Mathematisches Forschungsinstitut Oberwolfach

Report No. 35/2013

DOI: 10.4171/OWR/2013/35

Explicit Methods in Number Theory

Organised by
Karim Belabas (Talence)
Bjorn Poonen (MIT)
Don B. Zagier (Bonn)

July 14th – July 20th, 2013

Abstract. These notes contain extended abstracts on the topic of explicit methods in number theory. The range of topics includes effectiveness in rational points on curves and especially on modular curves, modularity, L-functions, and many other topics.

Mathematics Subject Classification (2010): 11-xx, 12-xx, 13-xx, 14-xx.

Introduction by the Organisers

The workshop Explicit Methods in Number Theory was organised by Karim Belabas (Talence), Bjorn Poonen (MIT), and Don B. Zagier (Bonn), and it took place July 14–20, 2013. Seven previous workshops on the topic had been held every 2 years since 1999. 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 two hours highlighting important recent developments: by Bilu, Parent and Rebolledo, on their partial solution to Serre's uniformity problem, and by Villegas on Hypergeometric Motives and their L-functions.

In addition to the lectures, a hike was organised on Wednesday afternoon. Participants walked to St Roman, where they had a drink and enjoyed a share of Black Forest cake. After that they walked back to the institute, and arrived just in time for a truly excellent barbecue.

As always in Oberwolfach, the atmosphere was lively and active, providing an ideal environment for the exchange of ideas and productive discussions. The

meeting was well-attended, with 53 participants from a variety of backgrounds, including some young researchers with an OWLG-grant. There were 24 talks of various lengths, and ample time was allotted to informal collaboration. Moreover, the quality of the food served at the institute was praised by the participants.

Workshop: Explicit Methods in Number Theory

Table of Contents

Abstracts

Hypergeometric Motives

Fernando Rodriguez Villegas

These talks were a report on ongoing work to compute explicitly the L-function of hypergeometric motives. Ultimately the goal is to use these L-functions, which cover a very wide range of possible parameters (degrees, Hodge numbers, etc.), to test conjectures on special values and the distribution of zeros, while simultaneously verifying numerically standard conjectures on analytic continuation and functional equations for these L-functions.

The people currently involved in this project are:

B. Allombert, F. Beukers, H. Cohen, A. Mellit, P. Molin, D. Roberts, F. Rodriguez Villegas, M. Vlasenko, M. Watkins.

A hypergeometric motive is determined by the following hypergeometric data: $\alpha, \beta \subseteq \mathbb{Q}/\mathbb{Z}$ two disjoint multisets of same size d. This data determines a family of motives

$$\mathcal{H}(\alpha;\beta\,|\,t) \quad \text{for} \quad t \in \mathbb{P}^1 \setminus \{0,1,\infty\}\,,$$

over a cyclotomic field K, of rank d and pure weight w.

Let m be the least common denominator of α, β. The field $K \subseteq \mathbb{Q}(\mu_m)$ is the fixed field of the Galois automorphisms $\zeta_m \mapsto \zeta_m^a$ for integers a such that $\gcd(a,m) = 1$ and $a\alpha = \alpha, a\beta = \beta$. The weight w equals the multiplicity of 0 in $\alpha \cup \beta$ minus one.

The classical incarnation of $\mathcal{H}(\alpha;\beta\,|\,t)$ is given by a hypergeometric differential equation with parameters $\tilde{\alpha}_1, \ldots, \tilde{\alpha}_d; \tilde{\beta}_1, \ldots, \tilde{\beta}_d \in \mathbb{Q}$ representing the elements of α and β respectively. Concretely, let $\theta := t\dfrac{d}{dt}$ and consider the linear differential operator

$$L := (\theta - 1 + \tilde{\beta}_1)\cdots(\theta - 1 + \tilde{\beta}_d) - t(\theta + \tilde{\alpha}_1)\cdots(\theta + \tilde{\alpha}_d)\,.$$

It has regular singularities at $t = 0,\ 1,\ \infty$. Let V be the space of local solutions to $L = 0$ around some fixed regular point. We obtain a monodromy representation by analytic continuation of solutions

$$\rho: \quad \pi_1(\mathbb{P}^1 \setminus \{0,1,\infty\}) \mapsto \mathrm{GL}(V)\,.$$

Our assumption that α and β are disjoint guarantees that ρ is irreducible. The image of small loops around the excluded points give local monodromies h_0, h_1, $h_\infty \in \mathrm{GL}(V)$ satisfying $h_0 h_1 h_\infty = id_V$. The characteristic polynomials of h_∞ and h_0^{-1} are respectively

$$q_\infty := \prod_{j=1}^{d}(T - e^{2\pi i\tilde{\alpha}_j}), \qquad q_0 := \prod_{j=1}^{d}(T - e^{2\pi i\tilde{\beta}_j})$$

depending only on α, β. The local monodromy h_1 fixes a codimension one subspace of V. Levelt proved that ρ is uniquely determined up to isomorphism by the conjugacy classes of the local monodromies. In other words, the data α, β determines a rigid local system.

The rigidity implies, somewhat tautologically, that all features of the motive $\mathcal{H}(\alpha; \beta \,|\, t)$ are uniquely determined by the hypergeometric data α, β and the choice of parameter t. Our goal is to make this as explicit as possible.

Concretely, assume to simplify that $K = \mathbb{Q}$ and pick $t \in \mathbb{P}^1(\mathbb{Q}) \setminus \{0, 1, \infty\}$. This yields a motive $\mathcal{H}(\alpha; \beta \,|\, t)$ defined over $\mathbb{Q}$. We would like to compute numerically its complete L-function. I will briefly discuss each of the various aspects of what this entails.

- **Gamma factors**
  The gamma factors of the L-function are derived from the Hodge numbers of the motive and the action of complex conjugation by a well-known recipe. These Hodge numbers can be computed combinatorially in terms of the relative position of representatives of α_i and β_j in the interval $[0, 1]$. The resulting recipe has been proved by Corti and Golyshev for the case where the motive can be described by means of toric geometry. The action of complex conjugation depends on which interval $(-\infty, 0), (0, 1)$ or $(1, \infty)$ contains t.

- **Good primes**
  If p is a prime not diving m, t, t^{-1} or $t - 1$ then $\mathcal{H}(\alpha; \beta \,|\, t)$ has good reduction at p and the trace of Frobenius in $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ acting on it can be computed using a hypergeometric sum defined by Katz. This sum has the form
  $$\frac{1}{1-q} \sum_{\chi} \frac{J(\alpha\chi, \beta\chi)}{J(\beta, \alpha)} \chi(t),$$
  where the sum is over all characters of $\mathbb{F}_q^\times$ and $J(\alpha\chi, \beta\chi)$ are certain Jacobi sums built out of the hypergeometric data α, β. Using the Gross-Koblitz formula these sums can be evaluated p-adically in a quite efficient way.

- **Tame primes** If p is a prime not diving m but dividing t, t^{-1} or $t - 1$ then $\mathcal{H}(\alpha; \beta \,|\, t)$ is at worst tamely ramified at p. Suppose p divides t for example. Then the Euler factor of the L-function of the motive at p is given by certain Hecke characters depending on the decomposition $t = t_0 p^k$. These characters are precisely of the form $J(\alpha\chi, \beta\chi)/J(\beta, \alpha)$ for certain χ's. The resulting expression of the Euler factor matches a combinatorial description of the degeneration of the mixed Hodge structure at $t = 0$ refining the calculation of Hodge numbers mentioned above. The case of p dividing t^{-1} corresponding to $t = \infty$ is completely analogous. For primes p dividing $t-1$ Katz's hypergeometric sum still yields the trace of Frobenius and can be used to computed the Euler factor.

- **Wild primes** If p is a prime diving m then typically the motive $\mathcal{H}(\alpha; \beta \,|\, t)$ is wildly ramified at p. Computation of the corresponding Euler factor and

the exponent of p in the conductor is more challenging. At the moment we have a conjectural upper bound for the exponent and we have made significant progress in understanding its behavior in terms of the decompositions of the type $t = t_0 p^k$ at $t = 0$ mentioned above.

Much of our knowledge of hypergeometric motives comes from a constant back and forth between experimentation and theory. The main computational tool we use to gauge hypotheses on missing information of a particular L-function is to test for the validity of the appropriate functional equation. Several sophisticated computational methods were specifically devised and implemented for this purpose.

M. Watkins has written a package for MAGMA to compute the L-function of hypergeometric motives that incorporates our current knowledge on the subject.

Rational points on modular curves (I, II, III)

Yu. Bilu, P. Parent, M. Rebolledo

Let X_G be the modular curve of level N corresponding to a subgroup G of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ with $\det G = (\mathbb{Z}/N\mathbb{Z})^\times$. Then X_G has a standard geometrically irreducible model over $\mathbb{Q}$. We are interested in the following problem:

Problem 1. *Describe the set of rational points $X_G(\mathbb{Q})$.*

This statement is somewhat vague: what does "describe" mean?

First of all, we restrict to the three cases that we deem most interesting for applications, and which accumulate all the principal difficulties presented by the problem. These are the cases when $N = p$ is a prime number and G is one of the following maximal subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$:

- a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$;
- the normalizer of a split Cartan subgroup;
- the normalizer of a non-split Cartan subgroup.

The corresponding modular curves are denoted $X_0(p)$, $X^+_{\mathrm{sp}}(p)$ and $X^+_{\mathrm{ns}}(p)$, respectively.

Next, recall that if $E/\mathbb{Q}$ is an elliptic curve with complex multiplication and $\mathcal{O} = \mathrm{End}(E)$ then E gives rise to a rational point on one of the curves $X_0(p)$, $X^+_{\mathrm{sp}}(p)$ or $X^+_{\mathrm{ns}}(p)$, depending on whether the prime p is ramified, split or inert in the order $\mathcal{O}$. Rational points obtained this way are called *CM-points*.

We can now state a more precise problem:

Problem 2. *Show that for $p > 37$ there is no rational points on the curves $X_0(p)$, $X^+_{\mathrm{sp}}(p)$ and $X^+_{\mathrm{ns}}(p)$ other than the cusps and the CM-points.*

For $X_0(p)$ the problem was solved in the classical work of Mazur [5]. Recently, in [3], we solved it for the curves $X^+_{\mathrm{sp}}(p)$.

Theorem 3. *For $p \geq 17$ and $p = 11$, the set $X^+_{\mathrm{sp}}(p)$ has no points besides the cusps and the CM-points.*

The result of Mazur and our result apply to Serre's celebrated "uniformity problem" on surjectivity of Galois representations. Let p be a prime number and $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. Serre proved that the associated Galois representation $\rho_{E,p} : \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ is surjective for $p > p_0(E)$. He asked whether this can be made uniform in E:

Problem 4 (Serre's uniformity problem)**.** *Does it exist a positive number p_0 such that for every $E/\mathbb{Q}$ without CM and every $p > p_0$ the Galois representation $\rho_{E,p}$ is surjective?*

Solution of Problem 2 implies the positive answer with $p_0 = 37$.

The proof of Theorem 3 splits into several rather independent ingredients.

(1) (integrality) If P is a non-cuspidal rational point then $j(P) \in \mathbb{Z}$.
(2) (upper bound) If $j(P) \in \mathbb{Z}$ then $\log|j(P)| \leq 10\sqrt{p}$.
(3) (lower bound) If P is not a CM-point then $\log|j(P)| \geq 10^{-4}p$.
The previous items imply that the statement holds true for $p \geq 10^8$.
(4) (small p) The statement holds true for $p = 11$ and for $17 \leq p \leq 10^{14}$.

Item 1 follows from the results of Mazur, Momose and Merel and is obtained by Mazur's method. Item 2 is proved using Runge's method. Item 3 follows from the modern isogeny estimates (Masser-Wüstholz, Pellarin, Gaudron and Rémond). Item 4 is based on Mazur's strategy and computations using Gross vectors.

In our mini-course of three lectures, we briefly explained the proof of Theorem 3, focusing on steps 1, 2 and 4.

References

[1] Yu. Bilu, P. Parent, Serre's uniformity problem in the split Cartan case, *Ann. Math. (2)*, **173** (2011), 569–584; `arXiv:0807.4954`.

[2] Yu. Bilu, P. Parent, Runge's method and modular curves, *Int. Math. Research Notices* **2011** (2011) 1997–2027; `arXiv:0907.3306`.

[3] Yu. Bilu, P. Parent, M. Rebolledo,Rational points on $X_0^+(p^r)$, *Ann. Inst. Fourier*, to appear. `arXiv:0907.3306`.

[4] É. Gaudron, G. Rémond, Théorème des périodes et degrés minimaux d'isogénies, *Annales ENS*, to appear.

[5] B. Mazur, Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.* **44** (1978), 129–162.

[6] L. Merel, Sur la nature non-cyclotomique des points d'ordre fini des courbes elliptiques, avec un appendice de E. Kowalski et Ph. Michel, *Duke Math. J.* **110** (2001), 81-119.

[7] L. Merel, Normalizers of split Cartan subgroups and supersingular elliptic curves, in "Diophantine Geometry" (edited by U. Zannier), pp. 237–255; CRM Series **4**, Edizioni della Normale, Pisa, 2007.

[8] F. Momose, Rational points on the modular curves $X_{\mathrm{split}}(p)$, *Compositio Math.* **52** (1984), 115–137.

[9] F. Momose, Rational points on the modular curves $X_0^+(p^r)$, J. Fac. Sci. Univ. Tokyo, Sect. IA, Math. **33** (1986), 441-446.

[10] P. Parent, Towards the triviality of $X_0^+(p^r)(\mathbb{Q})$ for $r > 1$, *Compositio Math.* **141** (2005), 561–572.

[11] F. Pellarin, Sur une majoration explicite pour un degré d'isogénie liant deux courbes elliptiques, *Acta Arith.* **100** (2001), 203–243.

[12] M. Rebolledo, Module supersingulier, formule de Gross-Kudla et points rationnels de courbes modulaires, *Pacific J. Math.* **234** (2008), 167–184.

