \times \mathfrak{H}$ and some related varieties. Our work is in the spirit of van der Geer and Zagier's study [6] of Hilbert modular surfaces over $\mathbb{Q}(\sqrt{13})$, and uses many of the same techniques: toroidal compactifications, the Shimizu trace formula [4], the action of the finite group $\Gamma/\Gamma(\mathfrak{p})$, and explicit construction of some modular forms of level $\mathfrak{p}$. We used [2, 5] for many computations. We discussed the following results:

(1) Let X be the minimal compactification of X°, and let X_{ch} be the singular toroidal compactification built using the fans determined by taking the cones on the faces of the convex hulls of the totally positive lattice points in the cusp data. Then X_{ch} is the canonical model of X.

(2) We construct parallel weight 1 Eisenstein series F_0, F_1, F_2, F_4 and a parallel weight 2 Eisenstein series E_2 that generate the ring of symmetric Hilbert modular forms of level $\mathfrak{p}$ and parallel weight (i.e., the subring of the parallel weight Hilbert modular forms invariant under the action of the Galois group $G = G(F/\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$). This uses work of Yang [7], who clarified and generalized constructions of Hecke [3].

(3) There is a weighted homogeneous polynomial P of degree 8 with 42 terms such that $P(F_0, F_1, F_2, F_4, E_2) = 0$. This polynomial generates the ideal of relations on the F_i and E_2, and the symmetric Hilbert modular threefold $X_{Gal} = X/G$ is the hypersurface cut out by $P = 0$ in the weighted projective space $\mathbb{P}(1, 1, 1, 1, 2)$.

(4) Let Q be the polynomial obtained from P by setting the weight 2 variable to zero. Then Q has 24 terms and defines a degree 8 hypersurface in $\mathbb{P}^3$ with singular locus being 84 quotient singularities of type A_2.

For details we refer to [1].

References

[1] L. Borisov and P. E. Gunnells, *On Hilbert modular threefolds of discriminant* 49, preprint 2011.

[2] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993).

[3] E. Hecke, *Analytische Funktionen und algebraische Zahlen, zweiter Teil*, Abh. Math. Sem. Hamburg Univ. **3** (1924), 213–236.

[4] H. Shimizu, *On discontinuous groups acting on a product of upper half planes*, Ann. of Math. **77** (1963), 33–71.

[5] The PARI Group, Bordeaux, *PARI/GP*, 2005.

[6] G. van der Geer and D. Zagier, *The Hilbert modular group for the field* $\mathbb{Q}$, Inv. Math. **42** (1977), 93–133.

[7] T. Yang, *CM number fields and modular forms*, Pure Appl. Math. Q. **1** (2005), no. 2, 305–340.

Secondary terms in the counting function of cubic fields

Arul Shankar
(joint work with Manjul Bhargava and Jacob Tsimerman)

The classical theorem of Davenport and Heilbronn [7] provides an asymptotic formula for the number of cubic fields having bounded discriminant. Specifically, the theorem states:

Theorem 1 (Davenport–Heilbronn)**.** *Let $N_3(\xi,\eta)$ denote the number of cubic fields K, up to isomorphism, that satisfy $\xi < \mathrm{Disc}(K) < \eta$. Then*

$$\begin{aligned} N_3(0,X) &= \frac{1}{12\zeta(3)}X + o(X), \\ N_3(-X,0) &= \frac{1}{4\zeta(3)}X + o(X). \end{aligned} \tag{1}$$

Subsequent to this result, extensive computations were undertaken to numerically verify the Davenport–Heilbronn theorem (see, e.g., Llorente–Quer [11] and Fung–Williams [9]). These computations agreed quite poorly with the result, leading to questions about the size of the error term in the theorem, and the problem of determining a precise second main term.

Belabas [2] developed a method to enumerate cubic fields very quickly, allowing him to make tables of cubic fields up to absolute discriminant 10^{11}. Using these latter computations in conjunction with certain theoretical considerations, Roberts [12] conjectured a precise *second main term* in the Davenport–Heilbronn theorem. This conjectural second main term took the form of a certain explicit constant times $X^{5/6}$. More precisely, Roberts conjectured that

Conjecture 2 (Roberts [12])**.** *Let $N_3(\xi,\eta)$ denote the number of cubic fields K, up to isomorphism, that satisfy $\xi < \mathrm{Disc}(K) < \eta$. Then*

(2)

$$\begin{aligned} N_3(0,X) &= \frac{1}{12\zeta(3)}X + \frac{4\zeta(1/3)}{5\Gamma(2/3)^3\zeta(5/3)}X^{5/6} + O_\epsilon(X^{5/6-1/48+\epsilon}), \\ N_3(-X,0) &= \frac{1}{4\zeta(3)}X + \frac{\sqrt{3}\cdot 4\zeta(1/3)}{5\Gamma(2/3)^3\zeta(5/3)}X^{5/6} + O_\epsilon(X^{5/6-1/48+\epsilon}). \end{aligned}$$

In this talk, we discuss our proof of the Roberts conjecture using methods very similar to those that were used in Davenport's and Heilbronn's original proof of their theorem. The Roberts conjecture has also been proven independently (see [15]) by Taniguchi and Thorne using very different methods.

As our techniques are related to those in the original paper of Davenport and Heilbronn, we start with a sketch of their proof. There are essentially three steps in the proof of the Davenport–Heilbronn theorem:

- The Delone–Faddeev correspondence (see [8]) yields a bijection between isomorphism classes of cubic rings and $\mathrm{GL}_2(\mathbb{Z})$-orbits on integral binary cubic forms. Davenport and Heilbronn determined conditions on the coefficients of the integral binary cubic forms in a $\mathrm{GL}_2(\mathbb{Z})$-orbit to ensure that such an orbit corresponds to a maximal order in a cubic field. These conditions are given by infinitely many congruence conditions (conditions modulo p^2, for every prime p) on the coefficients of the integral binary cubic forms.
- The second step is to count the number of all $\mathrm{GL}_2(\mathbb{Z})$-orbits on irreducible integral binary cubic forms having bounded discriminant. This is accomplished by counting integer points, having bounded discriminant, in a fundamental domain for the action of $\mathrm{GL}_2(\mathbb{Z})$ on the space of all binary cubic forms having real coefficients.
- Finally, a simple sieve is used to count those $\mathrm{GL}_2(\mathbb{Z})$-orbits on integral binary cubic forms that correspond to maximal orders in cubic fields.

Our proof of the Roberts conjecture involves a number of new ideas and refinements both on the algebraic and the analytic side. We obtain the main term of the asymptotics of the number of $\mathrm{GL}_2(\mathbb{Z})$-orbits on irreducible integral binary cubic forms having bounded discriminant by counting points not in a single fundamental domain, but on average in a continuum of fundamental domains, using a technique of [3]. This leads directly to stronger error terms. We immediately obtain an error term of $O(X^{5/6})$ for the number of $\mathrm{GL}_2(\mathbb{Z})$-orbits on integral binary cubic forms having discriminant less than X, improving on Davenport's original $O(X^{15/16})$. The $O(X^{5/6})$ term is seen to come from the "cusps" of the fundamental regions.

Then, in order to count points more efficiently in the cusps of these fundamental regions, we "slice" the regions along the x^3-coefficient of the binary cubic forms. This allows us to obtain a precise second main term in the counting function of $\mathrm{GL}_2(\mathbb{Z})$-orbits on integral binary cubic forms having bounded discriminant. This technique works equally well when counting integral binary cubic forms satisfying any finite set of congruence conditions.

Finally, we use a refined sieve that allows us to preserve the second main terms when certain sets of infinitely many congruence conditions are imposed on the coefficients of binary cubic forms thus concluding the proof the the Roberts conjecture.

References

[1] K. Belabas, M. Bhargava, and C. Pomerance, Error terms for the Davenport-Heilbronn theorems, *Duke Math. J.* **153** (2010), 173-210.

[2] K. Belabas, A fast algorithm to compute cubic fields, *Math. Comp.* **66** (1997), no. 219, 1213–1237.

[3] M. Bhargava, The density of discriminants of quartic rings and fields, *Annals of Math.* **162** (2005), 1031–1063.

[4] M. Bhargava, A. Shankar, and J. Tsimerman, On the Davenport-Heilbronn theorem and second order terms, preprint.

[5] H. Davenport, On a principle of Lipshitz, *J. London Math. Soc.* **26** (1951), 179–183. Corrigendum: "On a principle of Lipschitz", *J. London Math. Soc.* **39** (1964), 580.
[6] H. Davenport, On the class-number of binary cubic forms I and II, *J. London Math. Soc.* **26** (1951), 183–198.
[7] H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields II, *Proc. Roy. Soc. London Ser. A* **322** (1971), no. 1551, 405–420.
[8] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, AMS Translations of Mathematical Monographs **10**, 1964.
[9] G. W. Fung and H. C. Williams, On the computation of a table of complex cubic fields with discriminant $D > -10^6$, *Math. Comp.* **55** (1990), no. 191, 313–325.
[10] W.-T. Gan, B. H. Gross, and G. Savin, Fourier coefficients of modular forms on G_2, *Duke Math. J.* **115** (2002), 105–169.
[11] P. Llorente and J. Quer, On totally real cubic fields with discriminant $D < 10^7$, *Math. Comp.* **50** (1988), no. 182, 581–594.
[12] D. P. Roberts, Density of cubic field discriminants, *Math. Comp.* **70** (2001), no. 236, 1699–1705 (electronic).
[13] M. Sato and T. Shintani, On zeta functions associated with prehomogeneous vector spaces, *Annals of Math.* (2) **100** (1974), 131–170.
[14] T. Shintani, On Dirichlet series whose coefficients are class-numbers of integral binary cubic forms, *J. Math. Soc. Japan* **24** (1972), 132–188.
[15] T. Taniguchi and F. Thorne, The secondary term in the counting function for cubic fields, preprint.

Secondary terms in counting functions for cubic fields

Takashi Taniguchi
(joint work with Frank Thorne)

Let $N_3^{\pm}(X)$ be the number of cubic fields K with $0 < \pm\mathrm{Disc}(K) < X$. In this talk, we briefly explain our proof of the following formula:

$$N_3^{\pm}(X) = \frac{C^{\pm}}{12\zeta(3)}X + K^{\pm}\frac{4\zeta(1/3)}{5\Gamma(2/3)^3\zeta(5/3)}X^{5/6} + O(X^{7/9+\epsilon}),$$

where $C^+ = K^+ = 1$ and $C^- = 3, K^- = \sqrt{3}$.

The primary term of this formula is due to Davenport and Heilbronn. Two independent proofs of this secondary term are recently given. One proof is due to Bhargava, Shankar and Tsimerman [2] in terms of geometry-of-numbers. Our another proof [5] is based on analytic properties of *Shintani zeta function*, which we recall the definition below.

Let $G = \mathrm{GL}_2$, and $V = \mathrm{Sym}^3\mathrm{Aff}^2$ be the space of binary cubic forms. The Delone-Faddeev correspondence asserts that there is a canonical discriminant preserving bijection between the set of cubic rings and the set of integer orbits $G(\mathbb{Z})\backslash V(\mathbb{Z})$. On the other side, (G, V) is an example of what is called a *prehomogeneous vector space*, and Sato and Shintani [3] discovered that there are zeta functions naturally associated with such (G, V). For our space of binary

cubic forms, the zeta function is defined by

$$\xi^{\pm}(s) := \sum_{f \in G(\mathbb{Z})\backslash V(\mathbb{Z}), \pm\mathrm{Disc}(f)>0} \frac{|\mathrm{Stab}(f)|^{-1}}{|\mathrm{Disc}(f)|^s}.$$

This was introduced by Shintani [4], and he proved that they are holomorphic except for simple poles at $s = 1, 5/6$ and that they satisfy functional equations of the form $\xi(1-s) = (\Gamma\text{-factors}) \cdot \xi^*(s)$, where $\xi^*(s)$ are zeta functions associated with the dual representation (G, V^*). Using these results, Shintani showed that the number of *all cubic rings* R with $0 < \pm\mathrm{Disc}(R) < X$ are asypmtotically $\alpha^{\pm}X + \beta^{\pm}X^{5/6} + O(X^{3/5+\epsilon})$. Here $\alpha^{\pm} = \mathrm{Res}_{s=1}\xi^{\pm}(s)$ and $\beta^{\pm} = \frac{6}{5}\mathrm{Res}_{s=5/6}\xi^{\pm}(s)$.

To prove the formula for $N_3^{\pm}(X)$, we would like to count only *maximal cubic rings*. Note that the maximality is a local condition. For a squarefree integer q, let $M^{\pm}(q; X)$ be the number of cubic rings R with $0 < \pm\mathrm{Disc}(R) < X$ and R is not maximal at all prime factors of q. Then by inclusion-exclusion, the number of maximal cubic rings $N^{\pm}(X)$ is given by $N^{\pm}(X) = \sum_q \mu(q) M^{\pm}(q; X)$. Here μ is the Möbius function. Note that $N^{\pm}(X)$ is different from $N_3^{\pm}(X)$ since this also counts reducible maximal rings. However reducible maximal cubic rings are easy to count, and hence it is enough to work for $N^{\pm}(X)$.

We choose Q and split the sum above into $q < Q$ and $q \geq Q$. The idea of this sieve is due to Belabas, Bhargava and Pomerance [1], and the latter sum is bounded by $O(X/Q^{2-\epsilon})$. Hence we would like to understand $M(q; X)$ for small q.

