Mathematisches Forschungsinstitut Oberwolfach

Report No. 32/2005

Explicit Methods in Number Theory

Organised by
Henri Cohen (Talence)
Hendrik W. Lenstra (Leiden)
Don B. Zagier (Bonn)

July 17th – July 23rd, 2005

Abstract. These notes contain extended abstracts on the topic of explicit methods in number theory. The range of topics included modular forms, varieties over finite fields, rational and integral points on varieties, class groups, and integer factorization.

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

Introduction by the Organisers

The workshop *Explicit Methods in Number Theory* was organised by Henri Cohen (Talence), Hendrik W. Lenstra (Leiden), and Don B. Zagier (Bonn) and was held July 17–23, 2005. Three previous workshops on the topic had been held in 1999, 2001, and 2003. The goal of this meeting was to present new methods and results on concrete aspects of number theory. In many cases, this included computational and experimental work, but the primary emphasis was placed on the implications for number theory rather than on the computational methods employed.

There was a 'mini-series' of five 1-hour morning talks given by Bas Edixhoven, Johan Bosman, Robin de Jong, and Jean-Marc Couveignes on the topic of computing the coefficients of modular forms. Let

$$\Delta = q \prod_{n \geq 1} (1 - q^n)^{24} = \sum_{n \geq 1} \tau(n) q^n$$

be Ramanujan's tau function, a newform of weight 12 for $SL_2(\mathbb{Z})$. The speakers exhibited a method to compute $\tau(p)$ for p prime in time polynomial in $\log p$.

Some of the other main themes included:

- Modular forms, q-expansions, and Arakelov geometry
- Rational and integral points on curves and higher-dimensional varieties
- Integer factorization

- Counting points on varieties over finite fields
- Class groups of quadratic and cubic fields and their relationship to geometry, analysis, and arithmetic.

As always in Oberwolfach, the atmosphere was lively and active, providing an ideal environment for the exchange of ideas and productive discussions. This meeting was well-attended—with over 50 participants from a variety of backgrounds and with broad geographic representation from all continents, including a number of younger researchers. There were 30 talks of various lengths, and ample time was allotted for informal collaboration.

Workshop: Explicit Methods in Number Theory

Table of Contents

Abstracts

On the computation of the coefficients of a modular form, I: introduction

Bas Edixhoven
(joint work with Jean-Marc Couveignes, Robin de Jong)

The following text is based on notes taken by Bjorn Poonen. I thank him for letting me use his notes. The responsibility for mistakes in this text is mine. As this text has been edited shortly after the conference, it also reflects some comments from and discussions with the audience.

Let

$$\Delta = q\prod_{n\geq 1}(1-q^n)^{24} = \sum_{n\geq 1}\tau(n)q^n$$

with $q = e^{2\pi iz}$ for $z \in \mathcal{H}$ (the upper half plane). This Δ is a newform of weight 12 for $\mathrm{SL}_2(\mathbb{Z})$.

If one has the factorization of n, one can easily compute $\tau(n)$ in terms of the $\tau(p)$ for primes p dividing n. (If one can compute the coefficient $\sigma_{k-1}(n)$ of the Eisenstein series E_k, one can go backwards, and factor n. It's not clear that one can do this for τ.)

Theorem 1 (Deligne 1969)**.** *For all primes ℓ, there is a unique continuous semi-simple representation*

$$\rho_\ell\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(V_\ell)$$

where V_ℓ is a 2-dimensional $\mathbb{F}_\ell$-vector space, unramified outside ℓ, such that for all primes $p \neq \ell$,

$$\det(1 - x\,\mathrm{Frob}_p\,|V_\ell) = 1 - x\tau(p) + x^2p^{11}$$

in $\mathbb{F}_\ell[x]$.

Later Deligne showed also that $|\tau(p)| < 2p^{11/2}$. (Hecke had proved $|\tau(p)| = O(p^6)$, with an explicit constant, and this will suffice for our purposes.)

Aim of the project:

(1) To show that ρ_ℓ can be computed in time polynomial in ℓ.
(2) To show that for big primes p, the value of $\tau(p)$ can be computed in time polynomial in $\log p$. (Question of René Schoof)

The first can be used to do the second. We claim that these can be done in deterministic polynomial time, but our presentation will use randomness.

Theorem 2 (Swinnerton-Dyer and Serre 1972)**.** *For $\ell \notin \{2,3,5,7,23,691\}$, we have $\mathrm{Im}\,\rho_\ell \supseteq \mathrm{SL}(V_\ell)$; i.e.,*

$$\mathrm{Im}(\rho_\ell) = \{g \in \mathrm{GL}(V_\ell) : \det g \textit{ is an } 11\textit{-th power}\}.$$

In what follows we will suppose that $\ell \notin \{2,3,5,7,23,691\}$.

Theorem 3 (Deligne 1969)**.** *The dual representation $V_\ell^\vee$ is contained in the* 11*th étale cohomology group $H^{11}(E^{10}_{\overline{\mathbb{Q}},\mathrm{et}}, \mathbb{F}_\ell)$ of the* 11*-dimensional variety that is the* 10*-th fibered power of the universal elliptic curve over the j-line. Also,*

$$V_\ell^\vee = H^1(j\text{-}line_{\overline{\mathbb{Q}},\mathrm{et}}, \mathrm{Sym}^{10}(R^1\pi_*\mathbb{F}_\ell)).$$

Let X_ℓ be the modular curve $X_1(\ell)$, and let J_ℓ be its Jacobian. Then $V_\ell \subset J_\ell(\overline{\mathbb{Q}})[\ell]$. We have

$$X_\ell(\mathbb{C}) = \Gamma_1(\ell)\backslash(\mathcal{H} \cup \mathbb{P}^1(\mathbb{Q}))$$

where $\Gamma_1(\ell)$ is the inverse image in $\mathrm{SL}_2(\mathbb{Z})$ of the subgroup $\begin{pmatrix} 1 & * \\ & 1 \end{pmatrix}$ of $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$. This is related to the fact that Δ is congruent modulo ℓ to a weight 2 form of level ℓ. The genus of X_ℓ is about $\ell^2/24$. Let $\mathbb{T}_\ell \subset \mathrm{End}(J_\ell)$ be the Hecke algebra, generated by the T_n, $n \geq 1$, and $\langle a \rangle$, for $a \in \mathbb{F}_\ell^\times$. As a $\mathbb{Z}$-module, it is free of rank g_ℓ. Then

$$V_\ell = \bigcap_{1 \leq i \leq (\ell^2-1)/6} \ker\left(T_i - \tau(i), J_\ell(\overline{\mathbb{Q}})[\ell]\right) :$$

this follows from a multiplicity 1 result and a result of Jacob Sturm bounding the number of i needed.

Strategy: Choose an effective divisor $D = P_1 + \cdots + P_{g_\ell}$ of degree g_ℓ on $X_{\ell,\mathbb{Q}}$ and a map $f\colon X_{\ell,\mathbb{Q}} \twoheadrightarrow \mathbb{P}^1_{\mathbb{Q}}$. Then:

$$X_1(\mathbb{C})^{g_\ell} \to J_\ell(\mathbb{C}) = \mathbb{C}^{g_\ell}/\Lambda_\ell$$

$$(Q_1, \ldots, Q_{g_\ell}) \mapsto [Q_1 + \cdots + Q_{g_\ell} - D] = \sum_{i=1}^{g_\ell} \int_{P_i}^{Q_i} (\omega_1, \ldots, \omega_{g_\ell}),$$

where the ω_i are newforms, normalized by $a_1(\omega_i) = 1$, and $\Lambda_\ell = H_1(X_\ell(\mathbb{C}), \mathbb{Z})$. Since the induced map $\mathrm{Sym}^{g_\ell} X_\ell \to J_\ell$ is a birational morphism, with some luck, for all nonzero $x \in V_\ell$, there exists a unique effective $D'_x = Q_{x,1} + \cdots + Q_{x,g_\ell}$ of degree g_ℓ with $[D'_x - D] = x$, and D'_x is disjoint from the poles of f. The uniqueness of D'_x satisfying $[D'_x - D] = x$ is equivalent to $h^0(X_{\ell,\overline{\mathbb{Q}}}, \mathcal{L}_x(D)) = 1$, where $\mathcal{L}_x$ is the line bundle corresponding to x.

Consider the polynomial

$$P_\ell := \prod_{x \in V_\ell - \{0\}} (T - \sum_i f(Q_{x,i})) \in \mathbb{Q}[T]$$

of degree $\ell^2 - 1$. One could use a variant

$$\prod_{\text{lines } L \subset V_\ell} (T - \sum_{0 \neq x \in L} \sum_i f(Q_{x,i})),$$

which has degree $\ell + 1$.

Now P_ℓ can be approximated in $\mathbb{C}[T]$, or computed modulo p in $\mathbb{F}_p[T]$ for many p.

Theorem 4. *(not completely written up yet) There exists an explicit c (maybe $c = 16$) such that for all ℓ, one can choose D and f so that the logarithmic height of the coefficients of P_ℓ are $O(\ell^c)$.*

The proof of this theorem is the subject of lectures 3 and 4 of this series.

Choice of D: We will do this on X_ℓ redefined as $X_1(5\ell)$, and with D over $\mathbb{Q}(\zeta_\ell)$ (this not change anything above significantly).

Idea: Specialize to $X_{\ell,\overline{\mathbb{F}}_\ell}$. As $x \rightsquigarrow 0$, $\mathcal{L}_x \rightsquigarrow \mathcal{O}_{X_{\ell,\overline{\mathbb{F}}_\ell}}$. For a place of $\overline{\mathbb{Q}}$ over ℓ, the kernel of reduction modulo ℓ in V_ℓ is a line if $\ell \nmid \tau(\ell)$, and is V_ℓ if $\ell \mid \tau(\ell)$.

Note: $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_\ell))$ acts transitively on $V_\ell - \{0\}$, and fixes D, so $h^0(X_{\ell,\overline{\mathbb{Q}}}, \mathcal{L}_x(D))$ is independent of x. All we need is that $h^0(X_{\ell,\overline{\mathbb{F}}_\ell}, \mathcal{O}(D)) = 1$. Equivalently by Riemann-Roch and Serre duality, we need $h^0(X_{\ell,\overline{\mathbb{F}}_\ell}, \Omega(-D)) = 0$.

Let X_1, X_2 be the two components of $X_{\ell,\overline{\mathbb{F}}_\ell}$, and let $\Sigma = X_1 \cap X_2$. Then $X_1 \to X_1(5)_{\overline{\mathbb{F}}_\ell} \overset{x}{\tilde{\to}} \mathbb{P}^1_{\overline{\mathbb{F}}_\ell}$. The curve X_1 has an equation $y^{\ell-1} = f(x)$ where f has degree $\ell - 1$ and simple zeros, and Σ is the set of zeros of y. Then $D = D_1 + D_2$ with D_1 on X_1 and D_2 on X_2.

Recipe for D_1: distribute the multiplicities $0, 1, \ldots, \ell - 2$ over the $\ell - 1$ zeros of x on X_1. For D_2: — $0, 0, 1, 2, \ldots, \ell - 3$.

Characterizing characteristic 0 function fields

Bjorn Poonen

Consider first-order formulas in the language of rings. We will not give a precise definition of first-order formula here, but loosely speaking it is an expression built up from the symbols $+, \cdot, 0, 1, =, (,)$, the logical relations $\wedge$ ("and"), $\vee$ ("or"), $\neg$ ("not"), the quantifers $\forall$ ("for all") and $\exists$ ("there exists"), and variables $x, y, z, \ldots$. For instance,

$$(\forall y)(\exists z)(\exists w) \quad (x \cdot z + 1 + 1 = y^2) \ \vee \ \neg(z = x + w)$$

is a first-order formula. In this example, the variables y, z, w are bound by quantifiers, and the variable x is free. A first-order formula in which all variables are bound by quantifiers is called a first-order sentence. From now on, it will be understood that formulas and sentences are first-order formulas and sentences.

If we fix a ring R, then it is understood that the variables represent elements in R. (In contrast, second-order logic allows variables ranging over subsets.) Then for each assignment of elements of R to the free variables, we get a truth value. In particular, a sentence has a truth value for each ring R.

It is important, especially when trying to transfer results from one ring to another, to know whether a ring-theoretic property can be expressed by the truth of a first-order sentence. For example, it is a basic theorem of model theory that a sentence true for one algebraically closed field of characteristic 0 is true for all algebraically closed fields of characteristic 0; it is because of this that many

theorems proved for $\mathbb{C}$ using analytic methods are known to hold for arbitrary algebraically closed fields of characteristic 0.

By compactness, there does not exist a sentence that for each field K is true if and only if K is of characteristic 0. We prove that, on the other hand, there is a sentence with this property if we consider only *finitely generated* fields, that is, fields that are finitely generated (as a field) over the prime subfield. Such fields are the finite extensions of rational function fields $\mathbb{F}_p(t_1, \ldots, t_n)$ or $\mathbb{Q}(t_1, \ldots, t_n)$.

Theorem 1. *There is a sentence that is true for all finitely generated fields of characteristic* 0*, and false for all finitely generated fields of characteristic* > 0*.*

The proof makes use of two earlier results. To state these, we need a few definitions.

Definition 2. The Kronecker dimension of a finitely generated field K is

$$\operatorname{Krdim} K := \begin{cases} \operatorname{trdeg}(K/\mathbb{F}_p), & \text{if } \operatorname{char} K = p > 0 \\ \operatorname{trdeg}(K/\mathbb{Q}) + 1, & \text{if } \operatorname{char} K = 0. \end{cases}$$

A global field is a finitely generated field K with $\operatorname{Krdim} K = 1$; such a field is either a number field (finite extension of $\mathbb{Q}$) or a global function field (function field of a curve over a finite field).

Definition 3. The Pfister form $\langle\langle a_1, \ldots, a_n\rangle\rangle$ is the diagonal quadratic form in 2^n variables whose coefficients are $\prod_{i\in S} a_i$ as S ranges through subsets of $\{1, \ldots, n\}$. For example, $\langle\langle a, b\rangle\rangle$ is the quadratic form

$$x_1^2 + ax_2^2 + bx_3^2 + abx_4^2.$$

Among other things, R. Rumely proved our Theorem 1 for global fields:

Theorem 4 ([Rum80])**.** *There is a sentence that is true for all number fields and false for all global function fields.*

Rumely's idea was to build on work of J. Robinson to define the family of valuation rings of a global field K in a uniform first-order way, and then to observe that a global field is a number field if and only if the intersection of the valuation rings is not a field.

F. Pop, as part of his work on the "elementary equivalence versus isomorphism" problem for finitely generated fields, discovered that recent work on isotropy of Pfister forms could be used to characterize fields of given Kronecker dimension:

Theorem 5 ([Pop02])**.** *For each* $n \in \mathbb{N}$ *and finitely generated field* K*, we have* $\operatorname{Krdim} K \leq n$ *if and only if either*

- $2 = 0$ *and* $[K : K^2] \leq 2^n$*, or*
- $2 \neq 0$ *and every Pfister form* $\langle\langle a_1, \ldots, a_{n+2}\rangle\rangle$ *over* $K(\sqrt{-1})$ *represents* 0 *over* $K(\sqrt{-1})$*.*

Thus, for each $n \in \mathbb{N}$*, there is a sentence* σ_n *that for a finitely generated field* K *holds if and only if* $\operatorname{Krdim} K = n$*.*

Definition 6. If ϕ is a first-order formula with $n+1$ free variables, then for any field K, the set of $\bar{a} \in K^{n+1}$ satisfying ϕ is a subset $A \subseteq K^{n+1}$. We have a projection $K^{n+1} \twoheadrightarrow K^n$ that discards the last coordinate. The fibers of the composition $A \hookrightarrow K^{n+1} \twoheadrightarrow K^n$ form a family of subsets of K. Such a family will be called a definable family of subsets. We will call it a uniformly definable family of subsets in the situation where we have a definable family of subsets of K for many different fields K, and the formula that defines it is independent of K.

Now we list the main steps in the proof of Theorem 1. It suffices to find a sentence that works for the finitely generated fields with $\sqrt{-1} \in K$, so we assume this from now on. In the case where $\operatorname{char} K = 0$, we let k be the relative algebraic closure of $\mathbb{Q}$ in K, so k is a number field. With this notation, the following steps give a proof that there is a uniformly definable family $\mathcal{F}$ of K such that whenever K is a finitely generated field of characteristic 0 containing $\sqrt{-1}$, we have $k \in \mathcal{F}$.

(1) Prove that there exists an elliptic curve E over $\mathbb{Q}$ such that $E(\mathbb{Q})$ is infinite and $E(K) = E(k)$. The key here is to reinterpret $E(K)$ as the set of k-rational maps $\operatorname{Alb} V \dashrightarrow E_k$ where $\operatorname{Alb} V$ is the Albanese variety of a k-variety V with function field K, and $E_k = E \times_{\mathbb{Q}} k$.

(2) Observe that for such E, the set of values of the rational function x/y (a uniformizing parameter at ∞ for a Weierstrass model) on $E(K)$ is a subset R of k such that $R \cap \mathbb{Q}$ is p-adically dense in a neighborhood of 0 in $\mathbb{Q}_p$ for all primes p.

(3) Ratios of elements from this R form a subset S of k such that $S \cap \mathbb{Q}$ is p-adically dense in $\mathbb{Q}_p$ for all primes p.

(4) For $t \in K$,

$$t \in k \iff \forall s_1, s_2, s_3 \in S,\ \langle\langle s_1, s_2, t - s_3 \rangle\rangle \text{ represents 0 over } K.$$

(5) For each $(a, b) \in K^2$, we get a curve $E\colon y^2 = x^3 + ax + b$ over K, and a subset of K defined in the previous step. These form a uniformly definable family $\mathcal{F}$ of subsets indexed by $(a, b) \in K^2$. If (a, b) define the special E described in the first step, then the corresponding subset of K equals k.

Now, given any finitely generated field K containing $\sqrt{-1}$, we can say that $\operatorname{char} K = 0$ if and only if there exists a subset $S \in \mathcal{F}$ such that S is a field and $\operatorname{Krdim} S = 1$ and S is a number field. The conditions on S can be expressed in a first-order sentence, because of Theorems 4 and 5. This completes the sketch of the proof of Theorem 1.

With a lot more work, one can find also a formula with one free variable that for any finitely generated field K defines the relative algebraic closure k of the prime field in K, and a formula $\phi_n(x_1, \ldots, x_n)$ with n free variables that holds in a finitely generated field K for elements $x_1, \ldots, x_n$ if and only if $x_1, \ldots, x_n$ are algebraically dependent over k.

One can also prove some geometric analogues, for function fields over algebraically closed or other large fields: these geometric analogues will appear in a joint paper with F. Pop.

References

[Pop02] Florian Pop, *Elementary equivalence versus isomorphism*, Invent. Math. **150** (2002), no. 2, 385–408. MR1933588 (2003i:12016).

[Rum80] R.S. Rumely, *Undecidability and definability for the theory of global fields*, Trans. Amer. Math. Soc. **262** (1980), no. 1, 195–217. MR583852 (81m:03053).

Computing zeta functions of surfaces

Kiran S. Kedlaya

We describe an ongoing project with two MIT undergraduates (Tim Abbott and David Roe) to compute the zeta function of a smooth projective surface over the field $\mathbb{F}_p$, for p a small prime, by adapting the Griffiths-Dwork algorithm for computing Picard-Fuchs equations of pencils of smooth projective hypersurfaces over $\mathbb{C}$ [3, §5], in the spirit of the author's algorithm for computing zeta functions of hyperelliptic curves [7]. (The technique can be applied more generally to smooth toric hypersurfaces over finite fields of small characteristic; see for example [5, §5] for the analogue of the Griffiths-Dwork algorithm.)

Let X be the smooth projective surface defined by the homogeneous polynomial $\overline{Q}(w,x,y,z)$ of degree d, and choose a lift $Q(w,x,y,z)$ to a homogeneous polynomial over $\mathbb{Z}_p$ of degree d. The zeta function of X can be obtained as

$$\zeta_X(t) = \prod_{i=0}^{4} \det(1 - Ft, H^i(X))^{(-1)^{i+1}}$$

for any Weil cohomology H^i. By Lefschetz, in fact we have

$$\zeta_X(t) = \frac{1}{(1-t)(1-pt)(1-p^2t)\det(1 - Ft, H^2_{\mathrm{prim}}(X))},$$

where $H^2_{\mathrm{prim}}(X)$ denotes the primitive part of $H^2(X)$.

For our computations, we use Berthelot's rigid cohomology [1], [2]; in this case $H^2_{\mathrm{prim}}(X)$ can be identified (via a Gysin map) with the algebraic de Rham cohomology of the affine variety $U = \mathbb{P}^3_{\mathbb{Q}_p} \setminus V(Q)$ over $\mathbb{Q}_p$. The cohomology of the latter can be described (following Griffiths) as follows. Write

$$\Omega = w\,dx \wedge dy \wedge dz - x\,dw \wedge dy \wedge dz + y\,dw \wedge dx \wedge dz - z\,dw \wedge dx \wedge dy.$$

Then every 3-form on U has the form $P\Omega/Q^m$ for some integer $m \geq 4/d$ and some homogeneous polynomial P of degree $md - 4$. The cohomology space is the quotient of the space of these forms by the space spanned by relations of the form

$$\frac{mA_wQ\Omega - AQ_w\Omega}{Q^{m+1}},$$

for A a homogeneous polynomial of degree $md - 3$, and similarly with w replaced by x, y, z. (The subscript denotes partial differentiation.) This gives efficient algorithms for computing a basis of cohomology and for expressing an arbitrary form as a linear combination of basis elements plus an exact form.

The action of Frobenius on the rigid cohomology is given by the ring homomorphism F on the weak completion (in the Monsky-Washnitzer sense) of $\mathbb{Z}_p[w, x, y, z, Q^{-1}]_0$ (degree zero part) defined by

$$\begin{aligned} F(w) &= w^p \\ F(x) &= x^p \\ F(y) &= y^p \\ F(z) &= z^p \\ F(Q^{-1}) &= (Q^{-1})^p(1 + (F(Q)(Q^{-1})^p - 1))^{-1}; \end{aligned}$$

the point here is that $(F(Q)(Q^{-1})^p - 1)$ is divisible by p, so we may expand $(1 + (F(Q)(Q^{-1})^p - 1))^{-1}$ as a geometric series. (One can also compute this inverse using a Newton iteration, but we do not need enough terms of the series to make this worth doing.)

Since one wishes to perform a finite computation, one cannot compute F exactly; instead, one must retain enough terms so that when one applies F to a basis of cohomology, reduces, and extracts a matrix for Frobenius, the resulting characteristic polynomial is close enough to the right answer that the right answer is uniquely determined by some size estimates (derived optimally using the Weil conjectures). There is a subtlely here in that the reduction of some $P\Omega/Q^m$ may have worse denominators than does P, since one divides by as much as $(m-1)!$ in the course of doing the reduction. However, the experience of [7] and the comparison theorem between rigid and de Rham cohomology suggest that because of massive cancellation, the true precision loss is closer (in valuation) to $\log_p m$ than to $m/(p-1)$; we are still in the process of determining the precise nature of the cancellation in this situation.