Bad reduction for curves

Tim Dokchitser
(joint work with Vladimir Dokchitser)

Associated to a curve $C/\mathbb{Q}$ is its L-function

$$L(C,s) = \sum_{n\geq 1} \frac{a_n}{n^s} = \prod_p \frac{1}{F_p(p^{-s})}.$$

The question we would like to address is how to compute the local factors $F_p(T)$ for primes p of bad reduction, and other related invariants such as the conductor and the root number. There are traditionally two approaches to this:

One is to compute the regular model $\mathcal{C}/\mathbb{Z}_p$. Say its special fibre is a $\bar{C}/\mathbb{F}_p$, and write I_p for the inertia group of $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$. Provided the multiplicities of the components of $\bar{C}$ have gcd 1, there is a comparison theorem on étale cohomology,

$$H^1(C)^{I_p} = H^1(\bar{C}),$$

which reduces the problem of determining the local factor $F_p(T)$ (characteristic polynomial of Frobenius on the left-hand side) to counting points on $\bar{C}$. This is the approach that is currently implemented in Magma, but the regular models are quite difficult to compute sometimes, their classification is rather complicated, and they do not give information about other invariants of the L-function, such as the conductor.

Another approach, which is the one that we take, is using the semistable model. Take a Galois extension $K/\mathbb{Q}_p$ where C acquires semistable reduction. Then

$$H^1(C)^{I_p} = H^1(\bar{C}/I_p),$$

where $\bar{C}$ is the special fibre of a semistable model; I_p acts naturally on it (at least if the semistable model is minimal or 'sufficiently canonical'), through a finite quotient. It acts by geometric transformations and $\bar{C}/I_p$ is the geometric quotient.

It appears that the second approach is neater from the classification point of view, well suited for computations and gives the whole l-adic representation of the Jacobian of C, not just the local factor. (This relies on a theorem that every semisimple Weil representation is determined by its local factors over the extensions over the ground field.) It seems particularly well-suited to hyperelliptic curves in odd residue characteristic, and this is the case that we are working out first. This relies on the results of Grothendieck, Bosch, and a recent paper by Bouw and Wewers.

Uniform bounds for the number of rational points on hyperelliptic curves with small Mordell-Weil rank

Michael Stoll

We sketch a proof of the following result.

Theorem A. *Let $d \geq 1$ and $g \geq 3$ be integers. There is a constant $R(d,g)$ depending only on d and g such that whenever K is a number field of degree at most d, C is a hyperelliptic curve over K of genus g with Jacobian J, and the rank of $J(K)$ is at most $g-3$, then*

$$\#C(K) \leq R(d,g)\,.$$

We remark that the fact that the curve is hyperelliptic is only used in one step in the proof. It appears likely that the relevant result holds in fact for all curves, so that one should be able to remove the condition at some point.

Theorem A is an immediate consequence of the following.

Theorem B. *Let k be a p-adic field with p odd and let $g \geq 3$ be an integer. Then there is a constant $N(k,g)$ depending only on the field k and on g such that whenever C is a hyperelliptic curve over k of genus g with Jacobian J, $P_0 \in C(k)$, and $\Gamma \subset J(k)$ is a subgroup of rank at most $g-3$, then*

$$\#\{P \in C(k) : [P - P_0] \in \Gamma\} \leq N(k,g)\,.$$

To see that Theorem B implies Theorem A, fix some odd prime p. Up to isomorphism, there are only finitely many p-adic fields k of degree at most d over $\mathbb{Q}_p$. Let $R(d,g)$ be the maximum of the $N(k,g)$ for these fields k. If $C(K) = \emptyset$, there is nothing to prove. Otherwise we can take $P_0 \in C(K)$ and apply Theorem B with k a completion of K at a place above p and $\Gamma = J(K)$. Then

$$C(K) \subseteq \{P \in C(k) : [P - P_0] \in \Gamma\}$$

and therefore

$$\#C(K) \leq \#\{P \in C(k) : [P - P_0] \in \Gamma\} \leq N(k,g) \leq R(d,g)\,.$$

For the proof of Theorem B, we can assume in addition that C has (split) semistable reduction over k, since we can achieve this after making a field extension of degree bounded in terms of p and g only, for which there are only finitely many possibilities.

Under this additional assumption, we can cover $C(k)$ by a collection of $\ll qg$ residue disks (where q is the size of the residue class field κ of k) and $\ll g$ residue annuli. The latter correspond to maximal chains of (-2)-curves in the special fiber of the (semistable) minimal proper regular model of C over the ring of integers of k: the k-points of such an annulus are exactly the points in $C(k)$ whose reduction is a smooth κ-point on one of the components of the chain. The residue disks correspond in the same way to smooth κ-points on the remaining components.

A standard application of the Chabauty-Coleman method (see for example [1]) shows that the total number of points in $C(k)$ mapping into Γ that are contained

in one of the residue disks is $\ll qg$. (This bound is even valid for rank $\leq g-1$). The main new ingredient is a bound on the corresponding number for a residue annulus. Fixing such an annulus, we can show that the number of k-points in the annulus mapping into Γ is $\ll g$, provided the rank of Γ is at most $g-3$.

The bound is obtained by considering the zeros in the annulus of a suitable integral function associated to a regular differential ω on C. If ω satisfies up to two linear constraints (depending on the annulus), then this function can be expressed on the annulus as a converging Laurent series. A consideration of Newton polygons then leads to the bound. It is at this point that we need a condition on the location of the 'relevant part' of this Newton polygon. This condition can be shown to hold for hyperelliptic curves and p odd by explicit computation, but should also hold for general curves.

In total, we obtain a bound of the form $O(qg+g^2)$ for the number of k-points mapping into Γ. Note that we have assumed semistable reduction to simplify the argument. We expect, however, that a bound of the same general shape will be valid without assumptions on the reduction.

For details, see the arXiv preprint [2].

References

[1] M. Stoll, *Independence of rational points on twists of a given curve*, Compos. Math. **142**:5 (2006), 1201–1214.

[2] M. Stoll, *Uniform bounds for the number of rational points on hyperelliptic curves with small Mordell-Weil rank*, Preprint (2013), arXiv:1307.1773 [math.NT].

On the discrete logarithm problem for curves over extension fields

Claus Diem

We consider the discrete logarithm problem in the degree 0 class groups of curves of a fixed genus over finite fields of the form $\mathbb{F}_{q^n}$ for growing q and n. Here and in the following, q is always a prime power and n a natural number.

An important special case of this problem is the discrete logarithm problem in the groups of rational points of elliptic curves over fields $\mathbb{F}_{q^n}$ with growing q and n. In [1] and [2] I have addressed this problem. The main result of the work [2] is the following theorem on this problem.

Theorem. *The indicated problem can be solved in an expected time of*

$$e^{O(\max(\log(q),n\cdot(\log(q))^{1/2},n^{3/2}))}\,.$$

More precisely, the algorithm is randomized, and for each instance the expected running time with respect to the internal randomizations of the algorithm is taken.

The theorem has the following corollaries.

1. Let $a < b \in \mathbb{R}_{>0}$ be fixed. Then restricted to instances with
$$a \log(q)^{1/2} \leq n \leq b \log(q)^{1/2}$$
the problem can be solved in an expected time of
$$e^{O(\log(q^n)^{2/3})} .$$
2. Let $a, b \in \mathbb{R}_{>0}$ be fixed. Then restricted to instances with
$$a \log(q)^{1/3} \leq n \leq b \log(q)$$
the problem can be solved in an expected time of
$$e^{O(\log(q^n)^{3/4})} .$$

Various other results of similar type can be derived from the Theorem.

Currently, I am working on a generalization of the Theorem. The goal is to prove the statement in the Theorem for curves of an arbitrary but fixed genus.

The algorithm follows the usual index calculus or relation generation and linear algebra method. The essential steps are:

- Definition of a factor base,
- generation of relations between the input elements and the factor base elements,
- a linear algebra operation to obtain a single relation just between the input elements.

The *factor base* is defined in an algebraic way:

Let the input curve $\mathcal{C}$ be birationally defined by an equation $f(x, y) = 0$. Then for an appropriately chosen natural number $m \leq n$ the factor base is defined as follows:

An appropriate decomposition of $\mathbb{F}_{q^n}$ as $\mathbb{F}_q$-vector spaces
$$K = \bigoplus_{j=1}^{m} U_j$$
with $\dim(U_i) \approx \frac{n}{m}$ is chosen. Then for appropriate $a_1, \ldots, a_g \in \mathbb{F}_{q^n}$ and
$$\mathcal{F}_{i,j} := \{P \in \mathcal{C}(\mathbb{F}_{q^n}) \ : \ x(P) \in U_j + a_i\}$$
the factor base is
$$\mathcal{F} := \bigcup_{i,j} \mathcal{F}_{i,j} .$$

The *relation generation* is based on an algorithm for a "decomposition problem" which can roughly be stated as follows.

Given the data as above and $c \in \mathrm{Cl}^0(\mathcal{C})$, output a tuple $(P_{i,j})_{i,j} \in \prod_{i,j} \mathcal{F}_{i,j}$ with
$$c = \sum_{i=1}^{g} \sum_{j=1}^{m} F_{i,j}$$

or "failure".

The corresponding algorithm relies on solving multivariate systems of polynomial equations over $\mathbb{F}_q$. Here one uses an algorithm which outputs all isolated rational solutions of a given multivariate polynomial system (i.e. all isolated rational points of the scheme defined by the system). Such an algorithm is given in [3].

Under suitable heuristic assumptions one obtains rather easily an expected running time of

$$e^{O(\max(\log(q),n(\log(q))^{1/2})} . \tag{1}$$

To establish the theorem one has to show that this estimate does indeed hold under the condition that $n \leq C \cdot \log(q)$ for some constant $C > 0$. If then an instance is given for which the estimate is not satisfied, one enlarges q appropriately. For this in turn one has to show that under the given condition for uniformly randomly distributed $c \in \mathrm{Cl}^0(\mathcal{C})$ the probability that the corresponding polynomial system has an isolated solution is large enough.

The proof shall rely on a geometric description of the factor base by subschemes of the Weil restriction of the curve $\mathcal{C}$ and its Jacobian with respect to $\mathbb{F}_{q^n}|\mathbb{F}_q$. As mentioned the proof has been completed for elliptic curves but is work in progress for curves of higher genus.

Finally, I mention two open problems:

Problem 1. The problem consists in showing that the heuristic expected time given in (1) can be achieved for larger input classes of elliptic curves or maybe even curves of any fixed genus. For this the condition that $n \leq C \cdot \log(q)$ for an appropriate constant $C > 0$ in the analysis of the algorithm in [2] should be weakened or removed.

Problem 2. For the relation generation one needs a small generating system of the degree 0 class group. Now, for curves of a fixed genus, one can first compute the L-polynomial and from this the group order (as $L(1)$) in polynomial time by the algorithm of Schoof-Pila. One can then compute in polynomially bounded expected time a uniformly randomly distributed element of the group, and given this, one can easily obtain a polynomial time algorithm which outputs a "potential generating system" which is a generating system with probability at least a half. However, for curves of any fixed genus larger than 1, no efficient algorithm is known which outputs a generating system with certainty, so it is an open problem to obtain such an algorithm.

For our application, there is however an easy way around: One can use the "potential generating system" and then stop and repeat the whole computation if a predefined time bound has been reached.

References

[1] C. Diem, *On the discrete logarithm problem in elliptic curves*, Compositio Mathematica **147** (2012), 75–104.

[2] C. Diem, *On the discrete logarithm problem in elliptic curves II*, accepted at Algebra and Number Theory.
[3] M. Rojas, *Solving degenerate sparse polynomial systems faster*, Journal of Symbolic Computation **28** (1999), 155-186

Determinantal differential operators with Frobenius structure

Masha Vlasenko

For rational parameters $\alpha_1, \alpha_0, \beta$ a power-series solution $u(t) = \sum_{n=0}^{\infty} u_n t^n$ to the differential equation

$$f(t)\frac{d^2u}{dt^2} + f'(t)\frac{du}{dt} + (t+\beta)u = 0 \quad \text{where} \quad f(t) = t^3 + \alpha_1 t^2 + \alpha_0 t \tag{1}$$

will not generically have integral coefficients because the recurrence satisfied by those coefficients

$$u_0 = 1$$
$$\alpha_0(n+1)^2 u_{n+1} + (\alpha_1 n^2 + \alpha_1 n + \beta)u_n + n^2 u_{n-1} = 0$$

involves division by $\alpha_0(n+1)^2$ at every step, so that one would expect growing denominators. However there are examples, like

$$\alpha_1 = 11\,,\ \alpha_0 = -1\,,\ \beta = 3\,,$$

when we have $u(t) \in \mathbb{Z}[[t]]$. In [Zagier09] the list of such $(\alpha_1, \alpha_0, \beta)$ was compiled by doing a computer search through a large domain of triples. Restricting to the non-degenerate case, that is when the polynomial $f(t)$ has three different roots ($\alpha_0 \neq 0$, $\alpha_1^2 \neq 4\alpha_0$), only 7 examples with $u(t) \in \mathbb{Z}[[t]]$ were found (modulo obvious linear change of variable), and Zagier conjectures that this list is complete.

Recently Vasily Golyshev and the autor studied the same question for the differential equation with 5 parameters

$$f(t)\frac{d^3u}{dt^3} + \frac{3}{2}f'(t)\frac{d^2u}{dt^2} + \Big(\frac{1}{2}f''(t) + g(t)\Big)\frac{du}{dt} + \frac{1}{2}g'(t)u = 0$$
$$\text{where} \quad f(t) = t^2 + \alpha_3 t^3 + \alpha_2 t^4 + \alpha_1 t^5 + \alpha_0 t^6 \tag{2}$$
$$g(t) = 3\alpha_0 t^4 + 2\alpha_1 t^3 + \alpha_2 t^2 + \beta t$$

Equations (1) and (2) are the cases of orders 2 and 3 respectively of so called determinantal differential equations introduced by Golyshev and Stienstra in [GS07]. Equation (2) with $\alpha_3 = -34, \alpha_2 = 1, \alpha_1 = \alpha_0 = 0, \beta = -10$ corresponds to the famous Apéry recurrence

$$(n+1)^3 u_{n+1} = (34n^3 + 51n^2 + 27n + 5)u_n - n^3 u_{n-1}\,,$$

whose integral solution was used in the proof of irrationality of $\zeta(3)$. In [GV12] we give complete lists of non-degenerate equations (1) and (2) with $u(t) \in \mathbb{Z}[[t]]$ which satisfy certain additional assumptions. In the case of (1) our list coincides with Zagier's list.