Thus we arrive at the following definition: Let $V(\mathbb{Z}) \supset V(\mathbb{Z}; q)$ be the set of binary cubic forms whose corresponding cubic rings are not maximal at all prime factors of q. We denote by $\Phi_q \colon V(\mathbb{Z}) \to \{0, 1\}$ the indicator function of $V(\mathbb{Z}; q)$, and define the q-nonmaximal zeta function by

$$\xi_q^{\pm}(s) := \sum_{f \in G(\mathbb{Z})\backslash V(\mathbb{Z}), \pm\mathrm{Disc}(f)>0} \Phi_q(f) \frac{|\mathrm{Stab}(f)|^{-1}}{|\mathrm{Disc}(f)|^s},$$

which is the Dirichlet series corresponding to the counting function $M^{\pm}(q; X)$. A crucial observation is that $V(\mathbb{Z}; q)$ is definable by congruence conditions modulo q^2. In other words, Φ_q factors through the reduction map $V(\mathbb{Z}) \twoheadrightarrow V(\mathbb{Z}/q^2\mathbb{Z})$. The theory of prehomogeneous vector spaces allows us to study zeta functions of this variation, and the description of the functional equation is reduced to the study of the finite Fourier transform $\widehat{\Phi}_q \colon V^*(\mathbb{Z}/q^2\mathbb{Z}) \to \mathbb{C}$ defined by

$$\widehat{\Phi}_q(b) := q^{-8} \sum_{a \in V(\mathbb{Z}/q^2\mathbb{Z})} \Phi_q(a) \exp\left(\frac{2\pi\sqrt{-1} \cdot [a, b]}{q^2}\right).$$

From the explicit computation of $\widehat{\Phi}_q$, we obtain a good uniform estimate of $M(q; X)$ and thus obtain the desired formula of $N_3^{\pm}(X)$.

We also prove a variety of generalizations. For a quadratic field F, let $\mathrm{Cl}_3(F)$ denote the 3-torsion subgroup of the ideal class group of F. Then we have

$$\sum_{\substack{[F:\mathbb{Q}]=2 \\ 0<\pm\mathrm{Disc}(F)<X}} \#\mathrm{Cl}_3(F) = \frac{3+C^{\pm}}{\pi^2}X + K^{\pm}\frac{8\zeta(1/3)}{5\Gamma(2/3)^3}\prod_p \left(1-\tfrac{p^{1/3}+1}{p(p+1)}\right) X^{\frac{5}{6}} + O(X^{\frac{18}{23}+\epsilon}),$$

where the product in the secondary term is over all primes. It is well known that this problem is equivalent to count nonwhere totally ramified cubic fields, and thus accomplished by a different choice of Φ_q.

We can also count cubic fields in arbitrary arithmetic progressions. In this case, we discover a curious bias in the secondary term. For example, the formula for cubic field discriminants less than X and congruent to $a \pmod 7$ is different for every value of a. This is a reflection of the exotic fact that the twisted Shintani zeta functions by a non-trivial Dirichlet character χ have a pole at $s = 5/6$ if and only if χ is cubic! For details, see [5]. Similar results are obtained for 3-torsions in ideal class groups of quadratic fields.

References

[1] M Belabas, M. Bhargava, and C. Pomerance. Error estimates for the Davenport-Heilbronn theorems. *Duke. Math. J.*, 153:173–210, 2010.

[2] M. Bhargava, A. Shankar, and J. Tsimerman. On the Davenport-Heilbronn theorem and second order terms. preprint 2010, arXiv:1005.0672.

[3] M. Sato and T. Shintani. On zeta functions associated with prehomogeneous vector spaces. *Ann. of Math.*, 100:131–170, 1974.

[4] T. Shintani. On Dirichlet series whose coefficients are class-numbers of integral binary cubic forms. *J. Math. Soc. Japan*, 24:132–188, 1972.

[5] T. Taniguchi and F. Thorne. Secondary terms in counting functions for cubic fields. preprint 2011, arXiv:1102.2914.

An algorithm to compute relative cubic fields

Anna Morra

Given a number field K, a positive integer n and a bound $X > 0$, we define $\mathcal{F}_{K,n}(X)$ to be the set of isomorphism classes of extensions L/K such that

$$[L:K] = n, \quad \text{and} \quad \mathcal{N}_{K/\mathbb{Q}}(\mathfrak{d}(L/K)) \leq X,$$

where $\mathfrak{d}(L/K)$ is the relative discriminant ideal of the extension L/K.

Sets of this type may be enumerated algorithmically (usually over $\mathbb{Q}$) using the geometry of numbers, following Hunter-Martinet's theorem [8]. Asymptotically, their cardinality as X tends to infinity is the subject of folklore conjectures, predicting for instance that it should be of the order of X, strikingly refined by Malle [7] who also fixes the Galois group of the Galois closure of L/K. Small values of n are of particular interest since computer tests become comparatively easier and more theoretical results are available; see [2] for a recent survey.

In this talk we focus on the case $n = 3$, we consider the problem of generalizing Belabas algorithm [1] for enumerating cubic extensions of $\mathbb{Q}$ to other base fields, and we solve it completely when K is imaginary quadratic, with class number 1.

Our main result is the following [9, 10]:

Theorem. *Let K be an imaginary quadratic number field with class number $h_K = 1$. There exists an algorithm which lists all cubic extensions in $\mathcal{F}_{K,3}(X)$ in time $O_\varepsilon(X^{1+\varepsilon})$, for all $\varepsilon > 0$.*

For an arbitrary fixed number field K, Datskovsky and Wright [5, Theorem I.1] proved that the cardinality of $\mathcal{F}_{K,3}(X)$ is asymptotic to a constant (depending on K) times X as $X \to \infty$. It follows:

Corollary. *The algorithm runs in time essentially linear in the size of the output.*

The algorithm uses two main ingredients : a general description of isomorphism classes of cubic extensions L/K as classes of suitable binary quadratic forms in $K[x, y]$ modulo a GL_2 action (using a Theorem by Tanighuchi [12]) and classical reduction theory (see [6, 4, 14]) in the special case where K is imaginary quadratic. Enumerating cubic extensions then amounts to enumerating integer points in an explicit fundamental domain, cut out by the extra condition $\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{d}(L/K)) \leq X$.

It is interesting to compare our algorithm with the classical one, using class field theory (see Section 9.2.3 of [3]): the latter works in time $O_\varepsilon(X^{3/2+\varepsilon})$, unless we assume the Generalized Riemann Hypothesis to obtain $O_\varepsilon(X^{1+\varepsilon})$. So our algorithm has better *unconditional* complexity. Moreover, even assuming GRH, as we did in our PARI/GP [11] implementation, the ray class field algorithm is slower than ours. We present some numerical data in the following table :

X	$N(X)$	t	t'
10^4	276	5 s	16 s
$4 \cdot 10^4$	1339	19 s	1mn 18 s
$9 \cdot 10^4$	3305	56 s	3mn 45 s
10^6	42692	24 mn 1 s	2h 52mn 9 s
$4 \cdot 10^6$	181944	2 h 49 mn	34h 24 mn 8 s
$9 \cdot 10^6$	421559	9 h 37 mn	$>$ 134 h
10^8	4990974	359 h 25 mn	$>$ 2720 h

Here $K = \mathbb{Q}(i)$, X is the bound on $\mathcal{N}\mathfrak{d}(L/K)$, $N(X)$ is the number of cubic extensions over K up to the fixed bound, t is the timing of our algorithm, and t' is the timing of the ray class algorithm (except for the last line, that we computed only with our algorithm). All these computations were done on a Intel Xeon 5160 dual core, 3.0 GHz.

Finally, we also compare our numerical data with asymptotic heuristics [13], coming from Datskovsky-Wright method [5] and Robert's conjecture:

X	$N(X)$ (Morra)	$N(X)$ (Taniguchi-Thorne)
10^4	276	270.2
10^6	42692	42655.6
$9 \cdot 10^6$	421559	421260
10^8	4990974	4990962

The results are strikingly similar.

References

[1] K. Belabas, *A fast algorithm to compute cubic fields*, Math. Comp. **66** (1997), no.219.
[2] K. Belabas, *Parametrisation de structures algabriques et densites de discriminants [d'apr?s Bhargava]*, *Astérisque* **299**, Séminaire Bourbaki. Vol. 2003/2004, 267–299.
[3] H. Cohen, *Advanced Topics in Computational Number Theory*, Graduate Texts in Math. **193**, Springer-Verlag, 2000.
[4] J. Cremona, *Reduction of binary cubic and quartic forms*, London Mathematical Society ISSN 1461–1570, 1999.
[5] B. Datskovsky and D. J. Wright, *Density of discriminants of cubic extensions*, J. reine angew. Math. **386** (1988) 116–138.
[6] G. Julia, *Etude sur les formes binaires non quadratiques à indéterminées réelles ou complexes*, Mémoires de l'Académie des Sciences de l'Institut de France **55** (1917) 1–296.
[7] G. Malle, *On the distribution of Galois groups*, J. Number Theory **92** (2002), 315–329.
[8] G. Malle, *The totally real primitive number fields of discriminant at most* 10^9, Lecture Notes in Comput. Sci., **4076**, Springer, Berlin (2006), 114–123.
[9] A. Morra, *An algorithm to compute relative cubic fields*, preprint, available online at `http://arxiv.org/abs/1103.2901`.
[10] A. Morra, *Comptage asymptotique et algorithmique d'extensions cubiques relatives*, Thèse (in english), Université Bordeaux 1, 2009.
[11] PARI/GP, version `2.5.0`, Bordeaux, 2011, `http://pari.math.u-bordeaux.fr/`.
[12] T. Taniguchi, *Distribution of discriminants of cubic algebras*, preprint 2006, arXiv:math.NT/0606109v1.
[13] T. Taniguchi and F. Thorne, *Secondary terms in counting functions for cubic fields*, preprint 2011, arXiv:math.NT/1102.2914v1.
[14] T. Womack, *Explicit descent on elliptic curves*, PhD Thesis, Nottingham (2003).

7-adic Galois representations and a curve of genus 12

Michael Stoll

(joint work with Ralph Greenberg, Karl Rubin and Alice Silverberg)

Let E be an elliptic curve over $\mathbb{Q}$, and let p be a prime number. Then there is the associated p-adic Galois representation

$$\rho_{E,p} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}_{\mathbb{Z}_p}(T_pE) \cong \mathrm{GL}_2(\mathbb{Z}_p)$$

coming from the action of the Galois group on the p-power torsion points on E. The isomorphism depends on the choice of a basis of the free rank-2 $\mathbb{Z}_p$-module $T_pE = \varprojlim_n E[p^n]$.

As Serre has shown, the homomorphism $\rho_{E,p}$ is usually, but not always, surjective. One situation in which it fails to be surjective is when E has a $\mathbb{Q}$-defined

isogeny $h : E \to E'$ of degree p. In this case, the kernel $E[h] \subset E[p]$ is stabilized by the Galois action, and so the mod-p representation

$$\bar{\rho}_{E,p} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}_{\mathbb{F}_p}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$$

takes the form (with respect to a suitable basis)

$$\bar{\rho}_{E,p} = \begin{pmatrix} \psi & * \\ 0 & \varphi \end{pmatrix}$$

with characters $\psi, \varphi : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_p^\times$ such that ψ gives the action on $E[h]$. The existence of the Weil pairing forces the relation $\psi\varphi = \omega$, where ω is the cyclotomic character.

Now the question arises if or when $\rho_{E,p}$ is 'as surjective as possible', given the constraint coming from the existence of the p-isogeny. 'As surjective as possible' in this case means that the image of $\rho_{E,p}$ contains a Sylow pro-p subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$. We therefore make the following definition.

Definition. An elliptic curve $E/\mathbb{Q}$ is said to be *p-exceptional* if E has a $\mathbb{Q}$-defined isogeny of degree p and the image of $\rho_{E,p}$ does not contain a Sylow pro-p subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$.

One way in which E can be p-exceptional is when E has complex multiplication. So the question is, are there any non-CM p-exceptional curves?

If $p \leq 5$, there are many such curves (for example curves with two independent p-isogenies or with a p^2-isogeny). For $p \geq 7$, Greenberg [1] has shown the following.

(1) If $p \geq 7$ and E is p-exceptional, then $\psi^4 = \omega^2$.
(2) If $p > 7$ and E has a p-isogeny such that $\psi^4 = \omega^2$, then E has CM.

(Note that (2) is false for $p = 7$.) This only leaves the question open for $p = 7$. Our result is as follows.

Theorem. *If $E/\mathbb{Q}$ is a 7-exceptional elliptic curve whose 7-isogeny has character ψ such that $\psi^4 = \omega^2$, then E has CM. In particular, the only 7-exceptional elliptic curves are CM curves.*

Since $\#\mathbb{F}_7^\times = 6$, the condition on ψ implies that $(\psi\omega)^2 = 1$. So up to quadratic twist (which does not affect p-exceptionality or CM), we can assume that $\psi = \omega^{-1}$.

We consider the quotient $\Delta_E/\Delta_{E'}$ of the minimal discriminants of E and the 7-isogenous curve E'. We prove the following.