In the interim, we have made some computations to gauge the feasibility of this approach, using a combination of the packages Singular [6] (for calculations using Gröbner bases) and Magma [4] (for other calculations). It seems that computing, say, the full zeta function of a degree 4 surface over a small $\mathbb{F}_p$ may be tractable via this approach, while a degree 5 surface looks much less so because of space constraints. However, one does extract some useful information by computing the Frobenius matrix modulo a small power of p; for instance, this can be used to determine the Newton polygon and to bound from above the number of roots which are equal to p times roots of unity, thus limiting the (geometric) Picard number of the surface via the easy half of Tate's conjecture. In particular, we expect to be able to produce many examples of degree 5 surfaces over $\mathbb{F}_2$ with geometric Picard number 1; this would answer a question of Voloch (private communication).

References

[1] P. Berthelot, Géométrie rigide et cohomologie des variétés algebriques de caractéristique p, in Introductions aux cohomologies p-adiques (Luminy, 1984), *Mém. Soc. Math. France* **23** (1986), 7–32.

[2] P. Berthelot, Finitude et pureté cohomologique en cohomologie rigide (with an appendix in English by A.J. de Jong), *Invent. Math.* **128** (1997), 329–377.

[3] P.A. Griffiths, On the periods of certain rational integrals: I, *Ann. Math.* **90** (1969), 460–495.
[4] J. Cannon et al, MAGMA 2.12, `http://magma.maths.usyd.edu.au`.
[5] D.A. Cox and S. Katz, *Mirror symmetry and algebraic geometry*, Amer. Math. Soc., 1999.
[6] G.-M. Greuel, G. Pfister, and H. Schönemann, SINGULAR 2.0, `http://www.singular.uni-kl.de`.
[7] K.S. Kedlaya, Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology, *J. Ramanujan Math. Soc.* **16** (2001), 323–338.

Annihilation of Sha on Jacobians

E. VICTOR FLYNN
(joint work with Nils Bruin)

We discuss work on the problem of determining the free rank of the Mordell-Weil group $J(K)$ of an Abelian variety J over a number field K. Due to failures of the local-to-global principle, the bounds obtained from Selmer groups need not be sharp. The Shafarevich-Tate group of J over K measures this failure and the standard exact sequence

$$0 \to J(K)/mJ(K) \to S^{(m)}(J/K) \to Ш(J/K)[m] \to 0$$

gives the relation between the Selmer group and $J(K)/mJ(K)$.

If $\delta \in S^{(m)}(J/K)$ does come from an element in $J(K)/mJ(K)$, one can show this by exhibiting a point $P \in J(K)$ that maps to δ. Since such a point is of finite height, one can find it in finite time. The converse is harder to decide. Suppose that $\delta \in S^{(m)}(J/K)$ represents a suspected non-trivial element in $Ш(J/K)[m]$. Since we do not have an upper bound on the smallest height of a possible point $P \in J(K)$ that maps to δ, a failure to find such a point does not prove that δ is not in the image of $J(K)$.

Several methods are available to refine the bounds on $\#J(K)/mJ(K)$ and thus possibly decide if $\delta \in S^{(m)}(J/K)$ represents a non-trivial element in $Ш(J/K)$: comparing bounds obtained from different descents (see [11], for example), deeper descents (as in [5], [9]), the use of isogenous Abelian varieties, and visualisation (as in [1], [2], [7], [4], [8]).

Of these methods, the last is the most amenable to generalisation to the Jacobian J of a higher genus curve. We can construct another Abelian variety B such that the product $J \times B$ has a non-trivial isogenous Abelian variety A. The relevant groups for product varieties are easily expressed in terms of the factors:

$$\begin{aligned} (J \times B)(K) &\simeq J(K) \times B(K) \\ S^{(m)}(J \times B/K) &\simeq S^{(m)}(J/K) \times S^{(m)}(B/K) \\ Ш(J \times B/K) &\simeq Ш(J/K) \times Ш(B/K). \end{aligned}$$

It follows that $\mathrm{rk}A(K) = \mathrm{rk}J(K) + \mathrm{rk}B(K)$. By comparing $S^{(m)}(A/K)$ and $S^{(m)}(J \times B/K)$ one may be able to conclude that $Ш(J \times B/K)[m]$ is non-trivial and a further analysis may allow the conclusion that $Ш(J/K)[m]$ is non-trivial.

We focus on *annihilation by base field extension*, which is a special case of visualisation, where A is taken to be the Weil restriction of scalars of J with

respect to a suitable extension L of K in the following way. Let $\delta \in S^{(m)}(J/K)$ represent a non-trivial element $\overline{\delta} \in Ш(J/K)[m]$, in which case we have $Ш(J/K) \subset H^1(K, J)$. We take L to be an extension such that the restriction of $\overline{\delta}$ from $\mathrm{Gal}(\overline{K}/K)$ to $\mathrm{Gal}(\overline{K}/L)$ is trivial. In particular, we apply this method to Jacobians of hyperelliptic curves.

The term *visualisation* originates from Mazur and refers to the fact that the homogeneous spaces represented by the relevant elements of $S^{(m)}(J/K)$ occur as *fibres* of the map $A \to B$. This description of the homogeneous spaces is considered so explicit that the homogeneous space is *visualised*. Given an short exact sequence of Abelian varieties

$$0 \to J \to A \to B \to 0,$$

one defines the *visualised subgroup* of $H^1(K, J)$ by

$$0 \to \mathrm{Vis}_K(J \to A) \to H^1(K, J) \to H^1(K, A) \to H^1(K, B).$$

It is straightforward to check that for $\delta \in S^{(m)}(J/K)$, one can only expect to prove that the class $\overline{\delta}$ of δ in $Ш(J/K)$ is non-trivial via comparison with $S^{(m)}(A/K)$ if $\overline{\delta} \in \mathrm{Vis}_K(J \to A)$. If that is the case, by abuse of terminology we will say that δ is *visualised* in A.

For example, using the field extension from $\mathbb{Q}$ to $\mathbb{Q}(\sqrt{-3})$, we can show the following.

Example 1. *Let J be the Jacobian over $\mathbb{Q}$ of*

$$C : y^2 = x^5 - 81x - 243.$$

Then $J(\mathbb{Q}) = \{0\}$ and $Ш(J/\mathbb{Q})[2] = (\mathbb{Z}/2\mathbb{Z})^2$.

Independently of visualisation methods, if C is a curve of genus 2 with a rational Weierstrass point then $\delta \in H^1(K, J[2])$ has a degree 4 del Pezzo surface V_δ related to it. If $\delta \in S^{(2)}(J/K)$ and V_δ has no rational points then δ represents a non-trivial element of $Ш(J/K)[2]$. We can use the Brauer-Manin obstruction on del Pezzo surfaces of degree 4 to infer information about $Ш(\mathrm{Jac}(C)/K)[2]$ for curves C of genus 2. In fact, we exploit an example in [3] of a violation of the Hasse principle on a degree 4 del Pezzo surface to obtain the following explicit infinite family.

Proposition 2. *Let $\mathbb{C}_{\ell,\lambda} : Y^2 = \ell\big(X^2 - 2\big)\Big(X - \frac{\lambda+2}{\lambda+1}\Big)\big(X - \lambda\big)\Big(X - \frac{3\lambda+4}{2\lambda+3}\Big)$, and let $J_{\ell,\lambda}$ be the Jacobian of $\mathbb{C}_{\ell,\lambda}$. There exists a nontrivial member of $Ш(J_{-2k,-\frac{13}{8}}/\mathbb{Q})[2]$ for any k of the form*

$$k = 80(t^5 - t + 1)^2\big((t^5 - t + 1)^2 + 10\big)^2 + \big((t^5 - t + 1)^2 - 10\big)^4, \tag{1}$$

for any $t \in \mathbb{Q}$. Furthermore, $J_{-2k,-\frac{13}{8}}$ is absolutely simple.

There are also infinite families of nontrivial $Ш(J/\mathbb{Q})[2]$ in [6] and [10], but the nature of our examples (being a familiy of twists) and the method of proof (using the Brauer-Manin obstruction on degree 4 del Pezzo surfaces) is quite different.

As a consequence, we recover a proof of [2, Proposition 2.3] that any element of $H^1(K, J)$ represented by $\delta \in H^1(K, J[2])$ can be visualised in an Abelian variety of dimension at most $d2^{2d}$. In fact, we prove the small improvement that if $\delta \in S^{(2)}(J/K)$ and C has at least $\dim J$ rational Weierstrass points then it can be visualised in an Abelian variety of dimension at most $d2^{2d-1}$.

Conditional on the conjecture that the Brauer-Manin obstruction is the only obstruction for del Pezzo surfaces having rational points, it would follow that one can either show that δ represents a non-trivial element in $H^1(K, J)$ by local methods or the Brauer-Manin obstruction on V_δ, or δ can be visualised in an Abelian variety of dimension 4. This is better than than the general bound of 32 on the visualisation dimension.

References

[1] Amod Agashe and William Stein. Visible evidence in the Birch and Swinnerton-Dyer Conjecture for rank 0 modular abelian varieties. *J. number theory.*

[2] Amod Agashe and William Stein. Visibility of Shafarevich-Tate groups of abelian varieties. *J. Number Theory*, 97(1):171–185, 2002.

[3] B. J. Birch and H. P. F. Swinnerton-Dyer. The Hasse problem for rational surfaces. *J. Reine Angew. Math.*, 274/275:164–174, 1975. Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, III.

[4] Nils Bruin. Visualising Sha[2] in abelian surfaces. *Math. Comp.*, 73(247):1459–1476 (electronic), 2004.

[5] J. W. S. Cassels. Second descents for elliptic curves. *J. Reine Angew. Math.*, 494:101–127, 1998. Dedicated to Martin Kneser on the occasion of his 70th birthday.

[6] Jean-Louis Colliot-Thélène and Bjorn Poonen. Algebraic families of nonzero elements of Shafarevich-Tate groups. *J. Amer. Math. Soc.*, 13(1):83–99, 2000.

[7] John E. Cremona and Barry Mazur. Visualizing elements in the Shafarevich-Tate group. *Experiment. Math.*, 9(1):13–28, 2000.

[8] E. V. Flynn and J. Redmond. Application of covering techniques to families of curves. *J. Number Theory*, 101(2):376–397, 2003.

[9] J. R. Merriman, S. Siksek, and N. P. Smart. Explicit 4-descents on an elliptic curve. *Acta Arith.*, 77(4):385–404, 1996.

[10] Bjorn Poonen. An explicit algebraic family of genus-one curves violating the Hasse principle. *J. Théor. Nombres Bordeaux*, 13(1):263–274, 2001. 21st Journées Arithmétiques (Rome, 2001).

[11] Edward F. Schaefer and Michael Stoll. How to do a p-descent on an elliptic curve. *Trans. Amer. Math. Soc.*, 356(3):1209–1231 (electronic), 2004.

Computing maximal orders of quaternion algebras

John Voight

Let F be a number field, specified in the usual way in bits by an irreducible polynomial over $\mathbb{Q}$, and let $\mathbb{Z}_F$ be its maximal order, encoded by a $\mathbb{Z}$-basis. It is well-known that the problem of computing $\mathbb{Z}_F$ given F is deterministic polynomial-time equivalent to the problem of given a positive integer finding its largest squarefree divisor. We prove an analogous statement in a noncommutative setting.

A *quaternion algebra* over F is a central simple F-algebra with $\dim_F A = 4$, or equivalently an F-algebra which is generated by $\alpha, \beta \in A$ such that

$$\alpha^2 = a, \quad \beta^2 = b, \quad \alpha\beta = -\beta\alpha$$

for some $a, b \in F^*$, denoted $A = \left(\frac{a,b}{F}\right)$. A quaternion algebra is encoded in bits by the pair a, b. A $\mathbb{Z}_F$*-lattice* of A is a finitely generated $\mathbb{Z}_F$-submodule Λ of A satisfying $F\Lambda = A$. An *order* of A is a $\mathbb{Z}_F$-lattice which is also a subring; an order is maximal if it is not properly contained in any other order. We specify an order $\mathcal{O}$ by a $\mathbb{Z}$-basis.

We are therefore interested in the following problem ($\mathcal{O}$): Given A, find a maximal order $\mathcal{O} \subset A$. We prove the following theorem.

Theorem. *Problem* ($\mathcal{O}$) *for any fixed* F *is probabilistic polynomial-time equivalent to the problem of factoring integers.*

The implication ($\Leftarrow$) follows from the work of [1, Theorem 5.3]; their algorithm works in the more general setting of semisimple algebras over $\mathbb{Q}$. We are able to provide an algorithm which is simpler and may run more efficiently for the specific case of quaternion algebras over number fields.

To prove the implication ($\Rightarrow$), we suppose that we wish to factor the integer $a \in \mathbb{Z}_{>0}$. Then we select an appropriate $b \in \mathbb{Z}_F/a\mathbb{Z}_F$ such that the quaternion algebra $A = \left(\frac{a,b}{F}\right)$ has the property that a maximal order $\mathcal{O} \subset A$ has discriminant $\mathfrak{d}(\mathcal{O}) \subset \mathbb{Z}_F$ whose norm yields a proper factor of a. The choice of b requires a random choice which is analogous to finding a nonresidue modulo a prime, a problem which has satisfactory probabilistic polynomial-time solutions but for which no deterministic polynomial-time algorithm is known. For the details of the proof, we refer the reader to [2].

References

[1] Gábor Ivanyos and Lajos Rónyai, *Finding maximal orders in semisimple algebras over* $\mathbb{Q}$, Comput. Complexity **3** (1993), 245–261.

[2] John Voight, *Quadratic forms and quaternion algebras: Algorithms and arithmetic*, Ph.D. thesis, University of California, Berkeley, 2005.

Ratios of factorial and algebraic hypergeometric functions

Fernando Rodriguez-Villegas

Chebychev in his work on the distribution of primes numbers used the following fact

$$u_n := \frac{(30n)!n!}{(15n)!(10n)!(6n)!} \in \mathbb{Z}, \qquad n = 0, 1, 2, \ldots$$

This is not immediately obvious (for example, this ratio of factorials is not a product of multinomial coefficients) but it is not hard to prove. The only proof I know proceeds by checking that the valuations $v_p(u_n)$ are non-negative for every

prime p; an interpretation of u_n as counting natural objects or being dimensions of natural vector spaces is far from clear.

As it turns out, the generating function

$$u := \sum_{\nu \geq 1} u_n \lambda^n$$

is algebraic over $\mathbb{Q}(\lambda)$; i.e. there is a polynomial $F \in \mathbb{Z}[x, y]$ such that

$$F(\lambda, u(\lambda)) = 0.$$

However, we are not likely to see this polynomial explicitly any time soon as its degree is $483,840$ (!).

What is the connection between u_n being an integer for all n and u being algebraic? Consider the more general situation

$$u_n := \prod_{\nu \geq 1} (\nu n)!^{\gamma_\nu},$$

where the sequence $\gamma = (\gamma_\nu)$ for $\nu \in \mathbb{N}$ consists of integers which are zero except for finitely many.

We assume throughout that γ is *regular*, i.e.,

$$\sum_{\nu \geq 1} \nu \gamma_\nu = 0,$$

which, by Stirling's formula, is equivalent to the generating series $u := \sum_{\nu \geq 1} u_n \lambda^n$ having finite non-zero radius of convergence. We define the *dimension* of γ to be

$$d := -\sum_{\nu \geq 1} \gamma_\nu.$$

To abbreviate, we will say that γ is *integral* if $u_n \in \mathbb{Z}$ for every $n = 0, 1, 2, \ldots$.

We can now state the main theorem of the talk.

Theorem 1. *Let $\gamma \neq 0$ be regular; then u is algebraic if and only if γ is integral and $d = 1$.*

One direction is fairly straightforward. If u is algebraic, by a theorem of Eisenstein, there exists an $N \in \mathbb{N}$ such that $N^n u_n \in \mathbb{N}$ for all $n \in \mathbb{N}$. It is not hard to see that in our case if such an N exists then it must equal 1. To see that $d = 1$ we need to introduce the *monodromy representation.*

The power series u satisfies a linear differential equation $Lu = 0$. After possibly scaling λ this equation has singularities only at $0, 1$ and ∞. Indeed, u is a hypergeometric series. Moreover, these singularities are regular singularities precisely because we assumed γ to be regular.

If we let V be the space of local solutions to $Lu = 0$ at some base point not $0, 1$ or ∞ then analytic continuation gives a representation

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

We let the *monodromy group* Γ be the image of ρ and let B, A, σ be the monodromies around $0, \infty, 1$, respectively, with orientations chosen so that $A = B\sigma$.

The main use of the monodromy group for us is the fact that u is algebraic if and only if Γ is finite.

As it happens the multiplicity of the eigenvalue 1 for B is d and it is also true that the corresponding Jordan block of B is of size d. Hence, Γ is not finite if $d > 1$.

To prove the converse we appeal to the work of Beukers and Heckman [1] who extended Schwartz work and described all algebraic hypergeometric functions. Let p and q be the characteristic polynomials of A and B respectively. In our situation p and q are relatively prime polynomials in $\mathbb{Z}[x]$ (which are products of cyclotomic polynomials). Their work tells us that Γ is finite if and only if the roots of p and q interlace in the unit circle.

The key step in the proof of this beautiful fact is to determine when Γ fixes a non-trivial positive definite Hermitian form H on V (which guarantees that Γ is compact). I explained in my talk how H can be defined using a variant of a construction going back to Bezout. Consider the two variable polynomial

$$\frac{p(x)q(y) - p(y)q(x)}{x - y} = \sum_{i,j} B_{i,j} x^i y^k$$

and define the *Bezoutian* of p and q as

$$\mathrm{Bez}(p, q) = (B_{i,j}).$$

We need two facts about this matrix. First, the determinant of $\mathrm{Bez}(p, q)$ equals the resultant of p and q (in passing I should mention that this is a useful fact computationally since the matrix is of smaller size than the usual Sylvester matrix). Second, note that $\mathrm{Bez}(p, q)$ is symmetric. Hence it carries more information than just its determinant as it defines a quadratic form H. It is a classical fact (due to Hermite and Hurwitz) that the signature of H has a topological interpretation.

Consider the continuous map $\mathbb{P}^1(\mathbb{R}) \to \mathbb{P}^1(\mathbb{R})$ given by the rational function p/q. Since $\mathbb{P}^1(\mathbb{R})$ is topologically a circle we have $H^1(\mathbb{P}^1(\mathbb{R}), \mathbb{Z}) \simeq \mathbb{Z}$ and the induced map $H^1(\mathbb{P}^1(\mathbb{R}), \mathbb{Z}) \to H^1(\mathbb{P}^1(\mathbb{R}), \mathbb{Z})$ is multiplication by some integer s, which is none other than the signature of H. In particular, H is definite if and only if the roots of p and q interlace on $\mathbb{R}$. A twisted form of this construction and analogous signature result can be applied to the hypergeometric situation; in this way we recover the facts about the Hermitian form fixed by Γ proved by Beukers and Heckman.

Finally, to make the connection with the integrality of γ we define the *Landau function*

$$\mathcal{L}(x) := -\sum_{\nu \geq 1} \gamma_\nu \{\nu x\}, \qquad x \in \mathbb{R}$$

where $\{x\}$ denotes fractional part. It is simple to verify that

$$v_p(u_n) = \sum_{k \geq 1} \mathcal{L}\left(\frac{n}{p^k}\right).$$

Landau [2] proved a nice criterion for integrality: γ is integral if and only if $\mathcal{L}(x) \geq 0$ for all $x \in \mathbb{R}$.

Write

$$p(t) = \prod_{j=1}^{r}(t - e^{2\pi i\alpha_j}), \qquad q(t) = \prod_{j=1}^{r}(t - e^{2\pi i\beta_j}),$$

where $r = \dim V$ and $0 \leq \alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_r < 1$ and $0 \leq \beta_1 \leq \beta_2 \leq \cdots \leq \beta_r < 1$ are rational.

The function $\mathcal{L}$ satisfies a number of simple properties: it is locally constant (by regularity), periodic modulo 1, right continuous with discontinuity points exactly at $x \equiv \alpha_j \bmod 1$ or $x \equiv \beta_j \bmod 1$ for some $j = 1, \ldots, r$ and takes only integer values. More precisely,

$$\mathcal{L}(x) = \#\{j \mid \alpha_j \leq x\} - \#\{j \mid 0 < \beta_j \leq x\}.$$

Away from the discontinuity points of $\mathcal{L}$ we have

$$\mathcal{L}(-x) = d - \mathcal{L}(x).$$

In particular, $\mathcal{L}(x) \geq 0$ if and only if $\mathcal{L}(x) \leq d$.

It is now easy to verify that if $d = 1$ and $\mathcal{L}(x) \geq 0$ then the roots of p and q must necessarily interlace on the unit circle finishing the proof. (Some further elaboration would also yield the other implication in the theorem independently of our previous argument.)

As a final note, let me mention that the examples in the theorem are a case of the ADE phenomenon; up to the obvious scaling $n \mapsto dn$ for some $d \in \mathbb{N}$, they come in two infinite families A and D, which are easy to describe, and some sporadic ones (10 of type E_6, 10 of type E_7 and 30 of type E_8).

References

[1] F. Beukers and G. Heckman *Monodromy for the hypergeometric function ${}_nF_{n-1}$*, Invent. Math. **95** (1989), 325–354.

[2] E. Landau *Sur les conditions de divisibilité d'un produit de factorielles par un autre.* Collected works, I, p. 116, Thales-Verlag, Essen, 1985.

On the computation of the coefficients of a modular form, II: explicit calculations

Johan Bosman

(joint work with Bas Edixhoven)

Many thanks go to John Voight for making and supplying me the notes that he took from my talk about this subject.

Let $\tau(n)$ be defined by $\Delta(q) = q\prod_{n\geq 1}(1-q^n)^{24} = \sum_{n\geq 1}\tau(n)q^n$. We wish to calculate $\tau(p) \bmod \ell$. For all ℓ, there exists a representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(K_\ell/\mathbb{Q}) \to GL_2(\mathbb{F}_\ell)$ such that $\mathrm{tr}(\mathrm{Frob}_p) \equiv \tau(p) \bmod \ell$ and $\det(\mathrm{Frob}_p) \equiv$

$p^{11} \bmod \ell$ for $p \neq \ell$. For $\ell \geq 11$, there exists a 2-dimensional subspace $V_\ell \subset \mathrm{Jac}(X_1(\ell))[\ell]$ such that ρ is given by the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on V_ℓ.

Let $f_1, \ldots, f_g$ be a basis of newforms for the modular forms space $S_2(\Gamma_1(\ell))$. This space is isomorphic to $H^0(X_1(\ell), \Omega^1)$ by $f \mapsto f(dq/q)$. We have $J_1(\ell)(\mathbb{C}) \cong \mathbb{C}^g/\Lambda$ where $\Lambda = \{\int_\gamma (f_1, \ldots, f_g) dq/q : [\gamma] \in H_1(X_1(\ell)(\mathbb{C}), \mathbb{Z})\}$ is a lattice.