Integrality of the coefficients is a strong property which suggests that the respective differential operators are the Picard-Fuchs operators related to certain families of algebraic varieties (see e.g. [Chudnovsky87]). And indeed, we can explicitly relate our operators with one-parametric families of hypersurfaces, which in the case of (1) are families of elliptic curves with semi-stable reduction (see [Zagier09]). For example, the Apéry sequence $\{u_n; n \geq 0\}$ which arises from (1) with $\alpha_1 = 11, \alpha_0 = -1, \beta = 3$ can be written as

$$u_n \;=\; \text{the constant term of} \Lambda(x,y)^n$$
$$\Lambda(x,y) = \Big(1+\frac{1}{x}\Big)\Big(1+\frac{1}{y}\Big)\big(1+x+y\big)\,,$$

and (1) is the Picard-Fuchs operator of the family given by $t\Lambda(x,y) = 1$. Therefore this sequence satisfies strong congruences modulo prime powers:

Theorem 1 ([MV13]). *Let $\Lambda(x) \in \mathbb{Z}_p[x_1^{\pm 1}, \ldots, x_d^{\pm 1}]$ be a Laurent polynomial, and consider the sequence of the constant terms of powers of Λ*

$$u_n \;=\; \Big[\Lambda(x)^n\Big]_0\,, \quad n = 0, 1, 2, \ldots$$

Define

$$u(t) \;=\; \sum_{n=0}^{\infty} u_n t^n$$

and

$$u_s(t) \;=\; \sum_{n=0}^{p^s-1} u_n t^n\,, \quad s = 0, 1, 2, \ldots$$

If the Newton polyhedron of Λ contains the origin as its only interior integral point, then for every $s \geq 1$ one has the congruence

$$\frac{u(t)}{u(t^p)} \;\equiv\; \frac{u_s(t)}{u_{s-1}(t^p)} \mod p^s \mathbb{Z}_p[[t]]\,,$$

or, equivalently, for every $s \geq 1$

$$u_{s+1}(t)u_{s-1}(t^p) \;\equiv\; u_s(t)u_s(t^p) \mod p^s \mathbb{Z}_p[t]\,.$$

This result states explicit p-adic approximation of $u(t)/u(t^p)$ by rational functions and allows one to apply to the families $t\Lambda(x) = 1$ Dwork's methods (see [Katz71, Kedlaya10] in general, and [MV13] for the discussion of our case).

References

[Zagier09] D. Zagier, *Integral solutions of Apéry-like recurrence equations,* CRM Proceedings and Lecture Notes 47, pp. 349–366 (2009).

[GS07] V. Golyshev, J. Stienstra, *Fuchsian equations of type DN*, Commun. Number Theory Phys. 1 (2007), no. 2, pp. 323–346

[GV12] V. Golyshev, M. Vlasenko, *Equations D3 and spectral elliptic curves*, arXiv:1212.0205

[Chudnovsky87] D. V. Chudnovsky, G. V. Chudnovsky, *Transcendental methods and theta-functions.* Theta functions – Bowdoin 1987, Proc. Sympos. Pure Math., 49, Part 2, pp. 167–232

[Katz71] N.Katz, *Traveaux de Dwork*, Séminaire N. Bourbaki, 1971-1972, exp. no. 409, pp. 167–200

[Kedlaya10] K.Kedlaya, *p-adic differential equations*, Cambridge University Press, 2010, 380 p.

[MV13] A. Mellit, M. Vlasenko, *Dwork's congruences for the constant terms of powers of a Laurent polynomial*, arxiv:1306.5811

Explicit high ranks for Jacobians over function fields

Douglas Ulmer

(joint work with L. Berger, C. Hall, R. Pannekoek, J. Park, R. Pries, S. Sharif, A. Silverberg)

Let p be a prime number, let $F = \mathbb{F}_p(t)$ be the rational function field over the field of p elements, and let $r > 0$ be an integer not divisible by p. Let C be the smooth, projective curve over $\mathbb{F}_p(t)$ associated to the plane curve

$$y^r = x^{r-1}(x+1)(x+t).$$

The genus of C is $r-1$. Let Q_∞ be the unique point at infinity on C. We imbed C in its Jacobian $J = \mathrm{Jac}(C)$ by sending P to the class of $P - Q_\infty$ and we identify C with its image in J.

For this example and many others, we know (by the methods of [Ulm13] and [Ulm07]) that (i) the BSD conjecture holds for J over the extensions $\mathbb{F}_q(t^{1/d})$ for all powers q of p and all positive integers d; and (ii) the rank of $J(\mathbb{F}_p(t^{1/d}))$ is unbounded as d varies. Our aim in this project is to make high ranks explicit by exhibiting divisors generating a large rank, finite index subgroup of $J(K)$ for certain extensions K of $F = \mathbb{F}_p(t)$. Most of the results below were proven earlier in the case $r = 2$ in [Ulm10].

For the rest of the talk we assume:

$$d = p^f + 1, \qquad r|d, \quad \text{and} \quad K = \mathbb{F}_p(\mu_d, u) \text{ with } u^d = t,$$

and we fix a primitive d-th root of unity ζ_d and write $\zeta_r = \zeta_d^{d/r}$.

Over K, we have a rational point on C:

$$P_{0,0} = \left(u, u(u+1)^{d/r}\right)$$

and a corresponding class in $J(K)$. Using the Galois group of K over F and the automorphism group of C, we get points

$$P_{i,j} = \left(\zeta_d^i u, \zeta_r^j \zeta_d^i u(\zeta_d^i u + 1)^{d/r}\right)$$

indexed by $i \in \mathbb{Z}/d\mathbb{Z}$ and $j \in \mathbb{Z}/r\mathbb{Z}$.

Theorem 1. *Let $V \subset J(K)$ be the subgroup generated by the divisors $P_{i,j}$. Then the rank of V is $(r-1)(d-2)$ and the index of V in $J(K)$ is finite.*

The most interesting point in the theorem is the lower bound on the rank, and the best way to prove this is to compute height pairings. These are related to intersection pairings on a model of C over $\mathbb{P}^1$ (the curve whose function field is K). Writing $\langle , \rangle$ for the canonical height pairing without the factor $\log q$, we find that $\langle P_{i,j}, P_{i',j'} \rangle = \langle P_{i-i',j-j'}, P_{0,0} \rangle$ and

$$\langle P_{i,j}, P_{0,0} \rangle =$$

$$\frac{d-1}{rd} \begin{cases} (r-1)(d-2) & \text{if } i = j = 0 \\ 2-r & \text{if } i \not\equiv 0 \pmod{r},\ j = 0 \\ 2-2r & \text{if } i \equiv 0 \pmod{r},\ i \not\equiv 0 \pmod{d},\ j = 0 \\ 2-d & \text{if } i = 0,\ j \not\equiv 0 \pmod{r} \\ 2 & \text{if } i \not\equiv 0 \pmod{d},\ j \not\equiv 0 \pmod{r},\ i+j \not\equiv 0 \pmod{r} \\ 2-r & \text{if } i \not\equiv 0 \pmod{r},\ i+j \equiv 0 \pmod{r} \end{cases}$$

It is a not-so-pleasant exercise to check that the rank of the resulting matrix of pairings is $(r-1)(d-2)$, thus obtaining a lower bound on the rank of V.

Another approach gives very interesting information on V. Namely, let R be the integral group ring of $\mu_d \times \mu_r$:

$$R = \frac{\mathbb{Z}[\sigma, \tau]}{(\sigma^d - 1, \tau^r - 1)}.$$

Then R acts on $J(K)$ via $\mu_d \subset \mathrm{Gal}(K/F)$ and $\mu_r \subset \mathrm{Aut}(C)$. By definition, V is the cyclic R-submodule of $J(K)$ generated by $P_{0,0}$.

Writing down explicit functions on C leads to relations among the $P_{i,j}$, and we find that if $I \subset R$ is the ideal generated by

$$(\tau - 1)\sum_{i=1}^{d} \sigma^i \qquad (\tau - 1)\sum_{i=1}^{d} \sigma^i \tau^{d-i} \qquad \sum_{j=1}^{r} \tau^j$$

then we have a surjection of R modules $R/I \to V$. The following is a refined version of the first part of the previous theorem.

Theorem 2. *We have an isomorphism of R-modules $R/I \to V$ and an isomorphism of $\mathbb{Z}$-modules $R/I \cong \mathbb{Z}^{(r-1)(d-2)} \oplus$ (torsion group of order r^3).*

We sketch a proof that $R/I \to V$ is injective modulo torsion. Write $R^0 = R \otimes \mathbb{Q}$ and $I^0 = I \otimes \mathbb{Q}$. Since R^0 is the group algebra of an abelian group, it has multiplicity one as a module over itself. This implies that there is a unique R^0-equivariant splitting of the exact sequence

$$0 \to I^0 \to R^0 \to R^0/I^0 \to 0.$$

Using this splitting we get an R-module homorphism $R/I \to R^0$. Now introduce a (Euclidean) pairing $(,)$ on R^0 by declaring that for two group elements $g, h \in \mu_d \times \mu_r$ we have $(g, h) = \delta_{gh}$. This pairing is obviously positive definite. It is a pleasant exercise to compute the induced pairing on R/I.

We have another pairing on R/I induced by the canonical height pairing on $J(K)$ and the homomorphism $R/I \to V \subset J(K)$. One finds that the two pairings agree up to a constant factor. This shows that the pairing on R/I induced by $R/I \to V \subset J(K)$ is positive definite modulo torsion, which in turn implies that $R/I \to V$ is injective modulo torsion. Computing the rank of R/I gives the desired lower bound on the rank of V.

One way to get an upper bound is to compute the degree of the L-function of J as a polynomial in q^{-s}. We find that the degree is $(r-1)(d-2)$, and this implies an upper bound on the rank, as well as an equality between the order of vanishing of the L-function and the rank.

A bonus of the method above is that it allows for a simple calculation of the discriminant of the height pairing on V. Using this and an integrality result analogous to [Ulm10, 9.1] we find that the index $[J(K) : V]$ is a power of p. More precisely,

$$[J(K) : V]^2 \text{ divides } p^{f(r-1)(d-2)}.$$

We observed above that the order of vanishing of the L-function of J at $s = 1$ is equal to the rank of $J(K)$ (i.e., the basic BSD conjecture holds) and it is known that this implies the refined conjecture on the leading coefficient of the L-function. Unwinding this leads to an "analytic class number formula"

$$|Ш(J/K)| = [J(K) : V]^2.$$

We conclude by mentioning results which are currently proven only for $r = 2$ but which are very likely to have analogues for all r. First, there should be many values of d which are not divisors of $p^f + 1$ for which the rank of $J(\mathbb{F}_p(t^{1/d}))$ is large (say $\geq \phi(d)$). The case $r = 2$ is worked out in [CHU13] and we expect analogous phenomena, for example high ranks when $d = r(p^f - 1)$.

Second, we expect that it will be possible to compute the p-groups $J(K)/V$ and $Ш(J/K)$ as modules over $\mathbb{Z}_p[\mathrm{Gal}(K/F)]$. In the case $r = 2$, these groups are non-trivial if and only if $f > 2$ and they have the same Jordan-Holder factors (an analogue of the Gras conjecture). Also, we expect that there is a polynomial F_f (depending only on f, not on p) with rational coefficients such that

$$|Ш(J/K)| = p^{F_f(p)}.$$

References

[CHU13] R. Conceição, C. Hall, and D. Ulmer, Explicit points on the Legendre curve II, Preprint, arXiv:1307.4251.

[Ulm07] D. Ulmer. L-functions with large analytic rank and abelian varieties with large algebraic rank over function fields. *Invent. Math.*, 167:379–408, 2007.

[Ulm10] D. Ulmer. Explicit points on the Legendre curve. Preprint, arXiv:1002.3313.

[Ulm13] D. Ulmer. On Mordell-Weil groups of Jacobians over function fields. *J. Inst. Math. Jussieu*, 12:1–29, 2013.

Non-critical L-values as periods

Wadim Zudilin

A *period* is a complex number whose real and imaginary parts are values of absolutely convergent integrals of algebraic functions (with algebraic coefficients) over domains in $\mathbb{R}^n$ given by polynomial inequalities (with algebraic coefficients) [1]. The set of periods $\mathcal{P}$ admits a ring structure, and the extended period ring $\widehat{\mathcal{P}} = \mathcal{P}[1/(2\pi i)]$ contains many natural quantities. For example, a general theorem due to Beilinson and Deninger–Scholl states that the (non-critical) value of the L-series attached to a cusp form $f(\tau)$ of weight k at a positive integer $m \ge k$ belongs to $\widehat{\mathcal{P}}$. In spite of the effective nature of the proof of the theorem, computing these L-values as periods remains a difficult problem even for particular examples. Many such computations are motivated by (conjectural) evaluations of the logarithmic Mahler measures of multi-variate polynomials.

With the purpose of establishing such evaluations in the two-variate case, together with Rogers [3, 4] we have developed a machinery for writing the L-values $L(f,2)$ attached to cusp forms $f(\tau)$ of weight 2 as periods, the machinery which is different from that of Beilinson. In the talk I outline the novelty of our method in more general settings [5] and indicate the following explicit period evaluations of L-values.

Theorem 1. *For the cusp form*

$$f(\tau) = q\prod_{m=1}^{\infty}(1-q^{4m})^2(1-q^{8m})^2, \qquad q=\exp(2\pi i\tau),$$

we have

$$\begin{aligned} L(f,2) &= \frac{\pi}{16}\int_0^1 \frac{1+\sqrt{1-x^2}}{(1-x^2)^{1/4}}\,\mathrm{d}x \int_0^1 \frac{\mathrm{d}y}{1-x^2(1-y^2)} = F_2(\tfrac54)+F_2(\tfrac34),\\ L(f,3) &= \frac{\pi^2}{128}\int_0^1 \frac{(1+\sqrt{1-x^2})^2}{(1-x^2)^{3/4}}\,\mathrm{d}x \int_0^1\int_0^1 \frac{\mathrm{d}y\,\mathrm{d}w}{1-x^2(1-y^2)(1-w^2)}\\ &= F_3(\tfrac54)+2F_3(\tfrac34)+F_3(\tfrac14), \end{aligned}$$

where

$$F_k(a) = \frac{\pi^{k-1/2}\Gamma(a)}{2^{3k-1}\Gamma(a+\frac12)}\sum_{n=0}^{\infty}\frac{n!^{k-1}(\frac12)_n}{(\frac32)_n^{k-1}(a+\frac12)_n}, \qquad (b)_n = \frac{\Gamma(b+n)}{\Gamma(b)} = \prod_{m=0}^{n-1}(b+m).$$

Also, $L(f,1) = 2F_1(\frac54)$.