(1) If E is 7-exceptional, then $\Delta_E/\Delta_{E'} = 7^a w^7$ for integers $a \geq 0$ and w.
(2) If E has a 7-isogeny with character $\psi = \omega^{-1}$, then for some $x \in \mathbb{Q}$,

$$\Delta_E/\Delta_{E'} = \left(7^{\pm 1}\frac{x^3 - 2x^2 - x + 1}{x^3 - x^2 - 2x + 1}\right)^6.$$

The first statement is based on looking at the ramification in $\mathbb{Q}(E[7]) = \mathbb{Q}(E'[7])$. The second statement comes from an explicit form of the universal family over the relevant twist of $X_1(7) \cong \mathbb{P}^1$. Combining these two statements shows that

a 7-exceptional elliptic curve E with a fixed identification of the Galois modules $E[h]$ and $\mu_7^{\otimes(-1)}$ gives rise to a *rational point* on one of the curves

$$C_j : y^7 = 7^j \frac{x^3 - 2x^2 - x + 1}{x^3 - x^2 - 2x + 1}$$

for some $j \in \{0, \pm 1, \pm 2, \pm 3\}$. It is easily verified that $C_j(\mathbb{Q}_7) = \emptyset$ for $j \neq 0$, so it remains to determine the set of rational points on $C = C_0$.

Homogenizing the equation given above with respect to x and y separately, we obtain a model of C as a smooth curve of type $(3, 7)$ in $\mathbb{P}^1 \times \mathbb{P}^1$ with bad reduction only at 7. In particular, C has genus 12. Six rational points $(0, 1)$, $(1, 1)$, $(\infty, 1)$, $(-1, -1)$, $(2, -1)$, $(\frac{1}{2}, -1)$ on C are easily found; they correspond to curves with CM. To show that these are the only rational points, we first determine the rank of the Mordell-Weil group. The special form of the curve allows us to bound the rank by a descent based on [3]. The bound obtained is 6, whereas the known rational points only generate a subgroup of rank 4. A search for higher-degree prime divisors reveals the missing two independent points in the Mordell-Weil group. Using this explicit subgroup of finite index, we can carry out a Chabauty computation at the prime 5, making use of the fact that the known rational points biject onto $C(\mathbb{F}_5)$. The necessary computations (in Magma) took about 16 hours. We find a differential killing the Mordell-Weil group whose reduction mod 5 does not vanish at any of the $\mathbb{F}_5$-points on C; this shows that there is at most one rational point in each residue class, see for example [4]. So we know all the rational points already. Details can be found in [2].

References

[1] R. Greenberg, *The image of Galois representations attached to elliptic curves with an isogeny,* to appear in Amer. J. Math.

[2] R. Greenberg, K. Rubin, A. Silverberg, M. Stoll, *On elliptic curves with an isogeny of degree 7*, Preprint (2011), arXiv:1007.4617v2 [math.NT].

[3] B. Poonen, E.F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line,* J. Reine Angew. Math. **488** (1997), 141–188.

[4] M. Stoll, *Independence of rational points on twists of a given curve,* Compos. Math. **142** (2006), 1201–1214.

Computation of Galois groups over p-adic fields

Jürgen Klüners

(joint work with Christian Greve)

Let $K/\mathbb{Q}_p$ be a p-adic field and $g \in K[x]$ be an irreducible monic polynomial. The goal is to compute its Galois group. The "trivial" approach would be to compute the splitting field which we would like to avoid. One cruical part in the algorithms over number fields [2] is that we have easy access to (approximations of) the roots of the given polynomial, e.g. we can use complex approximations or p-adic approximations for some unramified prime p. In the p-adic case we have no access to the roots (except in the splitting field). Therefore we cannot

express the final result as a permutation group acting on its roots. We present the Galois group by generators with relations. On the other hand there is much more structure for p-adic fields, e.g. the Galois groups are solvable and the Galois group of the maximal pro-p-extension is known.

In case the given extension is at most tame, the Galois group can be easily computed as a group with two generators in probabilistic polynomial time (we need to factor polynomials over finite fields).

For Eisenstein polynomials of p–power degree we introduce the ramification polynom and its corresponding ramification polygon. If this polygon is one-sided, we can easily write down the splitting field and its Galois group. The latter one is a semidirect product, where a group $H \leq \mathrm{GL}_m(p)$ is acting on C_p^m. The group H is the Galois group of a tame subextension of the splitting field of g which can be explicitely computed.

In case the ramification polygon has more than one segment, we can compute in probabilistic polynomial time a tame subextension T of the splitting field of g such that the Galois group of g over T is a p-group. Furthermore we know a tower of subfields of the stem field of g such that each relative step is elementary abelian. In case of two segments the complete Galois group can be computed by the use of the canonical class. These computations are difficult to carry out and will not be practical for more than two segments. More details can be found in the PhD-thesis [1] of Christian Greve.

References

[1] C. Greve, *Galoisgruppen von Eisensteinpolynomen über p-adischen Körpern*, Dissertation Universität Paderborn, 2010.

[2] K. Geißler and J. Klüners, *Galois Group Computation for Rational Polynomials*, J.Symb.Comput. **30** (2000), 675–716.

Artin's conjecture and character sums

Peter Stevenhagen

(joint work with Hendrik Lenstra, Pieter Moree)

We show how the "correction factors" arising in a large number of variants of Artin's primitive root conjecture can be obtained in a simple way, by

- describing the associated Galois groups of radical extensions as subgroups of "generic" automorphism groups
- exploiting the abelian characters "cutting out" these Galois groups to express all density correction factors as character sums.

A Herbrand-Ribet theorem for function fields

Lenny Taelman

Let p be a prime number and $K = \mathbf{Q}(\zeta_p)$ and $Y_p = \operatorname{Spec} O_K$. Let $\omega\colon \operatorname{Gal}(K/\mathbf{Q}) \to \mathbf{F}_p^\times$ be the canonical isomorphism. Consider the $\mathbf{F}_p$-vector space

$$H_p = (\operatorname{Pic} Y) \otimes \mathbf{F}_p.$$

It carries a natural action of $\operatorname{Gal}(K/\mathbf{Q})$ and decomposes in isotypical components

$$H_p = \bigoplus_{n=1}^{p-1} H_p(\omega^n)$$

The *Herbrand-Ribet theorem* states that for all even n such that $1 \leq n < p-1$ one has that $H_p(\omega^{1-n})$ is non-zero if and only if p divides the Bernoulli number B_n. *Vandiver's conjecture* is the statement that $H_p(\omega^{1-n})$ vanishes if n is odd.

In this talk we describe an analogue of this theorem for the polynomial ring $A = \mathbf{F}_q[t]$. Before stating it we note that by the Kummer sequence the vector space H_p above can be described as a flat cohomology group

$$H_p = \mathrm{H}^2(Y_{p,\mathrm{fl}}, \mu_p).$$

In this way, the central role of the group scheme μ_p becomes apparent: on the one hand the *base* Y is defined in terms of the splitting field of μ_p, on the other hand we are taking cohomology with *coefficients* in μ_p. In our analogy, both occurrences of μ_p will be replaced with the $\mathfrak{p}$-torsion scheme of the Carlitz module, for some nonzero prime ideal $\mathfrak{p} \subset A$.

The *Carlitz module* is a certain A-module scheme C over $\operatorname{Spec} A$. From the point of view of explicit class field theory it is an analogue of the multiplicative group $\mathbf{G}_m$, in the sense that (many) abelian extensions of $\mathbf{F}_q(t)$ are constructed by adjoining torsion points of C. Its formal definition is as follows: the underlying group scheme of C is just $\mathbf{G}_a$, and the endomorphism t maps a section x to $tx + x^q$. For more details and background see [1].

Let $\mathfrak{p} \subset A$ be a nonzero prime ideal and now let K be the extension of $\mathbf{F}_q(t)$ obtained by adjoining the $\mathfrak{p}$-torsion of the *Carlitz module*. Then K is an Abelian extension of $\mathbf{F}_q(t)$, unramified outside $\mathfrak{p}$ and ∞, and there is a natural isomorphism $\omega\colon \operatorname{Gal}(K/\mathbf{F}_q(t)) \to (A/\mathfrak{p})^\times$. Let $Y_\mathfrak{p}$ be the spectrum of the integral closure of A in K.

Consider the flat cohomology group with compact support

$$H_\mathfrak{p} = \mathrm{H}^2_c(Y_{\mathfrak{p},\mathrm{fl}}, C[\mathfrak{p}]),$$

where $C[\mathfrak{p}]$ is the finite flat $\mathfrak{p}$-torsion scheme of C. This is a vector space over $A/\mathfrak{p}$ with a natural action of $\operatorname{Gal}(K/\mathbf{F}_q(t))$ and hence decomposes as

$$H_\mathfrak{p} = \bigoplus_{n=1}^{q^d-1} H_\mathfrak{p}(\omega^n)$$

where d is the degree of the prime $\mathfrak{p}$. The announced analogue of the Herbrand-Ribet theorem is the following statement [2]. For $1 \leq n < q^d - 1$ which are divisible

by $q-1$ one has that $H_{\mathfrak{p}}(\omega^{1-n})$ is nonzero if and only if $\mathfrak{p}$ divides the n-th so-called *Bernoulli-Carlitz number*. (Which is not a number but a function, an element of $\mathbf{F}_q(t)$.)

By analogy with Vandiver's conjecture it is natural to ask if the other components vanish. This turns out to be *false* in general. Bruno Anglès has shown how one can use Artin-Schreier base change to construct pairs ($\mathfrak{p}$, n) with n not divisible by $q-1$ such that $H_{\mathfrak{p}}(\omega^{1-n})$ is nonzero.

Finally one may ask if the $A/\mathfrak{p}$-module $H_{\mathfrak{p}}$ "comes from" an A-module in the same way that the group H_p comes from the class group. This is indeed the case, one can define for every finite extension of $\mathbf{F}_q(t)$ a certain finite A-module which shares many properties with the class group of a number field, and the module $H_{\mathfrak{p}}$ before is precisely the "mod $\mathfrak{p}$" part of this module. See [2] and [3].

References

[1] D. Goss, Basic structures of function field arithmetic, Springer 1996.

[2] L. Taelman, *A Herbrand-Ribet theorem for function field*, Inv. Math. (2011), DOI:10.1007/s00222-011-0346-3.

[3] L. Taelman, *Special L-values of Drinfeld modules*, to appear in Ann. Math. (2011)

Explicit local reciprocity for tame extensions

Rachel Newton

Let L/K be a tame finite abelian extension of local fields. The local reciprocity map, denoted $\theta_{L/K}$, is a canonical isomorphism

$$\theta_{L/K} : K^*/N_{L/K}(L^*) \to \mathrm{Gal}(L/K).$$

Fix uniformizers π_K, π_L for K, L respectively. Let $\mathfrak{v}$ denote the discrete valuation on L, normalised so that $\mathfrak{v} : K^* \to \mathbb{Z}$ is surjective. Let q be the size of the residue field of K. Let $e = e_{L/K}$ denote the ramification index of L/K.

This talk exhibits the following explicit formula for the local reciprocity map in the tame setting:

Theorem 1. *The local reciprocity map $\theta_{L/K}$ is determined by*

$$\frac{\theta_{L/K}\left(u\pi_K^i\right)(\beta)}{\beta} \equiv \frac{\beta^{(q^i-1)}}{((-1)^{(e-1)}\pi_K)^{(q^i-1)\mathfrak{v}(\beta)}u^{(q-1)\mathfrak{v}(\beta)}} \pmod{\pi_L}$$

for all $i \in \mathbb{N}$, for all $u \in \mathcal{O}_K^*$ and for all $\beta \in L^*$.

The tameness of the extension L/K means, by definition, that the ramification group

$$G_1 = \left\{ g \in \mathrm{Gal}(L/K) \mid \frac{g(x)}{x} \equiv 1 \pmod{\pi_L} \ \forall x \in \mathcal{O}_L \backslash \{0\} \right\}$$

is trivial. Hence, the congruences of Theorem 1 are enough to determine $\theta_{L/K}$.

There has been much previous work on explicit reciprocity laws. However, the approach taken by Artin-Hasse [1], Iwasawa [5], Coates-Wiles [2], De Shalit [3]

and Fesenko-Vostokov [4] is that of establishing an explicit formula for (analogues of) the Hilbert norm residue symbol. But the Hilbert symbol can only be used to calculate local reciprocity for an extension L/K when K contains a primitive root of unity of degree $[L : K]$.

Theorem 1 gives the first completely general explicit formula for tame local reciprocity, using only the arithmetic of the extension L/K.

This formula was obtained using a definition of the local reciprocity map in terms of cyclic algebras and the Brauer group. We first describe the approach taken for a tame cyclic extension L/K of prime-power degree:

The strategy is to choose generators for both $K^*/N_{L/K}(L^*)$ and $\mathrm{Gal}(L/K)$ and form the relevant cyclic K-algebra. Then we construct an unramified extension F/K which splits the cyclic algebra and use the Hasse invariant to compare our original choice of generator for $\mathrm{Gal}(L/K)$ with the canonical generator $\mathrm{Frob}_{F/K}$ of $\mathrm{Gal}(F/K)$.

For the more general case of a tame finite abelian extension, we decompose the finite abelian group $\mathrm{Gal}(L/K)$ into a direct product of cyclic groups of prime-power degree and use functorial properties of the local reciprocity map to prove that Theorem 1 holds for any tame finite abelian extension L/K.