We have

$$\phi : X_1(\ell)^g \to \mathbb{C}^g/\Lambda \supset V_\ell$$
$$(Q_1, \ldots, Q_g) \mapsto \sum_{i=1}^{g} \int_0^{Q_i} (f_1, \ldots, f_g)\, dq/q.$$

If we choose $Y_1(\ell) \subset X_1(\ell)$ to be the moduli space of pairs (E, P) where E is an elliptic curve and P is a point on E of order ℓ, then this gives us a model for $X_1(\ell)$ over $\mathbb{Q}$ in which the cusp at 0 is rational. Hence the map ϕ is defined over $\mathbb{Q}$ in this setting.

For each $x \in V_\ell$ we want to approximate $Q \in X_1(\ell)^g$ such that $\phi(Q) = x$. Pick a random Q and compute $\phi(Q)$. Then draw a small vector from $\phi(Q)$ in the direction of x. Getting the Jacobian matrix, we then find a Q' such that $\phi(Q')$ is closer to x. Repeat this step until we are really close. Once in a neighborhood of x, we use Newton-Raphson iteration. We use a low calculation precision until we get in the Newton-Raphson part, where we start increasing the precision. This way the first part of the approximation can be performed much faster than the NR part, in spite of the fact that it needs more steps.

What we need to show is that we can calculate $f_i(z)$ and $\int_0^z f_i(z)(dq/q)$ to a high precision.

Let F be the standard fundamental domain for the action of $SL_2(\mathbb{Z})$ and let f be a newform. Write $z = \gamma z'$ with $\gamma \in SL_2(\mathbb{Z})$ and $z' \in F$. This is for computational reasons: in $SL_2(\mathbb{Z})$ we can do exact calculations and in the upper half plane we want to stay away from the real line.

Because f is a newform, there is a character $\epsilon : (\mathbb{Z}/\ell\mathbb{Z})^* \to \mathbb{C}^*$ such that $f\left(\frac{az+b}{cz+d}\right) = \epsilon(d)(cz+d)^2 f(z)$ for all matrices in $\Gamma_0(l)$. Furthermore, $\Gamma_0(\ell)\backslash SL_2(\mathbb{Z})$ has the following set of coset representatives:

$$S = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \cup \left\{ \begin{pmatrix} 0 & -1 \\ 1 & j \end{pmatrix} : j \in \{-(\ell-1)/2, \ldots, (\ell+1)/2\} \right\}.$$

So if we write $\gamma = \gamma_1\gamma_2$ with $\gamma_1 \in \Gamma_0(\ell)$ and $\gamma_2 \in S$, then the calculation of $f(\gamma z)$ is reduced to the calculation of $f(\gamma_2 z)$.

Now, $S \cdot F$ is a fundamental domain for $\Gamma_0(\ell)\backslash\mathbb{H}$, in which 0 is the only cusp apart from ∞. If $\Im z \gg 0$, then $|q| \ll 1$ so $\sum_n a_n(f)q^n$ converges rapidly, so we can calculate $f(z)$. This works if z is not near the cusp 0. If $z \in S \cdot F$ is near 0, then we have an Atkin-Lehner operator on $S_2(\Gamma_1(\ell))$ by $(w_\ell f)(z) = \ell z^{-2} f(-1/\ell z)$. If f is a newform, then $w_\ell f = c_f \widetilde{f}$, where $\widetilde{f} = \sum \overline{a_n(f)} q^n$, the complex conjugate and c_f is a constant depending on f.

Plug in a value of z such that $\Im z \gg 0$, $\Im(-1/\ell z) \gg 0$ to get c_f. For points in $S \cdot F$ near the cusp 0, $-1/\ell z$ is near ∞, so we can calculate $\widetilde{f}(-1/\ell z)$. From this we can get $w_\ell f(-1/\ell z)$, hence also $f(z)$.

With similar tricks plus some more we can also calculate integrals of modular forms to a high precision (think of at least hundreds of decimals).

Given $\psi \in \mathbb{Q}(X_1(\ell))$ (quotients of two modular forms of the same weight), we obtain

$$P_\ell = \prod_{Q \in V_\ell \setminus \{0\}} (X - \sum_{i=1}^{g} \psi(Q_i)) \in \mathbb{Q}[X].$$

We can approximate $P_\ell \in \mathbb{R}[X]$. Using continued fractions, we find rational numbers near the coefficients. If $|p/q - \alpha| \ll 1/q^2$, then we are psychologically convinced that $\alpha = p/q$, although a mathematical proof still lacks. This polynomial should define the field of definition of a nonzero point in V_ℓ and its splitting field should be K_ℓ.

We do this for $\ell = 13$, $\ell = 17$.

We also have another polynomial

$$P'_\ell = \prod_{L \in \mathbb{P}^1(V_\ell)} (X - \sum_{Q \in L \setminus \{0\}} \sum_i \psi(Q_i))$$

which gives the extension $PGL_2(\mathbb{F}_\ell)$.

Multiplication by n on V_ℓ gives a map $x \mapsto \psi_n(x)$ in $\mathbb{Q}[x]/P_\ell(x)$, which we want to calculate. The cycle type of Frob_p acting on V_ℓ is the same as the decomposition type of $P_\ell \bmod p$. One ends up with a set of candidate matrices M for $\rho(\mathrm{Frob}_p)$. Find an r such that $M^r = nI$ for all candidates. Then, in $\mathbb{F}_p[x]/(P_\ell)$, the congruence $\psi_n \equiv x^{p^r} \bmod P_\ell$ holds. If you do this for sufficiently many p, one can use LLL to find the polynomial ψ_n.

We can use this to calculate $\tau(p) \bmod \ell$ if $\rho(\mathrm{Frob}_p)$ has its eigenvalues in $\mathbb{F}_\ell$. Factor P_ℓ in $\mathbb{F}_p[x]$, say $P_\ell(x) = P_1 \dots P_k$. Then n is an eigenvalue of $\rho(\mathrm{Frob}_p)$ iff $x^p \equiv \psi_n \bmod P_i$ for some i.

Polynomial Selection for NFS I

Thorsten Kleinjung

In this talk some aspects of the polymonial selection step for the (general) number field sieve (NFS) were discussed ([2], [1]). The NFS is currently the best known algorithm for factoring integers (at least heuristically). Given an integer N the first step of NFS, called polymonial selection step, consists in finding two irreducible coprime polynomials $f, g \in \mathbb{Z}[x]$ sharing a common root modulo N. The runtime of NFS depends on the quality of the polynomials f and g. For this talk we use the size of the absolute value of the coefficients of f and g as a first approximation for the quality, leading to the following problem:

Problem: Given d_f and d_g find two irreducible coprime polynomials $f, g \in \mathbb{Z}[x]$ of degree d_f resp. d_g with a common root modulo N such that the absolute value of their coefficients is as small as possible.

Except for one method of P. Montgomery there are good solutions for this problem only if one of the polynomials is linear (wlog $d_g = 1$). It is easy to find polynomials whose coefficients are of size $\sqrt[d_f+1]{N}$. By generating many polynomials in this way one may hope to find some among them which have smaller coefficients. A method of P. Montgomery and B. Murphy ([2]) allows to construct polynomials such that the first two coefficients of f are "small". So far g has always been monic.

In the first part of this talk the Montgomery-Murphy method was generalized to non monic linear polynomials g. Fixing the leading coefficients of f and g, this allows to construct f and g if a certain congruence is solvable. In this case the size of the coefficients can be bounded as in the method of Montgomery and Murphy. The second part explained how to exploit the non monicness by considering many polynomial pairs simultaneously. More precisely, for a small l: d_f^l polynomial pairs depending on $d_f l$ values are considered. A method for quickly approximating the third coefficients of the polynomials f was given. This only depends on the $d_f l$ values as above. The effort to identify good pairs among the d_f^l polynomial pairs considered above is $O(d^{\frac{l}{2}} \log d)$.

References

[1] T. Kleinjung, *Polynomial Selection for the General Number Field Sieve*, submitted to: Math. of Comp.

[2] B. A. Murphy, *Polynomial selection for the Number Field Sieve Integer Factorisation Algorithm*, PhD thesis, The Australian National University, 1999.

Polynomial Selection for NFS II

Daniel Bernstein

I discussed the smoothness of the values $(a - bm)(a^5 + f_4 a^4 b + ... + f_0 b^5)$ that appear in the number-field sieve. In particular, I mentioned choosing pairs (a, b) to produce the smallest values; using superelliptic integrals to approximate the number of pairs (a, b); using smoothness probabilities for ideals to approximate smoothness probabilities for $a - bx$; using power series to approximate Dirichlet series; handling more general notions of smoothness; and, as a future possibility to explore, generalizing to $(a - bm + cm^2)(\ldots)$.

Automorphic forms and rational homology spheres

Frank Calegari
(joint work with Nathan Dunfield)

In 1900, Poincare made the following conjecture (updated into modern language):

Conjecture 1. *Let M be a compact connected orientable three manifold. Suppose that $H_1(M, \mathbf{Z}) = \{1\}$. Then $M \simeq S^3$.*

Poincare himself found a counterexample. The manifold S^3 admits an action of the group $\widetilde{A_5}$, a double cover of A_5, and the quotient space M has trivial first homology. Any compact connected M with $H_1(M, \mathbf{Z}) = \{1\}$ is known as a homology sphere. If the weaker condition $H_1(M, \mathbf{Q}) = \{1\}$ is satisfied then one says that M is a *rational homology sphere*. One has the following conjecture.

Conjecture 2 (Virtual Betti Number Conjecture)**.** *Let M be a compact connected orientable three manifold with $\pi_1(M)$ infinite. Then there exists a finite cover $\widetilde{M} \to M$ such that $b_1(M) := \dim H_1(M, \mathbf{Q}) > 0$.*

This conjecture implies the virtual Haken conjecture, and thus can be considered very difficult. Assuming geometrization one may assume that M is hyperbolic, but even in this case the problem seems very difficult. One approach that has been suggested is to try and prove that any sufficiently *big* M will have non-trivial first Betti number, for some concept of "big". Clearly one can ask that M has large volume (defined topologically by Mostow Rigidity), but this is not sufficient as can be seen by considering examples arising from Dehn surgery. A recent suggestion was to talk manifolds with sufficiently large injectivity radius $r(M)$. One defines $r(M)$ as the supremum over real numbers r such that for every $x \in M$ there exists a ball of radius r centered at x inside M that does not intersect itself. Since every M has a cover with arbitrarily large injectivity radius, this would suffice to prove the conjecture.

Our main result is that this hope is too optimistic, namely, we construct a particular M and covers M_n of arbitrarily large injectivity radius with $b_1(M_n) = 0$. Our proof that $b_1(M_n) = 0$ actually requires us to use some as yet unknown conjectures from number theory (such as the GRH), but even with this caveat one should conclude conjecture 2 is unlikely to fall by the optimistic approach mentioned above.

The link to number theory is through automorphic forms. Certain hyperbolic manifolds (arithmetic manifolds) have homology which corresponds to spaces of automorphic forms. Moreover, these automorphic forms can in certain situations be associated to Galois representations, due to a result of Taylor [1]. The precise nature of our M_n imply that one can control the ramification behavior of these Galois representations, and with some work one can show that such Galois representations do not exist. This implies that the homology is trivial, and that M_n is a rational homology sphere. The precise result we prove is the following:

Theorem 3. *Let D be the (unique) quaternion algebra over $K = \mathbb{Q}(\sqrt{-2})$ ramified at π and $\overline{\pi}$, where $3 = \pi\overline{\pi}$. Let $\mathcal{O}$ be a maximal order of D. Let $\mathfrak{m}$ be a maximal bi-ideal of $\mathcal{O}$ trivial away from π. Finally, let B_n be the complex embedding of $1+\mathfrak{m}^n$ into $\mathrm{SL}_2(\mathbf{C})$, and let $M_n = \mathcal{H}/(B_n \cap \mathcal{O}^\times)$. The manifolds M_n have arbitrarily large injectivity radius as $n \to \infty$. Moreover, assuming the Langlands conjecture for $\mathrm{GL}_2(\mathbb{A}_K)$ and the GRH, M_n is a rational homology sphere for all n.*

References

[1] R. Taylor, *l-adic representations associated to modular forms over imaginary quadratic fields. II*, Invent. Math. **116** (1994), no. 1-3, 619–643.

Cohen–Lenstra heuristics for 4–ranks of class groups of quadratic number fields

Jürgen Klüners
(joint work with Étienne Fouvry)

Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic number field of discriminant D. Denote by Cl_D the ordinary class group of K and by C_D the narrow class group of K. We remark that these two groups are always the same if $D < 0$. For a prime ℓ we denote by $\mathrm{rk}_\ell(A) := \dim_{\mathbb{F}_\ell}(A/A^\ell)$ the ℓ–rank of an abelian group A. Furthermore we introduce the 4–rank $\mathrm{rk}_4(A) := \mathrm{rk}_2(A^2)$. A special case of the Cohen–Lenstra heuristics [1, p.57] states for odd primes ℓ:

$$\lim_{X\to\infty} \frac{\sum_{0<D\le X} \ell^{\mathrm{rk}_\ell(\mathrm{Cl}_D)}}{\sum_{0<D\le X} 1} = 1 + \ell^{-1}$$

and

$$\lim_{X\to\infty} \frac{\sum_{0<-D\le X} \ell^{\mathrm{rk}_\ell(\mathrm{Cl}_D)}}{\sum_{0<-D\le X} 1} = 2,$$

where the sums are over discriminants D of quadratic fields. This result is only proven for $\ell = 3$ as a consequence of the Davenport–Heilbronn theorem [2]. The original paper [1] does not state anything about the 2–part of the class group. By genus theory it is clear that $\mathrm{rk}_2(C_D) = \omega(D) - 1$, where ω counts the number of prime factors. We remark that $\mathrm{rk}_2(C_D) - 1 \le \mathrm{rk}_2(\mathrm{Cl}_D) \le \mathrm{rk}_2(C_D)$. By averaging the corresponding expressions we get

$$\sum_{0<\pm D\le X} 2^{\mathrm{rk}_2(\mathrm{Cl}_D)}, \sum_{0<\pm D\le X} 2^{\mathrm{rk}_2(C_D)} \sim cX\log X,$$

for some positive constant c and for X tending to infinity.

Frank Gerth [4] put forward the idea to consider Cl_D^2 instead of Cl_D. With this new interpretation he conjectures the analogous results for $\mathrm{rk}_2(\mathrm{Cl}_D^2) = \mathrm{rk}_4(\mathrm{Cl}_D)$, i.e.

$$\lim_{X\to\infty} \frac{\sum_{0<D\le X} 2^{\mathrm{rk}_4(\mathrm{Cl}_D)}}{\sum_{0<D\le X} 1} = 1 + 1/2 \tag{2}$$

and

$$\lim_{X\to\infty} \frac{\sum_{0<-D\leq X} 2^{\mathrm{rk}_4(\mathrm{Cl}_D)}}{\sum_{0<D\leq X} 1} = 2. \tag{3}$$

The goal of our talk will be to prove these two formulas, i.e.

Theorem 1. *Formulae* (2) *and* (3) *are true.*

Let us state the main ideas of the proof. In order to simplify we assume that $D < 0$ and $D \equiv 1 \bmod 4$. Then we get the following formula which was already known by Redei [6].

Theorem 2.

$$2^{\mathrm{rk}_4(C_D)} = \frac{1}{2}\#\{b \mid b > 0 \text{ squarefree}, b \mid D,\ (b|(-D/b) = 1\},$$

where the symbol $(a|b) = 1$ *iff* $x^2 - ay^2 - bz^2 = 0$ *has a non-trivial solution.*

After doing suitable transformations we arrive at the sum:

Theorem 3.

$$\sum_{\substack{-D\leq X\\ D\equiv 1 \bmod 4}} 2^{\mathrm{rk}_4(C_D)} = \frac{1}{2} \sum_{\substack{ab\leq X\\ ab\equiv 3 \bmod 4}} \mu^2(ab)(a|b), \tag{4}$$

where μ *denotes the Moebius* μ*-function.*

Then we use the fact that $(a|b) = 1$ iff a is a square mod b and b is a square mod a. This condition can be expressed using Legendre symbols and we finally arrive at

Theorem 4.

$$\sum_{\substack{-D\leq X\\ D\equiv 1 \bmod 4}} 2^{\mathrm{rk}_4(C_D)} =$$

$$\frac{1}{2} \sum_{\substack{m_1m_2n_1n_2\leq x\\ m_1m_2n_1n_2\equiv 3 \bmod 4}} \frac{\mu^2(m_1m_2n_1n_2)}{2^{\omega(m_1m_2n_1n_2)}}(-1)^{(n_1-1)(m_2-1)/4}\big(\frac{m_1}{n_1}\big)\big(\frac{m_2}{n_2}\big).$$

The task of the proof will be to compute the asymptotics of this sum. It will turn out that the main term corresponds to the four choices:

$$n_1 = 1 = n_2, n_1 = 1 = m_2, m_1 = 1 = n_2, \text{ and } m_1 = 1 = m_2.$$

For the rest of the sum we show that it can be bounded by $O(x\log(x)^{-1/2+\epsilon})$ for all $\epsilon > 0$ using Siegel-Walfisz theorem and large sieve techniques introduced by Heath-Brown [5].

References

[1] H. Cohen and H. W. Lenstra, Jr. Heuristics on class groups of number fields. In: *Number theory, Noordwijkerhout 1983*, volume 1068 of *Lecture Notes in Math.*, pages 33–62. Springer, Berlin, 1984.

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

[3] F. Gerth, III. The 4-class ranks of quadratic fields. *Invent. Math.*, 77(3):489–515, 1984.

[4] F. Gerth, III. Extension of conjectures of Cohen and Lenstra. *Exposition. Math.*, 5(2):181–184, 1987.

[5] D.R. Heath–Brown. A mean value estimate for real characters sums. *Acta. Arith.*, 72 :235–275, 1995.

[6] L. Redei. Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper. *J. Reine Angew. Math.*, 171:55–60, 1934.

Class numbers, elliptic curves, and hyperelliptic curves

Dongho Byeon

Cohen and Lenstra conjectured that the probability a prime p divides the class numbers of imaginary quadratic fields is

$$1-\prod_{i=1}^{\infty}(1-\frac{1}{p^i})$$

and the probability a prime p divides the class numbers of real quadratic fields is

$$1-\prod_{i=2}^{\infty}(1-\frac{1}{p^i}).$$

However nothing is known. The best known quantitative result for imaginary quadratic fields is;

> (Soundararajan) *If $g \geq 3$ is an odd positive integer, then the number of imaginary quadratic fields whose absolute discriminant is $\leq X$ and whose ideal class group has an element of order g is $\gg X^{\frac{1}{2}+\frac{1}{g}-\epsilon}$, for any $\epsilon > 0$.*

and for real quadratic fields is;

> (Yu) *If $g \geq 3$ is an odd positive integer, then the number of real quadratic fields whose absolute discriminant is $\leq X$ and whose ideal class group has an element of order g is $\gg X^{\frac{1}{g}-\epsilon}$, for any $\epsilon > 0$.*

Let $D > 0$ be the fundamental discriminant of the real quadratic field $\mathbb{Q}(\sqrt{D})$ and $h(D)$ be its class number. In this talk, applying Stewart and Top's result on square free sieve to Mestre's work (or Leprévost's work) on ideal class groups and elliptic curves (or modular hyperelliptic curves), we improve Yu's result for $g = 5, 7, 11, 23, 29$.

Theorem 1. If $g = 5$ or 7,

$$\#\{0 < D < X | h(D) \equiv 0 \pmod{g}\} \gg X^{\frac{1}{2}}.$$

Theorem 2.

$$\#\{0 < D < X | h(D) \equiv 0 \pmod{11}\} \gg X^{\frac{1}{3}}$$

$$\#\{0 < D < X | h(D) \equiv 0 \pmod{23}\} \gg X^{\frac{1}{5}}$$

$$\#\{0 < D < X | h(D) \equiv 0 \pmod{29}\} \gg X^{\frac{1}{6}}.$$

Finite coverings and rational points

Michael Stoll

1. Introduction

The purpose of this talk is to put forward a conjecture. The background is given by the following

Basic Question.

Given a (smooth projective) curve C over a number field k, can we determine explicitly the set $C(k)$ of rational points?

One possible approach to this is to consider an *unramified covering* $D \xrightarrow{\pi} C$ that is *geometrically Galois*. By standard theory, there are only finitely many *twists* $D_j \xrightarrow{\pi_j} C$ of this covering (up to isomorphism over k) such that D_j has points everywhere locally, and

$$C(k) = \coprod_j \pi_j(D_j(k))\,.$$

Moreover, the set of these twists is computable (at least in principle).

In particular, if it turns out that there are *no* such twists, then this proves that $C(k)$ is empty. More generally, in this way, we obtain restrictions on the possible location of rational points inside the adelic points of C.

2. The Conjecture

Let me now state a conjecture that essentially says that this approach provides all the information that it possibly can.

Let us define a *residue class* on C to be a subset X of the adelic points $C(\mathbb{A}_k) = \prod_v C(k_v)$ of the form

$$X = \prod_{v \in S} X_v \times \prod_{v \notin S} C(k_v)$$

with a finite set S of places, where X_v is an open and closed subset of $C(k_v)$.

There will be two versions of the conjecture, a weaker and a stronger one.

Main Conjecture (weak version).
If $X \subset C(\mathbb{A}_k)$ is a residue class such that $X \cap C(k) = \emptyset$, then there exists an unramified covering $D \xrightarrow{\pi} C$ such that for all twists $D_j \xrightarrow{\pi_j} C$, we have $\pi_j(D_j(\mathbb{A}_k)) \cap X = \emptyset$.

In other words, we can actually *prove* that $X \cap C(k) = \emptyset$ using some unramified covering.

Main Conjecture (strong version).
Same as before, but we require the unramified covering $D \to C$ to be abelian.

Here are some consequences.

- The weak version implies that we can decide if $C(k) = \emptyset$: we search for a point by day and run through the coverings by night (they can be enumerated), until one of the two attacks is successful.
- When $C(k)$ is empty, the strong version is equivalent to saying that the Brauer-Manin obstruction is the only obstruction against rational points on C.

3. Evidence

Now I want to give some evidence for these conjectures.
First a few general facts.

- The strong conjecture is true for curves of genus zero. (Use Hasse Principle and weak approximation.)
- Let C be a curve of genus 1, with Jacobian E. If C represents an element of $Ш(k, E)$ that is not divisible, then the strong conjecture is true for C. It is true for E if and only if the divisible subgroup of $Ш(k, E)$ is trivial.
- Similarly, if C is of genus ≥ 2 and Pic^1_C is a non-divisible element in $Ш(k, J)$ (where J is the Jacobian of C), then the strong conjecture holds for C.
- If $C \to A$ is a nonconstant morphism into an abelian variety A such that $A(k)$ is finite and $Ш(k, A)_{\mathrm{div}} = 0$, then the strong conjecture is true for C. (Stoll, partial results by Colliot-Thélène and Siksek in the context of the Brauer-Manin obstruction)
- Bjorn Poonen has heuristic arguments supporting an even stronger version of the conjecture in case $C(k)$ is empty.

From this and by other means, we get a number of concrete examples.