Note that $L(f,s) = L(E,s)$ for the cusp form $f(\tau)$ in the theorem and E an elliptic curve of conductor 32. Though the theorem produces amazingly similar hypergeometric forms of $L(E,k)$ for $k=1,2,3$ (namely, the L-value $L(E,k)$ can be written as a (simple) $\mathbb{Q}$-linear combination of $F_k(\frac74-\frac{m}{2})$ for $m=1,\dots,k$), this pattern does not seem to work for $k>3$.

Another application of the method in [3, 4, 5] was recently given by A. Mellit and F. Brunault. They obtain a general formula for the regulator of two modular units which allows one to identify several two-variable (logarithmic) Mahler measures

$$\mathrm{m}\big(P(x,y)\big) = \frac{1}{(2\pi i)^2} \int_{|x|=|y|=1} \cdots \int \log|P(x,y)| \,\frac{\mathrm{d}x}{x}\,\frac{\mathrm{d}y}{y}$$

with the L-values $L(E,2)$, where E is the elliptic projective curve given as the zero locus of a (Laurent) polynomial $P(x,y)$.

More specifically, for two rational non-constant functions g and h on E, we consider the 1-form $\eta(g,h) = \log|g|\,\mathrm{d}\arg h - \log|h|\,\mathrm{d}\arg g$, where $\mathrm{d}\arg g$ is globally defined as $\mathrm{Im}(\mathrm{d}g/g)$. The form η is a real 1-form infinitely many times differentiable on $E \setminus S$, where S is the set of zeros and poles of g and h. Furthermore, it is not hard to verify that the form η is antisymmetric, bi-additive and closed; the latter fact implies that the regulator map

$$r(\{g,h\})\colon \gamma \mapsto \int_\gamma \eta(g,h)$$

only depends on the homology class $[\gamma]$ of γ in $H_1(E \setminus S, \mathbb{Z})$.

Factorising $P(x,y)$ as a polynomial in y with coefficients from $\mathbb{C}[x]$,

$$P(x,y) = a_0(x) \prod_{j=1}^{n} (y - y_j(x)),$$

and applying Jensen's formula, we can write the Mahler measure of P in the form

$$\mathrm{m}\big(P(x,y)\big) = \mathrm{m}\big(a_0(x)\big) + \frac{1}{2\pi}\, r(\{x,y\})([\gamma]),$$

where $\gamma = \{(x,y) \in E : |x| = 1,\ |y| \geq 1\}$ and $\mathrm{m}(a_0(x))$ is the single-variable Mahler measure of $a_0(x)$.

In case the curve $E : P(x,y) = 0$ admits a parametrisation by means of modular *units* $x(\tau)$ and $y(\tau)$, one can change to the variable τ in the above integral for $r(\{x,y\})$; the class $[\gamma]$ in this case becomes a union of paths joining certain cusps of the modular functions $x(\tau)$ and $y(\tau)$. The following general result completes the computation of the Mahler measure in the case when $x(\tau)$ and $y(\tau)$ are given as quotients/products of modular units

$$g_a(\tau) = q^{NB(a/N)/2} \prod_{\substack{n\geq 1\\ n\equiv a \bmod N}} (1-q^n) \prod_{\substack{n\geq 1\\ n\equiv -a \bmod N}} (1-q^n), \qquad q = \exp(2\pi i\tau),$$

where $B(x) = B_2(x) = \{x\}^2 - \{x\} + \frac{1}{6}$ is the second Bernoulli polynomial.

Theorem 2 (Mellit–Brunault [6])**.** *For a, b and c integral, with ac and bc not divisible by N,*

$$\int_{c/N}^{i\infty} \eta(g_a, g_b) = \frac{1}{4\pi}\, L(f(\tau) - f(i\infty), 2),$$

where $f(\tau) = f_{a,b;c}(\tau) = e_{a,bc}e_{b,-ac} - e_{a,-bc}e_{b,ac}$ *is a weight* 2 *modular form and*

$$e_{a,b}(\tau) = \frac{1}{2}\left(\frac{1+\zeta_N^a}{1-\zeta_N^a} + \frac{1+\zeta_N^b}{1-\zeta_N^b}\right) + \sum_{m,n\geq 1}(\zeta_N^{am+bn} - \zeta_N^{-(am+bn)})q^{mn}$$

are weight 1 *level* N^2 *Eisenstein series*; $\zeta_N = \exp(2\pi i/N)$.

The most classical example corresponds to the Mahler measure of $x + 1/x + y + 1/y + 1$, when the elliptic curve $E : x + 1/x + y + 1/y + 1 = 0$ has conductor $N = 15$ and can be parametrised by the modular units

$$\begin{aligned} x(\tau) &= \frac{1}{q}\prod_{n=0}^{\infty}\frac{(1-q^{15n+7})(1-q^{15n+8})}{(1-q^{15n+2})(1-q^{15n+13})} = \frac{g_7(\tau)}{g_2(\tau)},\\ y(\tau) &= -\frac{1}{q}\prod_{n=0}^{\infty}\frac{(1-q^{15n+4})(1-q^{15n+11})}{(1-q^{15n+1})(1-q^{15n+14})} = -\frac{g_4(\tau)}{g_1(\tau)}, \end{aligned}$$

and the path of integration γ corresponds to the range of τ between the two cusps $-1/5$ and $1/5$ of $\Gamma_0(15)$. Therefore, Theorem 2 results in

$$\begin{aligned} \mathrm{m}\Big(x + \frac{1}{x} + y + \frac{1}{y} + 1\Big) &= \frac{1}{2\pi}\Big(\int_{-1/5}^{i\infty} - \int_{1/5}^{i\infty}\Big)\eta(g_7/g_2, g_4/g_1)\\ &= \frac{1}{8\pi^2}L(2f_{7,4;-3} - 2f_{7,1;-3} - 2f_{2,4;-3} + 2f_{2,1;-3}, 2)\\ &= \frac{15}{4\pi^2}L(\eta(\tau)\eta(3\tau)\eta(5\tau)\eta(15\tau), 2) = \frac{15}{4\pi^2}L(E,2), \end{aligned}$$

which is precisely a conjecture of Boyd.

Another example, for the conductor 40 elliptic curve $x - 1/x + y - 1/y + 2 = 0$, was considered earlier by Mellit in [2].

References

[1] M. Kontsevich and D. Zagier, *Periods*, in "Mathematics Unlimited — 2001 and Beyond" (Springer, Berlin 2001), 771–808.

[2] A. Mellit, *Mahler measures and q-series*, in "Explicit methods in number theory" (MFO, Oberwolfach, Germany, 17–23 July 2011), Oberwolfach Reports **8** (2011), no. 3, 1990–1991.

[3] M. Rogers and W. Zudilin, *From L-series of elliptic curves to Mahler measures*, Compositio Math. **148** (2012), 385–414.

[4] M. Rogers and W. Zudilin, *On the Mahler measure of* $1 + X + 1/X + Y + 1/Y$, Intern. Math. Res. Not. (to appear); doi: 10.1093/imrn/rns285.

[5] W. Zudilin, *Period(d)ness of L-values*, in "Number Theory and Related Fields, In memory of Alf van der Poorten", J. M. Borwein et al. (eds.), Springer Proceedings in Math. Stat. **43** (Springer, New York, 2013), 381–395.

[6] W. Zudilin, *Regulator of modular units and Mahler measures*, Preprint at http://arxiv.org/abs/1304.3869 (2013), 15 pp.

New directions in modularity

Frank Calegari

The work of Wiles and Taylor-Wiles provides a framework for proving, given suitable initial hypotheses, that a Galois representation is modular. An early application was the proof that all curves X of genus one over the rational numbers are modular. In the 20 years since this result was announced, the method has been generalized significantly.

However, despite the advances, the problem of proving that curves of genus two are modular is still completely open. Similarly, the problem of genus one curves over imaginary quadratic fields is open. One common theme is that the Taylor-Wiles method is restricted to situations in which the underlying automorphic representations are discrete series representations at infinity. In these situations, the desired automorphic representations can be detected in the cohomology of Shimura varieties. In this talk, we explain in detail the method of Wiles, and indicate a new approach with David Geraghty to extending this method to new contexts beyond Shimura varieties. Together with recent results of Peter Scholze, this opens the door to new advances in modularity.

Kac-Wakimoto character and almost harmonic weak Maass forms

Kathrin Bringmann

In this talk I answer a question of Kac concerning the modularity of certain characters arising in Lie superalgebras.

The connection between classical modular forms and the representation theory of infinite dimensional Lie algebras has been known for some time. Probably the most famous example is given by "Monstrous moonshine". Moonshine starts with the observation by Mc Kay that

$$\begin{aligned} 196884 &= 196883 + 1 \\ 21493760 &= 21296876 + 196883 + 1 \\ &\vdots \end{aligned}$$

The left-hand sides are the coefficients of the modular j-function, the right-hand sides count dimensions of irreducible representations of the monster group, the largest finite sporadic group. These equations hint to the existence of a monster module

$$V = V_{-1} \oplus V_1 \oplus V_2 \oplus \dots$$

and a graded representation such that $V_{-1} = \rho_0, V_1 = \rho_1 \oplus \rho_2, \dots$ so that the j-function is the generating function for the graded dimensions

$$j(\tau) - 744 = \dim(V_{-1})\, q^{-1} + \sum_{n \geq 1} \dim(V_n)\, q^n.$$

What is now deep is that one can also consider twists T_g of this, as suggested by Thompson. The dimensions are here replaced by traces of certain representations. Conway and Norton then conjectured that T_g is a Hauptmodule for some subgroup Γ_g of $\mathrm{SL}_2(\mathbb{Z})$ having genus zero. Frenkel-Lepowsky-Meurman explicitly constructed the monster module V. Borcherds then fully solved the Conway-Norton moonshine conjecture using generalized Kac-Moody algebras.

Recently we showed that harmonic (weak) Maass forms (which are non-holomorphic companions of classical modular forms) and their generalizations also play an important role in understanding modularity properties of certain characters. The starting point was specialized character formulas for irreducible highest weight $s\ell(m,n)^\wedge$ modules found by Kac and Wakimoto. Kac raised the question concerning the modularity of these characters. In the last years we made significant progress on this conjecture and solved important cases. The starting point is the explicit form of the generating function found by Kac and Wakimoto ($n, m \in \mathbb{N}$)

$$chF\,(z;\tau) = \sum_{\ell\in\mathbb{Z}} chF_\ell \zeta^\ell \doteq \varphi\left(z+\frac{\tau}{2};\tau\right)\eta^{n-m}(\tau),$$

where $q := e^{2\pi i\tau}$, $\zeta := e^{2\pi iz}$, $\eta(\tau) := q^{\frac{1}{24}}\prod_{\ell\geq 1}\left(1-q^\ell\right)$ is Dedekind's modular form of weight $\frac{1}{2}$, and

$$\varphi(z;\tau) := \frac{\vartheta\left(z+\frac{1}{2};\tau\right)^m}{\vartheta(z;\tau)^n}.$$

Here

$$\vartheta(z;\tau) := \sum_{\nu\in\frac{1}{2}+\mathbb{Z}} e^{\pi i\nu^2\tau+2\pi i\nu\left(z+\frac{1}{2}\right)}$$

is a Jacobi form of weight $\frac{1}{2}$ and index $\frac{1}{2}$. The notation $\doteq$ means up to constants and powers of q and ζ. Note that the coefficient functions $\mathrm{ch}F_\ell$ depend upon the range in which ζ is. So we are interested in Fourier coefficients of a certain meromorphic Jacobi form of weight 0. For holomorphic Jacobi forms there is a well-developed theory due to Eichler and Zagier. In particular, there exists an important correspondence between them and modular forms of half-integral weight given by the so-called theta decomposition. In contrast, for meromorphic Jacobi forms wall-crossing behaviors occur and one does not just get classical modular forms. In the case of poles of order at most two (in the Jacobi variable) such a phenomenon was first observed in the study of quantum black holes by Dabolkar, Murthy, and Zagier, yielding functions related to harmonic Maass forms. But in general the situation is much more complicated, yielding totally new classes of functions. These new objects, which we call almost harmonic Maass form, are sums of harmonic Maass forms under iterates of the Maass raising operator (thus themselves non-harmonic Maass forms) multiplied by almost holomorphic modular form. We call the associated holomorphic parts almost mock modular forms. Our main theorem is

Theorem 1. *(B-Folsom) For $0 < n < m$ with $n \equiv m \equiv 0 \pmod 2$, the Kac-Wakimoto characters are almost mock modular forms.*

Everything here can be made explicit, the multiplier and the group as well as the completed object. The condition on the range is essential for the result to be true, the congruence condition is just a technical restriction and my PhD student René Olivetto removed it. The case $n = 2$ is particularly nice and has been previously considered using multivariable Appell functions.

Corollary 2. *(B-Ono) In the case $n = 2$ we obtain a product of a modular form with a mock modular form. Note that this is also called mixed modular form.*

Note that one can also make a modularity statement in the case $n = m$. This is joint work with Folsom and Mahlburg. What is not clear is whether any modularity statement can be made if $n > m$. In the somewhat degenerate case $n = 1, m = 0$ one gets a false theta function divided by a power of η.

Effective Chabauty for symmetric powers of curves

Jennifer Park

We aim to generalize the following theorem of Coleman [Col85] to the case of higher-dimensional varieties:

Theorem 1 (Coleman, 1985)**.** *Let $X/\mathbb{Q}$ be a curve of genus g, satisfying $g > \operatorname{rank} \operatorname{Jac}(X)$, with a basepoint $O \in X(\mathbb{Q})$. Suppose that X has good reduction at a prime p. Then there exists a number $N(g, p)$ that can be computed effectively satisfying*

$$\#X(\mathbb{Q}) \leq N(g, p).$$

These bounds are sometimes sharp, and can be realistically used to find all rational points of a given curve.

More generally, let Y be an algebraic variety. In theory, it seems plausible that Chabauty's method could still apply, where the Albanese variety $\operatorname{Alb}(Y)$ is substituted in place of the Jacobian. There exist several difficulties in generalizing the above theorem (often called Chabauty's method) to arbitrary higher-dimensional varieties.

- $\operatorname{Alb}(Y)$ may be trivial: $\dim \operatorname{Alb}(Y) = h^0(Y, \Omega_1)$ (for example, if Y is a K3 surface or an Enriques surface, $h^{0,1} = 0$). In this case, the analogue of Chabauty's method does not yield anything.
- $\operatorname{Alb}(Y)$ and the image of the Albanese map $j : Y \to \operatorname{Alb}(Y)$ may be too complicated for an explicit method.
- Sometimes we have $\#Y(\mathbb{Q}) = \infty$: if $Y = \operatorname{Sym}^2 X$ for a hyperelliptic curve $X : y^2 = f(x)$ with $\deg(f)$ odd, then $\{(t, \sqrt{f(t)}), (t, -\sqrt{f(t)})\} \in \operatorname{Sym}^2 X(\mathbb{Q})$ for all $t \in \mathbb{Q}$.

However, choosing $Y = \mathrm{Sym}^d X$ for a smooth projective curve of sufficiently high genus g (to be chosen later) ensures that $\mathrm{Alb}(Y) = \mathrm{Jac}(X)$. Further, being able to describe $(\mathrm{Sym}^d X)(\mathbb{Q})$ means that one can find all degree-d points on X. To deal with the last issue, we recall:

Theorem 2 (Faltings)**.** *Let $A/\mathbb{Q}$ be an abelian variety, and $X \subseteq A$ be a closed subvariety. Then there exists finitely many subvarieties $Y_i \subset X$ such that each Y_i is a coset of an abelian subvariety of A and*

$$X(\mathbb{Q}) = \bigcup Y_i(\mathbb{Q}).$$

Apply this theorem to the map

$$\begin{aligned} j : (\mathrm{Sym}^d X)(\mathbb{Q}) &\to J(\mathbb{Q}) \\ \{P_1, \ldots, P_d\} &\mapsto [P_1 + \cdots + P_d - d \cdot O], \end{aligned}$$

where $J := \mathrm{Jac}(X) = \mathrm{Alb}(\mathrm{Sym}^d(X))$. Then if $Q \in (\mathrm{Sym}^d X)(\mathbb{Q})$, one of the following options hold:

(1) $\#j^{-1}(j(Q)) \neq 1$, or
(2) $Q \in Y_i(\mathbb{Q})$ with $\dim Y_i > 0$, or
(3) Neither (1) nor (2).

Option (1) happens when two divisors $[P_1 + \cdots + P_d - d \cdot O]$ and $[P_1' + \cdots + P_d' - d \cdot O]$ are linearly equivalent to one another. Thus, if $\#j^{-1}(j(Q)) \neq 1$, then there exists $n \geq 1$ such that $\#j^{-1}(j(Q)) \cong \mathbb{P}^n$.

Option (2) has also been studied in the past, most notably in [HS91]:

Theorem 3 (Harris-Silverman, 1991)**.** *If $\mathrm{Sym}^2 X$ contains an elliptic curve, then X is either bielliptic or hyperelliptic.*

Hence, we make the following definition:

Definition. *A point $P \in \mathrm{Sym}^d X(\mathbb{Q})$ is said to belong to the **infinite locus** if it satisfies options (1) or (2). Otherwise, it is said to be in the **finite locus**.*

In this paper, we focus on $\#\{Q \in (\mathrm{Sym}^d X)(\mathbb{Q}) \mid Q \text{ satisfies option (3)}\}$. Relatively less has been known for $Q \in (\mathrm{Sym}^d X)(\mathbb{Q})$ satisfying option (3); [Sik09] partially deals with the case when $d = 2$, and nothing was known about when $d \geq 3$.

The main result of this talk is the following:

Theorem 4 (P, 2013)**.** *Let $d \geq 1$, p a prime, and let $X/\mathbb{Q}$ be a smooth projective curve of good reduction at p with $\mathrm{rank}\, J \leq g - d$. Then there exists a number $N(p, d, g)$ that can be computed effectively satisfying*

$$\#\{Q \in (\mathrm{Sym}^d X)(\mathbb{Q}) \mid Q \text{ is in the finite locus}\} \leq N(p, d, g).$$

This theorem has some interesting consequences, including:

Corollary 5. *Let $X/\mathbb{Q}$ be a hyperelliptic curve whose affine model $y^2 = f(x)$ satisfies* $\deg(f) = 7$ *(so that $g = 3$). Suppose further that* $\operatorname{rank} J \leq 1$*, and that X has good reduction at $p = 2$. Then*

$$N(p, d, g) \leq 1357.$$

In this talk, we explain the interplay of number theory and nonarchimedean geometry that is involved to prove the above theorem.

References

[Col85] Robert F. Coleman, *Effective Chabauty*, Duke Math. J. 52 (1985), no. 3, 765–770, DOI 10.1215/S0012-7094-85-05240-8. MR808103 (87f:11043).

[HS91] Joe Harris and Joe Silverman, *Bielliptic curves and symmetric products*, Proc. Amer. Math. Soc. 112 (1991), no. 2, 347–356, DOI 10.2307/2048726. MR1055774 (91i:11067).

[Sik09] Samir Siksek, *Chabauty for symmetric powers of curves*, Algebra Number Theory 3 (2009), no. 2, 209–236, DOI 10.2140/ant.2009.3.209. MR2491943 (2010b:11069).

Imaginary quadratic fields with isomorphic abelian class groups

Peter Stevenhagen

I discussed to which extent the invariants commonly associated to algebraic number fields determine the number field.

From earlier work (Gassman, Perlis), we know that there exist non-isomorphic number fields that have the same Dedekind zeta-function, or (topologically) isomorphic adele rings. In contrast with this, number fields having (topologically) isomorphic absolute Galois groups are known to be isomorphic (Neukirch-Uchida).

The talk focused on imaginary quadratic fields, which were known to admit topologically isomorphic absolute *abelian* Galois groups due to work of Onabe. However, no concrete description of any absolute abelian Galois group had been obtained from this work.

We sketched recent results (joint with Athanasios Angelakis) that show that for imaginary quadratic fields of discriminant $D < -4$, the absolute abelian Galois group always contains a universal open subgroup

$$A_0 \cong \widehat{\mathbb{Z}} \times \prod_{n=1}^{\infty} \mathbb{Z}/n\mathbb{Z}$$

of index dividing the class number.

Based on numerical calculations, we conjecture that for 100% of all imaginary quadratic fields of *prime* class number, the absolute abelian Galois group is in fact isomorphic to A_0.

Modularity and the Fermat Equation over Totally Real Fields

Samir Siksek
(joint work with Nuno Freitas)

We sketched the proofs of the following two theorems.

Theorem 1 (Calegari, Le Hung, Freitas–S.)**.** *Let K be a totally real field. Then there are at most finitely many non-modular j-invariants of elliptic curves defined over K.*

Theorem 2 (Freitas–S.)**.** *Let K be a real quadratic field. Then all elliptic curves over K with full 2-torsion are modular.*

These two theorems build on powerful modularity lifting results of Gee [6], of Barnet-Lamb, Gee and Geraghty [1], [2], and of Breuil and Diamond [3, Théorème 3.2.2]. Our proofs merely supply the 'modularity switching' inspired by the work of Wiles [19], Taylor [18], Manoharmayum [13], [14] and Ellenberg [5]. The proof of Theorem 1 makes use of Faltings' Theorem to reduce to finitely many j-invariants, and so does not give an algorithm for determining these j-invariants. We acknowledge that a proof of Theorem 1 was independently sketched by Frank Calegari (unpublished), and that a more powerful result was recently proved by Bao Le Hung [12].

We also mentioned the following two theorems concerning the Fermat equation over totally real fields, which make use of the above modularity theorems, and also level lowering results due to Fujiwara [7], Jarvis [9] and Rajaei [15].

Theorem 3. *Let $d > 6$ be squarefree, satisfying $d \equiv 3 \pmod 8$ or $d \equiv 6,\ 10 \pmod{16}$, and write $K = \mathbb{Q}(\sqrt{d})$. There is an effectively computable constant B_K such that for all primes $p \geq B_K$, the equation*

$$x^p + y^p = z^p, \qquad x, y, z \in K \tag{1}$$

does not have solutions satisfying $xyz \neq 0$.

Theorem 4. *Let K be a totally real number field. Let S be the set of prime ideals $\mathfrak{P} \mid 2$, and let T be the subset of S consisting of ideals $\mathfrak{P}$ having residual degree $f(\mathfrak{P}/2) = 1$. Suppose T is non-empty. Write $\mathcal{O}_S^*$ for the set of S-units of K. Suppose that every solution (λ, μ) to the S-unit equation*

$$\lambda + \mu = 1, \qquad \lambda,\ \mu \in \mathcal{O}_S^* \tag{2}$$

satisfies the following condition: there is some $\mathfrak{P} \in T$ such that

$$\max\{|\upsilon_{\mathfrak{P}}(\lambda)|, |\upsilon_{\mathfrak{P}}(\mu)|\} \leq 4 \cdot e(\mathfrak{P}/2) \tag{3}$$

where $e(\mathfrak{P}/2)$ is the ramification index of $\mathfrak{P}$. Then there is some constant B_K such that for all $p \geq B_K$, the equation (1) does not have solutions satisfying $xyz \neq 0$.

As far as we are aware, the only previous work on Fermat using modularity over a totally real field (other than $\mathbb{Q}$!) is due to Jarvis and Meekin [11] who showed that the Fermat equation $x^n + y^n = z^n$ has no solutions $x,\ y,\ z \in \mathbb{Q}(\sqrt{2})$ with

$xyz \neq 0$ and $n \geq 4$. For this they needed the modularity of semistable elliptic curves over $\mathbb{Q}(\sqrt{2})$ which was proved by Jarvis and Manoharmayum [10].

We make the following remarks.

- In contrast to Theorem 3, the constant B_K in Theorem 4 is ineffective, though it can be made effective if we assume a suitably powerful modularity statement, such as modularity of all elliptic curves over totally real number fields with full 2-torsion. Indeed, Theorem 2 enables us to make the constant B_K in Theorem 3 effectively computable.
- By a famous theorem of Siegel [16], S-unit equations have finitely many solutions, and there are effective algorithms for determining the solutions (e.g. [17, Chapter IX]). Thus for any totally real field K, there is an algorithm for deciding whether the hypotheses of Theorem 4 are satisfied.
- The S-unit equation (2) has precisely three solutions in $\mathbb{Q} \cap \mathcal{O}_S^* = \mathbb{Z}[1/2]$, namely $(\lambda, \mu) = (2, -1)$, $(-1, 2)$, $(1/2, 1/2)$; these trivially satisfy the bound in (3) for any $\mathfrak{P} \in T$. In fact, we deduce Theorem 3 from Theorem 4 by showing, for the quadratic fields appearing in Theorem 3, that the only solutions to the S-unit equation (2) are the above three solutions.

References

[1] T. Barnet-Lamb, T. Gee and D. Geraghty, *Congruences between Hilbert modular forms: constructing ordinary lifts*, Duke Math. Journal **161** (2012), 1521–1580.

[2] T. Barnet-Lamb, T. Gee and D. Geraghty, *Congruences between Hilbert modular forms: constructing ordinary lifts II*, Mathematical Research Letters, to appear.

[3] C. Breuil and F. Diamond *Formes modulaires de Hilbert modulo p et valeurs d'extensions galoisiennes*, preprint, 2013.

[4] J. Cremona, J.-C. Lario, J. Quer, K. Ribet (editors), *Modular Curves and Abelian Varieties*, Progr. Math. **224**, Birkhäuser, Basel, 2004.

[5] J. Ellenberg *Serre's conjecture over* $\mathbb{F}_9$, Ann. of Math. (2) **161** (2005), 1111–1142.

[6] T. Gee, *Automorphic lifts of prescribed types*, Mathematische Annalen **350** (2011), 107–144.

[7] K. Fujiwara, *Level optimisation in the totally real case*, `arXiv:math/0602586v1 [math.NT]` (2006), preprint.

[8] F. Jarvis, *Level lowering for modular mod ℓ representations over totally real fields*, Math. Ann. **313** (1999), no. 1, 141–160.

[9] F. Jarvis *Correspondences on Shimura curves and Mazur's principle at p*, Pacific J. Math., **213** (2), 2004, 267–280.

[10] F. Jarvis and J. Manoharmayum, *On the modularity of supersingular elliptic curves over certain totally real number fields* , Journal of Number Theory **128** (2008), no. 3, 589–618.

[11] F. Jarvis and P. Meekin, *The Fermat equation over* $\mathbb{Q}(\sqrt{2})$, Journal of Number Theory **109** (2004), no. 1, 182–196.

[12] B. Le Hung, personal communication, 11 July 2013.

[13] J. Manoharmayum, *On the modularity of certain* $\mathrm{GL}_2(\mathbb{F}_7)$ *Galois representations*, Math. Res. Lett. **8** (2001), no. 5-6, 703–712.

[14] J. Manoharmayum, *Serre's conjecture for mod 7 Galois representations* pages 141–149 of [4].

[15] A. Rajaei, *On the levels of mod ℓ Hilbert modular forms*, J. Reine Angew. Math. **537** (2001), 33–65.

[16] C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. Preuss. Akad. Wiss. (1929), 1–41.

[17] N. P. Smart, *The Algorithmic Resolution of Diophantine Equations*, London Mathematical Society Student Texts **41**, 1998.
[18] R. Taylor *On icosahedral Artin representations II*, American Journal of Mathematics **125** (2003), 549–566.
[19] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Mathematics **141** (1995), no. 3, 443–551.

Arithmetic invariant theory

Dick Gross
(joint work with Manjul Bhargava and Xiaoheng Wang)

Let G be a reductive group over the field k and V a linear representation of G which is defined over k. Arithmetic invariant theory studies the orbits of $G(k)$ on V, assuming that one has information on the orbits over a separable closure k^s. Let $V \to V/\!\!/G$ be the map to the canonical quotient, which is defined by evaluation of the invariant polynomials. Let f be a k rational point of $V/\!\!/G$ and let V_f denote the fiber above f in V. We will always assume that the group $G(k^s)$ acts transitively on $V_f(k^s)$, and will attempt to describe the orbits of $G(k)$ on $V_f(k)$ using Galois cohomology.