References

[1] A. Artin and H. Hasse, *Die beiden Ergänzungsätze zum Reziprozitätsgesetz der l^n-ten Potenzreste in Körper der l^n-ten Einheitswurzeln*, Abh. Math. Sem. Univ. Hamburg **6** (1928), 146–162.

[2] J. Coates and A. Wiles, *Explicit reciprocity laws*, Soc. Math. France, Astérisque **41-42** (1977), 7–17.

[3] E. De Shalit, *The explicit reciprocity law in local class field theory*, Duke Math. J. **53**, Number 1 (1986), 163–176.

[4] I. B. Fesenko and S. V. Vostokov, *Local Fields and Their Extensions: Second Edition*, American Mathematical Society, 2002.

[5] K. Iwasawa, *On explicit formulas for the norm residue symbol*, Math. Soc. Japan **20** (1968), 151–164.

Using algebraic values of modular forms to obtain models of modular curves

Kamal Khuri-Makdisi

Let $X \subset \mathbf{P}^n$ be a projective smooth curve over a field K, and let $I = I_X \subset \mathcal{R} = K[T_0, \ldots, T_n]$ be the ideal of X. Write I_k for the kth graded part of I. Let $V = \mathrm{Span}\{T_0, \ldots, T_n\}$, so that $\mathcal{R}_k = \mathrm{Sym}^k V$ is the space of homogeneous k-forms. The degree k part of the projective coordinate ring $\mathcal{R}/I$ of X is then $\mathcal{R}_k/I_k \subset H^0(X, \mathcal{L}^{\otimes k})$, where $\mathcal{L} = \mathcal{O}_X(1)$ is the line bundle on X coming from $\mathbf{P}^n$; the degree of the projective curve X is $d = \deg \mathcal{L}$.

We will use the following approach to describe models of algebraic curves. Suppose I is generated by its elements in degree $\leq m$. Then X is completely described by $md+1$ points $\{P_0, \ldots, P_{md}\} \subset X \subset \mathbf{P}^n$. Indeed, we can compute I_k for $k \leq m$

by linear algebra (interpolation!) through the points P_i, since $f \in I_k$ if and only its image in $H^0(X, \mathcal{L}^{\otimes k})$ vanishes, which is equivalent to vanishing just at the P_i.

For example, suppose X has genus g, $V = H^0(X, \mathcal{L})$ (i.e., we use a complete linear series), and $\deg \mathcal{L} \geq 2g + 2$. Then a well-known theorem [3] due (independently) to Fujita and St. Donat, building on results of Castelnuovo and Mumford, says that I is generated by I_2, i.e., that X is cut out by quadrics.

We study the above approach in the context of the modular curve $X = X(N)$, for $N \geq 3$. There exists a line bundle $\mathcal{L}$ on X such that $H^0(X, \mathcal{L}^{\otimes k}) = \mathcal{M}_k(\Gamma(N))$, the space of weight k modular forms on $\Gamma(N)$. We take $V = \mathcal{E}is_1$, the space of weight 1 Eisenstein series; this (nontrivially) gives rise to a projective embedding of X, for which we wish to find I. Now finding elements of I_k by interpolation requires us to "evaluate" weight k modular forms (given as polynomials in elements of $\mathcal{E}is_1$) at sufficiently many points of X.

Since the points $P \in X$ parametrize (generalized) elliptic curves with full level N structure, we can hope to describe a family of "moduli-friendly" modular forms that are easy to evaluate at a point P from the moduli viewpoint, i.e., in terms of the elliptic curve and other data parametrized by P. More precisely, in the style of Katz, we view a modular form f as a function of tuples (E, ω, α) where $\omega \in \Omega^1(E)$ is a nonzero global differential, and $\alpha : (\mathbb{Z}/N\mathbb{Z})^2 \cong E[N]$ is the level structure. To say that f has weight k means that $f(E, c\omega, \alpha) = c^{-k} f(E, \omega, \alpha)$. For example, the weight 4 and weight 6 Eisenstein series G_4 and G_6 on $SL(2, \mathbb{Z})$ can be evaluated on a pair (E, ω) (no level structure is necessary) by writing E in Weierstrass form $y^2 = x^3 + ax + b$, normalized so that $\omega = dx/2y$; then the values of G_4 and G_6 are essentially a and b. Similarly, if $T = \alpha(i, j) \in E[N]$ is a torsion point with coordinates (x_T, y_T) in the Weierstrass model, then for $E = \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$, $T = (i\tau + j)/N$ we can identify x_T, y_T with the Weierstrass functions $\wp(T; \tau), \wp'(T; \tau)$, which are essentially Eisenstein series of weights 2 and 3 on $\Gamma(N)$. More generally, using Laurent expansions of elements of the function field of E with prescribed poles and zeros in $E[N]$, one can define [2] a family of moduli-friendly modular forms on $\Gamma(N)$ that includes all Eisenstein series, even in weight 1. (The weight 1 Eisenstein series are also related to slopes $(y_T - y_U)/(x_T - x_U)$ of lines joining two torsion points $T, U \in E[N]$.) We have:

Theorem [2]**:** All modular forms in the above family belong to the ring of modular forms generated by $V = \mathcal{E}is_1$. Over $\mathbb{C}$, this ring contains all forms in weights ≥ 2. (Only $\mathcal{S}_1(\Gamma(N))$ is missing). The projective coordinate ring is $\mathcal{R}/I = \mathbb{C} \oplus \mathcal{E}is_1 \oplus \mathcal{M}_2 \oplus \mathcal{M}_3 \oplus \cdots$. Moreover, I is generated by $I_{\leq 3}$.

To choose the points $P \in X(N)$ where one evaluates modular forms, one can fix an elliptic curve E_0 over $\mathbb{Q}$ (e.g., $y^2 = x^3 + 314159x + 271828$), and take all possible level structures on E_0. This gives sufficiently many points for us to determine $I_{\leq 11}$ by interpolation, including the relations we need in degrees ≤ 3. We thus obtain the statement that a *single* elliptic curve E_0 and the slopes between its N-torsion points suffice to determine a model for $X(N)$, which parametrizes *all* elliptic curves with their N-torsion. The calculations take place in $\mathbb{Q}(E_0[N])$, but one can descend the field to $\mathbb{Q}(\zeta_N)$ and perhaps even to $\mathbb{Q}$.

The above method allows one to find generators of I for any given N. It would be desirable to give a general formula for generators of I. The elements of I_1 are linear relations between Eisenstein series of weight 1, and these were already known to Hecke. (There is a subtle symmetry, related to the Weil pairing on $E[N]$, which "explains" why $\dim \mathcal{E}is_1$ is half the number of cusps of $X(N)$.) In weights 2 and 3, various relations are known, most notably a weight 2 identity that was used in [1] to give a model for $X_1(\ell)$ with ℓ prime. However, the known relations appear not to generate all of I: in our numerical experimentation, we have seen examples where the subideal $J \subset I$ generated by the known relations does not equal I. For example, when $N = 13$, the degree 2 parts I_2 and J_2 differ, and we experimentally find 28 "mysterious" relations in degree 2. Curiously, $I_k = J_k$ in all degrees $k \neq 2$. We carried out these calculations modulo $p = 10037$, to avoid coefficient explosion over a number field; we also chose E_0 over $\mathbf{F}_p$ with all of $E_0[13]$ rational over $\mathbf{F}_p$. Then the points for interpolation were also rational over $\mathbf{F}_p$, simplifying the computations.

For future work, it would be interesting to generalize this approach of finding equations by interpolation to Shimura curves with respect to an indefinite quaternion algebra B over $\mathbb{Q}$. This would require (i) some "simple" modular forms on $B^\times$ with a nice moduli interpretation — perhaps restriction of simple Hilbert modular forms on a quadratic field $F \subset B$ might work — and (ii) enough understanding of the ring of modular forms on $B^\times$ generated by the "simple" forms, so as to be able to control the ideal of relations I and to bound the degrees of its generators.

References

[1] Lev A. Borisov, Paul E. Gunnells, and Sorin Popescu, *Elliptic functions and equations of modular curves*, Math. Ann. **321** (2001), no. 3, 553–568.

[2] Kamal Khuri-Makdisi, *Moduli interpretation of Eisenstein series*, Arxiv preprint, 2009, may be downloaded from `http://arxiv.org/abs/0903.1439`

[3] Robert Lazarsfeld, *A sampling of vector bundle techniques in the study of linear series*, Lectures on Riemann Surfaces (Trieste, 1987) (M. Cornalba, X. Gomez-Mont, and A. Verjovsky, eds.), World Sci. Publishing, Teaneck, NJ, 1989, pp. 500–559.

Rank 7 quadratic twist(s) of the congruent number curve

Mark Watkins

(joint work with Andrew Granville)

Let $E : y^2 = x^3 - x$ be the congruent number curve, so that d is a congruent number precisely when the dth quadratic twist $E_d : dy^2 = x^3 - x$ has positive rank. We are interested in how the rank behaves as d varies.

In 2003, Rogers (see [1]) found that $d = 797507543735$ yields E_d of rank 7, and found 14 quadratic twists of rank 6. Later work of Dujella, Janfada, and Salami [1] determined about 25 more such rank 6 quadratic twists.

One method to find such high rank twists is to loop over $1 \leq v < u \leq L$ for some L, and for each (u, v) determine the (unique) d with x-coordinate u/v by

removing square factors from $uv(u+v)(u-v)$. Our computations (others ordered the steps differently) then computed the 2-Selmer rank via $\mathbf{F}_2$-linear algebra using a result of Monsky, and for the twists that allowed "large" rank then computed a Mestre-Nagao sum $\sum_{p\le X} \frac{2-a_p\chi_d(p)}{\#E_d(\mathbf{F}_p)}\log p$ as a heuristic for large rank, before trying 2-descent on isogenous curves and searching for more points (on 2-covers).

The twist $d = 797507543735$ is first found with $(v,u) = (79873, 235280)$, taking at most a cpu-hour to find. The first rank 6 twist is $d = 6611719866$ and the first rank 5 twist is $d = 48242239$, so we might offhandedly predict the first rank 8 twist to appear before $d \approx 10^{15}$. We searched up to $L = 10^7$, and up to $L = 10^8$ with more restrictions, such as requiring $d < 2^{55}$ or the square-free part of u to be small. Using about 1000 cpu-hours, we did not find any rank 8 twists. We only found [after the talk] a mere nine new rank 7 twists, whereas we found over 250 new rank 6 twists, including one with nontrivial Ш[2] for all isogenous curves.

A second search method, suggested/implemented by Elkies (with further implementations by Hart/Watkins), parametrises the square divisors of $uv(u^2-v^2)$ via

$$d_1^2|u,\ \ d_2^2|v,\ \ d_3^2|(u+v),\ \ d_4^2|(u-v),$$

and then loops over (d_1,d_2,d_3,d_4) and looks for short vectors in the (u,v) plane. For instance, $(40,169,3,389)$ leads to the pair $(u,v) = (18822400, 13526165)$ and $d = 797507543735$ as above. This takes more than 5 cpu-hours to find, and so the usefulness of this search method is not all that clear as of yet.

The second half of the talk gave a heuristic of Granville for upper bounds on ranks of curves in quadratic twist families. We fix $E : Y^2 = f(X) = X^3 + aX + b$, and consider the quadratic twists in projective form (with z a cube) as

$$E_d : y^2z = x^3 + ad^2xz^2 + bd^3z^3.$$

Granville's idea is that we can guess an upper bound on the number of (integral) (d,x,y,z) points on this surface (in some range, considering d as a variable) while *one* twist of sufficiently large rank will produce more points than this upper bound.

In particular, the displayed equation gives congruence/divisibility conditions, namely that $x \equiv 0 \pmod{\sqrt[3]{z}}$ and $\tilde{f}(x,dz) \equiv 0 \pmod{y^2}$, where $\tilde{f}$ is a projective version of f. We next split into intervals of a dyadic nature, taking $|d| \sim D$, and also $|x| \sim T$ and $z \sim U/D$. We also assume that $(x^3 + ad^2xz^2 + bd^3z^3)$ does not generically have much cancellation, so that typically we have $y \sim \sqrt{DV^3/U}$ where $V = \max(T, U/D)$.

Following Granville's lead, we then proceed to estimate the number $N_D(T,U)$ of (d,x,y,z) points with $|d| \sim D$ and $|x| \sim T$ and $z \sim U/D$ as

$$N_D(T,U) \underset{?}{\ll} \sum_{d\sim D} \sum_{y\sim\sqrt{DV^3/U}} \sum_{\tilde{z}\sim\sqrt[3]{U/D}} \sum_{\substack{x\sim T,\tilde{z}|x \\ \tilde{f}(x,d\tilde{z}^3)\equiv 0\,(y^2)}} 1.$$

The y^2-congruence has a density of solutions given by approximately $\sigma_f(y^2)/y^2$, where $\sigma_f(y^2)$ is the number of roots of f modulo y^2.

Granville uses this density to make the heuristic guess that

$$N_D(T,U) \underset{??}{\ll} \sum_{d\sim D} \sum_{y\sim\sqrt{DV^3/U}} \frac{\sigma_f(y^2)}{y^2} \sum_{\tilde{z}\sim\sqrt[3]{U/D}} \frac{T}{\tilde{z}} \ll TD\sqrt{\frac{U}{DV^3}}\big(\log DV^3/U\big)^{\eta-1},$$

where $\eta \in \{1,2,3\}$ is the average number of roots of f modulo primes.