- The strong conjecture is true for all modular curves $X_0(N)$, $X_1(N)$ and $X(N)$ over $\mathbb{Q}$. (Use Mazur and W. Stein's tables)
- Computations have shown the strong conjecture to hold for all but 1488 genus 2 curves of the form $y^2 = f(x)$, where f has integral coefficients of absolute value at most 3, such that the curve does not have a rational point (here $k = \mathbb{Q}$). Under the assumption that $Ш(k, J)_{\mathrm{div}} = 0$ for the Jacobian J of such a curve, the strong conjecture holds for 1383 out of these 1488 curves. Assuming in addition the Birch and Swinnerton-Dyer

conjecture (plus standard conjectures on L-series), the strong conjecture holds for 42 of the remaining 105 curves. We hope to be able to deal with the other 63 curves in due course. (Bruin, Stoll)
- Successful Chabauty computations verify the strong conjecture for residue classes defined in terms of just one place v.

There are also some relative statements that allow us to conclude that some version of the conjecture holds for one curve, if we know it for one or more other curves.

- If either version of the conjecture holds for C/K, where K/k is a finite extension, and $C(K)$ is finite, then it holds for C/k. (Stoll)
- If $C(k)$ is finite and $D \to C$ is a nonconstant morphism, and either version of the conjecture holds for C, then it also holds for D. (Stoll, partial result by Colliot-Thélène in the context of the Brauer-Manin obstruction)
- If $D \to C$ is an unramified covering, $C(k)$ is finite, and the weak version of the conjecture holds for all twists D_j, then it also holds for C. (Stoll)

This allows us to show that one of the two versions holds for a given curve in many cases.

We can also use these results to prove a statement of a somewhat different flavor.

- If the weak conjecture holds for $y^2 = x^6 + 1$ over all number fields k, then it also holds for all hyperelliptic curves of genus ≥ 2 (and many more, perhaps all curves with $g \geq 2$) over any number field. (Use Bogomolov-Tschinkel)

4. More Conjectures

Let me state two more rather plausible conjectures.

"Strong Chabauty" Conjecture.

Assume that $C \to A$ is a nonconstant morphism into an abelian variety such that the image of C is not contained in a proper abelian subvariety. Also assume that $\operatorname{rank} A(k) \leq \dim A - 2$. *Then there is a set of places v of k of density 1 and a zero-dimensional subscheme $Z \subset C$ such that $C(k_v)$ intersects the topological closure of $J(k)$ in $J(k_v)$ only in points from Z.*

The motivation for this conjecture comes from the fact that in this situation, the system of equations for the intersection is overdetermined. Hence you do not expect solutions unless there is a good reason for them.

- If C satisfies assumptions and conclusion of the above conjecture, and $Ш(k, A)_{\mathrm{div}} = 0$, then the strong version of the main conjecture is true for C. (Stoll)

"Eventually Small Rank" Conjecture.

Let C be a curve of genus ≥ 2. Then there is some $n \geq 1$ such that for all twists D_j of the multiplication-by-n covering of C with $D_j(\mathbb{A}_k) \neq \emptyset$, the Jacobian of D_j has a factor A such that $\operatorname{rank} A(k) \leq \dim A - 2$.

Since the genus of the D_j grows rapidly with n, this essentially says that one does not expect Mordell-Weil ranks to be large compared to the dimension.

- Assume
  (1) $Ш(k,A)_{\mathrm{div}} = 0$ for all abelian varieties,
  (2) the "Strong Chabauty" conjecture,
  (3) the "Eventually Small Rank" conjecture.
  Then the weak version of the main conjecture holds for all curves over k, and $C(k)$ can be determined.

References

[1] M. Stoll, *Finite descent and rational points on curves*, Preprint (2005).

On the computation of the coefficients of a modular form, III: Application of Arakelov intersection theory

Robin de Jong

(joint work with Jean-Marc Couveignes, Bas Edixhoven)

Let $X/\overline{\mathbb{Q}}$ be a smooth proper curve of genus $g > 0$, let D be an effective divisor of degree g on X, and let $f : X \to \mathbb{P}^1$ be a non-constant morphism. Let U_D be the open subvariety of x in $\mathrm{Pic}_0(X)$ such that there is a unique effective divisor D'_x such that $x = [D'_x - D]$. On $U_D(\overline{\mathbb{Q}})$ we have a natural Weil height function $h_{D,f}$ sending $x \mapsto h(\sum_i f(Q_{x,i}))$ if $D'_x = \sum_i Q_{x,i}$, where h is the usual naive height function on $\mathbb{P}^1$. The object of the present lecture is to prove the following theorem.

Theorem. There is a second natural Weil height function $\tilde{h}_{D,f} : U_D(\overline{\mathbb{Q}}) \to \mathbb{R}$ and there are effectively computable functions $B_1 = B_1(X)$ and $B_2 = B_2(X, D, f)$ such that

$$(i) \qquad h_{D,f}(x) \leq \tilde{h}_{D,f}(x) + B_1(X) \quad \text{for all } x \in U_D(\overline{\mathbb{Q}})$$

and

$$(ii) \qquad \tilde{h}_{D,f}(x) \leq B_2(X, D, f) \quad \text{for all torsion points } x \in U_D(\overline{\mathbb{Q}})\,.$$

The first estimate should be seen as providing an effective comparison between two different but equivalent height functions, and the second estimate should be seen as expressing the idea that the height of a torsion point x is small independent of x (compare with the Neron-Tate height, which is always zero on torsion points). The construction of $\tilde{h}_{D,f}$ is done using Arakelov intersection theory [1] [2]. Explicitly, we find

$$B_1(X) = \frac{g}{[K:\mathbb{Q}]} \sum_{\sigma} \log G_{\sigma,\sup}(X_\sigma) + \log g\,,$$

where K is any number field over which K is defined, and where the $G_{\sigma,\sup}(X_\sigma)$ are the sups of the Arakelov-Green function [1] [2] on the compact Riemann surfaces X_σ associated to X/K using the various complex embeddings σ of K. The

number $B_1(X)$ is independent of the choice of K. Next we find that $B_2(X, D, f)$ is $\deg f/[K : \mathbb{Q}]$ times

$$-\frac{1}{2}(D, D-\omega) + 4g^2 \sum_s \delta_s \log \#k(s) + \frac{1}{2} \deg \det Rp_*\omega + \sum_\sigma \log \|\vartheta\|_{\sigma,\sup} + (f^*\infty, D) + \frac{g}{2}[K : \mathbb{Q}] \log(2\pi) .$$

Here K is so large as to have X, D, f and x defined over K, and so that X has semi-stable reduction over K. The intersections are Arakelov intersections on a regular semi-stable model of X over K. The various other terms occurring have their usual meaning as in say [2]. Again, the whole expression for B_2 is independent of the choice of K.

Recall that Bas Edixhoven has proved in an earlier lecture that for $X = X_1(l)$ one can choose D, f such that $V_l \setminus \{0\}$ is in U_D. Using our explicit formulas for B_1, B_2, he will prove in a subsequent lecture that the naive height of the coefficients of the polynomial $P_l(T) = \prod_{x \in V_l \setminus \{0\}} (T - \sum_i f(Q_{x,i})) \in \mathbb{Q}[T]$, where again $D'_x = \sum_i Q_{x,i}$, is bounded by a polynomial in l. This, in turn, is instrumental in proving that the running time of our proposed algorithm for computing $\tau(p)$ mod l is at worst polynomial in l.

References

[1] Arakelov, S. Ju. *An intersection theory for divisors on an arithmetic surface.* Izv. Akad. Nauk SSSR Ser. Mat. 38 (1974), 1179–1192.

[2] Faltings, Gerd *Calculus on arithmetic surfaces.* Ann. of Math. (2) 119 (1984), no. 2, 387–424.

Solvability of polynomial equations over finite fields

Neeraj Kayal

We investigate the complexity of the following polynomial solvability problem: given a finite field $\mathbb{F}_q$ and a set of polynomials $f_1, f_2, \cdots, f_m \in \mathbb{F}_q[x_1, x_2, \cdots, x_n]$ of total degree at most d determine the $\mathbb{F}_q$-solvability of the system $f_1 = f_2 = \cdots = f_m = 0$. That is, determine whether there exists a point $\bar{a} \in \mathbb{F}_q^n$ such that

$$f_1(\bar{a}) = f_2(\bar{a}) = \cdots = f_m(\bar{a}) = 0$$

This problem is easily seen to be **NP**-complete even when the field size q is as small as 2 and the the degree of each polynomial is bounded by $d = 2$. Here we investigate the deterministic complexity of this problem when *the number of variables in the input is bounded*. We show that for a fixed number of variables, there is a *deterministic* algorithm for this problem whose running time is bounded by a polynomial in d, m and $\log q$.

References

[1] M. D. Huang, Y. C. Wong *Solving Systems of Polynomial Congruences Modulo a Large Prime.*, Proceedings of the Foundations of Computer Science (FOCS) conference **1996**, 115-124.

Random matrix theory and Heegner points

Mark Watkins

Fix a rational elliptic curve E. Random matrix theory gives a rather precise estimate for the number of d with $|d| < D$ such that the twisted curve E_d has even analytic rank at least two. This number is conjectured to be asymptotically equal to $c_E D^{3/4} (\log D)^{b_E}$ where b_E depends on the rational 2-torsion structure of E and the squareness of its discriminant, and c_E is rather mysterious [1]. This prediction comes first from the RMT-based heuristic that the probability that $L(E_d, 1) \leq x$ is like $c\sqrt{x}(\log D)^{3/8}$ for small x, and then a discretisation of values of $L(E_d, 1)$ via the Birch–Swinnerton-Dyer formula, using the fact that the analytic value of $Ш_d$ is square (and $Ш_d = 0$ corresponds to a curve of analytic rank 2 or more). For odd twists there is no precise prediction from random matrix theory; we have the RMT-based heuristic that the probability that $L'(E_d, 1) \leq x$ is like $cx^{3/2}(\log D)^{3/8}$ but have little understanding of how to discretise the values of $L'(E_d, 1)$.

The data of Rubinstein [2] lend credence to the estimate in the even rank case; with a data set of 2398 curves, they consider negative fundamental discriminants up to 10^8 that satisfy a Heegner-type hypothesis, and suggest that the exponent of D is 0.75 ± 0.01 and b_E is within 0.1 of its predicted value. The calculation method of Rubinstein involves weight-3/2 modular forms, and can compute up to D in time $D^{3/2}$ naïvely, or in time $D^{1+\epsilon}$ using convolution methods. For odd twists, Elkies [3] has done experimentation up to 10^7 for the congruent number curve using Heegner points; his method adds up (on the complex torus) the images of the h conjugates under the modular parametrisation map, and sees if it is close to a torsion point. This takes $D^{3/2}$ time, and there does not seem to be any possibility to improve this via convolution techniques.

Elkies now suggests a different method to identify odd twists that (are likely to) have analytic rank 3 or more. The idea is to compute the Heegner point modulo p for many small primes p, which is possible in some cases due to the fact that under appropriate conditions the complex multiplication points on $X_0(N)$ are supersingular points mod p. If the computed point is the image of a torsion point for many primes p, then we might guess that it really is a torsion point (a similar idea can also be used to test for divisibility of the Heegner point).

We fix a rank zero elliptic curve E and run over small p up to some limit, say $(\log D)^3$. We then run over all negative fundamental discriminants that both satisfy a Heegner hypothesis and have p inert in the corresponding quadratic field. For each of these, we compute the images of the supersingular points of $X_0(N)$ modulo p on E_d modulo p. This step might be difficult in general, but for specific curves like $X_0(11)$ or $X_0(32)$ it is not too problematic. Then we wish to know the

multiplicity of each of these images in an appropriate Heegner sum. This is given by counting embeddings of the imaginary quadratic field into the endomorphism algebra of the supersingular point, which is in turn given by the Fourier coefficient of a Θ-series of a translate of a rank 3 lattice. This last fact should allow us to use convolution techniques and reduce the running time to $D^{1+\epsilon}$, but we have not yet determined if the method is practical. There are other theoretical directions that can be pursued; for instance, we can try to study p-adic weight-3/2 modular forms via repeating the above argument modulo higher powers of p.

References

[1] J. B. Conrey, J. P. Keating, M. O. Rubinstein, N. C. Snaith, *On the frequency of vanishing of quadratic twists of modular L-functions.* In *Number theory for the millennium, I* (Urbana, IL, 2000), edited by M. A. Bennett, B. C. Berndt, N. Boston, H. G. Diamond, A. J. Hildebrand and W. Philipp, A K Peters, Natick, MA (2002), 301–315. Available online at `www.arxiv.org/math.NT/0012043`

[2] J. B. Conrey, J. P. Keating, M. O. Rubinstein, N. C. Snaith, *Random Matrix Theory and the Fourier Coefficients of Half-Integral Weight Forms.* Available online at `www.arxiv.org/math.NT/0412083`

[3] N. D. Elkies, *Heegner point computations.* In *Algorithmic Number Theory*, ANTS-I (Ithaca 1994), edited by L. M. Adleman and M. D. Huang, Springer Lecture Notes in Computer Science, **877** (1994), 122–133.
N. D. Elkies, *Curves $Dy^2 = x^3 - x$ of odd analytic rank.* In *Algorithmic number theory*, ANTS-V (Sydney 2002), edited by C. Fieker and D. R. Kohel, Springer Lecture Notes in Computer Science, **2369** (2002), 244–251. Available online at `www.arxiv.org/math.NT/0208056`

On the computation of the coefficients of a modular form, IV: the Arakelov contribution

Bas Edixhoven

(joint work with Jean-Marc Couveignes, Robin de Jong)

Recall $X_\ell := X_1(5\ell)$. Let $B_\ell := B_1 + B_2$, where B_1, B_2 are as in Robin's lecture. Then

$$\begin{aligned} B_\ell = &\frac{g}{[K:\mathbb{Q}]}\sum_\sigma \log G_{\sigma,\sup} + \log g + \frac{1}{[K:\mathbb{Q}]}(f^*\infty, D) - \frac{\deg f}{2[K:\mathbb{Q}]}(D, D-\omega) \\ &+ \frac{4g^2\deg f}{[K:\mathbb{Q}]}\sum_s \delta_s \log \#k(s) + \frac{\deg f}{2[K:\mathbb{Q}]}\deg\det Rp_*\omega + \frac{g\deg f}{2}\log(2\pi) \\ &+ \frac{\deg f}{[K:\mathbb{Q}]}\sum_\sigma \log\|\theta\|_{\sigma,\sup}. \end{aligned}$$

The polynomial we want to compute is $P_\ell = \prod_{i=1}^{\ell^2-1}(T-\alpha_i)$ with $h(\alpha_i) \le B_\ell$, where h is the absolute naive height on $\mathbb{P}^1(\overline{\mathbb{Q}})$. The expression above is independent of the field K, as long as X_ℓ has stable reduction over O_K and D is defined over K. We take $K = \mathbb{Q}(\zeta_{5\ell})$.

We need to show that there exists c such that $B_\ell = O(\ell^c)$. We have

(1) $g = O(\ell^2)$.
(2) $[K:\mathbb{Q}] = 4(\ell-1) \geq \ell$.
(3) $\deg f = O(\ell^2)$.
(4) $\sum_s \delta_s \log \#k(s) = O(\ell \log \ell) + O(l^3) = O(l^3)$: contributions only from $s|\ell$ and $s|5$, respectively; there are $O(\ell)$ supersingular points with $s|\ell$, and $O(\ell^2)$ with $s|5$.
(5) $\deg\det Rp_*\omega = [K:\mathbb{Q}]h_{\mathrm{abs,Falt}}(J_\ell) = O(\ell^3 \log \ell)$, where $h_{\mathrm{abs,Falt}}$ is the absolute Faltings height. Short sketch: Let vol′ be volume with respect to the inner product for which the basis $\omega_1, \ldots, \omega_g$ is orthonormal. Then

$$\begin{aligned}\frac{h_K(J_{\ell,K})}{[K:\mathbb{Q}]} &\leq h_{\mathbb{Q}}(J_{\ell,\mathbb{Q}}) \leq -\log \mathrm{vol}\, \frac{\mathbb{R}\otimes S_2(\Gamma_1(5\ell),\mathbb{Z})}{S_2(\Gamma_1(5\ell),\mathbb{Z})} = -\log \mathrm{vol}\, \frac{\mathbb{R}\otimes \mathbb{T}^\vee}{\mathbb{T}^\vee} \\ &= \log \mathrm{vol}\, \frac{\mathbb{R}\otimes\mathbb{T}}{\mathbb{T}} \leq \log \mathrm{vol}'\, \frac{\mathbb{R}\otimes\mathbb{T}}{\mathbb{T}} - \frac{g}{2}\log\pi + 2\pi g \\ &= O(\ell^2 \log \ell),\end{aligned}$$

where the last step comes from bounds on the coefficients $a_n(\omega_i)$. Remark: Abbes-Ullmo did X_0(squarefree N), but we needed X_1.

(6)
$$\sum_\sigma \log \|\theta\|_{\sigma,\sup} = [K:\mathbb{Q}] \log \|\theta\|_{\sup} = O(\ell\ell^4 (\log\ell)^2 \ell^6),$$
where the ℓ comes from $[K:\mathbb{Q}]$, the $\ell^4(\log\ell)^2$ comes from $\log(\det \operatorname{Im}\tau)$, and the ℓ^6 comes from $\log(e^{\cdots}|\theta|)$. (As of Tuesday, this no longer depends on Bost's preprint, but does depend on unpublished work of us!)

(7)
$$\sum_\sigma \log G_{\sigma,\sup} = [K:\mathbb{Q}] \log G_{\sup} = O(\ell\ell^8),$$
with a non-effective constant. Remark: There is a submitted article by Jorgenson and Kramer in which bounds on Green functions are given that imply that $\log G_{\sup}$ is bounded uniformly in ℓ.

The bound ℓ^8 uses a result of Franz Merkel. Let X be a compact Riemann surface, and μ a positive 2-form (volume form) with $\int_X \mu = 1$. Let $X = U^{(1)} \cup \cdots \cup U^{(n)}$ be an open covering, and let $z^{(i)}\colon U^{(i)} \to \mathbb{C}$ be a holomorphic function such that $z^{(i)}(U^{(i)}) \supset \overline{D(1)}$ (the closed unit disk). For $0 \leq r \leq 1$, let $U_r^{(i)} := \{x \in U^{(i)} : |z^{(i)}(x)| < r\}$. Fix $0 < r_1 < 1$ and suppose

(a) $\bigcup_i U_{r_1}^{(i)} = X$
(b) For all i, $\mu \leq c_1 |dz^{(i)} d\overline{z^{(i)}}|$ on $U_1^{(i)}$.
(c) For all i, j, we have
$$\sup_{U_1^{(i)} \cap U_1^{(j)}} \left| \frac{dz^{(i)}}{dz^{(j)}} \right| \leq M.$$

Then

$$\log G_{\sup} \leq n(c_4 + c_9 c_1 + c_7 \log M),$$

where c_4, c_7, c_9 depend only on r_1.

Application to $X_\ell(\mathbb{C})$. Replace X_ℓ by $X(5\ell)$, together with its action of $\mathrm{SL}_2(\mathbb{Z}/5\ell\mathbb{Z})$. We can take $c_1 = O(\ell^3)$. We have $q^{1/5\ell} = e^{2\pi iz/5\ell}$. There are $\approx \ell^2$ cusps. This gives $\approx \ell^2$ disks. Small disks: we need $O(\ell^4)$ of them. The choice $M = 5$ is good.

(8) $-\frac{1}{2}(D, D - \omega) = O(\ell\ell^4\ell^8)$, where the $O(\ell)$ comes from $[K : \mathbb{Q}]$, the ℓ^4 comes from g^2, and the ℓ^8 comes from the Green functions.

(9) $(f^*\infty, D) = O(\ell\ell^4\ell^8)$ similarly.

Conclusion: $B_\ell = O(\ell^{14})$.

Also $\log \#R^1 p_* \mathcal{L}_x(D) \leq O(\ell^{15})$, and the left hand side is at least the sum of $\log \#k(s)$ over s such that D'_x is not unique over $k(s)$.

Functions, reciprocity and the obstruction to divisors on curves

Samir Siksek

(joint work with Martin Bright)

Let K be a perfect field, C a smooth projective curve over K, and f a non-constant element of the function field $K(C)$. We define

$$G_f(k) := \prod_{P \in C(\overline{K})} \underset{K(P)/K}{\mathrm{Norm}} (K(P)^*)^{\mathrm{ord}_P(f)}.$$

The product makes sense since all but finitely many of the terms are $\{1\}$, and the result is clearly a subgroup of K^*. Our first theorem defines a homomorphism from the Picard group $\mathrm{Pic}(C)$ to the quotient group $K^*/G_f(K)$ In essence, this means that we are doing descent on the Picard group of the curve.

Theorem 2. *With notation as above, f induces a unique homomorphism*

$$\phi : \mathrm{Pic}(C) \to K^*/G_f(K)$$

satisfying the following property: if $\sum m_j Q_j$ is a divisor on C whose support is disjoint from the poles and zeros of f, then the class $[\sum m_j Q_j]$ of this divisor in $\mathrm{Pic}(C)$ is mapped, by ϕ, to the coset represented by

$$\prod f(Q_j)^{m_j}$$

in the group on the right-hand side.

This theorem subsumes many earlier results, by various authors, whereby certain functions on a curve C are shown to induce homomorphisms from the Jacobian J into groups of the form, say, L^*/L^{*q}, where L is some finite K-algebra, and q is some positive integer.

Now let K be a number field. We denote by $\mathbb{I}_K$ the idèle group of K, and $\mathrm{Cl}_K := \mathbb{I}_K/K^*$ the idèle class group of K. Again let C be a curve defined over

K and let f be a non-constant element of the function field $K(C)$ satisfying the following property: there is some $P \in C(\overline{K})$ such that $\mathrm{ord}_P(f) = \pm 1$. The condition on f forces the group

$$\prod_{P \in C(\overline{K})} \mathrm{Norm}_{K(P)/K} \left(\mathrm{Cl}_{K(P)} \right)^{\mathrm{ord}_P(f)}$$

to be an open subgroup of finite index in Cl_K. The Existence Theorem of class field theory then asserts the existence of a unique finite abelian extension L/K (*the class field of K beloging to this group*) such that

$$\mathrm{Norm}_{L/K}(C_L) = \prod_{P \in C(\overline{K})} \mathrm{Norm}_{K(P)/K} \left(\mathrm{Cl}_{K(P)} \right)^{\mathrm{ord}_P(f)}.$$

By abuse of language, we call L the class field of K belonging to the function f. The reader is warned that for almost all functions f the class field L will be the same as K. In this case the discussion below is true though certainly not interesting. To get useful information about the curve one needs a carful choice of function (or functions) with non-trivial class fields.