First assume that $V_f(k)$ is non-empty, and fix a vector v over k with invariant f. Let G_v denote its stabilizer in G. If w is another vector in $V_f(k)$, then by our assumption there is an element $g \in G(k^s)$ with $g(w) = v$. For any σ in the Galois group of k^s over k, ${}^\sigma g(w) = v$, so the composition

$$c_\sigma = g^{-1\sigma} g$$

takes values in $G_v(k^s)$. This defines a one-cocycle $(\sigma \to c_\sigma)$ on the Galois group with values in G_v which is clearly a coboundary in G. The orbit of w under $G(k)$ depends only on the cohomology class of c, and this gives a bijection from the orbits of $G(k)$ on $V_f(k)$ to the set of elements in the kernel of the map of pointed sets

$$\gamma : H^1(k, G_v) \to H^1(k, G).$$

As an example, consider the action of $G = \mathrm{SL}(W)$ by conjugation on the space V of endomorphisms $T : W \to W$ of trace zero. This is the adjoint representation, and the invariant polynomials are freely generated by the coefficients of the characteristic polynomial $f(x) = x^n + c_2 x^{n-2} + \ldots + c_n$ of T. Assume that $f = f(x)$ is separable, so that T is regular and semi-simple. Then the set $V_f(k)$ of endomorphisms with characteristic polynomial $f(x)$ is non-empty and $G(k^s)$ acts transitively on $V_f(k^s)$. The stabilizer G_v of a vector $v \in V_f(k)$ is a maximal torus in G, whose isomorphism class over k depends only on $f(x)$. If $L = k[x]/f(x)$ is the corresponding étale algebra, then G_v is isomorphic to the group $(\mathrm{Res}_{L/k} \mathbb{G}_m)_{N=1}$. In particular, $H^1(k, G_v) = k^\times / N(L^\times)$, by Hilbert's theorem 90. Since $H^1(k, \mathrm{SL}(V)) = 1$, the orbits with characteristic polynomial $f(x)$ form a principal homogeneous space for the group $k^\times / N(L^\times)$.

When the pointed set $H^1(k,G)$ has more than one element, one can ask about the fiber of the map γ over a non-trivial class in $H^1(k,G)$. Such a class gives a pure inner twisting G^* of the group, along with a representation V^* of G^* over k, and one can show that the set of elements in the fiber of γ over this class is in bijection with the $G^*(k)$ orbits on the set $V_f^*(k)$. For example, assume that the characteristic of k is not equal to 2, and let $G = \mathrm{SO}(W)$ be the special orthogonal group of a split orthogonal space of odd dimension over k. Let V be the representation by conjugation on the space of self-adjoint operators $T : W \to W$. The invariant polynomials are freely generated by the coefficients of the characteristic polynomial f of T. If we assume that f is separable, then the set $V_f(k)$ of self-adjoint operators with characteristic polynomial $f(x)$ is non-empty and the group $G(k^s)$ acts transitively on $V_f(k^s)$. In this case the stabilizer of a vector $v \in V_f(k)$ is the finite group scheme $G_v = (\mathrm{Res}_{L/k}\,\mu_2)_{N=1}$ and $H^1(k,G_v) = (L^\times/L^{\times 2})_{N\equiv 1}$. This maps via γ to the pointed set $H^1(k,\mathrm{SO}(W))$, which indexes the orthogonal spaces W^* with the same rank and discriminant. The pure inner form is the group $G^* = \mathrm{SO}(W^*)$ and the representation V^* is on the self-adjoint endomorphisms of W^*. Hence the fiber (which may be empty) indexes the orbits of this non-split orthogonal group on the self-adjoint operators with this characteristic polynomial. For example, if $k = \mathbb{R}$ and the space W^* is definite, then the fiber is non-empty if and only if the characteristic polynomial $f(x)$ splits completely. In that case, the fiber has a single element, by the spectral theorem.

There are rational invariants f in representations V where $V_f^*(k)$ is empty for all pure inner forms G^* of G. We study this situation under the additional assumption that the stabilizer G_v of a vector v in $V_f(k^s)$ is abelian. For each σ in the Galois group, the vector ${}^\sigma v$ also lies in $V_f(k^s)$, so there is an element g_σ in $G(k^s)$ with $g_\sigma({}^\sigma v) = v$. Conjugation by g_σ gives an isomorphism

$$\theta_\sigma : {}^\sigma G_v \to G_v.$$

Even though the choice of g_σ is not unique, it is well-defined up to left multiplication by an element in G_v. Since the stabilizer is assumed to be abelian, the isomorphism θ_σ is canonical. These isomorphisms satisfy the one-cocycle condition $\theta_{\sigma\tau} = \theta_\sigma \cdot {}^\sigma\theta_\tau$ so give a descent of G_v to a commutative group scheme over k. The composition

$$d_{\sigma,\tau} = g_\sigma \cdot {}^\sigma g_\tau \cdot g_{\sigma\tau}^{-1}$$

then defines a two-cocycle on the Galois group with values in $G_v(k^s)$. If an orbit exists over k the class d_f of this coocyle in the group $H^2(k,G_v)$ is trivial. Conversely, if the class of d_f is trivial, then an orbit exists for some pure inner form G^* of G. (This is really all that one can expect, as the class d_f is independent of the pure inner form used to define it.) When $d_f \neq 0$, there is no orbit for any pure inner form.

An example where this class can be non-trivial is given by the representation V of $G = \mathrm{SL}(W)$ on pairs (A,B) of symmetric bilinear forms on W, when the characteristic of k is not equal to 2.. Let $n = \dim(W)$. The polynomial invariants

are generated by the coefficients of the binary form

$$f(x,y) = (-1)^{n(n-1)/2} \det(xA - yB) = f_0 x^n + f_1 x^{n-1} y + \dots$$

Assume that the discriminant $\Delta(f)$ is non-zero in k. Then the group $G(k^s)$ acts transitively on $V_f(k^s)$ with stabilizer an elementary abelian 2-group of order 2^{n-1}. The above descent gives the group scheme $G_v = (\mathrm{Res}_{L/k}\,\mu_2)_{N=1}$, where L is the étale algebra given by f. Furthermore, the group $H^2(k, G_v)$ contains the subgroup $k^\times/N(L^\times)k^{\times 2}$, which is the kernel of the map to $H^2(k, \mathrm{Res}_{L/k}\,\mu_2)$.

In this case, the pointed set $H^1(k, G) = H^1(k, \mathrm{SL}(W))$ has a single element, so orbits will exist if and only if $d_f = 0$ in $H^2(k, G_v)$. What is the class d_f? Assume that the leading coefficient f_0 is non-zero, for simplicity. Then d_f is equal to the class of f_0 in $k^\times/N(L^\times)k^{\times 2}$. This subgroup is trivial when n is odd, so orbits always exist in that case. However, when $n = 2g + 2$ is even, the class d_f can be non-trivial in $H^2(k, G_v)$. In this case, the existence of orbits is closely related to the arithmetic of the hyperelliptic curve $z^2 = f(x, y)$ of genus g over k. Bhargava uses an integral form of this representation to show that most hyperelliptic curves of genus $g \geq 2$ over $\mathbb{Q}$ have no rational points.

The ternary Goldbach conjecture

Harald Helfgott

The ternary Goldbach conjecture (or *three-prime problem*) states that every odd number n greater than 5 can be written as the sum of three primes. Both the ternary Goldbach conjecture and the (stronger) binary Goldbach conjecture (stating that every even number greater than 2 can be written as the sum of two primes) have their origin in the correspondence between Euler and Goldbach (1742). See [1, Ch. XVIII] for the early history of the problem.

I. M. Vinogradov [7] showed in 1937 that the ternary Goldbach conjecture is true for all n above a large constant C. Unfortunately, while the value of C has been improved several times since then, it has always remained much too large ($C = e^{3100}$, [5]) for a mechanical verification up to C to be even remotely feasible.

In two recent papers ([2] and [3]), I prove the ternary Goldbach conjecture.

Main Theorem. *Every odd integer n greater than 5 can be expressed as the sum of three primes.*

The proof given in [2] and [3] works for all $n \geq C = 10^{29}$. The main theorem has been checked deterministically by computer for all $n < 10^{29}$ (and indeed for all $n \leq 8.875 \cdot 10^{30}$) [4].

I am able to set major arcs to be few and narrow because the minor-arc estimates in [3] are very strong; I am forced to take them to be few and narrow because of the kind of L-function bounds we will rely upon. ("Major arcs" are small intervals around rationals of small denominator; "minor arcs" are everything else.)

At issue are

(1) a fuller use of the close relation between the circle method and the large sieve;
(2) a combination of different smoothings for different tasks;
(3) the verification of GRH up to a bounded height for all conductors $q \leq 150000$ and all even conductors $q \leq 300000$ (due to David Platt [6]);
(4) better bounds for exponential sums $\sum_n \Lambda(n) e^{2\pi i \alpha n} \eta(n/x)$ for η smooth and α in the minor arcs, as in [3].

All major computations – including D. Platt's work in [6] – have been conducted rigorously, using interval arithmetic.

The improvements on bounds on exponential sums for α in the minor arcs are due to several new ideas of general applicability. In particular, I show a way to obtain cancellation from Vaughan's identity. Vaughan's identity is a two-log gambit, in that it introduces two convolutions (each of them at a cost of log) and offers a great deal of flexibility in compensation. One of the ideas in [3] is that at least one of two logs can be successfully recovered after having been given away in the first stage of the proof. This reduces the cost of the use of this basic identity in this and, presumably, many other problems.

If α is on the tail of a major arc, this can be exploited, rather than being a problem. This is so both in the large sieve (thanks to a scattered input to the large sieve) and in other contexts.

References

[1] L. E. Dickson, *History of the theory of numbers. Vol. I: Divisibility and primality*, Chelsea Publishing Co., 1966, xii+486.
[2] H. A. Helfgott, "Major arcs for Goldbach's problem", preprint. Available as `arXiv:1205.5252`.
[3] H. A. Helfgott, "Minor arcs for Goldbach's problem", preprint. Available as `arXiv:1305.2897`.
[4] H. A. Helfgott and D. Platt, "Numerical Verification of the Ternary Goldbach conjecture up to 8.875e30", preprint. Available as `arXiv.org:1305.3062`.
[5] M.-Ch. Liu and T. Wang, "On the Vinogradov bound in the three primes Goldbach conjecture", *Acta Arith.* **105** (2002), no. 2, pp. 133–175.
[6] D. Platt, "Numerical computations concerning GRH", preprint. Available as `arXiv:1305.3087`.
[7] I. M. Vinogradov, "Representation of an odd number as a sum of three primes", *Dokl. Akad. Nauk. SSR* **15** (1937), 291–294.

Denominators of Igusa class polynomials

Bianca Viray

(joint work with Kristin Lauter)

Let C be a genus 2 curve over a field k of characteristic 0 and let K be a totally imaginary quadratic extension of a real quadratic field F. We say that C has complex multiplication, or CM, by K if the maximal order $\mathcal{O}_K$ embeds into the endomorphism ring of the Jacobian $J := \mathrm{Jac}(C)$. The theory of complex multiplication shows that there are finitely many genus 2 curves over k, up to

twists, that have CM by K. Therefore, it is natural to consider the following problem.

Problem 1. *Compute all genus* 2 *curves over* k *(up to isomorphism and twists) that have CM by* K*, say, by giving the algebraic equations that define them.*

For a general genus 2 curve, its geometric isomorphism class is determined by its 3 absolute Igusa invariants $\iota_1, \iota_2, \iota_3$. Conversely, an algorithm of Mestre [9] takes as input a tuple of Igusa invariants, and gives as output a genus 2 curve C with those Igusa invariants. Thus, the above problem reduces to finding all tuples of Igusa invariants of CM curves. This in turn is essentially equivalent to computing the *Igusa class polynomials*

$$H_{j,K}(x) := \prod_{C \text{ with } CM \text{ by } \mathcal{O}_K} (x - i_j(C)), \quad j = 1, 2, 3,$$

which are polynomials defined over $\mathbb{Q}$.

Using the theory of Stoll, MichaelCM abelian varieties over $\mathbb{C}$, Spallek, van Wamelen, and Weng give an algorithm to compute a complex approximation of the Igusa class polynomials [10, 11, 12]. However, to recognize the rational coefficients from a complex approximation, one needs a formula, or at least a bound, on the denominators.

Yang showed that the denominators of Igusa class polynomials are a (known) multiple of the arithmetic intersection number $G_1.\mathrm{CM}(K)$ [13], which encodes the number of CM abelian surfaces which decompose as a product of elliptic curves with the product polarization (counted up to isomorphism and with multiplicity). Hence, the last ingredient needed to solve Problem 1 is an upper bound or exact formula for $G_1.\mathrm{CM}(K)$.

In joint work with Lauter, we prove:

Theorem 2 ([7])**.** *For any CM field* K*, there is an explicit upper bound for* $G_1.\mathrm{CM}(K)$ *in terms of the number of ideals in imaginary quadratic orders of a fixed norm and the number of solutions of certain quadratic equations over* $\mathbb{Z}/p^k\mathbb{Z}$*. Moreover, under some assumptions on* K*, this upper bound is exact. (The interested reader may refer to* [7] *for the exact formula.)*

Under strong assumptions on the ramification in $K/\mathbb{Q}$, there is another formula for the $G_1.\mathrm{CM}(K)$ which was conjectured by Bruinier and Yang [2] and later proved by Yang [13, 14]. However, without the assumption on ramification this formula can underestimate $G_1.\mathrm{CM}(K)$ [6], thus, it has limited use in regards to Problem 1.

Work of Goren and Lauter [3, 4] studies the *embedding problem* to give an upper bound, albeit far from sharp, for $G_1.\mathrm{CM}(K)$. The proof of Theorem 2 can be viewed as a refinement of the embedding problem, which enables us to obtain a sharp upper bound for $G_1.\mathrm{CM}(K)$. This refinement naturally involves a generalization of Gross and Zagier's formula for products of differences of j-invariants [5] (see [7, 8] for more details).

Recent work of Bouyer and Streng used Theorem 2 to *provably* compute Igusa class polynomials of CM genus 2 curves that are defined over their reflex field [1]; this demonstrates that our formula is explicit enough to use for computations.

References

[1] Florian Bouyer and Marco Streng. *Examples of CM curves of genus two defined over the reflex field*, Preprint.

[2] Jan Hendrik Bruinier and Tonghai Yang, *CM-values of Hilbert modular functions*, Invent. Math. **163** (2006), no. 2, 229–288.

[3] Eyal Z. Goren and Kristin E. Lauter, *Class invariants for quartic CM fields*, Ann. Inst. Fourier (Grenoble) **57** (2007), no. 2, 457–480 (English, with English and French summaries).

[4] Eyal Z. Goren and Kristin E. Lauter, *Genus 2 curves with complex multiplication*, Int. Math. Res. Not. IMRN 2012, no. 5, 1068–1142.

[5] Benedict H. Gross and Don B. Zagier, *On singular moduli*, J. Reine Angew. Math. 355 (1985), 191–220.

[6] Helen Grundman, Jennifer Johnson-Leung, Kristin Lauter, Adriana Salerno, Bianca Viray, and Erika Wittenborn, *Igusa class polynomials, embeddings of quartic CM fields, and arithmetic intersection theory*, Fields Institute Communications, vol. 60, American Mathematical Society, 2011. WIN - Women in Numbers, Research Directions in Number Theory.

[7] Kristin Lauter and Bianca Viray, *An arithmetic intersection formula for denominators of Igusa class polynomials*, Preprint.

[8] Kristin Lauter and Bianca Viray, *On singular moduli for arbitrary discriminants*, Preprint.

[9] Jean-François Mestre, *Construction de courbes de genre* 2 *à partir de leurs modules*, Effective methods in algebraic geometry (Castiglioncello, 1990), Progr. Math., vol. 94, Birkhäuser Boston, Boston, MA, 1991, pp. 313–334 (French).

[10] Anne-Monika Spallek, *Kurven vom Geschlecht 2 und ihre Anwendung in Public-KeyKryptosystemen*, 1994. Universität Gesamthochschule Essen, Ph. D. Thesis.

[11] Paul van Wamelen, *Examples of genus two CM curves defined over the rationals*, Math. Comp. **68** (1999), no. 225, 307–320.

[12] Annegret Weng, *Constructing hyperelliptic curves of genus* 2 *suitable for cryptography*, Math. Comp. **72** (2003), no. 241, 435–458.

[13] Tonghai Yang, *An arithmetic intersection formula on Hilbert modular surfaces*, Amer. J. Math. **132** (2010), no. 5, 1275–1309.

[14] Tonghai Yang, *Arithmetic intersection on a Hilbert modular surface and the Faltings height*, Preprint, to appear in Asian J. Math.

Computing modular Galois representations

Nicolas Mascot

Summary. We will see how to quickly compute a coefficient of a newform by using a Galois representation. We will show how to do so in time polynomial in the level, by using a half-algebraic, half-numerical method.

Modular forms and diophantine problems. The q-expansion coefficients of a modular form carry deep diophantine information. For instance, if Q is an r-variable definite positive quadratic form with integer coefficients, then the attached theta function

$$\vartheta_Q(q) = \sum_{x \in \mathbb{Z}^r} q^{Q(x)} = \sum_{n=0}^{+\infty} a_n q^n$$

is modular, and its coefficients a_n yield the number of solutions in $\mathbb{Z}^r$ of $Q(x) = n$. Also, in the case of elliptic curves, the Taniyama-Weil theorem asserts that if we consider an elliptic curve E over $\mathbb{Q}$ and let $a_p = |E_{\mathbb{F}_p}(\mathbb{F}_p)| - p - 1$ for p a prime where E has good reduction, then the a_p are the coefficients of a cuspform of weight 2. Consequently, it would be interesting to have fast algorithms to compute the coefficients of a modular form.

On the elliptic curves topic, a famous algorithm invented by R. Schoof computes the number $p + 1 - a_p$ of $\mathbb{F}_p$-rational points of an elliptic curve over $\mathbb{F}_p$ in time polynomial in $\log p$. For this, using the known bound $|a_p| < 2\sqrt{p}$, this algorithm evaluates a_p modulo ℓ for various small primes ℓ by seeing it as the trace of a Frobenius morphism, and deduces a_p using Chinese remainders.

The method to compute modular form coefficients which we will present follows the same pattern. Besides, this method is also interesting for making explicit an attached Galois representation, which can help getting a better understanding of the absolute Galois group of $\mathbb{Q}$, and which yields explicit solutions to the Gross problem, that is to say a non-solvable Galois number field which is ramified at only one prime. Historically, this algorithm idea was suggested by R. Schoof to B. Edixhoven.

The Galois representation attached to a modular form. Consider a newform (that is to say an eigen, new, normalised cuspform)

$$f = q + \sum_{n \geqslant 2} a_n q^n$$

of level N and weight k. The coefficients a_n then lie in the integer ring $\mathbb{Z}_{K_f}$ of a number field K_f. Pick a degree 1 prime $\mathfrak{l}$ of K_f lying above some $\ell \nmid N$. It is then known that there exists a Galois representation

$$\rho_{f,\mathfrak{l}} \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)$$

unramified outside ℓN and such that for every prime $p \nmid \ell N$,

$$\mathrm{Tr}\, \rho_{f,\mathfrak{l}}(\mathrm{Frob}_p) = a_p \bmod \mathfrak{l},$$

where Frob_p denotes (the conjugacy class of) the Frobenius element at p. Bounds are known on a_p, so by computing this representation for various ℓ, we can compute a_p using Chinese remainders.

We will present a method to compute this Galois representation in time polynomial in ℓN. We use the fact that, provided that $\ell > k + 1$, the eigenspace

$$V_{f,\mathfrak{l}} = \bigcap_{n \geqslant 2} \ker \left(T_n - (a_n \bmod \mathfrak{l})\right)\big|_{J_1(\ell N)[\ell]} \subset J_1(\ell N)[\ell]$$

of the ℓ-torsion $J_1(\ell N)[\ell]$ of the Jacobian $J_1(\ell N)$ of the modular curve $X_1(\ell N)$, where the T_n denote the Hecke operators, has dimension exactly 2 over $\mathbb{F}_\ell$, and that the Galois action on its points yields the Galois representation $\rho_{f,\mathfrak{l}}$.

We will first see how to efficiently compute the period lattice of the modular curve $X_1(\ell N)$, and then how to use these periods to compute complex approximations of the points of the space $V_{f,\mathfrak{l}}$. Our method is based on the application of

K. Khuri-Makdisi's algorithms to modular curves so as to invert the Abel-Jacobi map using Newton iteration.

Finally, we will see how effective Galois theory algorithms from the Dokchitser brothers can be used to compute the image in $\mathrm{GL}_2(\mathbb{F}_\ell)$ of the Frobenius element at p in time polynomial in $\log p$. This yields a quick method to compute $a_p \bmod \mathfrak{l}$ for huge p.

For instance, if we pick $f = \Delta$ and $\mathfrak{l} = 29$, we can compute the following :

p	Similarity class of $\rho_{\Delta,29}(\mathrm{Frob}_p)$	$\tau(p) \bmod 29$
$10^{1000} + 453$	$\begin{bmatrix} 0 & 5 \\ 1 & 21 \end{bmatrix}$	21
$10^{1000} + 1357$	$\begin{bmatrix} 0 & 28 \\ 1 & 8 \end{bmatrix}$	8
$10^{1000} + 2713$	$\begin{bmatrix} 0 & 9 \\ 1 & 11 \end{bmatrix}$	11
$10^{1000} + 4351$	$\begin{bmatrix} 0 & 26 \\ 1 & 0 \end{bmatrix}$	0
$10^{1000} + 5733$	$\begin{bmatrix} 20 & 0 \\ 0 & 2 \end{bmatrix}$	22
$10^{1000} + 7383$	$\begin{bmatrix} 19 & 0 \\ 0 & 10 \end{bmatrix}$	0

Complexity news: discrete logarithms in small-characteristic multiplicative groups — the algorithm of Barbulescu, Gaudry, Joux & Thomé

Dan Bernstein

We present a recent breakthrough [1] in the discrete logarithm problem, due to R. Barbulescu, P. Gaudry, A. Joux and E. Thomé.

References

[1] Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, and Emmanuel Thomé - **A quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic**. Preprint available on arXiv, http://arxiv.org/abs/1306.4244

Hurwitz number fields

David P. Roberts

The talk was an overview of a class of number fields called Hurwitz number fields which I have been studying along with Akshay Venkatesh for several years. It focused on why Hurwitz number fields are interesting from the point of view of mass heuristics, although there are many other reasons that Hurwitz number fields are of interest as well.

Call a degree m number field K *full* if its associated Galois group $\mathrm{Gal}(K)$ is all of A_m or S_m. For P a finite set of primes, let $F_P(m)$ be the number of full degree m number fields ramified within P. Bhargava's mass heuristic applied to this context says that one should expect that for any fixed P the sequence $F_P(m)$ is eventually zero.

Say that P is *anabelian* if it contains the set of primes dividing the order of a finite nonabelian simple group G. For example, the anabelian sets of size at most 3 are $\{2,3,p\}$ for $p = 5, 7, 13, 17$. In sharp contradiction to the mass heuristic, we conjecture the following:

Unboundedness Conjecture. *For anabelian P the sequence $F_P(m)$ is unbounded.*

After presenting the above material, the talk focused on Hurwitz number fields and how they support the above conjecture.

A "Hurwitz parameter" $h = (G, C, \nu)$ determines a cover of $\pi_h : \mathrm{HUR}_h \to \mathrm{CONF}_\nu$ of varieties defined over $\mathbb{Q}$. Here the cover HUR_h parametrizes covers of the projective line of type h, the base CONF_ν parameterizes suitable divisors in the projective line, and the map π_h sends a cover to its branch locus. The cover π_h has good reduction outside the set of primes dividing $|G|$. Hurwitz number fields then correspond to fibers $\pi_h^{-1}(u)$ above rational points $u \in \mathrm{CONF}_\nu(\mathbb{Q})$.

We have proved a geometric theorem analogous to the unboundedness conjecture as follows. For each finite nonabelian simple group G there are infinitely many pairs (C, ν) such that the degree m cover $\pi_{G,C,\nu}$ has monodromy group A_m or S_m. This geometric fullness result also applies to groups G that are sufficiently near to nonabelian simple, such as symmetric groups S_d.

To prove the unboundedness conjecture, the remaining step would be to prove that specialization is not extremely non-generic. We have worked out many examples suggesting that in fact specialization is extremely generic. The talk presented one example, based on $G = S_6$. The cover π_h has degree 202. There are exactly 2947 $PGL_2(\mathbb{Q})$-equivalence classes of specialization points which are guaranteed to produce algebras ramified within $\{2,3,5\}$. Computation shows that these algebras are all fields with Galois group A_{202} or S_{202} and they are all distinct. Already this example shows the mass heuristic does not apply in our vertical direction, as it gives approximately 10^{-16} as the expected value of $\sum_{m \geq 202} F_{\{2,3,5\}}(m)$.

Selmer groups and class groups

Kęstutis Česnavičius

Let l be a prime, K a number field, $\mathcal{O}_K$ its ring of integers, and $A \to \operatorname{Spec} K$ an abelian variety of dimension $g > 0$. Our goal was to explain how under certain assumptions on $A[l]$, the l-Selmer group $\operatorname{Sel}_l A$ relates to the l-torsion subgroup $\operatorname{Pic}(\mathcal{O}_K)[l]$ of the ideal class group of K. The talk was based on [2], which in turn relies on [1].

1. Fppf cohomological interpretation of Selmer groups

The l-Selmer group of A is defined by insisting that the diagram

$$\begin{array}{ccc} \operatorname{Sel}_l A & \hookrightarrow & H^1(K, A[l]) \\ \downarrow & & \downarrow \\ \prod_v A(K_v)/lA(K_v) & \hookrightarrow & \prod_v H^1(K_v, A[l]) \end{array}$$

be Cartesian (the products are indexed by the places of K). The finite l-torsion abelian group $\operatorname{Sel}_l A$ contains $A(K)/lA(K)$ as a subgroup.

Let $\mathcal{A} \to \operatorname{Spec} \mathcal{O}_K$ be the Néron model of A. For $v \nmid \infty$, let $\mathcal{O}_v$ and $\mathbb{F}_v$ be the ring of integers and the residue field of K_v and $c_v := \#(\mathcal{A}_{\mathbb{F}_v}/\mathcal{A}^0_{\mathbb{F}_v})(\mathbb{F}_v)$ the local Tamagawa factor of A at v. The promised relation between $\operatorname{Sel}_l A$ and $\operatorname{Pic}(\mathcal{O}_K)[l]$ will use the following interpretation of the l-Selmer group:

Theorem 1. *Suppose that A has semiabelian reduction at all $v \mid l$. Then the diagram*

$$\begin{array}{ccc} H^1_{\mathrm{fppf}}(\mathcal{O}_K, \mathcal{A}[l]) & \hookrightarrow & H^1(K, A[l]) \\ \downarrow & & \downarrow \\ \prod_{v \nmid \infty} H^1_{\mathrm{fppf}}(\mathcal{O}_v, \mathcal{A}[l]) & \hookrightarrow & \prod_{v \nmid \infty} H^1(K_v, A[l]) \end{array}$$

is Cartesian. If $l \nmid \prod_{v \nmid \infty} c_v$ and either l is odd or $A(K_v)$ is connected for every real v, then $\operatorname{Sel}_l A = H^1_{\mathrm{fppf}}(\mathcal{O}_K, \mathcal{A}[l])$ inside $H^1(K, A[l])$.

An analogous result holds in the case of a global function field.

2. Selmer groups and class groups in quadratic extensions

The following conjectures are folklore:

Conjecture 2. *As L/K ranges over quadratic extensions, $\#\operatorname{Pic}(\mathcal{O}_L)[l]$ is unbounded.*

Conjecture 3. *As L/K ranges over quadratic extensions, $\#\operatorname{Sel}_l A_L$ is unbounded.*

Not a single case of these conjectures is known for odd l. Due to the genus theory of Gauss, Conjecture 2 is known for $l = 2$, which allows the deduction of Conjecture 3 in certain $l = 2$ cases:

Theorem 4.

(a) If $\mu_l \subset A[l]$ or $\mathbb{Z}/l\mathbb{Z} \subset A[l]$ (over K), then Conjecture 2 for (K, l) implies Conjecture 3 for (A, l).