Summing dyadically over T, U up to a bound B accrues an extra logarithm (from the $T = U$ contributions), and this gives us an overall bound of

$$C_D(B) \underset{??}{\ll} \sqrt{D}(\log B)^{\eta}$$

for the number $C_D(B)$ of points (d, x, y, z) with $|x|, z \le B$ and $|d| \sim D$.

Remarks.

- Granville notes that something like this should be provable for $B \ll D^{\delta}$ for some $\delta > 0$ via sieve theory, but he applies it for $B \sim e^{D^l}$ with $l > 0$.
- The original Granville heuristic dealt with $dY^2 = Z(X^3 + aXZ^2 + bZ^3)$, where one seems to lose a logarithm due to the Z-factor on the right.

Next we count the number of points of "small" height on an elliptic curve of rank r and regulator R, where asymptotically the number of points up to (canonical) height h as $h \to \infty$ is $h^{r/2}/\sqrt{R}$. We assume (from ellipsoids) this is a lower bound for $h \gg R^{1/r}$ and that canonical and naïve heights are close. Upon noting the conjectural BSD formula implies $R \approx \sqrt{D}$ for quadratic twists $d \sim D$, we get

$$\frac{h^{r/2}}{D^{1/4}} \ll \begin{array}{l}\#\text{ of pts up to height } h \text{ on} \\ \text{one rank } r \text{ twist of size } D\end{array} \ll C_D(e^h) \ll \sqrt{D}h^{\eta}.$$

Finally, we must guess how large we can take $h = D^l$. Plugging into the above, we get $r \le 2\eta + \frac{3}{2l}$ as $D \to \infty$, so in particular any $l > 0$ gives an upper bound on ranks in twist families. Contrarily, allowing $l > 3/2$ implies $r \le 2$ for the generic case ($\eta = 1$), while data suggest otherwise. Granville offers, in relation to the size of solutions to Pell equations, that $l = \frac{1}{2}$ seems reasonable, leading to $r \le 2\eta + 3$.

For curves with full 2-torsion ($\eta = 3$) there is an additional subtlety, as every such curve is isogenous to one with only one 2-torsion point ($\eta = 2$), and it is unclear whether the bound for the latter should dominate. If so, one obtains an asymptotic bound of $r \le 7$ for quadratic twists of an elliptic curve with 2-torsion.

Remarks. Obvious additions allow heuristic guesses about densities. Honda [2] seems to be the first to theorise that ranks might be bounded in quadratic twist families. One can make a similar heuristic for cubic twists $dY^3 = X^3 + Z^3$.

References

[1] A. Dujella, A. S. Janfada, S. Salami, *A search for high rank congruent number elliptic curves,* J. Integer Seq. **12** (2009), 09.5.8.

[2] T. Honda, *Isogenies, rational points and section points of group varieties.* Japan. J. Math., **30** (1960), 84–101.

Mordell-Weil Generators of Cubic Surfaces

Samir Siksek

This talk summarizes some of my work on the arithmetic of cubic surfaces, part of which can be found in [4].

Let C be a smooth plane cubic curve over $\mathbb{Q}$. The Mordell-Weil Theorem can be restated as follows: there is a finite subset B of $C(\mathbb{Q})$ such that the whole of $C(\mathbb{Q})$ can be obtained from this subset by drawing secants and tangents through pairs of previously constructed points and consecutively adding their new intersection points with C. It is conjectured that a minimal such B can be arbitrarily large; this is indeed the well-known conjecture that there are elliptic curves with arbitrarily large ranks. This talk is concerned with the cubic surface analogues of the Mordell-Weil Theorem and the unboundedness of ranks.

Let K be a field and let S be a smooth cubic surface over K in $\mathbb{P}^3$. By a K-line we mean a line $\ell \subset \mathbb{P}^3$ that is defined over K. If $\ell \not\subset S$ then $\ell \cdot S = P + Q + R$ where P, Q, $R \in S$. If any two of P, Q, R are K-points then so is the third. The line ℓ is tangent at P if and only if P appears more than once in the sum $P+Q+R$. If $B \subseteq S(K)$, we shall write $\mathrm{Span}(B)$ for the subset of $S(K)$ generated from B by successive secant and tangent constructions. In view of the Mordell-Weil Theorem for cubic curves it is natural to ask, for $K = \mathbb{Q}$ say, if there is some finite subset $B \subset S(K)$ such that $\mathrm{Span}(B) = S(K)$. As far as we are aware, the possible existence of such an analogue of the Mordell-Weil Theorem was first mentioned by Segre [3, page 26] in 1943. Manin [1, page 3] asks the same question for fields K finitely generated over their prime subfields. He calls this [2] the Mordell-Weil problem for cubic surfaces. The results of numerical experiments by Zagier (described by Manin in [2]) and Vioreanu [5] lead different experts to different opinions about the validity of this Mordell-Weil conjecture. We are not aware of even a single example in the literature where the existence of a finite set B that generates $S(K)$ via the secant and tangent process is proven. In this talk we give a positive answer to a special case of the Mordell-Weil problem.

Theorem 1. *Let K be field with at least* 13 *elements. Let S be a smooth cubic surface over K. Suppose S contains a pair of skew lines both defined over K. Let $P \in S(K)$ be a point on either line that is not an Eckardt point. Then* $\mathrm{Span}(P) = S(K)$.

An *Eckardt point* is a point where three of the lines contained in S meet.

Now let us write

$$r(S,K) := \min\{\#B : B \subseteq S(K) \text{ and } \mathrm{Span}(B) = S(K)\}.$$

We are unable to show that $r(S,K)$ is finite for cubic surfaces without a skew pair of K-lines. However, in some cases we can bound $r(S,K)$ from below. We use this to show that $r(S,\mathbb{Q})$ is arbitrarily large as S varies among smooth cubic surfaces over $\mathbb{Q}$. To do this we introduce and study a simple analogue of the Picard group

of an elliptic curve. Let

$$G_S(K) = \bigoplus_{P \in S(K)} \mathbb{Z} \cdot P$$

be the free abelian group generated by the K-rational points of S. Let $G'_S(K)$ be the subgroup generated by all three point sums $P+Q+R$ with P, Q, $R \in S(K)$ such that

(i) there is K-line ℓ not contained in S with $\ell \cdot S = P+Q+R$, or
(ii) there is a K-line ℓ contained in S such that P, Q, $R \in \ell$.

The *degree map* $\deg : G_S(K) \to \mathbb{Z}$ is given by $\deg(\sum a_i P_i) = \sum a_i$. Let

$$G''_S(K) = \{D \in G'_S(K) : \deg(D) = 0\}.$$

Let $\Theta_S(K) := G_S(K)/G''_S(K)$. If $P \in S(K)$ we denote the image of P in $\Theta_S(K)$ by $[P]$. The degree map remains well-defined on $\Theta_S(K)$: we let $\deg : \Theta_S(K) \to \mathbb{Z}$ be given by $\deg(\sum a_i[P_i]) = \sum a_i$. We shall write

$$\Theta^0_S(K) = \{D \in \Theta_S(K) : \deg(D) = 0\}.$$

If $S(K) \neq \emptyset$ then the degree homomorphism clearly induces an isomorphism

$$\Theta_S(K)/\Theta^0_S(K) \cong \mathbb{Z}.$$

The group $\Theta_S(K)$ will allow us to study $r(S,K)$.

Theorem 2. *Let $p_1, \ldots, p_s$ ($s \geq 1$) be distinct primes such that*

(a) $p_i \equiv 1 \pmod 3$,
(b) *2 is a cube modulo p_i.*

Let $M = \prod p_i$ and let $S = S_M/\mathbb{Q}$ be the smooth cubic surface given by

$$S_M : x^3 + y^3 + z(z^2 + Mw^2) = 0. \tag{1}$$

Write $\Theta_S(\mathbb{Q})[2]$ for the 2-torsion subgroup of $\Theta_S(\mathbb{Q})$. Then $\Theta^0_S(\mathbb{Q}) = \Theta_S(\mathbb{Q})[2]$ and

$$r(S,\mathbb{Q}) \geq \dim_{\mathbb{F}_2} \Theta_S(\mathbb{Q})[2] \geq 2s.$$

A prime p satisfies conditions (a) and (b) of the theorem if and only if the polynomial $t^3 - 2$ has three roots modulo p. By the Chebotarëv Density Theorem such primes form a set with Dirichlet density $1/6$. We thus see that $r(S_M, \mathbb{Q})$ becomes arbitrarily large as M varies. The cubic surface S_M has precisely one $\mathbb{Q}$-rational line, which is given by $x + y = z = 0$.

References

[1] Yu. I. Manin, *Cubic Forms: Algebra, Geometry, Arithmetic*, North-Holland, 1974 and 1986.
[2] Yu. I. Manin, *Mordell-Weil problem for cubic surfaces*, pages 313–318 of *Advances in mathematical sciences: CRM's 25 years* (Montreal, PQ, 1994), CRM Proc. Lecture Notes **11**, Amer. Math. Soc., Providence, RI, 1997.
[3] B. Segre, *A note on arithmetical properties of cubic surfaces*, J. London Math. Soc. **18** (1943), 24–31.
[4] S. Siksek, *On the number of Mordell-Weil generators for cubic surfaces*, `arXiv:1012.1838v4`.
[5] B. G. Vioreanu, *Mordell-Weil problem for cubic surfaces, numerical evidence*, pages 223–240 of *Arithmetic geometry*, Clay Math. Proc. **8**, Amer. Math. Soc., Providence, RI, 2009.

Legendre polynomials and identities for π

Wadim Zudilin
(joint work with Heng Huat Chan and James Wan)

In 2011, Z.-W. Sun and G. Almkvist experimentally observed several new identities for $1/\pi$ of the form

$$\sum_{n=0}^{\infty} \frac{(s)_n(1-s)_n}{n!^2}(A+Bn)T_n(b,c)\lambda^n = \frac{C}{\pi}, \tag{1}$$

where $s \in \{1/2, 1/3, 1/4\}$, $A, B, b, c \in \mathbb{Z}$, $(s)_n = \Gamma(s+n)/\Gamma(s)$ is Pochhammer's symbol (the shifted factorial), and $T_n(b,c)$ denotes the coefficient of x^n in the expansion of $(x^2+bx+c)^n$, viz.

$$T_n(b,c) = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k}\binom{2k}{k} b^{n-2k}c^k,$$

while λ and C are either rational or (linear combinations of) quadratic irrationalities. The latter binomial sums can be expressed via the classical Legendre polynomials $P_n(x)$ by means of the formula

$$T_n(b,c) = (b^2-4c)^{n/2} P_n\biggl(\frac{b}{(b^2-4c)^{1/2}}\biggr),$$

so that equalities (1) assume the form

$$\sum_{n=0}^{\infty} \frac{(s)_n(1-s)_n}{n!^2}(A+Bn)P_n(x_0)z_0^n = \frac{C}{\pi}.$$

60 years ago, F. Brafman derived several "unusual" generating functions of the Legendre polynomials $P_n(x)$, in particular,

$$\sum_{n=0}^{\infty} \frac{(s)_n(1-s)_n}{n!^2}P_n(x)z^n = {}_2F_1\biggl(\begin{matrix}s,\,1-s\\1\end{matrix}\,\biggm|\,\frac{1-\rho-z}{2}\biggr)\cdot {}_2F_1\biggl(\begin{matrix}s,\,1-s\\1\end{matrix}\,\biggm|\,\frac{1-\rho+z}{2}\biggr),$$

where $\rho = (1-2xz+z^2)^{1/2}$ and notation ${}_2F_1$ is used for the hypergeometric function. His result was a consequence of Bailey's identity for a special case of Appell's hypergeometric function of the fourth type. Armed with Brafman's formula and the theory of modular forms, we can now prove all identities of Sun and Almkvist, as well as to derive many other ones.

In my talk I also indicate a generalisation of Bailey's identity and its implication to generating functions of Legendre polynomials of the form

$$\sum_{n=0}^{\infty} u_n P_n(x) z^n,$$

where u_n is an Apéry-like sequence, that is, a sequence satisfying

$$(n+1)^2u_{n+1} = (an^2+an+b)u_n - cn^2u_{n-1} \quad \text{for } n = 0,1,2,\dots, \quad u_{-1}=0,\ u_0=1,$$

for a given data a, b and c. Using this identity we construct many new identities for $1/\pi$.

References

[1] H.H. Chan, J. Wan and W. Zudilin, *Legendre polynomials and Ramanujan-type series for* $1/\pi$, Preprint MPIM 2011-36, 20 pages.
[2] J. Wan and W. Zudilin, *Generating functions of Legendre polynomials: a tribute to Fred Brafman*, Preprint MPIM 2011-37, 16 pages.

Computing modular forms using Voronoï polyhedra

Dan Yasaki
(joint work with Paul Gunnells, Farshid Hajir)

The cohomology of an arithmetic group is built out of certain automorphic forms. This allows computational investigation of Hecke eigenvalues using topological techniques. Specifically, Borel conjectured, and Franke proved [2], that the complex cohomology of Γ can be computed in terms of certain automorphic forms. Although not all automorphic forms arise in this way, these cohomological modular forms are widely believed to be connected with arithmetic geometry. In certain cases, these forms are amenable to explicit computation using topological tools.