It turns out that the construction of Theorem 2 induces the following commutative diagram

$$\begin{array}{ccccc} \mathrm{Pic}(C) & & \xrightarrow{\phi} & & K^*/\mathrm{Norm}(L^*) \\ \downarrow{\scriptstyle i} & & & & \downarrow{\scriptstyle i} \\ \prod_{v \in \mathfrak{M}(k)} \mathrm{Pic}(C_v) & \xrightarrow{\hat{\phi}} & \mathbb{I}_K/\mathrm{Norm}(\mathbb{I}_L) & \xrightarrow{\theta} & \mathrm{Gal}(L/K) \end{array}$$

where $\mathfrak{M}(K)$ is the set of primes of K, the i denote obvious diagonal maps and θ is the Artin map. We know from the Artin Reciprocity Theorem that $\theta \circ i = 1$. We deduce that the image of $\mathrm{Pic}(C)$ in $\prod \mathrm{Pic}(C_v)$ (under the diagonal map) is contained in the kernel of the map

$$\prod \mathrm{Pic}(C_v) \xrightarrow{\theta \circ \phi} \mathrm{Gal}(L/K).$$

This fact is perhaps theoretically interesting, though certainly useless for practical purposes; the problem is that the kernel of the map $\theta \circ \phi$ is too large to compute.

We now write $\hat{\phi} = (\phi_v)_v$ where ϕ_v are the obvious local maps, and we write $\theta = \prod \theta_v$ where θ_v are the local Artin maps. It turns out that $\theta_v \circ \phi_v = 1$ for all but finitely many primes v; we let $B \subset \mathfrak{M}(K)$ be the set of exceptions. We now deduce that the image of $\mathrm{Pic}(C)$ in $\prod \mathrm{Pic}(C_v)$ (under the diagonal map) is contained in the kernel of the map

$$\prod_{v \in B} \mathrm{Pic}(C_v) \xrightarrow{\prod_{v \in B} \theta_v \circ \phi_v} \mathrm{Gal}(L/K).$$

We now let $n = [L : K]$. Thus we obtain a meaningful homomorphism

$$\prod_{v \in B} \mathrm{Pic}(C_v)/n \,\mathrm{Pic}(C_v) \longrightarrow \mathrm{Gal}(L/K)$$

whose kernel contains the image of $\mathrm{Pic}(C)/n\,\mathrm{Pic}(C)$. The good thing is that $\mathrm{Pic}\,C_v/n\,\mathrm{Pic}(C_v)$ is finite and computable and that this allows us to compute the kernel.

Now an element of $\mathrm{Pic}(C_v)/n\,\mathrm{Pic}(C_v)$ does not have a well-defined degree, but it does have a well-defined degree modulo n. If $0 \le r < n$, we denote by

$$(\mathrm{Pic}(C_v)/n\,\mathrm{Pic}(C_v))_r$$

to be the **subset** of elements that have degree r modulo n. This subset contains the images of

$$\mathrm{Pic}^r(C), \quad \mathrm{Pic}^{r+n}(C), \quad \mathrm{Pic}^{r+2n}(C), \ldots$$

in $\mathrm{Pic}(C_v)/n\,\mathrm{Pic}(C_v)$. We immediately obtain the following theorem.

Theorem 3. *Consider the induced map*

$$\prod_{v\in B} (\mathrm{Pic}(C_v)/n\,\mathrm{Pic}(C_v))_r \longrightarrow \mathrm{Gal}(L/K).$$

The subset of elements of the set on the left-hand side sent to 1 *under this map is finite. If this subset is empty then* $\mathrm{Pic}^r(C)$, $\mathrm{Pic}^{r+n}(C)$, $\mathrm{Pic}^{r+2n}(C), \ldots$ *are all empty.*

Finally we give an example to show that the above scenario is realistic.

Example. Let $C/\mathbb{Q}$ be the genus 1 curve given by

$$C \;:\quad y^2 = -727x^4 - 104x^3 + 92x^2 + 4x - 4.$$

The curve C has points everywhere locally. We would like to show that C does not have any rational points. Take

$$f = \frac{x + 16/53}{x};$$

in this case it is possible to show that $L = \mathbb{Q}(i)$. We identify $\mathrm{Gal}(L/K)$ with $\mu_2 = \{1, -1\}$.

Primes	Basis for $\mathrm{Pic}(C_p)/2\,\mathrm{Pic}(C_p)$	$\phi(P)$	$(\theta_p \circ \phi)(P)$
$p = \infty$	$P_0 = (-0.3018\ldots, 0.0003\ldots)$	-0.00028	-1
$p = 2$	$P_0 = (2^{-1}, 2^{-2} + 1 + 2 + \cdots)$	$1 + 2^5 + \cdots$	1
	$P_1 = (2^{-4} + \cdots, 2^{-8} + \cdots)$	$1 + 2^8 + \cdots$	1

We see that the "Kernel" of $(\prod_p \mathrm{Pic}(C_p)/2\,\mathrm{Pic}(C_p))_1 \to \{1, -1\}$ is *empty*. Thus $C(\mathbb{Q}) = \emptyset$.

References

[1] S. Siksek, *Sieving for rational points on hyperelliptic curves*, Math. Comp. **70** (2000), 1661–1674.

[2] S. Siksek, *Descent on Picard groups using functions on curves*, Bull. Austral. Math. Soc. **66** (2002), 119–124.

[3] S. Siksek and A. Skorobogatov, *On a Shimura curve that is a counterexample to the Hasse principle*, Bull. London Math. Soc. **35** (2003), 409–414.

[4] M. Bright and S. Siksek, *Functions, reciprocity and the obstruction to divisors on curves*, in preparation.

Integral points on congruent number curves

Michael A. Bennett

(joint work with P.G. Walsh)

If N is a positive integer, then N is a congruent number, that is, there exists a right triangle with rational sides and area N, precisely when the elliptic curve

$$E_N \ : \ y^2 = x^3 - N^2 x$$

has infinitely many rational points. In this talk, we address the question of whether curves of the shape E_N possess *integral* points of infinite order, provided we know they have rational points with this property. We will concentrate on the case where $N = 2^a p^b$ for a and b nonzero integers and p an odd prime. Since E_N is rationally isomorphic to $E_{m^2 N}$ for each nonzero integer m, and since both E_1 and E_2 have rank 0 over $\mathbb{Q}$, we may suppose, without loss of generality, that b is odd.

¿From now on, we will fix p to be an odd prime number, and a and b to be nonnegative integers. We are interested in describing the integer solutions (x, y), with, say, $y > 0$ to the Diophantine equation.

$$y^2 = x(x + 2^a p^b)(x - 2^a p^b). \tag{5}$$

A solution (x, y) (with $y > 0$) to (5) will be called *primitive* if either

$$\min\{\nu_2(x), a\} \geq 2 \ \text{ or } \ \min\{\nu_p(x), b\} \geq 2.$$

¿From the above remarks, clearly it is enough to determine all primitive integer solutions. These correspond to the S-integral points on E_p and E_{2p}, where $S = \{2, p\}$.

Our main result is that all solutions are as follows. First, we have the following sporadic solutions; in each case $b = 1$.

(6)

p	a	x	p	a	x	p	a	x	p	a	x
3	1	-3	3	3	25	7	3	-7	29	0	284339
3	1	-2	5	0	-4	7	4	-63	41	6	42025
3	1	12	5	0	45	11	1	2178			
3	1	18	5	2	25	17	5	833			
3	1	294	7	1	112	17	7	16337			

The remaining solutions come in a number of families, many of which are, presumably, infinite.

$$\left(2^{a-1}\right)^2 - ps^2 = -1,\ a \text{ odd},\ b = 1,\ x = p^2 s^2. \tag{7}$$

$$r^4 + s^4 = p^b,\ a = 1,\ x = -(2rs)^2. \tag{8}$$

$$p^2 - 2s^2 = -1,\ a = 0,\ b = 1,\ x = s^2. \tag{9}$$

$$r^4 + 6r^2 s^2 + s^4 = p^b,\ a = 0,\ x = -(r^2 - s^2)^2. \tag{10}$$

$$p^{2b} \pm 6p^b + 1 = 8s^2,\ a = 1,\ x = \frac{1}{2}\left(p^b \pm 1\right)^2. \tag{11}$$

$$r^4 + 12r^2 s^2 + 4s^4 = p^b,\ a = 1,\ x = -2(r^2 - 2s^2)^2. \tag{12}$$

$$p^2 r^4 - 2s^2 = 1,\ p \equiv 1 \mod 8,\ a = b = 1,\ x = 2\,(pr)^2. \tag{13}$$

$$2^{2(a-2)} + 3 \cdot 2^{a-1} + 1 = ps^2,\ a \geq 3,\ b = 1,\ x = p\left(2^{a-2} + 1\right)^2. \tag{14}$$

An almost immediate corollary is that, if $N = 2^a p^b$ where $p \equiv \pm 3 \mod 8$ is prime, $p \neq 3, 5, 11, 29$, then

$$E_N(\mathbb{Z}) = \{(0,0), (\pm N, 0)\}.$$

Note here that, according to Monsky [3], we have that $p \equiv 5, 7 \mod 8$ are congruent, while the same is true for $2p$, when $p \equiv 3, 7 \mod 8$. These follow from Heegner and mock-Heegner point analysis.

The main method of proof is an elementary reduction of the problem to certain quartic Diophantine equations which may be treated by a variety of methods, classical and otherwise. We note further, that we may absolutely bound b in the above families, arguing as in Ellenberg [2] to "solve" families of ternary equations of Fermat-type. This is work in progress.

Finally, we should mention that an algorithm to solve equation (5) for fixed a, b and p has recently been given by Draziotis and Poulakis [1], using Wildanger's algorithm to solve a unit equation over a quartic field. As the above classification indicates, this is unnecessary.

References

[1] K. Draziotis and D. Poulakis, *Practical solution of the Diophantine equation* $y^2 = x(x + 2^a p^b)(x - 2^a p^b)$, preprint.

[2] J. Ellenberg, *Galois representations attached to Q-curves and the generalized Fermat equation* $A^4 + B^2 = C^p$, Amer. J. Math. **126** (2004), 763–787.

[3] P. Monsky, *Mock Heegner points and congruent numbers*, Math. Z. **204** (1990), 45–68.

Local Galois module structure for Artin-Schreier extensions of degree p

Bart de Smit
(joint work with Lara Thomas)

Let L/K be a Galois extension of local fields with $[L:K] = p = \mathrm{char}(K)$. Let G be the Galois group and $A \subset B$ the extension of valuation rings. By the normal basis theorem, L is free of rank 1 as a module over the group ring $K[G]$. The valuation ring B is free of rank 1 over $A[G]$ if and only if L/K is unramified. Let us assume that L/K is totally ramified, i.e., that the ramification index is p. Let k be the resdue field of A, which is also the residue field of B. We let r be the ramification number of L/K, so the filtration of G with ramification groups satisfies $G_r \neq G_{r+1}$.

The multiplier ring of B, or the associated order of B, is defined as $R = \{x \in K[G] : xB \subset B\}$. Note that R is the endomorphism ring of B as an $A[G]$-module. It is a complete local ring, which is free of rank p as an A-module. We let $e = \dim_k(\mathbf{m}_R/\mathbf{m}_R^2)$ be the embedding dimension of R, and we will show that it is tightly related to the number of R-module generators of B.

We first present a slight strengthening and an independent proof of a result of Aiba and Lettl [1, 4], whose characteristic 0 analog is given in [2]:

$$B \text{ is a free } R\text{-module} \iff e \leq 3 \iff s \mid p-1.$$

Here s is the remainder of r when we divide by p, which satisfies $0 < s < p$.

Our second result says that when $s \neq p-1$ the embedding dimension e of R is exactly $2d+1$, where d is the minimal number of R-module generators of B.

The proof uses the combinatorics of balanced sequences, which turns out to be encoded by the Hirzebruch continued fraction [3]. One can rewrite this in terms of the usual continued fraction [5] and obtain the following: If

$$-r/p = x_0 + \cfrac{1}{x_1 + \cfrac{1}{\ddots \quad \cfrac{\ddots}{x_{n-1} + \cfrac{1}{x_n}}}}$$

with $x_0, \ldots, x_n \in \mathbf{Z}$, and $x_1, \ldots, x_{n-1} \geq 1$ and $x_n \geq 2$, then

$$d = \sum_{i<n \text{ odd}} x_i.$$

This also gives rise to a polynomial time algorithm that given p and r computes d and e.

References

[1] A. Aiba, *Artin-Schreier extensions and Galois module structure*. J. Number Theory **102** (2003), 118–124.

[2] F. Bertrandias and M.-J. Ferton, *Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local*, C. R. Acad. Sci. Paris Sér. A-B **274** (1972), A1330–A1333.
[3] F. Hirzebruch, *Über vierdimensionale Riemannsche Fl"achen mehrdeutiger analytischer Functionen von zwei komplexen Veränderlichen*, Math. Ann. **126** (1953), 1–22.
[4] G. Lettl, *Note on a theorem of A. Aiba*, to appear in: J. Number Theory.
[5] D. B. Zagier, *Zetafunctionen und quadratische Körper*, Springer-Verlag Hochschultext, 1981.

Hecke operators and class numbers

Nicole Raulf

Let K be an imaginary quadratic number field of class number one and denote its ring of integers by $\mathcal{O}$ and the set of units of $\mathcal{O}$ by $\mathcal{O}^*$. Furthermore, let $q = [a, b, c]$ denote a primitive quadratic form whose coefficients belong to $\mathcal{O}$ and whose discriminant is an element of $\Omega := \{d \in \mathcal{O} \setminus \{0\} : d \equiv x^2 \mod 4, d \text{ no square}\}$. Remember that primitive means that the ideal generated by the coefficients of q is equal to $\mathcal{O}$. For $d \in \Omega$ let h_d be the class number of primitive quadratic forms, i. e. imposing the usual equivalence relation on primitive quadratic forms, h_d is the number of inequivalent primitive quadratic forms of discriminant d. Furthermore, for $d \in \Omega$ consider Pell's equation $t^2 - du^2 = 4$, t, $u \in \mathcal{O}$. ϵ_d is the fundamental solution of this equation and ζ_d is a root of unity of maximal order which can be written in the form $\zeta_d = \frac{t_1+u_1\sqrt{d}}{2}$, $t_1^2 - du_1^2 = 4$. If we write $\zeta_d = e^{\pi i/m_d}$, then $m_d \in \{1, 2, 3\}$. Having introduced all notations, we can now state the theorem.

Theorem 1. *For $v \in \mathcal{O} \setminus \{0\}$ we have:*

$$\sum_{|du^2| \le x} \frac{h_d \log|\epsilon_d|}{m_d} \sim \left(\frac{1}{4|v|^2} \sum_{\substack{d \in \mathcal{O}/\mathcal{O}^*, \\ d|v}} |d|^2 \right) x^2 \qquad \text{as } x \to \infty$$

where we sum over all $d \in \Omega$ and $u \in \mathcal{O}/\mathcal{O}^*$ such that $|du^2| \le x$ and $\exists t \in \mathcal{O}$ so that $t^2 - du^2 = 4v$ and $|\frac{t+u\sqrt{d}}{2\sqrt{v}}| \neq 1$.

This mean value theorem is proved with the help of Hecke operators. The Hecke operators we work with act on $\mathrm{PSL}_2(\mathcal{O})$ - invariant functions on the upper half - space $\mathbb{H}^3$. The upper half - space $\mathbb{H}^3$ is equipped with the hyperbolic metric and the corresponding Laplace operator is denoted by Δ. When trying to express the trace of the Hecke operator T_v, $v \in \mathcal{O} \setminus \{0\}$, on a fixed eigenspace of $-\Delta$ in terms of h_d and $\log|\epsilon_d|$, the following L - series appears:

$$L_v(s) := \sum_{d \in \Omega} \sum_{u} \frac{h_d \log|\epsilon_d|}{m_d |du^2|^s},$$

where the u - summation extends over all $u \in \mathcal{O} \setminus \mathcal{O}^*$ such that $\exists t \in \mathcal{O}$ with the property $t^2 - du^2 = 4v$ and $|\frac{t+u\sqrt{d}}{2\sqrt{v}}| \neq 1$. The discussion shows that $L_v(s)$ converges absolutely for $\mathrm{Re}\, s > 2$ and has an analytic continuation for $\mathrm{Re}\, s \ge 3/2$

except for a simple pole at $s = 2$. Hence a Tauberian theorem implies the theorem stated above.

References

[1] N. Raulf, *Traces of Hecke Operators Acting on Three - Dimensional Hyperbolic Space*, Dissertation Münster (2004).
[2] N. Raulf, *Traces of Hecke Operators acting on Three - Dimensional Hyperbolic Space*, to appear in J. Reine Angew. Math.

Class invariants in a non-archimedean setting

Reinier Bröker

The theory of complex multiplication provides us with a means of explicitly computing the Hilbert class field $H = H(K)$ of an imaginary quadratic number field K. Let $D = \mathrm{disc}(K) < 0$ be the discriminant of K and define

$$\mathrm{Ell}_D(\mathbf{C}) = \{E/\mathbf{C} \mid E \text{ is an elliptic curve over } \mathbf{C} \text{ with } \mathrm{End}(E) \cong \mathcal{O}_K\}_{\cong}$$

as the finite set of elliptic curves $E/\mathbf{C}$ with endomorphism ring isomorphic to the ring of integers $\mathcal{O}_K$ of K. We have the following theorem, usually called the first main theorem of complex multiplication.

Theorem. *For $[E] \in Ell_D(\mathbf{C})$ we have $H = K(j(E))$. Moreover the polynomial,*

$$f_D = \prod_{[E]\in \mathrm{Ell}_D(\mathbf{C})} (X - j(E)) \in \mathbf{Z}[X]$$

has integer coefficients.

The polynomial f_D is usually called the *Hilbert class polynomial*. We are interested in efficiently computing this polynomial.

The degree of f_D equals the class number of K and hence grows exponentially in $\log |D|$. Since any algorithm computing f_D has to write down the answer, this shows that there can't exist a polynomial time algorithm that computes f_D.

The classical algorithm of evaluating the modular function $j\colon \mathbf{H} \to \mathbf{C}$ in points $\tau \in \mathbf{H}$ corresponding to the ideal classes of the class group $\mathrm{Cl}(\mathcal{O})$ can be improved in two ways. Firstly, one can work in a non-archimedean setting as explained in [1]. This avoids the problem of rounding errors that might occur when expanding the product

$$f_D = \prod_{[E]\in \mathrm{Ell}_D(\mathbf{C})} (X - j(E)) \in \mathbf{Z}[X].$$

The second improvement is inspired by the fact that even for moderately small discriminants D, the coefficients of f_D are already huge. As example, for $D = -31$ we get coefficients of 16 digits. We can save a *constant factor* in the size of the coefficients by using other ('smaller') functions than the j-function.

Let f be a modular function (over $\mathbf{Q}$) of level $N \geq 1$. Writing $\mathcal{O} = \mathbf{Z}[\tau]$ with $\tau \in \mathbf{H}$, we have

$$f(\tau) \in H_N,$$

with H_N the ray class field of conductor N. If we have $K(f(\tau)) = K(j(\tau))$, then $f(\tau)$ is called a *class invariant*. We want to use 'smaller' function than j, because the coefficients of the corresponding polynomial will then be smaller than those of f_D.

Over the complex numbers, the modern tool to investigate class invariants is Shimura's reciprocity law (1970). It tells us if a given value $f(\tau)$ is a class invariant, and if so, in which points $\tau' \in \mathbf{H}$ we should evaluate f to compute the conjugates of $f(\tau)$ under $\mathrm{Gal}(H/K) \cong \mathrm{Cl}(\mathcal{O})$. The computation of $f(\tau)$ is easily done if we know the Fourier expansion of f.

We also want to use class invariants in a p-adic setting. For this we need a substitute of the evaluation of a function via its Fourier expansion. We note that a modular function f of level N is an element of the function field of the modular curve $X(N)$ over $\mathbf{Q}(\zeta_N)$. Hence, we can express f as a rational function in j and the x-coordinates of an elliptic curve with j-invariant j.

As example, consider an elliptic curve $E/\mathbf{Q}_p$ given by $Y^2 = X^3 + aX + b$. The cube root γ_2 of j with integral Fourier expansion is a modular function of level 3. For $3 \nmid D$, the function γ_2 yields class invariants. The coefficients of the minimal polynomial are a factor 3 smaller than the coefficients of f_D. We will write γ_2 in terms of 3-torsion points. Let $c_1, \ldots, c_4$ be the roots of the 3-division polynomial for E. A cube root of $j(E)$ is given by

$$\frac{-48a}{2a - 3(c_1c_2 + c_3c_4)}. \tag{1}$$

Note that this expression depends on an *ordering* of $c_1, \ldots, c_4$. We indeed get three distinct cube roots of $j(E)$.

Expression (1) enables us to work with cube roots of j over $\mathbf{Q}_p$. We can explicitly compute the action of the coprime to 3 ideals of $\mathcal{O}$ on the cube roots of $j(E)$. This allows to decide *which* cube root of $j(E)$ is contained in H, by checking which one is invariant under $\mathrm{Gal}(H_3/H) \cong (\mathcal{O}/3\mathcal{O})^*/\mathcal{O}^*$. If we find one that is contained in H, we can also compute its conjugates under $\mathrm{Gal}(H/K) \cong \mathrm{Cl}(\mathcal{O})$.

This approach works in general for any modular function f of level $N \geq 1$. However, we do have to write f in terms of N-torsion points. This may not be so easy, and perhaps even worse, we may have to factor the N-th division polynomial Ψ_N of degree $O(N^2)$. Hence, the gain in speed by considering 'smaller' functions might be lost.

One can work with *modular polynomials* to avoid this problem. The classical modular polynomial relates $j(\tau)$ and $j(p\tau)$. There exist similar polynomials relating $f(\tau)$ and $f(p\tau)$, where we require that p does not divide the level N of f. Using these modular polynomials, we are currently able to work with the classical Weber-$\mathfrak{f}$ function of level 48. Using normal computer power, we can now relatively easily compute the Hilbert class field of fields with discriminant up to -10^{10}.

References

[1] Couveignes, J.-M. and Henocq, T.: *Action of modular correspondences around CM points* in Algorithmic Number Theory Symposium V, Lecture Notes in Computer Science **2369**, (2002), 234–243.

Explicit computations on the Manin conjectures

Ronald van Luijk

Even though finding the set of rational points on a curve could be very hard, once the set is known, it is easy to describe. If it is not a finite set, then the genus g of the curve is at most 1. In case $g = 0$ we can give a parametrization of the curve and in case $g = 1$ the set naturally carries the structure of a finitely generated group, for which we can give a set of generators.