(b) If $A[l]$ has a filtration by K-subgroups with subquotients $\mathbb{Z}/l\mathbb{Z}$ or μ_l, then Conjecture 3 for (A, l) implies Conjecture 2 for (K, l).

For the proof, one establishes the corresponding structure claims for $\mathcal{A}[l]_U$ for a suitable nonempty open $U \subset \operatorname{Spec} \mathcal{O}_L$, relates $\#H^1_{\mathrm{fppf}}(\mathcal{O}_L, \mathbb{Z}/l\mathbb{Z})$ and $\#H^1_{\mathrm{fppf}}(\mathcal{O}_L, \mu_l)$ to $\#\operatorname{Pic}(\mathcal{O}_L)[l]$, and uses (a variant of) Theorem 1 for the relation to $\#\operatorname{Sel}_l A_L$. Similar techniques combine with the result of Shafarevich and Tate, which provides rank (and hence also l-Selmer) growth, to prove certain cases of the function field analogue of Conjecture 2:

Theorem 5. *Fix a prime p, and for a global field L of characteristic p, let S^L be the proper smooth curve with function field L. Then for each prime $l \neq p$, there is a $q = p^{n(l)}$ such that $\#\operatorname{Pic}(S^L)[l]$ is unbounded as $L/\mathbb{F}_q(t)$ ranges over quadratic extensions.*

3. An application to Iwasawa theory

Another setting where the growth of Selmer groups and class groups is considered is that of Iwasawa theory. Let K_∞/K be the cyclotomic $\mathbb{Z}_l$-extension of K, and let K_n/K be its degree l^n-subextension. Iwasawa proved the existence of integers μ, λ, ν with $\mu, \lambda \geq 0$ such that $\#\operatorname{Pic}(\mathcal{O}_{K_n})[l^\infty] = l^{\mu l^n + \lambda n + \nu}$ for large n and conjectured that $\mu = 0$. Thanks to [3], Iwasawa's conjecture is known for abelian $K/\mathbb{Q}$. The methods used to prove Theorems 4 and 5 also give

Theorem 6. *Iwasawa's $\mu = 0$ conjecture holds for K and l if there is an abelian variety $A \to \operatorname{Spec} K$ satisfying*

(1) A has good ordinary reduction at all $v \mid l$;

(2) $\mathbb{Z}/l\mathbb{Z} \subset A[l]$;

(3) $\operatorname{Hom}(\operatorname{Sel}_{l^\infty} A_{K_\infty}, \mathbb{Q}_l/\mathbb{Z}_l)$ is $\mathbb{Z}_l[[\operatorname{Gal}(K_\infty/K)]]$-torsion with μ-invariant 0.

In fact, it suffices to find such an A after replacing K by a finite extension. Although it is not clear how to do this in general, for $K = \mathbb{Q}$ and $l = 5$ one of the elliptic curves of conductor 11 satisfies 1-3.

References

[1] K. Česnavičius, *Selmer groups as flat cohomology groups*, preprint (2013), `http://arxiv.org/abs/1301.4724`.

[2] K. Česnavičius, *Selmer groups and class groups*, preprint (2013), `http://arxiv.org/abs/1307.4261`.

[3] B. Ferrero and L. C. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. (2) **109** (1979), 377–395.

Most hyperelliptic curves over $\mathbb{Q}$ are pointless

Manjul Bhargava

We consider all hyperelliptic curves C over $\mathbb{Q}$ of genus g expressed in the form

$$C : z^2 = f(x, y) = f_0x^n + f_1x^{n-1}y + \cdots + f_ny^n$$

where f is a separable polynomial over $\mathbb{Q}$ of degree $n = 2g + 2$ and the f_i are integers. Define the height of C by $\max\{|f_i|\}$. Then we prove that, if all such hyperelliptic curves C over $\mathbb{Q}$ of genus g are ordered by height, then as g tends to infinity:

- a density approaching 100% of hyperelliptic curves of genus g have no rational points;
- a density approaching 100% of hyperelliptic curves of genus g that have points everywhere locally fail the Hasse principle; and
- a density approaching 100% of hyperelliptic curves of genus g have empty Brauer set, i.e., have a Brauer-Manin obstruction to having a rational point.

We also prove positive proportion results of this type for individual small genera, including $g = 1$.

Automorphic period lattices

Akshay Venkatesh

Unfortunately, this speaker failed to submit a summary of his talk.

Computing zeta functions of low genus curves in average polynomial time

Andrew V. Sutherland
(joint work with David Harvey)

Let $X/\mathbb{Q}$ be a smooth projective curve of genus g, and let $X_p/\mathbb{F}_p$ denote its reduction modulo a prime p. For primes p of good reduction for X, we define the *L-polynomial* $L_p(T)$ as the numerator of the zeta function

$$Z(X_p; T) = \exp\left(\sum_{n=1}^{\infty} \#X_p(\mathbb{F}_{p^n})\frac{T^n}{n}\right) = \frac{L_p(T)}{(1-T)(1-pT)}.$$

Given a bound N, we consider the following problem: compute $L_p(T)$ for all primes $p \le N$ of good reduction for X. This problem arises, for example, when one wishes to compute the L-function

$$L(X; s) = \prod_p L_p(p^{-s})^{-1},$$

and when computing Sato-Tate distributions, as in [2].

In [1], Harvey gives an algorithm to solve this problem in the case that X is a hyperelliptic curve with a rational Weierstrass point, with a running time of $O(g^{8+\epsilon} N \log^{3+\epsilon} N)$. When averaged over primes $p \leq N$, this complexity is polynomial in both g and $\log p$, the first such result. Moreover, the dependence on $\log p$ is substantially better than existing methods for all $g > 1$. I will present joint work in progress to develop an efficient practical implementation of this algorithm for low genus curves, and discuss generalizations to non-hyperelliptic curves.

As an intermediate result, we obtain an efficient algorithm to compute the Hasse-Witt matrix W_p of X_p for all good primes $p \leq N$ in $O(g^{2+\omega} N \log^{3+\epsilon} N)$ time using $O(g^3 N)$ space, where $\omega \leq 3$ is the exponent of matrix multiplication. The matrix W_p determines $L_p(T) \bmod p$, which suffices to determine the trace of Frobenius for sufficiently large p. For $g \leq 3$ the full L-polynomial can then be determined in time $O(p^{1/4} \log^{1+\epsilon} p)$, which is in practice negligible compared to the average time to compute W_p for feasible values of $p \leq N$.

This algorithm is applicable to all hyperelliptic curves, not just those with a rational Weierstrass point, and we are currently working on extending the algorithm to handle arbitrary curves of genus 3. Its performance is already superior to existing methods in genus 2 for $N \geq 2^{21}$, which is well within the feasible range, and we expect even better results in genus 3.

References

[1] D. Harvey, *Counting points on hyperelliptic curves in average polynomial time*, arXiv:1210.8239, 2013.

[2] F. Fité, K.S. Kedlaya, V. Rotger, A.V. Sutherland, *Sato-Tate distributions and Galois endomorphisms in genus 2*, Compositio Mathematica **148** (2012), 1390–1442.

Effective S-unit and norm-form equations in several variables

Michael A. Bennett

If S is a finite set of primes in a number field K, containing S_∞, the infinite places, an equation of the shape

$$a_1 x_1 + \cdots + a_n x_n = 0,$$

where the a_i are fixed elements of K and the x_i are S-units, is called an *S-unit equation*. Such equations arise rather naturally in a variety of contexts, including, for example, the problem of finding all binary forms of a given degree and discriminant.

S-unit equations in more than 2 such homogeneous variables are known, via work of Evertse, to have at most finitely many "nontrivial" solutions. If, however, the number of such variables exceeds three, it is, in general, unknown how to make such a statement effective (the result for three variables is a consequence of Baker's lower bounds for linear forms in logarithms, complex and p-adic).

If we restrict the cardinality of S, however, Vojta [1] was able to prove

Theorem 1. *(Vojta, 1983) Let K be a number field, S a finite set of places of K, containing S_∞, and $a_1, \ldots, a_4$ be nonzero elements of K. If, additionally, we assume that S has at most 3 elements, then there is an effectively computable upper bound on the heights of nontrivial solutions of the equation*

$$a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4 = 0.$$

Note that this theorem is only applicable for certain signatures of number fields K with $[K : \mathbb{Q}] \leq 6$. This result actually follows from a more general one, namely :

Theorem 2. *(Vojta, 1983) Let n and m be positive integers with $n > m$. Let (a_{ij}) be an $m \times n$ matrix with elements in a number field K, such that no $m+1$ distinct columns of the matrix have rank less than m, and such that no column is identically zero. Assume further that S is a finite set of places of K, containing the infinite places and satisfying*

$$(n - m - 2)\,|S| < n.$$

Then solutions in S-units to the system of equations

$$a_{i1}x_1 + \cdots + a_{in}x_n = 0, \;\; 1 \leq i \leq m$$

may be "effectively determined".

Our main result is

Theorem 3. *Let n and m be positive integers with $n > m$. Let (a_{ij}) be an $m \times n$ matrix with elements in a number field K, such that no $m+1$ distinct columns of the matrix have rank less than m, and such that no column is identically zero. Assume further that S is a finite set of places of K, containing the infinite places and satisfying*

$$(n - m - 1)\,|S| < 2n.$$

Then solutions in S-units to the system of equations

$$a_{i1}x_1 + \cdots + a_{in}x_n = 0, \;\; 1 \leq i \leq m$$

may be "effectively determined".

This enables us to extend Vojta's result to 5-term equations :

Theorem 4. *Let K be a number field, S a finite set of places of K, containing S_∞, and $a_1, \ldots, a_5$ be nonzero elements of K. If, additionally, we assume that S has at most 3 elements, then there is an effectively computable upper bound on the heights of nontrivial solutions of the equation*

$$a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4 + a_5x_5 = 0.$$

Another corollary, stated rather vaguely, is the following :

Corollary 5. *We can "effectively solve" the norm form equation*

$$N_{K/\mathbb{Q}}(x\alpha_1 + y\alpha_2 + z\alpha_3 + w\alpha_4) = n$$

provided

- *K is totally-complex Galois*
- *The α_i are linearly independent over $\mathbb{Q}$*
- *The α_i/α_j generate K over $\mathbb{Q}$*

Our main new technique here is a simple, combinatorial lemma.

References

[1] P. Vojta, Integral Points on Varieties, Dissertation, Harvard University, 1983.

Reporter: Nicolas Mascot

Participants

Dr. Jennifer S. Balakrishnan
Department of Mathematics
Harvard University
Science Center
One Oxford Street
Cambridge MA 02138-2901
UNITED STATES

Prof. Dr. Karim Belabas
Laboratoire d'Algorithmique
Arithmetique
Université Bordeaux I
351, cours de la Liberation
33405 Talence Cedex
FRANCE

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

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
UNITED STATES

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

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

Prof. Dr. Yuri Bilu
A2X, IMB
Université Bordeaux I
351, cours de la Liberation
33405 Talence Cedex
FRANCE

Prof. Dr. Kathrin Bringmann
Mathematisches Institut
Universität zu Köln
50923 Köln
GERMANY

Prof. Dr. Nils Bruin
Dept. of Mathematics and Statistics
Simon Fraser University
Burnaby, B.C. V5A 1S6
CANADA

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

Kestutis Cesnavicius
Department of Mathematics
MIT
Cambridge, MA 02139
UNITED STATES

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

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

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

PD Dr. Claus Diem
Mathematisches Institut
Universität Leipzig
Johannisgasse 26
04103 Leipzig
GERMANY

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

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

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

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

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

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

Prof. Dr. Harald Helfgott
Dept. de Mathématiques et Applications
École Normale Superieure
45, rue d'Ulm
75230 Paris Cedex 05
FRANCE

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

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

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

Nicolas Mascot
Centre de Recherche en Mathématique de Bordeaux, CNRS
Université de Bordeaux 1
351, cours de la Liberation
33405 Talence Cedex
FRANCE

Dr. Anton Mellit
International Centre for Theoretical Physics (ICTP)
Strada Costiera 11
34100 Trieste
ITALY

Prof. Dr. Jean-Francois Mestre
U. F. R. de Mathématiques
Case 7012
Université Paris VII
75013 Paris
FRANCE

Dr. Pascal Molin
Inst. de Mathématiques de Jussieu
Université Paris VII
75013 Paris
FRANCE

Dr. Pierre Parent
Mathématiques et Informatique
Université Bordeaux I
351, cours de la Liberation
33405 Talence Cedex
FRANCE

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

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

Dr. Marusia Rebolledo
Laboratoire de Mathématiques
Université Blaise Pascal
Clermont-Ferrand II
Campus Univ. des Cézeaux
63177 Aubiere
FRANCE

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

Prof. Dr. Fernando Rodriguez-Villegas
Mathematics Section
The Abdus Salam Intern. Centre for Theoretical Physics (I.C.T.P.)
Strada Costiera 11
34151 Trieste
ITALY

Prof. Dr. Karl Rubin
Department of Mathematics
University of California, Irvine
Irvine, CA 92697-3875
UNITED STATES

Prof. Dr. Rene Schoof
Dipartimento di Matematica
Universita degli Studi di Roma II
Tor Vergata
Via della Ricerca Scientifica
00133 Roma
ITALY

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

Prof. Dr. Alice Silverberg
Department of Mathematics
University of California, Irvine
Irvine, CA 92697-3875
UNITED STATES

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

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

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

Prof. Dr. Peter Swinnerton-Dyer
Department of Pure Mathematics and
Mathematical Statistics
University of Cambridge
Wilberforce Road
Cambridge CB3 0WB
UNITED KINGDOM

Prof. Dr. Douglas Ulmer
School of Mathematics
Georgia Institute of Technology
686 Cherry Street
Atlanta, GA 30332-0160
UNITED STATES

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

Dr. Bianca Viray
Department of Mathematics
Brown University
Box 1917
Providence, RI 02912
UNITED STATES

Dr. Masha Vlasenko
School of Mathematical Sciences
Trinity College Dublin
College Green
Dublin 2
IRELAND

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

Xiaoheng Jerry Wang
Department of Mathematics
Harvard University
Science Center
One Oxford Street
Cambridge MA 02138-2901
UNITED STATES

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

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

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

Dr. David Zywina
School of Mathematics
Institute for Advanced Study
1 Einstein Drive
Princeton, NJ 08540
UNITED STATES