For example, consider the Eichler-Shimura isomorphism [5], which identifies the cohomology of congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ with holomorphic modular forms. For an integer $N \geq 1$, we have

$$H^1(\Gamma_0(N); \mathbb{C}) \simeq H^1(\Gamma_0(N) \backslash \mathfrak{H}; \mathbb{C}) \simeq S_2(N) \oplus \bar{S}_2(N) \oplus \mathrm{Eis}(N),$$

where $\Gamma_0(N) \subseteq \mathrm{SL}_2(\mathbb{Z})$ is the congruence subgroup of matrices that are upper triangular modulo N, $\mathfrak{H}$ is the complex upper half-plane, $S_2(N)$ is the space of weight 2 holomorphic cusp forms of level N, and $\mathrm{Eis}_2(N)$ is the space of weight 2 holomorphic Eisenstein series. In this case, one technique for explicitly computing such modular forms is the use of modular symbols. These symbols are intimately linked with a $\mathrm{SL}_2(\mathbb{Z})$-invariant tessellation of $\mathfrak{H}$ by ideal triangles.

One can generalize many of these ideas. Let F be a number field of class number one with ring of integers $\mathcal{O}$. Let $\mathbf{G}$ be the linear algebraic group given by the restriction of scalars $\mathbf{G} = \mathrm{Res}_{F/\mathbb{Q}}(\mathrm{GL}_n)$, and let $\Gamma \subseteq \mathrm{GL}_n(\mathcal{O})$ be a congruence subgroup. The associated symmetric space X can be interpreted as a certain space of Hermitian forms. The Voronoï polyhedron Π is an infinite polyhedron whose facets correspond to *perfect* Hermitian forms, those that are uniquely determined by their minimum value and their set of minimal vectors. The cones over the facets of Π give rise to a tessellation of X by ideal polytopes, analogous to the tessellation of $\mathfrak{H}$ by triangles. Modular symbols are replaced by elements of the *sharbly complex*, a resolution of the Steinberg module [1] that can be used to compute the cohomology of Γ.

Now we briefly mention two computational investigations using this technique. First, in joint work with P. Gunnells and F. Hajir [3], we consider the case $\mathbf{G} = \mathrm{Res}_{F/\mathbb{Q}}(\mathrm{GL}_2)$, where F is the cyclotomic field $\mathbb{Q}(\zeta_5)$. The associated symmetric space is 7-dimensional, $X \simeq \mathfrak{H}_3 \times \mathfrak{H}_3 \times \mathbb{R}$, and there is exactly one $\mathrm{GL}_2(\mathcal{O})$-class of perfect form [6]. This perfect form gives rise to a tessellation of X by a 7-dimensional polytope with 24 vertices. This tessellation is used to compute cohomological forms with trivial coefficients. Next, in joint work in progress with P. Gunnells [4], we consider the case $\mathbf{G} = \mathrm{Res}_{F/\mathbb{Q}}(\mathrm{GL}_2)$, where F is the complex cubic field of discriminant -23. The associated symmetric space is 6-dimensional, $X \simeq \mathfrak{H} \times \mathfrak{H}_3 \times \mathbb{R}$. There are exactly nine classes of perfect Hermitian forms. The resulting tessellation is used to compute cohomological forms with trivial coefficients.

In both cases, for each rational cuspidal Hecke eigenform we identified, we found an elliptic curve E over F with matching Hecke data, as far as we could compute both sides. Conversely, for any level $\mathfrak{n}$ where we found no rational eigen-classes, we did not find any elliptic curve over F of that conductor.

References

[1] Avner Ash, *Unstable cohomology of* $\mathrm{SL}(n, \mathcal{O})$, J. Algebra **167** (1994), no. 2, 330–342. MR MR1283290 (95g:20050)

[2] Jens Franke, *Harmonic analysis in weighted L_2-spaces*, Ann. Sci. École Norm. Sup. (4) **31** (1998), no. 2, 181–279. MR MR1603257 (2000f:11065)

[3] Paul E. Gunnells, Farshid Hajir, and Dan Yasaki, *Modular forms and elliptic curves over the field of fifth roots of unity*, Experimental Mathematics (2011), accepted.

[4] Paul E. Gunnells and Dan Yasaki, *Cusp forms over the complex cubic field of discriminant* -23, in preparation.

[5] Klaus Haberland, *Perioden von Modulformen einer Variabler and Gruppencohomologie. I, II, III*, Math. Nachr. **112** (1983), 245–282, 283–295, 297–315. MR 726861 (85k:11022)

[6] Dan Yasaki, *Binary Hermitian forms over a cyclotomic field*, J. Algebra **322** (2009), 4132–4142.

Nahm's conjecture about modularity of q-series

Masha Vlasenko

Let $r \geq 1$ be a positive integer, A a real positive definite symmetric $r \times r$-matrix, B a vector of length r, and C a scalar. The series

$$F_{A,B,C}(q) \;=\; \sum_{n \in (\mathbb{Z}_{\geq 0})^r} \frac{q^{\frac{1}{2} n^T A n + n^T B + C}}{(q)_{n_1} \dots (q)_{n_r}}.$$

converges for $|q| < 1$. Here we use the notation $(q)_n = \prod_{k=1}^{n}(1 - q^k)$. We are concerned with the following problem due to Werner Nahm [1, 2, 3]: describe all such A, B and C with rational entries for which $F_{A,B,C}$ is a modular form. In [4, 5, 10] it was solved by Michael Terhoeven and Don Zagier for $r = 1$ and the list contains seven triples $(A, B, C) \in \mathbb{Q}_+ \times \mathbb{Q} \times \mathbb{Q}$. We develop their approach

based on the computation of the asymptotics of $F_{A,B,C}(q)$ when $q \to 1$ and find several new examples of modular functions already for $r = 2$.

Nahm has also given a conjectural criterion for a matrix A to be such that there exist some B and C with modular $F_{A,B,C}$. The condition for the matrix A is given in terms of solutions of a system of algebraic equations

$$1 - Q_i = \prod_{j=1}^{r} Q_j^{A_{ij}}, \qquad i = 1, \dots, r.$$

Namely, for every solution the element $[Q_1] + \cdots + [Q_r]$ has to be torsion in the Bloch group $B_2(\mathbb{C})$. We give several examples where the matrix A doesn't satisfy the condition (there are solutions giving non-torsion elements) but corresponding modular forms exist. Certainly, it doesn't mean that the conjecture is completely wrong, rather that its correct formulation is an interesting open question.

References

[1] W. Nahm, *Conformal field theory and the dilogarithm.* In *11th International Conference on Mathematical Physics (ICMP-11) (Satelite colloquia: New Problems in General Theory of Fields and Particles)*, Paris, 1994, pp. 662–667.

[2] W. Nahm, *Conformal Field Theory, Dilogarithms and Three Dimensional Manifold.* In *Interface between physics and mathematics (Proceedings, Conference in Hangzhou, P.R.China, September 1993)*, eds. W. Nahm and J.-M.Shen, World Scientific, Singapore, 1994, pp. 154–165.

[3] W. Nahm, *Conformal Field Theory and Torsion Elements of the Bloch Group*, in *Frontiers in Number Theory, Physics and Geometry II*, Springer, 2007, pp. 67–132.

[4] W. Nahm, A. Recknagel and M.Terhoeven, *Dilogarithm identities in conformal field theory.* Mod. Phys. Lett. A8 (1993), pp. 1835–1847.

[5] M.Terhoeven, *Dilogarithm identities, fusion rules and structure constants of CFTs.* Mod. Phys. Lett. A9 (1994), pp. 133–142 .

[6] D. Zagier, *The Dilogarithm Function*, in *Frontiers in Number Theory, Physics and Geometry II*, Springer, 2007, pp. 3–65.

Index Formulae for Stark Units

Xavier-François Roblot

Let K/k be an abelian extension of number fields with Galois group G. Let S_∞ and S_{ram} denote respectively the set of infinite places of k and of finite places of k ramified in K/k, and let $S := S_\infty \cup S_{\mathrm{ram}}$. Assume that there exists at least one place in S, say v, which is totally split in K/k. Fix a place w of K dividing v. Finally, let w_K be the order of the group of roots of unity in K. In this setting, H. Stark [3] made the following conjecture.

Conjecture 1 (Stark)**.** *Assume that $|S| \geq 2$. Then there exists an S-unit $\varepsilon_{K/k} \in K$ such that:*

(1) *For all characters χ of G,*

$$L'_{K/k,S}(0,\chi) = \frac{1}{w_K}\sum_{\sigma\in G}\chi(\sigma)\log|\varepsilon^{\sigma}_{K/k}|_w$$

where $L_{K/k,S}(s,\chi)$ denotes the Hecke L-function associated to χ with the Euler factors for prime ideals in S deleted.

(2) *The extension $K(\varepsilon_{K/k}^{1/w_K})/k$ is abelian.*

(3) *If $|S|\geq 3$, then ε is actually a unit of K.*

We assume that k has at least two infinite places so that the condition of the conjecture always applies. We need some stronger assumptions to prove the index formulae. We make the following hypotheses:

(1) The place v is real.
(2) k is totally real and all infinite places of K not above v are complex.
(3) The maximal totally real subfield K^+ of K satisfies $[K:K^+]=2$.
(4) All finite primes in S are either ramified or inert in K/K^+.

Let $d := [k:\mathbb{Q}]$ and $m := [K^+:k]$, thus $[K:k]=2m$. **Assume that the conjecture is true** and let $\varepsilon := \varepsilon_{K/k}$. Let U_{Stark} be the multiplicative $\mathbb{Z}[G]$-module generated by ε and U_{K^+}, the group of units of K^+.

Theorem 2. *The index of U_{Stark} in the group of units of K is*

$$(U_K : U_{\mathrm{Stark}}) = 2^{t+dm-1}\frac{h_K}{h_{K^+}}$$

where t is the number of finite primes in K^+ above S that are inert in K/K^+.

Let $\mathcal{N}$ denote the norm map of the extension K/K^+. Define Cl_K^- and U_S^- as the kernel of $\mathcal{N}$:

$$\mathrm{Cl}_K^- := \mathrm{Ker}(\mathcal{N}:\mathrm{Cl}_K\to\mathrm{Cl}_{K^+}) \text{ and } U_K^- := \mathrm{Ker}(\mathcal{N}:U_K\to U_{K^+}).$$

One can prove that $\varepsilon\in U_K^-$. From the previous theorem and, for the second part, from combining the theorem with some previous results of Rubin [2], we get

Theorem 3. *We have*

$$\left(U_K^- : \mathbb{Z}[G]\cdot\varepsilon\right) = 2^{t+e}|\mathrm{Cl}_K^-| \tag{P1}$$

where $2^e = (U_{K^+} : \mathcal{N}(U_K))$. Furthermore, for all irreducible $\mathbb{Z}_p$-character ψ, we have

$$\left|(U_K^-/\mathbb{Z}[G]\cdot\bar{\varepsilon})^{\psi}\right| = \left|(\mathrm{Cl}_K^-)^{\psi}\right|. \tag{P2}$$

Now, **we do not assume the Stark conjecture to be true anymore** and we consider how the two conditions (P1) and (P2) characterize the Stark unit (if it exists) and if one can prove that they admit solutions independently of the conjecture. It is easy to see that (P1) and (P2) do not characterize the Stark unit in general since, if u is a unit of $\mathbb{Z}[G]$, and η is a solution to (P1) and (P2), then η^u is also a solution. If $u\in\pm G$, then it is *essentially* the same solution (such units are called trivial units). By a theorem of Higman [1], $\mathbb{Z}[G]$ has non-trivial units if

and only if there exist elements in G with order not dividing 4 or 6. In particular, if G is cyclic of order 4, then the solution to (P1) and (P2) is unique if it exists. In that case, we prove the following result.

Theorem 4. *Assume that K/k is a cyclic extension of degree 4 satisfying the hypotheses listed above. Then, there exists $\eta \in U_K^-$ satisfying* (P1) *and* (P2)*. Furthermore, η is unique up to a trivial unit, satisfies, for all $\chi \in \hat{G}$*

$$\left|L'_{K/k,S}(0,\chi)\right| = \frac{1}{2}\left|\sum_{\sigma\in G}\chi(\sigma)\log|\eta^\sigma|\right|$$

and the extension $K(\sqrt{\eta})/k$ is abelian.

References

[1] G. Higman. The units of group-rings. *Proc. London Math. Soc. (2)*, 46:231–248, 1940.

[2] K. Rubin. Stark units and Kolyvagin's "Euler systems". *J. Reine Angew. Math.*, 425:141–154, 1992.

[3] H. Stark. L-functions at $s = 1$. IV. First derivatives at $s = 0$. *Adv. in Math.*, 35(3):197–235, 1980.

Coregular Representations and Average Ranks of Elliptic Curves in Families

Wei Ho

(joint work with Manjul Bhargava)

Coregular representations of algebraic groups are those with a polynomial ring of (relative) invariants. We discuss a number of parametrizations of geometric data, such as genus one curves with specified line bundles or vector bundles, by orbits of coregular representations. Often the invariant theory of the representation has a geometric interpretation; for example, in some cases, the generators of the invariant ring are exactly the coefficients appearing in certain models of the Jacobians of the genus one curves.

Understanding the invariant theory of these spaces and applying geometry-of-numbers techniques give the average sizes of 2- and 3-Selmer groups of elliptic curves over $\mathbb{Q}$ in certain natural families. In particular, these averages give bounds on the limsup of the average rank of elliptic curves in these families. They also imply the existence of a large explicit family of elliptic curves of algebraic rank exactly 1, and conditionally on the finiteness of the Tate-Shafarevich group (or slightly weaker hypotheses), one of algebraic rank exactly 2 and one of rank 3.

Moduli of Marked Elliptic Curves

Noam D. Elkies

Fix a field k, a finitely-generated abelian group G that can appear in $E(k)$ for some elliptic curve E/k [e.g. if $k = \mathbf{Q}$ then $G_{\rm tors} = \mathbf{Z}/n\mathbf{Z}$ or $(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2n\mathbf{Z})$], and a finite symmetric subset $M = -M \subset G$ such that $M \cap G_{\rm tors} = \emptyset$. A "marked elliptic curve" is then an elliptic curve E/k, with coefficients in an integrally closed subring $A \subset k$, together with a homomorphism $m : G \to E(k)$, injective on $G_{\rm tors}$, such that $m(M)$ consists of A-integral points of E.

[NB The point 0 is never integral, so we can't have $0 \in M$; a nonzero n-torsion point is at least $A[1/n]$-integral (Nagell-Lutz), which is why we remove all nonzero torsion from M; and P is integral iff $-P$ is integral, so we may as well take $M = -M$.]

We mainly give examples, old and new, of such parametrizations and of various applications and connections, and conclude by asking for a more structural description.

Some known examples (assuming 2 and 3 are invertible), in terms of the usual coefficients $(a_1, a_2, a_3, a_4, a_6)$ of extended Weierstrass form:

i) Nothing: $(0, 0, 0, a_4, a_6)$

ii) 2-torsion point: $(0, a_2, 0, a_4, 0)$ with $T = (0, 0)$

iii) 3-torsion point: $(a_1, 0, a_3, 0, 0)$ with $T = (0, 0)$

iv) an integral point: $(0, a_2, a_3, a_4, 0)$ with $T = (0, 0)$

v) 2-torsion point T, and integral P and $P + T$: $y^2 = x^3 + a_2x^2 + a_4x$ with $x \mid a_4$, so $a_4 = \alpha_2\alpha_2'$ and $(x, y) = (\alpha_2, z_1\alpha_2)$. Then $z_1^2 = a_2 + \alpha_2 + \alpha_2'$. Now solve for α_2'. Get $(0,\ a_2,\ 0, \alpha_2\alpha_2', 0) = \big(0,\ a_2,\ 0,\ \alpha_2(z_1^2 - a_2 - \alpha_2),\ 0\big)$. [Subscripts of new parameters z, α, etc. are weights consistent with those of the a_i.]

Imposing the integrality condition also on $P+T$, not just P, actually simplifies the answer; it also yields an involution $P \leftrightarrow P+T$ of (G, M) [here $G = (\mathbf{Z}/2\mathbf{Z}) \times \mathbf{Z}$ with $M = \{(0, \pm1), (1, \pm1)\}$] that yields an involution $\alpha_2 \leftrightarrow \alpha_2'$ of the parametrization. In general a homomorphism $h : (G', M') \to (G, M)$ (not necessarily an injection) gives a map h^* from (G, M)-marked curves to (G', M')-marked curves.

Examples (i)–(v) are the same curves that arise in work described at this meeting by M. Bhargava and W. Ho on the average ranks of elliptic curves.

Further examples and applications:

$M = \{\pm P, \pm Q\}$ with P, Q generators of $G = \mathbf{Z}^2$ leads to $[a_6 =]\, x^3 + a_4x - y^2 = x'^3 + a_4x' - y'^2$ which is hard to parametrize, with about $H^8 \log H$ solutions of height $\le H$, i.e. such that $x, x' \ll H^2$, $y, y' \ll H^3$, and $a_4 \ll H^4$ [see [1]; also noted in an earlier Oberwolfach meeting on this topic; the $\log H$ factor arises from factoring $y^2 - y'^2 = (x - x')(x^2 + xx' + x'^2 + a_4)$]. But $M = \{\pm P, \pm Q, \pm(P + Q)\}$ works nicely. Let z_1 be the slope of the line joining $P, Q, -(P + Q)$. Then $z_1 \in A$ because $z_1^2 = x(P)+x(Q)+x(P+Q)$. So the line is $y = z_1x+b_3$ with some $b_3 \in A$, and we get the general marked curve $y^2 = (x - \xi_2)(x - \xi_2')(x - \xi_2'') + (z_1x + b_3)^2$ with $(\xi_2, \xi_2', \xi_2'') = (x(P), x(Q), x(P + Q))$ such that $\xi_2 + \xi_2' + \xi_2'' = z_1^2$. This would have simplified the search of [1]. For $r = 3$ and $r = 4$ (but no further) there's

likewise a family with G, M the A_r root lattice and system, and H^{10-n} curves up to height H; This may make it possible to push the search further. Already used $r = 3$ case to find the curves of rank $3, 4, 5$ of smallest conductor known over $\mathbf{Q}(\sqrt{5})$.

The curve $(b - d, cd, bcd, 0, 0)$ has integral nP for $n = 1, 2, 3, 4$ (namely $P = (0, 0)$ and $x(nP) = -cd, bd, c(b + c)$ for $n = 2, 3, 4$); this is the parametrization for $G = \mathbf{Z}$, $M = \{\pm 1, \pm 2, \pm 3, \pm 4\}$. Used to find (E, P) with small $\hat{h}(P)$ and/or many integral points, for elliptic surfaces [2] or curves (e.g. $P = (0, 0)$ on $(209, 23520, 2446080, 0, 0)$ [minimal model] has with nP integral for each $n \leq 14$ and also $n = 18$). Also related with $\mathrm{X}_1(N)$ as in K. Khuri-Makdisi's talk.

A nice family with $G = (\mathbf{Z}/2\mathbf{Z}) \times \mathrm{A}_2$: parameters w, w', w'', w''' each of weight 1; in $(0, a_2, 0, a_4, 0)$, take $a_2 = (w^2 + w'^2 + w''^2 + w'''^2) - (w + w' + w'' + w''')^2/4$ and $a_4 = ww'w''w'''$. Three points such as $(ww', ww'(w+w'-w''-w''')/2)$ sum to zero and are integral together with their 2-torsion translates. Again symmetries come from $\mathrm{Aut}(G, M)$. Used for a search *à la* [1] for curves with a 2-torsion point and moderately high rank r; e.g. for $r \in [4, 10]$ the rank-r curve of smallest conductor N that we have found has $(N; a_2, a_4)$ as follows:

$r = 4$: $(4405696;\ 106, -184)$
$r = 5$: $(232106304;\ 170, -6392)$
$r = 6$: $(44968690156;\ 1105, 9503)$
$r = 7$: $(22378025224048;\ -11645, 44520008)$
$r = 8$: $(6682940617328192;\ 76330, 28666568)$
$r = 9$: $(34335198295908849600;\ 379250, 19138775400)$
$r = 10$: $(14908677686287650358464;\ 2649530, 173184944968)$.

Once M gets large compared with the rank and torsion of M, the slopes have linear dependencies; e.g. for $(b - d, cd, bcd, 0, 0)$ the slopes for $(P, P, -2P)$, $(P, 2P, -3P)$, $(P, 3P, -4P)$, and $(2P, 2P, -4P)$ are $b - d$, $b + d$, $-(b + 2c + d)$, and $-(b + 2c - d)$. In general, if M contains $P_i - P_j$ $(i, j = 1, 2, 3, 4)$ then the slopes of $(P_i - P_j, P_j - P_k, P_k - P_i)$ [four choices of distinct i, j, k, in appropriate cyclic order] sum to zero. The slopes thus form an "additive homogeneous cocycle", which thus (at least if M_{tors} is prime to $\mathrm{char}\, k$) must be a coboundary. Over $\mathbf{C}$, we have $E = \mathbf{C}/L$ and it's the coboundary of the Weierstrass ζ function for L.

Questions: How are these moduli spaces related with more standard moduli spaces of elliptic curves with r points and a given torsion group (once $r > 0$)? How close are we to finding all (G, M) for which the moduli space for marked curves is just a weighted projective space? What about complete intersections weighted projective space? Any further applications or connections?

References

[1] Noam D. Elkies and Mark Watkins, *Elliptic Curves of Large Rank and Small Conductor*, Lecture Notes in Computer Science **3076** (proceedings of ANTS-6, 2004; D.Buell, ed.), 42–56. `math.NT/0403374`

[2] Noam D. Elkies, *Points of Low Height on Elliptic Curves and Surfaces I: Elliptic surfaces over* $\mathbf{P}^1$ *with small d*, (proceedings of ANTS-7, 2006; F.Hess, S.Pauli, and M.Pohst, ed.), 287-301. `math.NT/0608593`

Rigorous computations of complex L functions

Pascal Molin

Given a L function satisfying a known functional equation, we are interested in computing rigorously its complex values to arbitrary precision. Our work relies on the approximate functional equation method to reach large imaginary parts. We also use a rigorous numerical integration method derived from the Poisson formula. Assuming that the Dirichlet coefficients are given for free, we prove a binary complexity of

$$O\left(\sqrt{q}D^2(D+|t|)^{r/2}\log(D+|t|)^2\right)$$

for the evaluation of $L(\sigma+it)$ to absolute precision D, where r is the degree of the L function, and q is the arithmetic conductor.

On the computation of local components of a newform

David Loeffler
(joint work with Jared Weinstein)

1. The problem

Let f be a modular newform, of weight $k \geq 2$ and level N. As is well known, we can construct from f an automorphic representation of Π_f of $\mathrm{GL}(2, \mathbf{A})$, where $\mathbf{A}$ is the ring of adèles; and this decomposes as a restricted tensor product of representations $\Pi_{f,v}$ of $\mathrm{GL}(2, \mathbf{Q}_v)$ for each place v. We seek to compute these local factors $\Pi_{f,v}$. The local factor at ∞ is determined by the weight of f, so we take v to be a finite prime p. Via the local-global compatibility theorem of Carayol, this is equivalent to determining the restriction of the ℓ-adic Galois representation of f to a decomposition group at p (for any choice of auxilliary prime $\ell \neq p$).

The local factor $\Pi_{f,p}$ is an irreducible smooth representation of $G := \mathrm{GL}(2, \mathbf{Q}_p)$. These representations fall into three classes: *principal series*, *special*, and *supercuspidal*. The first two classes are the representations which occur as subquotients of the parabolic induction of some character of the diagonal torus of G. It is easy to show that $\Pi_{f,p}$ falls into one of these two classes if and only if f, or some twist of f by a Dirichlet character, has either level prime to p or non-zero Hecke eigenvalue at p; and the twist and the Hecke eigenvalue uniquely determine $\Pi_{f,p}$. Thus it is the remaining case of $\Pi_{f,p}$ supercuspidal that is interesting. (These supercuspidal representations correspond, under the local Langlands correspondence, to Weil-Deligne representations of $\mathbf{Q}_p$ which are irreducible.)

For $p \neq 2$, supercuspidal representations of G are known to be parametrised by "admissible pairs" (E, θ), where $E/\mathbf{Q}_p$ is a quadratic extension and $\theta : E^\times \to \mathbf{C}^\times$ is a smooth character (satisfying various mild conditions). Hence each such representation is determined by a finite amount of data, and one can ask: *given a form f, and an odd prime p such that $\Pi_{f,p}$ is supercuspidal, how do we calculate the corresponding pair (E, θ)?*

2. Our approach

One cannot hope to compute directly with the spaces $\Pi_{f,p}$, as they are infinite-dimensional. So in order to approach this problem, we needed to find a way to reformulate it solely in terms of finite, computable objects.

We reduce first to the case where the power of p dividing the the level of f is minimal among the set of twists of f by Dirichlet characters. Such forms are called *p-primitive* by Atkin and Li. It is clear that every form has a p-primitive twist, and there is a simple algorithm for finding such a twist.

Assuming that f is p-primitive and that $\Pi_{f,p}$ is supercuspidal, we use results of Casselman and Bushnell–Henniart to identify a finite-dimensional subspace $X_f \subseteq \Pi_{f,p}$, stable under a maximal compact-modulo-centre subgroup $K \subseteq G$, such that $\Pi_{f,p}$ is isomorphic to the compactly supported induction $\text{c-Ind}_K^G(X_f)$. We show that the space X_f (the *type space*) can be identified with the dual of a certain explicitly calculable space of modular symbols. The action of $K \cap \mathrm{SL}(2, \mathbf{Q}_p)$ on X_f can be calculated using the action of the Hecke algebra on modular symbols, and the action of the whole of K can be recovered by using the fact that the subgroup $\begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix}$ acts trivially on the new vector.

Having calculated X_f, we use a character formula which relates the admissible pair (E, θ) to the action of suitable elements of a maximal non-split torus in K on the space X_f. This allows us to identify E and the character θ (up to Galois conjugacy). These algorithms have been implemented in the computer algebra systems Sage and Magma, building on their existing implementations of modular symbols.

Heuristics on p-class towers of imaginary quadratic fields

Farshid Hajir
(joint work with Nigel Boston, Michael R. Bush)

Fix an odd prime p. For a number field K, let A_K be the p-Sylow subgroup of the ideal class group of K. Cohen and Lenstra [2] studied the frequency with which a given p-group occurs as A_K where K ranges over all imaginary quadratic fields, ordered according to the absolute value of discriminant. They showed that there is a probability measure on p-groups of fixed p-rank in which the measure of each group is inversely proportional to the size of its automorphism group. Positing that this measure is the frequency with which G occurs as A_K, they arrived at the following conjecture.

Conjecture 1 (Cohen-Lenstra)**.** *For a fixed positive integer g, among the imaginary quadratic fields K such that the p-rank of A_K is g, ordered by discriminant, the probability that A_K is isomorphic to $G = \mathbb{Z}/p^{r_1} \times \cdots \times \mathbb{Z}/p^{r_g}$ is*

$$\frac{1}{|\operatorname{Aut}(G)|} \cdot \frac{1}{p^{g^2}} \prod_{k=1}^{g} (p^g - p^{g-k})^2.$$

We extend the Cohen-Lenstra heuristic to a non-abelian setting by considering, for each imaginary quadratic field K, the pro-p fundamental group G_K of the ring of integers of K. Concretely, G_K is the Galois group of the p-class tower of K, i.e. $G_K := \mathrm{Gal}(K_\infty/K)$ where K_∞ is the maximal unramified p-extension of K. Note that, by class field theory, A_K is isomorphic to G_K^{ab}, the maximal abelian quotient of G_K.

Put $d(G) = \dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p), r(G) = \dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p)$ for the minimal number of generators and relations of a pro-p group G, respectively. Though the group G_K is rather mysterious for general number fields K, for imaginary quadratic K, it satisfies certain restrictive conditions, namely G_K is a Schur σ-group, in the terminology of Koch and Venkov [3]. We recall that a finitely generated pro-p group G is called a Schur σ-group of rank g if it satisfies the following properties: 1) $d(G) = r(G) = g$; 2) G^{ab} is finite; 3) There exists an element $\sigma \in \mathrm{Aut}(G)$ of order 2 acting as inversion on G^{ab}.

We establish that there is a natural Cohen-Lenstra measure in the category of Schur σ-groups. Our main heuristic assumption then is that for the sequence of p-class tower groups of imaginary quadratic fields, ordered by discriminant, or more generally for the sequence of maximal p-class c quotients of these p-class tower groups (where c is any fixed whole number), the frequency of any given group equals the measure of the group in a corresponding category of Schur σ-groups. Our main group-theoretical result is a computation of this measure, which then leads to the following conjecture.

Conjecture 2. *Suppose G is a finite p-group which is a Schur σ-group of generator rank $g \geq 1$ or, more generally, suppose c is a positive integer and G is the maximal p-class c quotient of a Schur σ-group of rank g. Then, among the imaginary quadratic fields K such that A_K has rank g, ordered by discriminant, the probability that G_K (or in the fixed p-class case, the maximal p-class c quotient of G_K) is isomorphic to G is equal to*

$$\frac{z(G)^g}{|\operatorname{Aut}(G)|} \cdot \frac{1}{p^{gh}} \prod_{k=1}^{g} (p^g - p^{g-k}) \prod_{k=1}^{h} (p^g - p^{h-k}),$$

where h is the difference between the p-multiplicator rank and nuclear rank of G (so $0 \leq h \leq g$ with $h = g$ for Schur σ-groups) and $z(G)$ is the number of fixed points of an automorphism σ acting as inversion on the abelianization of G.

The quantity $z(G)$ is independent of the choice of order 2 automorphism σ acting as inversion on G^{ab}; moreover, the ratio $z(G)^g/|\operatorname{Aut}(G)|$ can also be written as $1/|\operatorname{Aut}_\sigma(G)|$ where $\operatorname{Aut}_\sigma(G)$ is the subgroup of automorphisms which commute with σ. Comparing the form of Conjectures 1 and 2, we note that in the case of G being a Schur σ-group, for which we have $h = g$, the two predicted frequencies differ only in that $\mathrm{Aut}(G)$ is replaced by $\mathrm{Aut}_\sigma(G)$. Note that for abelian groups G, we have $z(G) = 1$, hence the two formulae match and indeed, suitably interpreted, Conjecture 2 generalizes Conjecture 1.

The numerical study of Conjecture 2 presents some interesting challenges, even in the simplest case of $p = 3, g = 2$ to which we limited our computations. Note that we do not even know an algorithm for determining whether G_K is finite, much less for computing it, and few examples have actually been completely worked out. One of the first examples of a computation of G_K in the literature appears in a 1934 article of Scholz and Taussky [4]: for the field $\mathbb{Q}(\sqrt{-4027})$, with $p = 3$, A_K is elementary abelian of rank 2 and the group G_K, of size 243, is isomorphic to the group denoted `SmallGroup(243,5)` in the terminology of the computer algebra software package `Magma`[1] which we used for all of our computations.

In order to test our heuristic hypothesis, we considered what kind of number-theoretical data (meaning about the groups G_K) was within reach and settled on the following: we computed the class groups of unramified extensions of K of degree 1 or p. In terms of group theory, this "index $\leq p$ abelianization data" or "IPAD," describes the abelianization of G_K as well as those of its index p subgroups. Though it is impractical at present to attempt the complete computation of G_K for all but a handful of fields K, it was possible for us to compute the IPADs of quite a few such p-class tower groups and to compare them to the group-theoretical prediction. Given the variability of the data and the general convergence trend toward the predicted value, we believe that, within the limitations of the computation, the data supports our conjecture. To cite one example, the group of largest measure among 3-groups which are Schur σ-groups of rank 2 is `SmallGroup(243,5)` and happens to be determined uniquely by its IPAD. Using our main theorem, we find its measure to be $128/729 \approx 0.1756$. For discriminants whose absolute values lie in the ranges $(0, 2 \cdot 10^5)$, $[2 \cdot 10^5, 4 \cdot 10^5)$, $[4 \cdot 10^5, 6 \cdot 10^5)$, $[6 \cdot 10^5, 8 \cdot 10^5)$, this group occurs as G_K with frequency approximately 21.07%, 21.87%, 17.50%, 17.27% for a cumulative total of 19.26%.

References

[1] W. Bosma, J. J. Cannon, C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput., **24** (1997), 235–265.

[2] H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups of number fields*, pp. 33–62 in: Number theory, Noordwijkerhout 1983, LNM **1068**, Springer, Berlin, 1984.

[3] H. Koch and B.B. Venkov, *Über den p-Klassenkörperturm eines imaginär-quadratischen Zahlkörpers*, Soc. Math. France, Astérisque **24-25** (1975), 57–67.

[4] A. Scholz and O. Taussky, *Die Hauptideale der kubischen Klassenkörper imaginär-quadratischer Zahlkörper*, J. Reine Angew. Math. **171** (1934), 19–41.

Cohen-Lenstra heuristics for groups of Lie type

Akshay Venkatesh

We discuss heuristics for the number of Galois representations of prescribed conductor and image along the lines of Cohen–Lenstra and Bhargava. We then report on Schaeffer's computations of weight 1 modular forms in characteristic p that do not lift to characteristic 0. The emphasis is on finding examples with "large" p.

Reporter: Michiel Kosters

Participants

Dr. Burcu Baran
Department of Mathematics
Stanford University
Stanford , CA 94305-2125
USA

Prof. Dr. Karim Belabas
Laboratoire d'Algorithmique Arithmetique
Universite Bordeaux I
351 cours de la Liberation
F-33405 Talence Cedex

Stephanie Belcher
Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn

Prof. Dr. Daniel J. Bernstein
Department of Computer Science
University of Illinois at Chicago
M/C 249, 322 SEO
851 S. Morgan Street
Chicago IL 60607-7045
USA

Prof. Dr. Manjul Bhargava
Department of Mathematics
Princeton University
Fine Hall
Washington Road
Princeton , NJ 08544
USA

Dr. Andrew Booker
Department of Mathematics
University of Bristol
University Walk
GB-Bristol BS8 1TW

Prof. Dr. Frank Calegari
Department of Mathematics
Lunt Hall
Northwestern University
2033 Sheridan Road
Evanston , IL 60208-2730
USA

Prof. Dr. Henri Cohen
Institut de Mathematiques de Bordeaux
Universite de Bordeaux I
351, cours de la Liberation
F-33405 Talence Cedex

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

Prof. Dr. Christophe Delaunay
Faculte des Sciences et Techniques
Laboratoire Mathematiques de Besancon
Universite de Franche-Comte
16, route de Gray
F-25030 Besancon Cedex

Prof. Dr. Tim Dokchitser
Dept. of Pure Mathematics and
Mathematical Statistics
University of Cambridge
Wilberforce Road
GB-Cambridge CB3 0WB

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

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

Dr. Tom A. Fisher
Centre for Mathematical Sciences
University of Cambridge
Wilberforce Road
GB-Cambridge CB3 0WB

Dr. Herbert Gangl
Dept. of Mathematical Sciences
Durham University
Science Laboratories
South Road
GB-Durham DH1 3LE

Prof. Dr. Alberto Gioia
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
NL-2300 RA Leiden

Prof. Dr. Paul E. Gunnells
Dept. of Mathematics & Statistics
University of Massachusetts
710 North Pleasant Street
Amherst , MA 01003-9305
USA

Prof. Dr. Farshid Hajir
Department of Mathematics
University of Massachusetts
Lederle Graduate Research Tower
710 North Pleasant Street
Amherst , MA 01003-9305
USA

Prof. Dr. Wei Ho
Department of Mathematics
Columbia University
2990 Broadway
New York , NY 10027
USA

Prof. Dr. Kiran S. Kedlaya
Department of Mathematics
MIT
77 Massachusetts Avenue
Cambridge , MA 02139-4307
USA

Prof. Dr. Kamal Khuri-Makdisi
Department of Mathematics
American University of Beirut
Riad El-Solh
P.O.Box 11-0236
Beirut 1107 2020
LEBANON

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

Prof. Dr. David R. Kohel
Institut de Mathematiques de Luminy
UMR 6206
Case 907
163 Avenue de Luminy
F-13288 Marseille

Anders Kolvraa
Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn

Michiel Kosters
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
NL-2300 RA Leiden

Prof. Dr. Emmanuel Kowalski
Departement Mathematik
ETH-Zentrum
Rämistr. 101
CH-8092 Zürich

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

Dr. David Loeffler
Mathematics Institute
University of Warwick
Gibbet Hill Road
GB-Coventry CV4 7AL

Dr. Anton Mellit
Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn

Prof. Dr. Jean-Francois Mestre
U. F. R. de Mathematiques
Case 7012
Universite Paris 7
2, Place Jussieu
F-75251 Paris Cedex 05

Dr. Pascal Molin
INRIA Lorraine
Technopole de Nancy-Brabois
615 rue de Jardin Botanique
F-54600 Villers-les-Nancy

Dr. Anna Morra
U. F. R. Mathematiques
I. R. M. A. R.
Universite de Rennes I
Campus de Beaulieu
F-35042 Rennes Cedex

Rachel Newton
Department of Pure Mathematics and
Mathematical Statistics
University of Cambridge
Wilberforce Road
GB-Cambridge CB3 0WB

Aurel Page
Departement de Mathematiques
Ecole Normale Superieure
45, rue d'Ulm
F-75230 Paris Cedex 05

Friedrich Panitz
FB 17: Mathematik/Informatik
Universität Paderborn
Warburger Str. 100
33098 Paderborn

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

Dr. Xavier-Francois Roblot
Department of Mathematics
Faculty of Science
Tokyo Institute of Technology
Ohokayama, Meguro-ku
Tokyo 152-8551
JAPAN

Prof. Dr. Fernando Rodriguez-Villegas
Department of Mathematics
The University of Texas at Austin
1 University Station C1200
Austin , TX 78712-1082
USA

Dr. Mehmet Haluk Sengun
Facultat de Matematiques
Universitat de Barcelona
Departament d'Algebra i Geometria
Gran Via 585
E-08007 Barcelona

Prof. Dr. Jean-Pierre Serre
6, Avenue de Montespan
F-75116 Paris

Arul Shankar
Department of Mathematics
Princeton University
609 Fine Hall
Washington Road
Princeton , NJ 08544
USA

Prof. Dr. Samir Siksek
Department of Mathematics
University of Warwick
GB-Coventry CV4 7AL

Dr. Bart de Smit
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
NL-2300 RA Leiden

Prof. Dr. Peter Stevenhagen
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
NL-2300 RA Leiden

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

Dr. Lenny Taelman
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
NL-2300 RA Leiden

Takashi Taniguchi
Graduate School of Science
and Technology
Kobe University
Rokko-dai 1-1, Nada-ku
Kobe 657-8501
JAPAN

Dr. Rebecca Torrey
Mathematics Department
Mount Holyoke College
South Hadley , MA 01075
USA

Prof. Dr. Akshay Venkatesh
Department of Mathematics
Stanford University
Stanford , CA 94305-2125
USA

Masha Vlasenko
Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn

Dr. John Voight
Department of Mathematics
University of Vermont
16 Colchester Ave.
Burlington VT 05405-3357
USA

Dr. Mark J. Watkins
MAGMA Computer Algebra Group
School of Mathematics & Statistics
F07
University of Sydney
Sydney NSW 2006
AUSTRALIA

Prof. Dr. Gabor Wiese
Institut f. Experimentelle Mathematik
Universität Duisburg-Essen
Standort Essen
Ellernstr. 29
45326 Essen

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

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

Prof. Dr. Wadim Zudilin
School of Mathematical and Physical Sciences
University of Newcastle
Callaghan NSW 2308
AUSTRALIA