For a higher-dimensional variety $X \subset \mathbb{P}^n$ over a number field k it is not so easy to describe the set $X(k)$ of rational points. To this extend we define a counting function N_U for any open subset U of X, based on a height function $H\colon \mathbb{P}^n(k) \to \mathbb{R}_{>0}$. For $k = \mathbb{Q}$ the height function is defined by

$$H(x) = \max_i(|x_i|) \quad \text{when} \quad \begin{cases} x = [x_0 : x_1 : \ldots : x_n] \\ x_i \in \mathbb{Z} \\ \gcd(x_0, \ldots, x_n) = 1 \end{cases}$$

and for higher degree number fields we use the standard generalization. The counting function $N_U\colon \mathbb{R}_{>0} \to \mathbb{Z}_{\geq 0}$ is defined by

$$N_U(B) = \#\{x \in U(k) : H(x) \leq B\}.$$

We want to understand the asymptotic behavior of N_U as B tends to infinity. For some easy to understand varieties X we find that there exists an open subset U of X such that we have

$$N_U(B) \approx CB^a(\log B)^b,$$

where C is some constant, a is a number such that the canonical sheaf ω_X is isomorphic to $\mathcal{O}(-a)$, and $b+1$ is the rank of the Néron-Severi group $\mathrm{NS}(X)$ of X. The conjecture of Batyrev and Manin states that if the canonical divisor of $X \subset \mathbb{P}^n_k$ is isomorphic to $\mathcal{O}(-a)$ for some $a > 0$, then there exists a finite field extension l of k, an open subset $U \subset X$, and a constant C such that with $b = \mathrm{rank}\mathrm{NS}(X_l) - 1$ we have

$$N_{U_l}(B) \approx CB^a(\log B)^b. \tag{15}$$

Even though Batyrev and Tschinkel found a counter example to this conjecture in dimension 5, there is a lot of evidence for the case of dimension 2. We look at the degenerate case of $a = 0$, namely those of trivial canonical sheaf, in particular the case of K3 surfaces. Martin Bright has computed $N_X(B)$ for many diagonal quartic surfaces X and B up to 10^6. Especially those with low Néron-Severi rank

tend to have too few points with low height to extrapolate from. We use the quartic surface in $\mathbb{P}^3$ given by

$$w(x^3+y^3+z^3+x^2z+xw^2) = 3x^2y^2 - 4x^2yz + x^2z^2 + xy^2z + xyz^2 - y^2z^2,$$

which has Néron-Severi rank 1 even over the algebraic closure. With a program written by Michael Stoll, based on a variation of an algorithm by Noam Elkies, we computed all points of height at most 15000, of which there turn out to be 46 that do not lie on the two rational curves given by $xw = 0$. Let U be the open subset outside these two rational curves. Then $N_U(B)$ appears to grow like $\log B$, rather than being bounded as one would conclude from (15). One explanation would be that the factor B^a in (15) comes from an integral $\int B^{a-1}db$, which for $a = 0$ yields $\log B$ instead of B^a. This potentially leads to an extension of the Manin conjecture to K3 surfaces.

[1] V. Batyrev and Y. Manin, Sur le nombre des points rationnel de hauteur borné des variétés algébriques, *Math. Ann.* **286** (1990), no. 1–3, pp. 27–43.

[2] E. Peyre, Counting points on varieties using universal torsors, *Arithmetic of Higher-Dimensional Algebraic Varieties, eds. B. Poonen and Y. Tschinkel*, Prog. in Math. **226** (2004).

[3] R. van Luijk, K3 surfaces with Picard number one and infinitely many rational points, *preprint.*

On the computation of the coefficients of a modular form, V: computational aspects

Jean-Marc Couveignes

This talk is the continuation of the ones by Johan Bosman, Bas Edixhoven and Robin de Jong. I will address the problem of computing torsion divisors, with prescribed Hecke action, on modular curves (e.g. divisor classes in the linear space V_ℓ image of the modulo ℓ Galois representation ρ_ℓ attached to the Ramanujan τ-function). We need algorithms that can be proven to be polynomial time.

We have three possible strategies for doing this. We first may calculate complex approximations for the divisors we are interested in. The difficulty is then to show that we can perform efficient and stable numerical computations in the jacobian of modular curves, in deterministic polynomial time in both the level and the required accuracy. These computations should include addition/subtraction in the jacobian and the explicit solution to the inverse Jacobi problem. This has been done in [1] for the curves $X_0(p)$ when p tends to infinity. Adapting these methods to the case of $X_1(5p)$ would suffice for the computation of the Ramanujan τ function. A second possibility would be to fix an auxiliary small prime p and compute the torsion divisors we are interested in modulo p. We may then Hensel lift these divisors and obtain good p-adic approximations. The third method which I want to present in this talk computes the divisors modulo many different small primes p and then recovers the actual divisors in characteristic zero by Chinese remainder

theorem. It is slightly less efficient than the previous one. But it is simpler to explain.

It should be stressed that the efficiency of all these methods depends on the bound on the height of torsion divisors that was presented by Edixhoven and de Jong. Indeed, this bound controls the accuracy (resp. the number of auxiliary primes p) we need.

As far as the complex analytic method is concerned, the bound is also necessary to prove the numerical stability of the algorithm. As far as the modulo p method is concerned, there could be some instability also : namely if one of the divisors we are looking for becomes special when reduced modulo p. The bound by Edixhoven and de Jong shows that the number of such bad primes p is bounded by a polynomial in ℓ.

The description and proof of the algorithm goes in four steps.

(1) define and compute some explicit model for the curve $X_1(\ell)$ or some small covering X_ℓ of it.
(2) provide enough information on this curve (in particular its singularities) to be able to compute in its jacobian using what is known as the Brill-Noether algorithm.
(3) construct elements in the ℓ-Sylow subgroup of the group of $\mathbb{F}_q$-points of the jacobian of $X_1(\ell)$.
(4) using Hecke operators, construct a point in $V_\ell = \cap_{n\geq 2} \mathrm{Ker}(T_n - \tau(n))$.

We now detail these four steps.

(1) — *The modular curve* $X(2)_1(\ell)$

Let $\ell \geq 5$ be a prime. We set $d_\ell = \frac{\ell^2-1}{4}$ and $m_\ell = \frac{\ell-1}{2}$. We denote by $X_\ell = X(2)_1(\ell)$ the moduli of elliptic curves with full 2-torsion plus one non-trivial ℓ-torsion point.

Let λ be an indeterminate and form the Legendre elliptic curve with equation $y^2 = x(x-1)(x-\lambda)$. Call $\mathcal{T}_\ell(\lambda, x)$ the ℓ-division polynomial of this curve. It has degree $2d_\ell = \frac{\ell^2-1}{2}$ in x and d_ℓ in λ. We denote by $T_\ell(\Lambda, X, Y) = \mathcal{T}_\ell(\frac{\Lambda}{Y}, \frac{X}{Y})Y^{2d}$ the associated homogeneous polynomial and call $C_\ell \subset \mathbb{P}^2$ the corresponding projective curve. This is a singular plane model for X_ℓ.

The morphism $\phi : X_\ell \to X_1(\ell)$ corresponding to forgetting the 2-torsion structure is Galois with group $\mathcal{S}_3$. The six corresponding automorphisms extend to $\mathbb{P}^2$ and C_ℓ in a way compatible with the maps $X_\ell \to C_\ell$ and $C_\ell \subset \mathbb{P}^2$. The group is generated by the two transpositions $\tau_{(0,\infty)}$ and $\tau_{(0,1)}$ defined in homogeneous coordinates by $\tau_{(0,\infty)} : [\Lambda, X, Y] \to [Y, X, \Lambda]$ and $\tau_{(0,1)} : [\Lambda, X, Y] \to [Y - \Lambda, Y - X, Y]$.

(2) — *Singularities on* C_ℓ

The only possible singularities of C_ℓ lie on one of the three lines with equations $\Lambda = 0$, $Y = 0$ and $\Lambda - Y = 0$. We study the branches at infinity on C_ℓ through the associated Tate's elliptic curves and deduce the $2d_\ell$ roots of $\mathcal{T}_\ell(\lambda, x)$ in the field $\overline{\mathbb{Q}}\{\{\lambda^{-1}\}\}$ of Puiseux series in λ^{-1}. We introduce Tate's q-parameter, defined implicitly by $j = \frac{1}{q} + 744 + \cdots$. For a and b integers such that either $b = 0$ and $1 \leq a \leq \frac{\ell-1}{2}$ or $1 \leq b \leq \frac{\ell-1}{2}$ and $0 \leq a \leq \ell - 1$ we consider the ℓ-torsion point $\zeta_\ell^a q^{\frac{b}{\ell}}$

on the Tate curve with parameter q and call $x_{a,b}$ the corresponding expansion of x as a series in $\lambda^{\frac{-1}{\ell}}$. We find

$$x_{a,b} = -4\zeta_\ell^a 2^{\frac{-8b}{\ell}} \lambda^{1-\frac{2b}{\ell}} + O(\lambda^{1-\frac{2b+1}{\ell}})$$

if $b \neq 0$ and $x_{a,0} = \frac{-4\zeta_\ell^a}{(1-\zeta_\ell^a)^2}\lambda + O(1)$. We call $\Sigma_\infty = [1,0,0]$ the unique singular point at infinity and for every $1 \leq b \leq \frac{\ell-1}{2}$ we call $\sigma_{\infty,b}$ the point above Σ_∞ on X_ℓ associated to the orbit $\{x_{0,b}, x_{1,b}, \cdots, x_{\ell-1,b}\}$ for the inertia group. We call $\mu_{\infty,a}$ the point on X_ℓ corresponding to the expansion $x_{a,0}$. The ramification index of the covering map $\lambda : X_\ell \to X(2)$ is ℓ at $\sigma_{\infty,b}$ and 1 at $\mu_{\infty,a}$.

The genus of X_ℓ is $g_\ell = \frac{(\ell-3)^2}{4} = (m_\ell - 1)^2$. The arithmetic genus of C_ℓ is $g_a = (m_\ell^2 + m_\ell - 1)(2m_\ell^2 + 2m_\ell - 1)$. We now compute the conductor of C_ℓ. Locally at Σ_∞ the curve C_ℓ consists of m_ℓ branches (one for each place $\sigma_{\infty,b}$) that are cusps with equations $\left(\frac{X}{\Lambda}\right)^\ell = -2^{2\ell-8b}\left(\frac{Y}{\Lambda}\right)^{2b} + \cdots$. The conductor of this later cusp is $\sigma_{\infty,b}$ times $(\ell-1)(2b-1)$ which is the next integer to the last gap of the additive semigroup generated by ℓ and $2b$. The conductor of the full singularity Σ_∞ is now given by Gorenstein's formula [5, Theorem 2] and is

$$\sum_{1 \leq b \leq m_\ell} \{b(4m_\ell^2 + 4m_\ell - 1) - 2m_\ell - (2m_\ell + 1)b^2\} \cdot \sigma_{\infty,b}.$$

The full conductor $\mathfrak{C}_\ell$ is the sum of this plus the two corresponding terms to the isomorphic singularities Σ_0 and Σ_1. Some authors call it the adjunction divisor.

The degree $\deg(\mathfrak{C}_\ell)$ of $\mathfrak{C}_\ell$ is $2m_\ell(2m_\ell^3 + 4m_\ell^2 - 2m_\ell - 1)$. So we have $\delta(\mathfrak{C}_\ell) = m_\ell(2m_\ell^3 + 4m_\ell^2 - 2m_\ell - 1)$ and we check that $g_a = g_\ell + \delta(\mathfrak{C}_\ell)$.

(2') — *The Brill-Noether algorithm*

Let $p \notin \{2, 3, \ell\}$ be a prime. Le $\mathbb{C}_p$ be the field of p-adics and $\overline{\mathbb{F}_p}$ its residue field. We embed $\overline{\mathbb{Q}}$ in $\mathbb{C}_p$ and also in $\mathbb{C}$. In particular $\zeta_\ell = \exp(\frac{2i\pi}{\ell})$ and $2^{\frac{1}{\ell}}$ are well defined as p-adic numbers.

We set $h_\ell = 3m_\ell(m_\ell+1)$. Let $\mathcal{S}^{h_\ell} = H^0(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(h_\ell))$ the linear space of degree h_ℓ homogeneous polynomials in Λ, X, and Y. Let $\mathcal{H}^{h_\ell}$ be the space of h_ℓ-forms on X_ℓ. If $m_\ell \geq 8$ then the dimension of $\mathcal{H}^{h_\ell}(\mathfrak{C}_\ell)$ is greater than $2g_\ell$ and the restriction map $\rho : \mathcal{S}^{h_\ell} \to \mathcal{H}^{h_\ell}$ contains $\mathcal{H}^{h_\ell}(\mathfrak{C}_\ell)$ according to the residue theorem. So we have a description of $\mathcal{H}^{h_\ell}(\mathfrak{C}_\ell)$ as a subspace of $\mathcal{S}^{h_\ell}$.

A place $\mathfrak{p}$ of the field $\mathbb{F}_q(X_\ell)$ is represented in the following way. Le P be an $\overline{\mathbb{F}_q}$-point on X_ℓ above $\mathfrak{p}$. If P lies on one of the lines with equations $\Lambda = 0$, $Y = 0$ and $\Lambda - Y = 0$ then it is one of the σ's or one of the μ's and we already know how to call it.

Otherwise, P is a smooth point and may be regarded as a point on the affine part of the plane curve C_ℓ. Let $r_\mathfrak{p}$ be the degree of $\mathfrak{p}$ which is also the degree of $\mathbb{F}_q(P)$ over $\mathbb{F}_q$. The point P can be given by its affine coordinates λ and x. We call r_λ the degree of $\mathbb{F}_q(\lambda(P))$ over $\mathbb{F}_q$ and set $r_{x/\lambda} = r_\mathfrak{p}/r_\lambda$. We call $F_\mathfrak{p}(\lambda) \in \mathbb{F}_q[\lambda]$ the unitary, irreducible polynomial with degree r_λ that cancels $\lambda(P)$. We call $G_\mathfrak{p}(\lambda, x) \in \mathbb{F}_q[\lambda, x] = \mathbb{F}_q[\lambda][x]$ the unique polynomial with degree

$r_{x/\lambda}$ in x and degree $< r_\lambda$ in λ such that the coefficient of $x^{r_{x/\lambda}}$ is $1 \in \mathbb{F}_q[\lambda]$ and $G_{\mathfrak{p}}(\lambda(P), x(P)) = 0$.

So we can represent forms and divisors on our modular curve. For every form in $\mathcal{H}^{h_\ell}(\mathfrak{C}_\ell)$ we can compute its divisor. And given a divisor, we can compute the subspace of $\mathcal{H}^{h_\ell}(\mathfrak{C}_\ell)$ consisting of forms that vanish at this divisor. This is enough to compute in the jacobian J_ℓ of X_ℓ.

(3) — The ℓ-Sylow subgroup of $J_1(\ell)(\mathbb{F}_q)$

Recall there is a covering map $\phi : X_\ell \to X_1(\ell)$ corresponding to forgetting the 2-torsion structure. This induces two morphisms $\phi^* : J_1(\ell) \to J_\ell$ and $\phi_* : J_\ell \to J_1(\ell)$ such that $\phi_* \circ \phi^* = [6]$ on $J_1(\ell)$.

We denote by $\mathcal{J}_\ell \subset J_\ell$ the image of $\nu = \phi^* \circ \phi_*$. This is a subvariety of J_ℓ isogenous to $J_1(\ell)$. The restriction of ν to $\mathcal{J}_\ell$ is multiplication by 6. The maps ϕ^* and ϕ_* induce Galois equivariant bijections between the N-torsion subgroups $J_1(\ell)[N]$ and $\mathcal{J}_\ell[N]$ for every prime to 6 integer N.

For any finite field k and abelian variety A/k and prime integer n, we denote by $A[n^\infty](k)$ the n-Sylow subgroup of $A(k)$. We note N_q the number of $\mathbb{F}_q$-points in $J_1(\ell)(\mathbb{F}_q)$ and set $N_q = L_q M_q$ where M_q is prime to ℓ and L_q is a power of ℓ. We check the map $[M_q] \circ \nu = \phi^* \circ M_q \circ \phi_* : J_\ell(\mathbb{F}_q) \to \mathcal{J}_\ell[\ell^\infty](\mathbb{F}_q)$ is surjective.

By Eichler-Shimura and results of Manin, Shokurov, Merel, Cremona, [6, 7, 2, 4], for $q = p^k$ a power of a prime $p \neq \ell$, the number of $\mathbb{F}_q$-rational points on $J_1(\ell)$ is computed in time polynomial in ℓ, p, and k.

Starting from elements in $J_\ell(\mathbb{F}_q)$ and applying the operator $[M_q] \circ \phi^* \circ \phi_*$, we construct elements in the group $\mathcal{J}_\ell[\ell^\infty](\mathbb{F}_q)$.

(4) — projecting into the Ramanujan subgroup

We choose an integer $\hat{6}$ such that $6\hat{6}$ is congruent to 1 modulo L_q. We set $\hat{T}_n = [\hat{6}] \circ \phi^* \circ T_n \circ \phi_*$ and notice that $\hat{T}_n \circ \phi^* = \phi^* \circ T_n$ on $J_1(\ell)[\ell^\infty]$. This way, the map $\phi^* : J_1(\ell)[\ell^\infty](\mathbb{F}_q) \to \mathcal{J}_\ell[\ell^\infty](\mathbb{F}_q)$ becomes a bijection of Hecke modules. The forecoming calculations are more naturally described in $J_1(\ell)[\ell^\infty](\mathbb{F}_q)$ but they will be performed in $\mathcal{J}_\ell[\ell^\infty](\mathbb{F}_q)$.

We call $\mathcal{A}$ the algebra of endomorphisms of $J_1(\ell)/\mathbb{F}_p$ generated by the operators T_n for all prime integers n. We set $\mathcal{B} = \mathcal{A}[F_p]$ where F_p is the p-Frobenius operator.

We assume the polynomial $X^2 - \tau(p)X + p^{11}$ splits modulo ℓ and call a and b the two roots in $\mathbb{Z}_\ell$ which we assume to be distinct modulo ℓ. The method can be easily adapted in the inert case.

We call $V_\ell^a \subset V_\ell$ the eigenspace associated to a and V_ℓ^b the eigenspace associated to b. We denote $\mathfrak{m}_a$ the maximal ideal in $\mathcal{B}$ generated by ℓ, the $T_n - \tau(n)$ and $F_p - a$. For every integer $n \geq 2$ we call $A_n(X) \in \mathbb{Z}[X]$ the characteristic polynomial of T_n acting on modular forms of weight 2 for $\Gamma_1(\ell)$. We factor $A_n(X) = b_n(X)(X - \tau(n))^{e_n}$ in $\mathbb{F}_\ell[X]$ with $b_n(X)$ unitary and $b_n(\tau(n)) \neq 0 \in \mathbb{F}_\ell$. We set $q = p^{k_a}$ where $k_a > 0$ is an integer that kills a in $(\mathbb{Z}/\ell\mathbb{Z})^*$ and observe that $V_\ell^a = V_\ell^a(\mathbb{F}_q)$. The ℓ-Sylow subgroup $J_1(\ell)[\ell^\infty](\mathbb{F}_q)$ of $J_1(\ell)(\mathbb{F}_q)$ is contained in $J_1(\ell)[L_q](\overline{\mathbb{F}_q})$. We set $L_q = \ell^{w_q}$. The polynomial factorization $A_n(X) = b_n(X)(X - \tau(n))^{e_n}$ modulo ℓ lifts modulo L_q as $A_n(X) = B_n(X)C_n(X)$.

We call Π_a the composite map of $(F_p - [b \bmod L_q])^{2g(X_1(\ell))}$ and all $B_n(T_n)$ for all n primes such that $2 \leq n \leq \ell^2$. The image of $J_1(\ell)[\ell^\infty](\mathbb{F}_q)$ by Π_a contains $V_\ell^a = J_1(\ell)[\mathfrak{m}_a]$ and is killed by $\mathfrak{m}_a^{2w_q g(X_1(\ell))}$.

Given a non-zero element x in the image of $J_1(\ell)[\ell^\infty](\mathbb{F}_q)$ by Π_a, we can test whether it is killed by $\mathfrak{m}_a$ by applying to it all the generators ℓ and $T_n - \tau(n)$ for $n \leq \ell^2$. If we always obtain zero this shows that x is in V_ℓ^a. Otherwise we produce some non zero element in $\mathfrak{m}x$ and we replace x by this element and iterate. This process stops after at most $2g(X_1(\ell))w_q$ steps and produces a non-zero element x in V_ℓ^a. We proceed in a similar way with V_ℓ^b and find a generating set for V_ℓ.

References

[1] Jean-Marc Couveignes. Jacobiens, jacobiennes et stabilité numérique. *http://www.univ-tlse2.fr/grimm/couveignes*, 2004.

[2] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, 1997.

[3] Sebastiaan Edixhoven. On computing coefficients of modular forms. *Talk at MSRI*, http://www.math.leidenuniv.nl/∼edix/public_html_rennes/talks/msridec2000.html, 2000.

[4] Gerhard Frey and Michael Müller. Arithmetic of modular curves and applications. In *On Artin's conjecture for odd 2-dimensional representations*, number 1585 in Lecture Notes in Math. Springer, 1994.

[5] D. Gorenstein. An arithmetic theory of adjoint plane curves. *Trans. Amer. Math. Soc.*, 72:414–436, 1952.

[6] Yuri Manin. Parabolic points and zeta function of modular curves. *Math. USSR Izvestija*, 6(1):19–64, 1972.

[7] Loïc Merel. Universal fourier expansions of modular forms. In *On Artin's conjecture for odd 2-dimensional representations*, number 1585 in Lecture Notes in Math. Springer, 1994.

Computations in non-commutative Iwasawa theory of elliptic curves

Tim Dokchitser

(joint work with Vladimir Dokchitser)

Recently a "Main Conjecture of non-commutative Iwasawa theory" has been formulated by J. Coates, T. Fukaya, K. Kato, R. Sujatha and O. Venjakob [1]. Take a number field F, an elliptic curve E/F, and an extension F_∞/F whose Galois group Γ is a compact p-adic Lie group, not necessarily commutative. With some restrictions on F, Γ and E, the conjecture predicts a relation between the non-abelian Euler characteristic (defined by the authors) of twists $E \otimes \tau$ of E in F_∞/F, and special values of L-functions $L(E, \tau, s)|_{s=1}$. We want to provide some of the first numerical evidence in favour of their conjecture.

Namely, take $F = \mathbb{Q}$, $F_n = \mathbb{Q}(\mu_{p^n}, \sqrt[p^n]{m})$ and $F_\infty = \bigcup_n F_n$. Then F_∞/F is Galois and its Galois group is possibly the simplest non-commutative compact p-adic Lie group,

$$\Gamma = \mathrm{Gal}(F_\infty/F) \cong \left\{ \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_p) \right\}.$$

This Lie group is 2-dimensional, and its first layer $\mathrm{Gal}(F_1/\mathbb{Q})$ is of order $p(p-1)$; it is somewhat similar to a dihedral group of order $2p$. It is not hard to see that

$$\text{The regular representation of } \mathrm{Gal}(F_1/\mathbb{Q}) \quad \cong \quad \sigma \oplus \rho^{p-1}\,.$$

Here σ is the regular representation of $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}$ and ρ is a sum of $p-1$ one-dimensional characters; ρ is irreducible of dimension $p-1$. The representations ρ and σ arise naturally when one describes L-functions of E over the subfields of F_1, for instance

$$\begin{array}{lcl} L(E/F_1,s) & = & L(E,\sigma,s)L(E,\rho,s)^{p-1} \\ L(E/\mathbb{Q}(\mu_p),s) & = & L(E,\sigma,s) \\ L(E/\mathbb{Q}(\sqrt[p]{m},s) & = & L(E,s)L(E,\rho,s) \end{array}$$

The Main Conjecture of [1] predicts relations between the non-abelian Euler characteristics (algebraic side) with special values of twisted L-functions (analytic side),

$$\begin{array}{lcl} L(E,\sigma,1) & = & \chi_{\text{non-ab}}(E\otimes\sigma)\ \cdot\ (\text{finite computable correction term}), \\ L(E,\rho,1) & = & \chi_{\text{non-ab}}(E\otimes\rho)\ \cdot\ (\text{finite computable correction term}). \end{array}$$

See [1], 5.6-5.10 and the penultimate paragraph of the paper for the precise formulation. Using results from non-abelian and from cyclotomic Iwasawa theory, we can prove the following relation between these Euler characteristics:

Theorem. Assume that $E/\mathbb{Q}$ has good ordinary reduction at $p>3$, the cyclotomic $\mu-$invariant of $E/\mathbb{Q}(\mu_p)$ is zero, and that $E/\mathbb{Q}(\mu_p)$ has trivial p^∞-Selmer group. Then

$$\chi_{\text{non-ab}}(E\otimes\sigma)=1 \quad \Longleftrightarrow \quad \chi_{\text{non-ab}}(E\otimes\rho)=1.$$

In combination with the main conjecture, this gives explicit relations between the p-parts of the suitably modified values $L(E,\sigma,1)$ and $L(E,\rho,1)$. We test these predictions numerically for $p=3,5$ and 7 for various elliptic curves and find that the computations support the main conjecture.

Next, I discussed one specific example that comes out of the computations (joint with V. Dokchitser, J. Coates and R. Sujatha).

Let E be the elliptic curve $y^2+y=x^3-x^2$ (conductor 11) over $\mathbb{Q}$ and $p=3$. The curve has Mordell-Weil rank 0 and the question is for which m does E acquire rational points over the field $\mathbb{Q}(\sqrt[3]{m})$ or, more generally, over $\mathbb{Q}(\sqrt[3^n]{m})$.

Using results from cyclotomic Iwasawa theory, it is not hard to see that over the field $\mathbb{Q}(\mu_{3^n})$ the curve has rank 0 and trivial Ш[3], so the question is also equivalent to the same one for E over F_n (which is the Galois closure $\mathbb{Q}(\sqrt[3^n]{m},\mu_{3^n})$, as above).

The answer depends on whether m is divisible by 11 (the only prime of bad reduction) and by anomalous primes in Mazur's terminology. A prime number $q\neq 11$ is anomalous for $E/\mathbb{Q}$ if the reduction $\tilde{E}(\mathbb{F}_q)$ has a non-trivial 3-torsion point. For instance, this happens for $q=23,59,71$. Then one can show:

(I) If m is neither divisible by 11 nor by any anomalous primes (e.g. $m=2,3,5,6,7,...$), then over the field F_n the curve E has rank 0 and trivial Ш[3].

(II) If m is not divisible by 11 but divisible by an anomalous prime (e.g. $m=29,53,2\cdot 29,...$), then either the Mordell-Weil rank of $E/\mathbb{Q}(\sqrt[p]{m})$ is positive or Ш[3]

is non-trivial over this field. However, we do not have a criterion how to distinguish between these two cases for a given m, and it would be very interesting to have at least a heuristical prediction of what to expect.

(III) Perhaps the most interesting case is the following: if m is divisible by 11 but not by anomalous primes, then one can show that the Mordell-Weil rank of $E/\mathbb{Q}(\sqrt[3^n]{m})$ is $\leq n$. On the other hand, a root number computation shows that the order of vanishing of $L(E/\mathbb{Q}(\sqrt[3^n]{m}), s)$ at $s = 1$ is $\geq n$. Thus, Tate's generalisation of the Birch-Swinnerton-Dyer conjecture [3] predicts that both inequalities are equalities. This means that on every step from $\mathbb{Q}(\sqrt[3^n]{m})$ to $\mathbb{Q}(\sqrt[3^{n+1}]{m})$ the rank goes up by exactly 1, so E acquires exactly one new generator in the Mordell-Weil group (for every $n \geq 1$!). It would be very interesting to have some kind of algebraic construction of these points to explain this curious phenomenon.

References

[1] J. Coates, T. Fukaya, K. Kato, R. Sujatha, O. Venjakob, *The GL_2 main conjecture for elliptic curves without complex multiplication*, available on http://arXiv.org/abs/math.NT/0404297, to appear in Publ. Math. IHES.

[2] T. Dokchitser, V. Dokchitser, *Computations in non-commutative Iwasawa theory of elliptic curves*, preprint, soon to appear on arXiv.org

[3] J. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, 18e année, 1965/66, no. 306.

Computational verification of the Birch and Swinnerton-Dyer conjecture for individual elliptic curves

William A. Stein

(joint work with G. Grigorov and A. Jorza and S. Patrikis and C. Tarniţă-Pătraşcu)

The L-function $L(E, s)$ of an elliptic curve E over $\mathbb{Q}$ is a holomorphic function on $\mathbb{C}$ that encodes deep arithmetic information about E. This project is about a connection between the behavior of $L(E, s)$ at $s = 1$ and the arithmetic of E.

We use theorems and computation to attack the following conjecture for many specific elliptic curves of conductor up to 1000:

Conjecture 1 (Birch and Swinnerton-Dyer)**.** *The order of vanishing* $\operatorname{ord}_{s=1} L(E, s)$ *equals the rank* r *of* E*, the group* Ш(E) *is finite, and*

$$\frac{L^{(r)}(E, 1)}{r!} = \frac{\Omega_E \cdot \operatorname{Reg}_E \cdot \prod_p c_p \cdot \#Ш(E)}{(\#E(\mathbb{Q})_{\mathrm{tor}})^2}.$$

For more about Conjecture 1, see [Lan91, Wil00] and the papers they reference. Henceforth we call it the BSD conjecture.

Definition 2 (Analytic Ш)**.** If E has rank r, let

$$\#Ш(E)_{\mathrm{an}} = \frac{L^{(r)}(E, 1) \cdot (\#E(\mathbb{Q})_{\mathrm{tor}})^2}{r! \cdot \Omega_E \cdot \operatorname{Reg}_E \cdot \prod_p c_p}$$

denote the order of $Ш(E)$ predicted by Conjecture 1. We call this the *analytic order* of $Ш(E)$.

Conjecture 3 (BSD(E,p))**.** *Let (E,p) denote a pair consisting of an elliptic curve E over $\mathbb{Q}$ and a prime p. We also call the assertion that* $\operatorname{ord}_{s=1} L(E,s)$ *equals the rank r, that $Ш(E)[p^\infty]$ is finite, and*

$$\operatorname{ord}_p(\#Ш(E)[p^\infty]) = \operatorname{ord}_p(\#Ш(E)_{\mathrm{an}})$$

the BSD conjecture at *p, and denote it* BSD(E,p).

The BSD conjecture is invariant under isogeny.

Theorem 4 (Cassels)**.** *If E and F are $\mathbb{Q}$-isogeneous and p is a prime, then* BSD(E,p) *is true if and only if* BSD(F,p) *is true.*

Proof. See [Cas65, Mil86, Jor05]. □

One way to give evidence for the BSD conjecture is to compute $\#Ш(E)_{\mathrm{an}}$ and note that it is the square of an integer, in accord with the following theorem:

Theorem 5 (Cassels)**.** *If E is an elliptic curve over $\mathbb{Q}$ and p is a prime such that $Ш(E)[p^\infty]$ is finite, then $\#Ш(E)[p^\infty]$ is a perfect square.*

Proof. See [Cas62, PS99]. □

Below we use the notation of [Crea] to refer to specific elliptic curves over $\mathbb{Q}$.

Conjecture 6 (Birch and Swinnerton-Dyer ≤ 1000)**.** *For* all *optimal curves of conductor up to* 1000 *we have $Ш(E) = 0$, except for the following four rank* 0 *elliptic curves, where $Ш(E)$ has the indicated order:*

Curve	571A	681B	960D	960N
$\#Ш(E)_{\mathrm{an}}$	4	9	4	4

Theorem 7 (Cremona)**.** *Conjecture 1 is true for all elliptic curves of conductor up to* 1000 *if and only if Conjecture 6 is true.*

Proof. In the book [Cre97], Cremona computed $\#Ш(E)_{\mathrm{an}}$ for every curve of conductor up to 1000. By Theorem 4 it suffices to consider only the optimal ones, and the four listed are the only ones with nontrivial $\#Ш(E)_{\mathrm{an}}$. □

In view of Theorem 7, the main goal of this paper is to obtain results in support of Conjecture 6. Combining our results, we obtain the following theorem.

Theorem 8. *Suppose that E is a non-CM elliptic curve of rank ≤ 1, conductor ≤ 1000 and that p is a prime. If p is odd, assume further that the mod p representation $\overline{\rho}_{E,p}$ is irreducible and p does not divide any Tamagawa number of E. Then* BSD(E,p) *is true.*

For example, if E is the elliptic curve 37A, then according to [Cre97], all $\overline{\rho}_{E,p}$ are irreducible and the Tamagawa numbers of E are 1. Thus Theorem 8 asserts that the full BSD conjecture for E is true.

There are 18 optimal curves of conductor up to 1000 of rank 2 (and none of rank > 2). For these E of rank 2, nobody has proved that $Ш(E)$ is finite in even a single case. We exclude CM elliptic curves from most of our computations. The methods for dealing with the BSD conjecture for CM elliptic curves are different than for general curves, and will be the subject of another paper. Similar remarks apply to BSD(E, p) when $\overline{\rho}_{E,p}$ is reducible.

References

[Cas62] J. W. S. Cassels, *Arithmetic on curves of genus* 1. *III. The Tate-Šafarevič and Selmer groups*, Proc. London Math. Soc. (3) **12** (1962), 259–296. MR 29 #1212

[Cas65] J. W. S. Cassels, *Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer*, J. Reine Angew. Math. **217** (1965), 180–199. MR 31 #3420

[Crea] J. E. Cremona, *Elliptic curves of conductor* ≤ 25000, `http://www.maths.nott.ac.uk/personal/jec/ftp/data/`.

[Cre97] ———, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997, `http://www.maths.nott.ac.uk/personal/jec/book/`.

[Jor05] A. Jorza, *The Birch and Swinnerton-Dyer Conjecture for Abelian Varieties over Number Fields*, Harvard University Senior Thesis (2005).

[Lan91] S. Lang, *Number theory. III*, Springer-Verlag, Berlin, 1991, Diophantine geometry. MR 93a:11048

[Mil86] J. S. Milne, *Arithmetic duality theorems*, Academic Press Inc., Boston, Mass., 1986.

[PS99] B. Poonen and M. Stoll, *The Cassels-Tate pairing on polarized abelian varieties*, Ann. of Math. (2) **150** (1999), no. 3, 1109–1149. MR 2000m:11048

[Wil00] ———, *The Birch and Swinnerton-Dyer Conjecture*, `http://www.claymath.org/prize_problems/birchsd.htm`.

The Brauer-Siegel theorem

H.M. Stark

I want to return to the origins of the study of class-numbers of CM fields by studying zeta functions of fields K with the property that $\zeta_K(0)$ has two real zeros $\beta_2 < \beta_1 < 1$, both near to $s = 1$. In the applications, K is normal over $\mathbb{Q}$ and in fact the two principal applications come with K being (i) a biquadratic field containing two quadratic subfields with Siegel zeros and (ii) a normal extension of $\mathbb{Q}$ with a real double zero of $\zeta_K(s)$ within (for = example) $(\log\log D)^{-10}$ of $s = 1$. Here D is the absolute value of the discriminant of K.

Our principal tool is the exact formula relating zeros and primes. Recall that $\zeta_K(s)$ satisfies a functional equation

$$\xi_K(s) = \xi_K(1 - s)$$

where

$$\xi_K(s) = \left(\frac{D}{2^{2r_2}\pi^n}\right)^{s/2} \Gamma(s/2)^{r_1}\Gamma(s)^{r_2}\zeta_K(s)s(s-1)$$

is an entire function of order one with Hadamard product,

$$\xi_K(s) = e^{A+Bs} \prod_\rho \left(1 - \frac{s}{\rho}\right) e^{s/\rho} = e^{A+B's} \prod_\rho{}' \left(1 - \frac{s}{\rho}\right)$$

where A and B are constants (depending on K and ρ runs through the non-trivial zeros of $\zeta_K(s)$. The first product over ρ is absolutely convergent. If we group the ρ in some manner so that $\sum_\rho{}' 1/\rho$ converges (conditionally) then

$$B' = B + \sum{}' 1/\rho$$

and in the second product $\prod'_\rho$ groups the ρ in the same way.

Let $F_c(x)$ be an even real-valued function whose two-sided Laplace transform

$$\widehat{F_c}(w) = \int_{-\infty}^{\infty} F_c(x) e^{-wx}\, dx,$$

converges absolutely at least in the strip $|\operatorname{Re}(w)| \le 1/2$. We also desire that

$$F_c(x) \ge 0$$

for all x. The variable c is a positive real scaling factor. It follows that $\widehat{F_c}(w)$ is even. Our first example of a function is

$$F_c(x) = E_c(x) = \frac{c}{\sqrt{\pi}} \exp(c^2 x^2)$$

which gives

$$\widehat{E_c}(w) = \exp\left(\frac{w^2}{4c^2}\right).$$

We evaluate the integral on the vertical line $\operatorname{Re}(s) = 2$,

$$\frac{1}{2\pi i} \int_{(2)} \frac{\xi'_K}{\xi_K}(s) \widehat{E_c}(s - 1/2)\, ds,$$

in the usual two ways. One way moves the line of integration leftwards to the line $\operatorname{Re}(w) = -1$ and picks up the residues. Applying the functional equation brings us back to $\operatorname{Re}(w) = 2$ and in this manner, we get

$$\begin{aligned}\frac{1}{2\pi i} \int_{(2)} \frac{\xi'_K}{\xi_K}(s) \widehat{E_c}(s - 1/2)\, ds &= \frac{1}{2} \sum_\rho{}' \operatorname{res}_{s=\rho} \widehat{E_c}(s - 1/2) + B' = E_c(0) \\ &= \frac{1}{2} \sum_\rho{}' = \exp\left(\frac{(\rho - 1/2)^2}{4c^2}\right) + \frac{c}{\sqrt{\pi}} B'.\end{aligned}$$

Serious homework problem. The integrals are absolutely convergent and indeed, very rapidly so. So is the sum of the residues. But B' is not unique. Explain.

In [3], it was shown, without the use of an integration, that when $\sum'$ means that ρ and $1-\rho$ are grouped together, $B'=0$. We use this grouping. Evaluating the integral from the other side of the equation leads to the following:

$$\frac{1}{2}(\log D)E_c(0)+\exp\left(\frac{1}{16c^2}\right)=\frac{1}{2}\sum_{\rho}\exp\left(\frac{(\rho-1/2)^2}{4c^2}\right)+R$$

where R is a collection of the remaining terms all of which are positive real. The $\exp(1/(16c^2))$ term comes from the $s=0,1$ pair. On the right side, we single out the $\beta_1, 1-\beta_1$ pair and the $\beta_2, 1-\beta_2$ pair. For convenience, set $\beta_0=1$ and

$$a_j=\exp\left(\frac{(\beta_j-1/2)^2}{4c^2}\right)$$

for $j=0,1,2$. Our identity now reads

$$\frac{1}{2}(\log D)E_c(0)+a_0=a_1+a_2+Z+R$$

where Z is the sum over the remaining zeros. Any further real zeros and all zeros with $\mathrm{Re}(\rho)=1/2$ make positive real contributions to the right-hand side. We can transfer these contributions from Z to R, and in this way we get a fundamental inequality,

$$\frac{1}{2}(\log D)E_c(0)+a_0>a_1+a_2+\widetilde{Z} \tag{16}$$

where $\widetilde{Z}$ is a sum over those zeros ρ which are neither real, nor on the line $\mathrm{Re}(s)=1/2$. These zeros represent violations of the "Modified Generalized Riemann Hypothesis" (MGRH), if they exist.

We have

$$a_0>a_1>a_2$$

always, nevertheless, if we choose the scaling factor c to be small enough [certainly, we will need c so small that $a_2>1/2(\log D)E_c(0)$ and then smaller still], we can arrange in both our principal applications that

$$\frac{1}{2}(\log D)E_c(0)+a_0<a_1+a_2 \tag{17}$$

Thus the obstruction to an effective proof that class-numbers of CM fields go to ∞ as the field varies or to an ineffective improvement of Siegel's theorem lies in the possible existence of normal extensions of $\mathbb{Q}$ whose zeta functions violate MGRH. Further analysis [4], leads to many such zeros very near to $s=1$.

A possible attack on this difficulty comes from the analytic discriminant bound methods which orginated in very crude form in [3] with the realization that with $B'=0$, the expansion for $\xi_K'(s)/\xi_K(s)$ yields an estimate for $\log D$ which is better than the Minkowski bounds. The method was tremendously improved by Odlyzko who took account of the zeros of $\zeta_K(s)$, as well as the primes of K, and then by Serre who proved the current best known bounds under the assumption of GRH by introducing the Weil formulas into the analysis. A way was then found to take account of zeros violating MGRH in a positive way. The new wrinkle was to find

functions $F_c(x)$ such that for some $a \geq 1/2$, Re $= \widehat{F_c}(w) \geq 0$ for all w in the strip $|w| \leq a$. See Odlyzko [1] and Poitou [2]. The use of such a function would eliminate all the terms in $\widehat{Z}$ from consideration in our fundamental inequality (1), but the cost is to lower the size of a_0, a_1, a_2 to a point where it appears we can no longer arrange to get the contradiction in (2) for any c. The best I have managed so far for the classic Siegel zero problem is with a value of a just slightly less than $\beta_2 - 1/2$.

References

[1] A.M. Odlyzko, *Bounds for discriminants and related estimates for class numbers, regulators, and zeros of zeta functions: a survey of recent results*, Sem. Theor. Nombres Bordeaux (2), 2 (1990), no. 1, 119–141.

[2] Poitou, George, *Minorations de discriminants (d'après A.M. Odlyzko)*, Seminaire Bourbaki, vol. 1975/76, 28ème année, Exp. No. 479, 136–153, Lecture Notes in Math. 567 (1977).

[3] H.M. Stark, Some effective cases of the Brauer-Siegel theorem, Invent. Math. 23 (1974), 135–152.

[4] H.M. Stark, Class-numbers of CM fields and Siegel zeros, to be published.

Theta null points of canonical lifts

Robert Carls

Our research is inspired by results of J.-F. Mestre who proposed the following generalisation of Gauss' *arithmetic geometric mean* (AGM)

$$a_u^{(n+1)} = \frac{1}{2^g} \sum_{v \in (\mathbb{Z}/2\mathbb{Z})^g} \sqrt{a_{v+u}^{(n)} a_v^{(n)}}, \quad u \in (\mathbb{Z}/2\mathbb{Z})^g.$$

Mestre introduced a point counting algorithm for ordinary hyperelliptic curves over a finite field of characteristic 2 based on the generalised AGM formulas. An optimised version of his algorithm is described in [4]. One of our aims is to broaden the understanding of Mestre's algorithm in order to generalise it to arbitrary residue field characteristic. The generalised AGM formulas can be deduced from a transformation formula for complex analytic theta functions (see [3, Ch. IV, Th. 2]) which describes their behaviour under the doubling of the period matrix. In order to use Mestre's formulas over the 2-adic numbers one has to apply the Lefschetz principle.

Our method yields equations satisfied by the canonical theta null point of a canonical lift over a 2-adic ring. The canonical theta null point is defined in terms of the canonical theta structure. The proof is done by purely algebraic means involving an algebraic version of the above mentioned theta transformation formula which is proven in [5]. In contrast to Mestre's formulas ours are integral. This allows one to keep track of the reduction modulo 2.

According to the theory of complex multiplication the invariants of a simple abelian variety with CM generate a certain class field of the reflex field of the endomorphism algebra. In Section 2 we compute Hilbert class fields of certain

imaginary quadratic fields using canonical theta null points. A 2-adic CM method for abelian surfaces using Igusa invariants instead of canonical theta null points is described in [2].

The results of Section 1 were proven with the help of Bas Edixhoven. I owe thanks to B. Moonen, F. Oort and M. Raynaud who contributed to the proof of the existence of the canonical theta structure.

1. The main results

Let R be a complete noetherian local ring with perfect residue field k of characteristic $p > 0$. Assume that R admits an automorphism σ lifting the p-th power Frobenius automorphism of k. Let A be an abelian scheme over R of relative dimension g having ordinary reduction and let $\mathcal{L}$ be an ample symmetric line bundle of degree 1 on A. Fix $j \geq 0$. Suppose we are given an isomorphism

$$(\mathbb{Z}/p^j\mathbb{Z})^g_R \xrightarrow{\sim} A[p^j]^{\mathrm{et}} \tag{18}$$

where $A[p^j]^{\mathrm{et}}$ denotes the maximal étale quotient of $A[p^j]$.

Theorem: *Assume that A is a canonical lift. There exists a canonical theta structure of type $(\mathbb{Z}/p^j\mathbb{Z})^g_R$ for the pair*

$$\left(A, \mathcal{L}^{\otimes p^j}\right)$$

depending on the isomorphism (18).

For a proof of the above theorem see [1]. Now let $p = 2$. In the following we assume that A is a canonical lift. Let $[x_u]_{u\in(\mathbb{Z}/2^j\mathbb{Z})^g_R}$ denote the theta null point of A with respect to the canonical theta structure for $(A, \mathcal{L}^{\otimes 2^j})$.

Theorem: *There exists a unique $\omega \in R^*$ such that for all $u \in (\mathbb{Z}/2^j\mathbb{Z})^g_R$ we have*

$$x_u^2 = \omega \sum_{v\in(\mathbb{Z}/2\mathbb{Z})^g_R} \sigma(x_{v+u})\sigma(x_v).$$

A proof of the above theorem is going to be published. Taking $j = 1$ and setting

$$a_u^{(n)} = \frac{1}{2^g\omega} x_u^2 \quad \text{and} \quad a_u^{(n+1)} = \sigma(x_u)^2$$

one obtains Mestre's generalised AGM formulas. We remark that in the case that $k = \mathbb{F}_q$ is a finite field the constant ω of the above theorem is expected to be related to the product of the invertible eigenvalues of the q-Frobenius endomorphism of $A_{\mathbb{F}_q}$.

2. Example

Let $\mathbb{Z}_q$ denote the Witt vectors with values in a finite field $\mathbb{F}_q$ of characteristic 2. Let E be an elliptic curve over $\mathbb{Z}_q$ having ordinary reduction. Let $\sigma \in \mathrm{End}(\mathbb{Z}_q)$ denote a lift of the 2nd-power Frobenius automorphism of $\mathbb{F}_q$. Assume that E is

a canonical lift. Let $\mathcal{L} = \mathcal{O}(0_E)$ where 0_E denotes the zero section of E. There exists a unique isomorphism

$$(\mathbb{Z}/2\mathbb{Z})_{\mathbb{Z}_q} \xrightarrow{\sim} E[2]^{\mathrm{et}}. \tag{19}$$

Hence there exists a canonical theta structure of type $(\mathbb{Z}/2\mathbb{Z})_{\mathbb{Z}_q}$ for the pair $(E, \mathcal{L}^{\otimes 2})$. By our second theorem there exists an $\omega \in \mathbb{Z}_q^*$ such that the coordinates of the theta null point $[x_0, x_1]$ satisfy the equations

$$x_0^2 = \omega\big(\sigma(x_0)^2 + \sigma(x_1)^2\big) \quad \text{and} \quad x_1^2 = 2\omega\sigma(x_0)\sigma(x_1).$$

We set $\mu = \frac{x_1}{x_0}$. Rewriting the above equations in terms of μ we get

$$\mu^2\big(\sigma(\mu)^2 + 1\big) = 2\sigma(\mu). \tag{20}$$

Suppose $[\mathbb{F}_q : \mathbb{F}_2] = 2$. Equation (20) implies that

$$(\mu^2 + \mu + 2) \cdot (\mu^4 + 4\mu^3 + 5\mu^2 + 2\mu + 4) = 0.$$

Let $L = \mathrm{End}^0(E) = \mathrm{End}(E) \otimes \mathbb{Q}$. If the j-invariant of $E_{\mathbb{F}_4}$ equals 1 then $L = \mathbb{Q}(\sqrt{-7})$. Note that L has class number 1 and the polynomial $x^2 + x + 2$ is reducible over L. If $E_{\mathbb{F}_4}$ cannot be defined over $\mathbb{F}_2$ then we have $L = \mathbb{Q}(\sqrt{-15})$ which has class number 2. The polynomial $x^4 + 4x^3 + 5x^2 + 2x + 4$ generates the Hilbert class field of $\mathbb{Q}(\sqrt{-15})$.

References

[1] R. Carls, *Canonical coordinates on the canonical lift*, preprint, available at `http://arxiv.org/abs/math.NT/0508007`.

[2] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, A. Weng, *The p-adic CM-method for genus* 2, preprint, available at `http://arxiv.org/abs/math.NT/0503148`.

[3] J.-I. Igusa, *Theta functions*, Grundl. d. math. Wiss. **194**, Springer-Verlag (1972).

[4] R. Lercier, D. Lubicz, *A quasi-quadratic time algorithm for hyperelliptic curve point counting*, preprint, available at `http://www.math.u-bordeaux.fr/~lubicz`.

[5] D. Mumford, *On the equations defining abelian varieties I*, Inventiones Math. **1** (1966), 287–354.

Mersenne primes and class field theory

Bas Jansen

The Lucas-Lehmer test is an algorithm to check whether a number of the form $M = 2^p - 1$, with p an odd positive integer, is prime. The algorithm produces a sequence of $p - 1$ numbers modulo M, starting with the starting value 4 and each time squaring the previous number and subtracting 2. Then the last number is zero modulo M if and only if M is prime. Lehmer observed that if the last number is zero then the penultimate number can be either PLUS or MINUS $2^{(p+1)/2}$ modulo M. Gebre-Egziabher showed that if you start your sequence with 2/3 instead of 4, then the test also works, and the sign will be plus if and only if p is 1 modulo 4 ($p > 5$). In my talk I generalize this result.

The Lucas-Lehmer test can be formulated in a little bit more general way.

Let $p \in \mathbb{Z}_{>1}$ odd,
$M = M_p = 2^p - 1$,
$s \in \mathbb{Z}/M\mathbb{Z}$ and
$s_1 = s$, $s_{i+1} = s_i^2 - 2$ for $i \in \{1, \ldots, p-1\}$.

Then we have the following theorem.

Theorem:

$$s_{p-1} = 0 \Leftrightarrow \left\{ \begin{array}{c} M \text{ is prime} \\ \& \\ \left(s - \frac{2}{M}\right) = \left(-s - \frac{2}{M}\right) = 1. \end{array} \right.$$

Lehmer's observation.

Lehmer observed that we can obtain a sign from the Lucas-Lehmer test. Namely first note that

$s_{p-1} = s_{p-2}^2 - 2 = s_{p-2}^2 - 2^{p+1} =$

$(s_{p-2} - 2^{(p+1)/2})(s_{p-2} + 2^{(p+1)/2})$.

Hence then we see that

$$s_{p-1} = 0 \Rightarrow s_{p-2} = \left\{ \begin{array}{c} \textbf{plus} \\ \text{or} \\ \textbf{minus} \end{array} \right\} 2^{(p+1)/2}.$$

Starting values in big field.

The starting values $4, 10$ and $\frac{2}{3}$ are all elements of $\mathbb{Q}$. We can create starting values in a much bigger field.

For every

$$s \in \bigcup_{n>0} \mathbb{Q}(\sqrt[n]{2})$$

there exists integer $k = k_s$ *such that*

$$(s \ mod M_p) \text{ has a natural meaning}$$

whenever

$$gcd(p, k) = 1.$$

Namely, write

$$s = (2^e d)^{-1} \cdot \sum_{i=0}^{n-1} c_i \sqrt[n]{2}^i$$

($e, d, c_i \in \mathbb{Z}$ with $e \geq 0$ and d odd).

Pick $k = n \cdot \text{order}(2 \bmod d)$.

Let $an \equiv 1 \bmod M_p$, then $(2^a)^n \equiv 2 \bmod M_p$. We define

$$(s \bmod M_p) := (2^e \cdot d \bmod M_p)^{-1} \cdot \sum_{i=0}^{n-1} (c_i \, 2^{a \cdot i} \bmod M_p).$$

Definition of $\epsilon_s(p)$.

For $s \in \bigcup_{n>0} \mathbb{Q}(\sqrt[n]{2})$ we define

$$P_s = \{p : \gcd(p, k_s) = 1, s_{p-1} = 0 \ \text{ for } \ s_1 = (s \bmod M)\}.$$

Define

$$\epsilon_s : P_s \to \{+1, -1\}$$

by

$$s_{p-2} = \epsilon_s(p) \cdot 2^{(p+1)/2}.$$

Example.

$P_4 = P_{10} = P_{2/3} = \{p > 2 : 2^p - 1 \text{ prime}\} = \{3, 5, 7, 13, 17, 19, \ldots\}$.

$\epsilon_4(5) = +1$ because $s_1 = (4 \bmod 31)$, $s_2 = 14$, $s_3 = 196 - 2 = 8 = +2^{(5+1)/2}$.

A generalisation of G-E result.

Let $s \in K = \bigcup_{n>0} \mathbb{Q}(\sqrt[n]{2})$,
$m = [\mathbb{Q}(s, \sqrt{2}, \sqrt{4 - s^2}) : \mathbb{Q}]$,
$d \in \mathbb{Z}_{>0}$ such that $d \cdot s \in \mathcal{O}_K$,
$c =$ odd part of radical(d) and
$N = \text{order}(\sqrt[m]{2} \bmod c)$.

Then we have the following theorem.

Main theorem: If

$$4 - s^2 \in (K^*)^2,$$

then $\forall p, q \in \mathbb{Z}_{>4m} \cap P_s$ we have

$$\epsilon_s(p) = \epsilon_s(q) \;\Leftarrow\; p \equiv q \bmod N.$$

Example $s = \frac{2}{3}$.

We have $4 - (\frac{2}{3})^2 = \frac{32}{9} = (\frac{4\sqrt{2}}{3})^2$,
$m = 2$,
$d = 3$,
$c =$ odd part of radical$(3) = 3$ and
$N =$ order$(\sqrt{2} \bmod 3) = 4$.

¿From the fact that $N = 4$ G-E result follows.

Now we give two corollaries which follow easily from the main theorem.

Corollary: Let $s = \frac{626}{363}$. Let $p \in P_s = \{p > 2 : 2^p - 1 \text{ prime}\}$. Then

$$\epsilon_s(p) = 1 \Leftrightarrow p \equiv 1, 7, 9, 13 \bmod 20.$$

Corollary: Let $s = -\frac{14}{75} + \frac{32}{25}\sqrt{2}$. Let $p \in P_s = \{p > 2 : 2^p - 1 \text{ prime}\}$. Then

$$\epsilon_s(p) = -1 \Leftrightarrow p \neq 3, 5.$$

Generating Subfields

Mark van Hoeij
(joint work with Jürgen Klüners)

Let K/k be a finite separable field extension of degree n. We describe an algorithm that computes all subfields of K that contain k. We assume that a primitive element α of K/k is given as well as its minimal polynomial $f \in k[x]$. The main result is that all subfields can be presented as intersections of a small number of subfields, and that those subfields can be calculated efficiently. The concepts of principal and generating subfields are introduced.

1. The main theorem

Let $\tilde{K}$ be a field containing K and $f = f_1 \cdots f_r$ be the factorization of f over $\tilde{K}$ where the $f_i \in \tilde{K}[x]$ are irreducible and monic, and $f_1 = x - \alpha$. We define the fields $\tilde{K}_i := \tilde{K}[x]/(f_i)$ for $1 \leq i \leq r$. We denote elements of K as $g(\alpha)$ where g is a polynomial of degree $< n$, and define for $1 \leq i \leq r$ the embedding

$$\phi_i : K \to \tilde{K}_i, \qquad g(\alpha) \mapsto g(x) \bmod f_i.$$

Note that ϕ_1 is just the identity map $id : K \to \tilde{K}$. We define for $1 \leq i \leq r$:

$$L_i := \mathrm{Ker}(\phi_i - id) = \{g(\alpha) \in K \mid g(x) \equiv g(\alpha) \bmod f_i\}.$$

The L_i are closed under multiplication, and hence fields, since $\phi_i(ab) = \phi_i(a)\phi_i(b) = ab$ for all $a, b \in L_i$.

Theorem 1. *If L is a subfield of K/k then L is the intersection of L_i, $i \in I$ for some $I \subseteq \{1, \ldots, r\}$.*

Proof. Let f_L be the minimal polynomial of α over L. Then f_L divides f since $k \subseteq L$, and $f_L = \prod_{i \in I} f_i$ for some $I \subseteq \{1, \ldots, r\}$ because $L \subseteq \tilde{K}$. We will prove

$$L = \{g(\alpha) \in K \mid g(x) \equiv g(\alpha) \bmod f_L\} = \bigcap_{i \in I} L_i.$$

If $g(\alpha) \in L$ then $h(x) := g(x) - g(\alpha) \in L[x]$ is divisible by $x - \alpha$ in $K[x]$. The set of polynomials in $L[x]$ divisible by $x - \alpha$ is (f_L) by definition of f_L. Then $h(x) \equiv 0 \bmod f_L$ and hence $g(x) \equiv g(\alpha) \bmod f_L$. Conversely, $g(x) \bmod f_L$ is in $L[x]$ (mod f_L) because division by f_L can only introduce coefficients in L. So if $g(x) \equiv g(\alpha) \bmod f_L$ then $g(\alpha) \in K \cap L[x] = L$.

By separability and the Chinese remainder theorem, one has $g(x) \equiv g(\alpha) \bmod f_L$ if and only if $g(x) \equiv g(\alpha) \bmod f_i$ (i.e. $g(\alpha) \in L_i$) for every $i \in I$. □

We can choose for $\tilde{K}$ any field that contains K (the set $S := \{L_1, \ldots, L_r\}$ is independent of this choice). The most convenient choice is to take $\tilde{K} = K$, but in some situations it might be better to let $\tilde{K}$ be some completion of K (this would save time on the factorization of f over $\tilde{K}$, but it complicates computing the Ker in the definition of L_i since this would then have to be done with LLL techniques instead of linear algebra over k. So if one has very efficient factoring code [3] then taking $\tilde{K} = K$ might still be the best choice).

Definition 2. We call the fields $L_1, \ldots, L_r$ the *principal subfields* of K/k. A set S of subfields of K/k is called a *generating set* of K/k if every subfield of K/k can be written as $\bigcap T$ for some $T \subseteq S$. Here $\bigcap T$ denotes the intersection of all $L \in T$, and $\bigcap \emptyset$ refers to K. A subfield L of K/k is called a *generating subfield* if it satisfies the following equivalent conditions

(1) The intersection of all fields L' with $L \subsetneq L' \subseteq K$ is not equal to L.
(2) There is precisely one field $L \subsetneq \tilde{L} \subseteq K$ for which there is no field between L and $\tilde{L}$ (and not equal to L or $\tilde{L}$).

The field $\tilde{L}$ in condition (2) is called *the field right above* L. It is clear that $\tilde{L}$ is the intersection in condition (1), so the two conditions are equivalent.

The field K is a principal subfield but not a generating subfield. A maximal subfield of K/k is a generating subfield as well. Theorem 1 says that the principal subfields form a generating set. By condition (1), a generating subfield can not be obtained by intersecting larger subfields, and must therefore be an element of every generating set. In particular, a generating subfield is also a principal subfield.

If S is a generating set, and we remove every $L \in S$ for which $\bigcap\{L' \in S | L \subsetneq L'\}$ equals L, then what remains is a generating set that contains only generating subfields. It follows that

Proposition 1. *S is a generating set if and only if every generating subfield is in S.*

Suppose that K/k is a finite separable field extension and that one has polynomial time algorithms for factoring over K and for linear algebra over k (for example when $k = \mathbb{Q}$). Then applying Theorem 1 with $\tilde{K} = K$ yields a generating set S with $r \leq n$ elements in polynomial time. We may want to minimize r by removing all elements of S that are not generating subfields. Then $r \leq n - 1$. In principle there are 2^r subsets of S to be considered, which may be substantially more than the number of subfields. So we design the algorithm in Section 2 in such a way that it finds each subfield only once. This way, when S is given, the cost of computing all subfields is proportional to the number of subfields.

2. Intersections

In this section we describe an algorithm to compute all subfields of K/k by intersecting elements of a generating set $S = \{L_1, \ldots, L_r\}$. The complexity is proportional to the number of subfields of K/k. Unfortunately there exist families of examples where this number is more than polynomial in n.

To each subfield L of K/k we associate a tuple $e = (e_1, \ldots, e_r) \in \{0, 1\}^r$, where $e_i = 1$ if and only if $L \subseteq L_i$.

Algorithm AllSubfields
Input: A generating set $S = \{L_1, \ldots, L_r\}$ for K/k.
Output: All subfields of K/k.

(1) Let $e := (e_1, \ldots, e_r)$ where $e_1 = 1$ if $L_i = K$ and $e_i = 0$ otherwise.
(2) ListSubfields := $[K]$.
(3) Call NextSubfields$(S, K, e, 0)$.
(4) Return ListSubfields.

The following function returns no output but appends elements to ListSubfields, which is used as a global variable. The input consists of a generating set, a subfield L, its associated tuple $e = (e_1, \ldots, e_r)$, and the smallest integer $0 \leq s \leq r$ for which $L = \bigcap\{L_i \mid 1 \leq i \leq s,\ e_i = 1\}$.

Algorithm NextSubfields
Input: S, L, e, s.

For all i with $e_i = 0$ and $s < i \leq r$ **do**

(1) Let $M := L \cap L_i$.
(2) Let $\tilde{e}$ be the associated tuple of M.
(3) **If** $\tilde{e}_j \leq e_j$ for all $1 \leq j < i$ **then** append M to ListSubfields and call NextSubfields$(S, M, \tilde{e}, i)$.

Subfields that are isomorphic but not identical are considered to be different in this text. Let m be the number of subfields of K/k. Since S is a generating set,

all subfields occur as intersections of $L_1, \ldots, L_r$. The condition in Step (3) in Algorithm NextSubfields holds if and only if M has not already been computed before. So each subfield will be placed in ListSubfields precisely once, and the total number of calls to Algorithm NextSubfields equals m. For each call, the number of i's with $e_i = 0$ and $s < i \leq r$ is bounded by r, so the total number of intersections calculated in Step (1) is $\leq rm$. Step (2) involves testing which L_j contain M. Bounding the number of j's by r, the number of subset tests is $\leq r^2 m$.

Theorem 3. *Given a generating set for K/k with r elements, Algorithm AllSubfields returns all subfields by computing at most rm intersections and at most $r^2 m$ subset tests, where m is the number of subfields of K/k.*

Thus the cost of computing all subfields is bounded by a polynomial times the number of subfields.

References

[1] Preliminary implementation: `http://www.math.fsu.edu/~hoeij/papers/subfields`
[2] J. Klüners, M. Pohst, *On Computing Subfields*, J. Symb. Comput., **24** (1997), 385–397.
[3] K. Belabas, *A relative van Hoeij algorithm over number fields*, J. Symb. Comput., **37** (2004), 641–668.

Reporter: John Voight

Participants

Prof. Dr. Karim Belabas

Mathematiques
Universite Paris Sud (Paris XI)
Centre d'Orsay, Batiment 425
F-91405 Orsay Cedex

Prof. Dr. Michael Bennett

Dept. of Mathematics
University of British Columbia
1984 Mathematics Road
Vancouver, BC V6T 1Z2
CANADA

Prof. Dr. Daniel J. Bernstein

Department of Mathematics
University of Illinois at Chicago
M/C 249, 322 SEO
851 S. Morgan Street
Chicago IL-60607-7045
USA

Prof. Dr. Manjul Bhargava

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

Dr. Wieb Bosma

Mathematisch Instituut
Radboud Universiteit Nijmegen
Toernooiveld 1
NL-6525 Nijmegen

Johan Bosman

Mathematisch Instituut
Universiteit Leiden
Postbus 9512
NL-2300 RA Leiden

Dr. Martin Bright

Dept. of Pure Mathematics
The University of Liverpool
P. O. Box 147
GB-Liverpool L69 3BX

Drs. Reinier Bröker

Mathematisch Instituut
Universiteit Leiden
Postbus 9512
NL-2300 RA Leiden

Prof. Dr. Dongho Byeon

School of Mathematical Sciences
Seoul National University
Seoul 151-747
Korea

Prof. Dr. Frank Calegari

Dept. of Mathematics
Harvard University
Science Center
One Oxford Street
Cambridge MA 02138-2901
USA

Dr. Robert Carls

Mathematisch Instituut
Universiteit Leiden
Postbus 9512
NL-2300 RA Leiden

Prof. Dr. Henri Cohen

Laboratoire A2X
UFR de Math. et Informatique
Universite Bordeaux I
351, cours de la Liberation
F-33405 Talence Cedex

Prof. Dr. Jean-Marc Couveignes

GRIMM, UFR S.E.S.
Universite Toulouse II
5, Allee Antonio Machado
F-31058 Toulouse Cedex 9

Prof. Dr. John E. Cremona

School of Mathematical Sciences
University of Nottingham
University Park
GB-Nottingham NG7 2RD

Dr. Robin de Jong

Department of Mathematics and
Computer Science
University of Leiden
Postbus 9512
NL-2300 RA Leiden

Prof. Dr. Christophe Delaunay

Institut Camille Jordan
Universite Claude Bernard Lyon 1
43 blvd. du 11 novembre 1918
F-69622 Villeurbanne Cedex

Prof. Dr. Tim Dokchitser

School of Mathematics
University of Edinburgh
James Clerk Maxwell Bldg.
King's Building, Mayfield Road
GB-Edinburgh, EH9 3JZ

Prof. Dr. Bas Edixhoven

Mathematisch Instituut
Universiteit Leiden
Postbus 9512
NL-2300 RA Leiden

Prof. Dr. Eugene Victor Flynn

Dept. of Pure Mathematics
The University of Liverpool
P. O. Box 147
GB-Liverpool L69 3BX

Prof. Dr. Gerhard Frey

FB 6 - Mathematik
Universität Duisburg-Essen
45117 Essen

Dr. Herbert Gangl

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn

Prof. Dr. Paul E. Gunnells

Dept. of Mathematics & Statistics
University of Massachusetts
710 North Pleasant Street
Amherst, MA 01003-9305
USA

Prof. Dr. Mark van Hoeij

Department of Mathematics
Florida State University
Tallahassee, FL 32306-4510
USA

Bas Jansen

Mathematisch Instituut
Universiteit Leiden
Postbus 9512
NL-2300 RA Leiden

Neeraj Kayal

Deparment of Computer Science and Engineering
IIT
Kanpur 208016
INDIA

Prof. Dr. Kiran S. Kedlaya

Department of Mathematics
MIT
77 Massachusetts Avenue
Cambridge, MA 02139-4307
USA

Dr. Thorsten Kleinjung

Mathematisches Institut
Universität Bonn
Beringstr. 1
53115 Bonn

Dr. Jürgen Klüners

FB 17 - Mathematik/Informatik -
Universität Kassel
Heinrich-Plett-Str. 40
34132 Kassel

Dr. David R. Kohel

School of Mathematics & Statistics
University of Sydney
Sydney NSW 2006
AUSTRALIA

Dr. Alan G. B. Lauder

Mathematical Institute
Oxford University
24-29, St. Giles
GB-Oxford OX1 3LB

Prof. Dr. Hendrik W. Lenstra

Mathematisch Instituut
Universiteit Leiden
Postbus 9512
NL-2300 RA Leiden

Dr. Ronald van Luijk

Department of Mathematics
University of California
Berkeley, CA 94720-3840
USA

Prof. Dr. Jean-Francois Mestre

U. F. R. de Mathematiques
Case 7012
Universite de Paris VII
2, Place Jussieu
F-75251 Paris Cedex 05

Prof. Dr. Michael E. Pohst

Fakultät II -Institut f. Mathematik
Technische Universität Berlin
Sekr. MA 8-1
Straße des 17. Juni 136
10623 Berlin

Prof. Dr. Bjorn Poonen

Department of Mathematics
University of California
Berkeley, CA 94720-3840
USA

Dr. Nicole Raulf

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn

Prof. Dr. Xavier-Francois Roblot

Institut Camille Jordan
Universite Claude Bernard Lyon 1
43 blvd. du 11 novembre 1918
F-69622 Villeurbanne Cedex

Prof. Dr. Fernando Rodriguez Villegas

Department of Mathematics
University of Texas at Austin
1 University Station C1200
Austin, TX 78712-1082
USA

Prof. Dr. Rene Schoof

Dipartimento di Matematica
Universita degli Studi di Roma II
Tor Vergata
Via della Ricerca Scientifica
I-00133 Roma

Dr. Samir Siksek

Department of Mathematics
University of Warwick
GB-Coventry CV4 7AL

Dr. Bart de Smit

Mathematisch Instituut
Universiteit Leiden
Postbus 9512
NL-2300 RA Leiden

Prof. Dr. Harold M. Stark

Dept. of Mathematics
University of California, San Diego
9500 Gilman Drive
La Jolla, CA 92093-0112
USA

Prof. Dr. William A. Stein

Department of Mathematics
University of California,San Diego
9500 Gilman Drive
La Jolla, CA 92093-0112
USA

Prof. Dr. Peter Stevenhagen

Mathematisch Instituut
Universiteit Leiden
Postbus 9512
NL-2300 RA Leiden

Prof. Dr. Michael Stoll

School of Engineering and Science
International University Bremen
Postfach 750561
28725 Bremen

Dr. Jaap Top

Mathematisch Instituut
Rijksuniversiteit Groningen
Postbus 800
NL-9700 AV Groningen

Dr. John Voight

Department of Mathematics
University of California
Berkeley, CA 94720-3840
USA

Ulrich Vollmer

Technische Universität Darmstadt
Fachbereich Informatik
Alexanderstr. 10
64283 Darmstadt

Mark J. Watkins

School of Mathematics
Bristol University
University Walk
GB-Bristol BS8 1TW

Gabor Wiese

Mathematisch Instituut
Universiteit Leiden
Postbus 9512
NL-2300 RA Leiden

Prof. Dr. Don B. Zagier

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn