Mathematisches Forschungsinstitut Oberwolfach

Report No. 33/2009/

DOI: 10.4171/OWR//33/2009

Explicit Methods in Number Theory

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

July 12th – July 18th, 2009

Abstract. These notes contain extended abstracts on the topic of explicit methods in number theory. The range of topics includes asymptotics for field extensions and class numbers, random matrices and L-functions, rational points on curves and higher-dimensional varieties, and aspects of lattice basis reduction.

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

Introduction by the Organisers

The workshop *Explicit Methods in Number Theory* was organised by Karim Belabas (Talence), Hendrik W. Lenstra (Leiden), and Don B. Zagier (Bonn), and it took place July 12–18, 2009. Five previous workshops on the topic had been held in 1999, 2001, 2003, 2005 and 2007. The goal of the meeting was to present new methods and results on concrete aspects of number theory. In several cases, this included algorithmic and experimental work, but the emphasis was on the implications for number theory. There were two 'mini-series' highlighting important recent developments: one of three hours, by Henri Darmon, on cycles on modular varieties and on rational points on elliptic curves via a generalisation of Heegner points; and one of three hours by Bjorn Poonen, on rational points on higher-dimensional varieties and on obstructions to weak approximation and to the Hasse principle. Some of the other themes were:

- Automorphic forms
- Rational and integral points on curves and higher-dimensional varieties
- Class numbers of number fields and of other rings
- Solving specific diophantine equations

- Computations of Tate-Shafarevich groups and of Selmer groups.

As always in Oberwolfach, the atmosphere was lively and active, providing an ideal environment for the exchange of ideas and productive discussions. The meeting was well-attended, with 50 participants from a variety of backgrounds, including a large number of younger researchers. There were 35 talks of various lengths, and ample time was allotted to informal collaboration.

Workshop: Explicit Methods in Number Theory

Table of Contents

Abstracts

Perfect Powers Expressible as Sums of Two Cubes

Samir Siksek
(joint work with Imin Chen)

Let p, q, $r \in \mathbb{Z}_{\geq 2}$. The equation

$$a^p + b^q = c^r \tag{1}$$

is known as the Fermat–Catalan equation with signature (p, q, r). As in Fermat's Last Theorem, one is interested in integer solutions a, b, c. Such a solution is called *non-trivial* if $abc \neq 0$, and *primitive* if a, b, c are coprime. Let $\chi = p^{-1} + q^{-1} + r^{-1}$. The parameterization of non-trivial primitive solutions for (p, q, r) with $\chi \geq 1$ has now been completed ([4], [11]). The Generalized Fermat Conjecture [3] is concerned with the case $\chi < 1$. It states that the only non-trivial primitive solutions to (1) with $\chi < 1$ are

$$1 + 2^3 = 3^2, \quad 2^5 + 7^2 = 3^4, \quad 7^3 + 13^2 = 2^9, \quad 2^7 + 17^3 = 71^2,$$
$$3^5 + 11^4 = 122^2, \quad 17^7 + 76271^3 = 21063928^2, \quad 1414^3 + 2213459^2 = 65^7,$$
$$9262^3 + 15312283^2 = 113^7, \; 43^8 + 96222^3 = 30042907^2, \; 33^8 + 1549034^2 = 15613^3.$$

The Generalized Fermat Conjecture has been established for many signatures (p, q, r), including for several infinite families of signatures: Fermat's Last Theorem (p, p, p) by Wiles and Taylor [17], [16]; $(p, p, 2)$ and $(p, p, 3)$ by Darmon and Merel [10]; $(2, 4, p)$ by Ellenberg [12] and Bennett, Ellenberg and Ng [2]; $(2p, 2p, 5)$ by Bennett [1]. For an exhaustive survey see [4]. All these infinite cases have been established through the same steps as Wiles' proof of Fermat's Last Theorem, or some strengthening of this approach. We call this approach via the modularity of Galois representations of elliptic curves and Ribet's Level-Lowering Theorem, the modular approach.

In this talk we are concerned with the following special case of the Generalized Fermat Conjecture.

Conjecture. *Let $n \geq 3$. The equation*

$$a^3 + b^3 = c^n \tag{2}$$

does not have any non-trivial primitive solutions.

We attack the conjecture (with only partial success) using a combination of the modular approach, together with an obstruction to solutions that is of the Brauer–Manin type.

Equation (2) has been studied by Kraus [13], Bruin [6] and Dahmen [8]. Indeed, Kraus studies this equation using Frey curves and Galois representations and deduces a practical criterion for proving the conjecture for a particular prime exponent $n \geq 17$. Kraus also used a computer program to check his criterion for prime exponents $17 \leq n < 10^4$. Bruin [6] proved the conjecture for $n = 4$, 5, using

descent and Chabauty. Dahmen [8, Section 3.3.2] strengthens Kraus' argument to prove the conjecture for $n = 5, 7, 11, 13$. Of course, for $n = 3$, the result is classical (a special case of Fermat's Last Theorem). Thus combined, the results of Kraus, Bruin and Dahmen show that equation (2) does not have non-trivial primitive solutions for $3 \leq n \leq 10^4$.

In this talk we give a partial explanation of the proof of the following theorem.

Theorem 1. *(Chen–Siksek) Let $n \geq 3$. Suppose n is divisible by some positive integer d satisfying* **any** *of the following congruences,*

(I) $d \equiv 2, 3 \pmod 5$,
(II) $d \equiv 17, 61 \pmod{78}$,
(III) $d \equiv 51, 103, 105 \pmod{106}$,
(IV) $d \equiv 43, 49, 61, 79, 97, 151, 157, 169, 187, 205, 259, 265, 277, 295, 313, 367, 373, 385, 403, 421, 475, 481, 493, 511, 529, 583, 589, 601, 619, 637, 691, 697, 709, 727, 745, 799, 805, 817, 835, 853, 907, 913, 925, 943, 961, 1015, 1021, 1033, 1051, 1069, 1123, 1129, 1141, 1159, 1177, 1231, 1237, 1249, 1267, 1285 \pmod{1296}$.

Then equation (2) *has no non-trivial primitive solutions.*

It follows that the set of *prime* exponents n that satisfy the conditions of the theorem has Dirichlet density $\frac{28219}{44928} \approx 0.628$. It also follows that the set of positive integers n satisfying the conditions of the theorem has natural density 1.

The proof of Theorem 1 relies in part on Kraus' earlier work. Roughly speaking, for any prime $\ell \neq 2, 3$, Kraus' method gives congruences modulo ℓ for unknowns a, b in (2). The proof also uses ideas from the work of Bright and Siksek [5]. Indeed the non-trivial primitive solutions to (2) give rise to rational points on the hyperelliptic curve

$$\delta^2 + \frac{1}{27} = 4\epsilon^n. \tag{3}$$

For odd exponent n, the function $f = \epsilon - 1$ on this hyperelliptic curve has a divisor which is a norm from the quadratic extension $\mathbb{Q}(\sqrt{321})$. In [5] (see also [15]) it is shown how a function on a curve whose divisor is a norm from an abelian extension can give rise to an obstruction to weak approximation (that is of Brauer–Manin type). In layman's terms, this merely means that we obtain congruence restrictions on the rational points of the curve. The congruence restrictions are obtained through an application of the Law of Quadratic Reciprocity; this is explained in a less conceptual but more elementary way in [14]. Combining these congruence restrictions with the congruences for a, b obtained via Kraus' modular approach shows that equation (2) has no non-trivial primitive solutions if the exponent n is divisible by some positive integer $d \equiv 51, 103, 105 \pmod{106}$. This is a part of Theorem 1.

To obtain the remaining results of Theorem 1 we needed to consider two other hyperelliptic curves associated to (2) defined over $\mathbb{K} = \mathbb{Q}(\omega)$ where ω is a primitive cube root of 1. The functions we employ are defined over $\mathbb{Q}(\zeta)$ and $\mathbb{K}(\zeta)$ for various roots of unity ζ, and we employ the Law of Quadratic Reciprocity over number

fields. Again the congruences obtained here are combined with the congruences from the modular approach and this is used to deduce the remainder of Theorem 1.

References

[1] M. Bennett, *On the equation* $x^{2n} + y^{2n} = z^5$, J. Théor. Nombres Bordeaux **18** (2006), 315–321.

[2] M. A. Bennett, J. S. Ellenberg and N. C. Ng, *The Diophantine equation* $A^4 + 2^\delta B^2 = C^n$, preprint.

[3] M. A. Bennett and C. M. Skinner, *Ternary Diophantine equations via Galois representations and modular forms*, Canad. J. Math. **56** (2004), no. 1, 23–54.

[4] F. Beukers, *The Diophantine equation* $Ax^p + By^q = Cz^r$, Lectures held at Institut Henri Poincaré, September 2004, `http://www.math.uu.nl/people/beukers/Fermatlectures.pdf`

[5] M. Bright and S. Siksek, *Functions, reciprocity and the obstruction to divisors on curves*, J. London Math. Soc. (2) **77** (2008), 789–807.

[6] N. Bruin, *On powers as sums of two cubes*, pages 169–184 of *Algorithmic number theory* (edited by W. Bosma), Lecture Notes in Comput. Sci. **1838**, Springer, Berlin, 2000.

[7] I. Chen and S. Dahmen, *Perfect powers expressible as sums of two cubes*, Journal of Algebra **322** (2009), 638–656.

[8] S. R. Dahmen, *Classical and modular methods applied to Diophantine equations*, University of Utrecht Ph.D. thesis, 2008.

[9] H. Darmon and A. Granville, *On the Equation* $z^m = F(x, y)$ *and* $Ax^p + By^q = Cz^r$, Bull. London Math. Society, **27** (1995), no. 6, 513–543.

[10] H. Darmon and L. Merel, *Winding quotients and some variants of Fermat's Last Theorem*, J. reine angew. Math. **490** (1997), 81–100.

[11] J. Edwards, *A complete solution to* $X^2 + Y^3 + Z^5 = 0$, J. reine angew. Math. **571** (2004), 213–236.

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

[13] A. Kraus, *Sur l'équation* $a^3 + b^3 = c^p$, Experimental Math. **7** (1998), 1–13.

[14] S. Siksek, *Sieving for rational points on hyperelliptic curves*, Math. Comp. **70** (2001), no. 236, 1661–1674.

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

[16] R. L. Taylor and A. Wiles, *Ring theoretic properties of certain Hecke algebras*, Annals of Math. **141** (1995), 553–572.

[17] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Math. **141** (1995), 443–551.

Some classical *p*-adic analysis

Fernando Rodriguez-Villegas

In [1] D. Zagier solves the Monthly problem: prove that

$$v_3\left(\sum_{k=0}^{n-1}\binom{2k}{k}\right) = v_3\left(n^2\binom{2n}{n}\right), \tag{1}$$

where v_p denote the p-adic valuation. He does this by proving that there is a continuous function $f : \mathbb{Z}_3 \longrightarrow -1 + 3\mathbb{Z}_3$ which interpolates the values

$$f(n) = \frac{\sum_{k=0}^{n-1}\binom{2k}{k}}{n^2\binom{2n}{n}}, \qquad n \in \mathbb{N}. \tag{2}$$

The talk was a description of a general form of these facts.

Define formally

$$H(n,t) := \frac{1}{\binom{2n}{n}} \sum_{k=0}^{n-1} \binom{2k}{k} (t+4)^{n-1-k}, \qquad n \in \mathbb{N}, \tag{3}$$

where t is a variable.

Proposition 1. *The following identity holds*

$$H(n,t) = \sum_{k=1}^{n} \frac{1}{\binom{2k}{k}} \binom{n}{k} t^{k-1}. \tag{4}$$

Fix once and for all a prime $p > 2$. Let $t \in \mathbb{Z}_p$ with $|t|_p < 1$. Then the Mahler series

$$H(x,t) := \sum_{k \geq 1} \frac{1}{\binom{2k}{k}} \binom{x}{k} t^{k-1}, \qquad x \in \mathbb{Z}_p \tag{5}$$

converges since the valuation $v_p(\binom{2k}{k})$ grows at most logarithmically with k. By proposition 1 the continuous function $H(\cdot, t)$ interpolates the values $H(n,t)$ of (3).

In fact, the function H is analytic in the unit disk in $\mathbb{C}_p$. Expanding (5) formally as a power series we find

$$H(x,t) = \sum_{n \geq 0} b_n(t) x^n, \tag{6}$$

where

$$b_0 = 0, \qquad b_n(t) = \sum_{k \geq n} \frac{t^{k-1}}{k! \binom{2k}{k}} c_{n,k}, \qquad n \in \mathbb{N}, \tag{7}$$

for certain integers $c_{n,k}$ obtained from

$$\binom{x}{k} = \frac{1}{k!} \sum_{n \geq 0} c_{n,k}\, x^n.$$

We have the following analogue of (1)

Theorem 2. *For $u \in \mathbb{C}_p$ such that $v_p(u-4) \geq 2/(p-1)$ we have*

$$\left| \sum_{k=0}^{n-1} \binom{2k}{k} u^{n-1-k} \right|_p \leq \left| n \binom{2n}{n} \right|_p, \qquad n \in \mathbb{N}. \tag{8}$$

Zagier proved that $H_3(x,1)$ is actually divisible by x^2 and hence gained an extra power of n in the right hand side of the theorem.

To see how this comes about it will be convenient to give t and u in terms of another variable w as follows:

$$t = (w - 1/w)^2, \qquad u := t + 4 = (w + 1/w)^2. \tag{9}$$

For example, if $w = \zeta_3$, a primitive cubic root of unity, then $t = (w - w^{-1})^2 = -3$ and $u = (w + w^{-1})^2 = 1$.

We have

$$b_1(t) := \left.\frac{H(x,t)}{x}\right|_{x=0} = \sum_{k\geq 1} \frac{(-1)^{k-1}}{k\binom{2k}{k}} t^{k-1}. \tag{10}$$

Proposition 3. *The following identity of formal power series in the variable z holds*

$$\frac{1}{w^2 - w^{-2}} \log w^2 = \sum_{k\geq 1} \frac{(-1)^{k-1}}{k\binom{2k}{k}} (w - w^{-1})^{2(k-1)}, \qquad w = 1 - z. \tag{11}$$

We now consider (11) p-adically for $|z|_p < 1$ (so that also $|w - w^{-1}|_p < 1$ with $w = 1 - z$) to obtain

$$b_1(t) = \frac{1}{w^2 - w^{-2}} \log w^2, \qquad |1 - w|_p < 1, \qquad t = (w - w^{-1})^2.$$

As a special case we find

Corollary 4. *Let $\zeta_p \in \mathbb{C}_p$ be a primitive p-th root of unity. Then*

$$b_1((\zeta_p - \zeta_p^{-1})^2) = 0. \tag{12}$$

Combining Theorem 2 with the above corollary we obtain a closer generalization of the original Monthly problem (1).

Theorem 5. *For $p > 2$ and $\zeta_p \in \mathbb{C}_p$ a primitive p-th root of unity we have*

$$\left| \sum_{k=0}^{n-1} \binom{2k}{k} (\zeta_p + \zeta_p^{-1})^{2(n-1-k)} \right|_p \leq \left| n^2 \binom{2n}{n} \right|_p, \qquad n \in \mathbb{N}. \tag{13}$$

The equality typically does not hold for all n but will, in fact, hold except for n's in some excluded congruence classes modulo p.

2

It is not hard to show that

$$b_n(t) = \frac{1}{2(n-1)!} \int_0^1 \frac{\log^{n-1}(1 + tz(1-z))}{1 + tz(1-z)}\, dz. \tag{14}$$

Manipulating the integral we find

$$\log(t+4) \log\left(\frac{\gamma^+}{\gamma^-}\right) + \sum_{k=0}^{n-1} \binom{n-1}{k} \int_{\gamma^-}^{\gamma^+} \log^k(1-v) \log^{n-k-1} v\, \frac{dv}{v}$$

where

$$\gamma^{\pm} := \tfrac{1}{2}(1 \pm \gamma), \qquad \gamma := \sqrt{\frac{t}{t+4}}.$$

The individual integrals in this sum are essentially what are know as Nielsen polylogarithms and can be expressed in terms of multi-polylogarithms. We can

express these multi-polylogarithms in terms of the usual polylogarithms for $n = 2, 3$. Here is the result for $n = 2$.

Proposition 6. *For $|t| < 1$ we have*

$$b_2(t) = \frac{\gamma^2 - 1}{2\gamma} \left[\tfrac{1}{2} \log^2(\gamma^+) - \tfrac{1}{2} \log^2(\gamma^-) + \mathrm{Li}_2(\gamma^+) - \mathrm{Li}_2(\gamma^-) \right]. \tag{15}$$

Alternatively, we also have for $n \in \mathbb{N}$

$$b_n(t) = \frac{1}{(t+4)} \sum_{0 \leq j_1 < j_2 < \cdots < j_n} \frac{(\frac{t}{t+4})^{j_n}}{(j_1 + \frac{1}{2})(j_2 + \frac{1}{2}) \cdots (j_n + \frac{1}{2})}. \tag{16}$$

In Zagier's case $p = 3, t = -3$ and hence $\gamma^{\pm}$ are the primitive cubic roots of unity. The above expressions suggest a relation between $b_2(-3)$ with $\zeta_3(2)$. Indeed, we find numerically that they are related up to a simple factor in $\mathbb{Q}$. Thanks to work done during the Oberwolfach workshop with H. Gangl and D. Zagier the proof of this fact seems reasonably close.

In general it seems that the higher coefficients $b_n(-3)$ are also related to values of 3-adic L-series at least up to $n = 6$; including the apparent equality $b_3(-3) = 0$, noticed by Zagier. It is not inconceivable that all of these could be proved in the near future. These identities should be part of the general picture of relations between periods and special values of L-functions in a p-adic context.

References

[1] D. Zagier; J. Shallit; N. Strauss, Problems and Solutions: 6625, Amer. Math. Monthly **99** (1992), no. 1, 66–69

An elliptic AKS test

Jean-Marc Couveignes
(joint work with R. Lercier and T. Ezome)

The following primality criterion is essentially due to Berrizbeitia [4] and Cheng [5]

Theorem 1. *Let $n \geqslant 3$ be an integer and set $R = \mathbf{Z}/\mathbf{nZ}$. Let $S = R[x]/(x^d - \alpha)$ where $d \geqslant 2$ divides $n - 1$. (Berritzbeitia case) or the case d a prime (Cheng case). Set $n - 1 = dm$ and assume $\zeta = \alpha^m$ has exact order d in R^*. Assume the congruence*

$$(x-1)^n = \zeta x - 1 \bmod (n, x^d - \alpha). \tag{1}$$

holds true in S.
If

$$2^d > n^{\lfloor \sqrt{d} \rfloor}, \tag{2}$$

then n is a prime power.

This criterion leads to a primality test which is a variant of the AKS test [1]. It is much faster than any other variant of the AKS test, but it is *not deterministic*. In this form, it can only be used for integers n such that $n-1$ has a factor d of the appropriate size: large enough to fulfill equation (2) but not too large, so that congruence (1) can be tested efficiently. Avanzi, Bernstein and Mihailescu [2, 4] found a variant of this criterion which makes use of a factor d of $n^f - 1$ instead. This leads to a general primality test.

We follow a different track: we first try to understand the exact role played by the ring $R[x]/(x^d - \alpha)$ in theorem 1. We then propose a variant using a residue ring of a different kind.

Here is a context free primality criterion in the style of Berrizbeitia:

Theorem 2. *Let $n \geqslant 2$ be an integer and set $R = \mathbf{Z}/\mathbf{nZ}$. Let $S \supset R$ be a free étale algebra of rank d over R. Let σ be an R-automorphism of S. Let $\mathcal{G}$ be the group generated by σ. Assume S is a free $R[\mathcal{G}]$-module of rank 1 : there exists an element ω in S such that $(\omega, \sigma(\omega), \ldots, \sigma^{d-1}(\omega))$ is an R basis of S. Let θ be a unit in S such that $\theta^n = \sigma(\theta)$. Let p be a prime divisor of n. Assume $\theta \bmod p$ generates a subgroup of order at least $n^{\lfloor\sqrt{d}\rfloor}$ in $(S/pS)^*$. Then n is a power of p.*

This criterion is of little interest unless we can find an R-algebra S and an element θ in S that generates a large subgroup modulo a prime divisor of n. It it difficult in general to prove that a unit has a large order in a finite ring. In the case of theorem 1 this is proved by a geometric argument: the ring S is the residue ring at a fiber of the multiplication-by-d isogeny

$$[d] : \mathbf{G}_m/R \to \mathbf{G}_m/R,$$

and the element θ is a residue class of a function with small degree on $\mathbf{G}_m$ having its polar divisor contained in the kernel of the isogeny $[d]$.

If we replace the multiplicative group $\mathbf{G}_m$ by an elliptic curve E over R we obtain a much more amenable primality criterion (due to the extra freedom in the choice of E).

See the arxiv [6] preprint for details.

References

[1] M. Agrawal, N. Kayal, and N. Saxena. PRIMES is in P. *Annals of Mathematics*, 160 (2004), no. 2, pp. 781-793.

[2] R. M. Avanzi and P. Mihăilescu. Efficient quasi-deterministic primality test improving AKS. http://www.math.uni-paderborn.de/∼preda/

[3] D. J. Bernstein. Proving primality in essentially quartic random time. *Math. Comp.*, 76(2007), pp. 389-403.

[4] P. Berrizbeitia. Sharpening PRIMES is in P for a large family of numbers. arXiv:math/0211334v1 [math.NT] (2002).

[5] Qi Cheng. Primality proving via one round in ECPP and one iteration in AKS, (2003). http://www.cs.ou.edu/∼qcheng/pub.html

[6] Jean-Marc Couveignes, Tony Ezome, Reynald Lercier. Elliptic periods and primality proving. arXiv:0810.2853

Torsors under tori and Néron models

Martin Bright

Let K be a finite extension of a p-adic field $\mathbb{Q}_p$, with ring of integers $\mathcal{O}$ and residue field k. Let T be a torus over K. Given a smooth variety X over K and an X-torsor $Y \to X$ under T, we can consider the map $X(K) \to \mathrm{H}^1(K, T)$ which associates to each point P of $X(K)$ the isomorphism class of the fibre Y_P.

For example, take $K = \mathbb{Q}_p$ with p odd, let $L = \mathbb{Q}_p(\sqrt{p})$, and let T be the norm torus for L/K, which is the variety defined by $\{x^2 - py^2 = 1\} \subset \mathbb{A}^2_K$. Then $\mathrm{H}^1(K, T) = K^\times / NL^\times$, and the latter group is isomorphic to $k^\times/(k^\times)^2$, the isomorphism being essentially reduction modulo p. Now any X-torsor under T is given locally by an equation of the form $\{u^2 - pv^2 = f\} \subset \mathbb{A}^2_K \times X$, where f is a non-zero rational function on X. If X has good reduction, we can see that the isomorphism class of the fibre above a point P depends only on the value of $f(P)$ modulo p, and hence only on the residue class of P. Moreover, the isomorphism class of the fibre at P depends on whether $f(P)$ is a square modulo P: we see that the problem of evaluating an X-torsor under T has turned into one of evaluating a torsor on the reduction of X under $\mathbb{Z}/2\mathbb{Z}$.

Our main result is the following, which generalises the above situation.

Theorem 1. *Let X be a smooth variety over K, and let $\mathcal{X}/\mathcal{O}$ be a smooth (but not necessarily proper) model of X. Let T be a torus over K split by a tame extension of K. Then, if Y is any X-torsor under T, the evaluation map $X(K) \to \mathrm{H}^1(K, X)$ fits into a commutative diagram as follows.*

$$\begin{array}{ccc} X(K)^0 & \longrightarrow & \mathcal{X}(k) \\ {\scriptstyle Y}\big\downarrow & & \big\downarrow{\scriptstyle \phi} \\ \mathrm{H}^1(K, T) & \xrightarrow{\cong} & \mathrm{H}^1(k, \Phi(T)) \end{array}$$

Here $X(K)^0$ denotes the subset of $X(K)$ consisting of points which extend to an $\mathcal{O}$-point of $\mathcal{X}$; $\Phi(T)$ is the group of components of the Néron model of T; and ϕ is the map coming from an $\mathcal{X}_k$-torsor under Φ. In particular, the isomorphism class of the fibre Y_P at a point $P \in X(K)^0$ depends only on the residue class of P.

We will not describe the proof of Theorem 1 in any detail. The main ingredient is a result of B. Brahm [1], which shows that, for T a K-torus split by a tamely ramified extension, we have $\mathrm{R}^1 j_* T = 0$, where $j : (\operatorname{Spec} K)_{\mathrm{sm}} \to (\operatorname{Spec} \mathcal{O})_{\mathrm{sm}}$ is the map of smooth sites induced by the inclusion $\operatorname{Spec} K \to \operatorname{Spec} \mathcal{O}$.

As an example of the application of Theorem 1, we deduce a well-known fact about torsors over cubic surfaces.

Application. *Let X be a smooth cubic surface over K, and suppose that X has a smooth proper model $\mathcal{X}/\mathcal{O}$. Let T be a torus over K split by a tamely ramified extension, and let Y be an X-torsor under T. Then the evaluation map $X(K) \to \mathrm{H}^1(K, T)$ is constant.*

Proof. The special fibre $\mathcal{X}_k$ is again a smooth cubic surface, so has geometric Picard group which is a finitely generated, free Abelian group. Therefore $\mathrm{H}^1(\mathcal{X}_{\bar{k}}, \Phi(T)) = 0$, and so the Hochschild–Serre spectral sequence shows that any torsor under $\Phi(T)$ on $\mathcal{X}_k$ is constant. Applying Theorem 1 gives the result. □

References

[1] B. Brahm. Néron-Modelle von algebraischen Tori. In *Äquivariante derivierte Kategorien rigider Räume. Néron Modelle von algebraischen Tori*, volume 31 of *Schriftenreihe Math. Inst. Univ. Münster 3. Ser.*, page 154. Univ. Münster, Münster, 2004.

Degenerations of Hypersurfaces

Alan G. B. Lauder

Let $f_0 \in \mathbb{Q}[x_0, x_1, \ldots, x_{n+1}]$ be homogeneous of degree d and define $f_1 := x_0^d + \cdots + x_{n+1}^d$. Consider the pencil of hypersurfaces of degree d and dimension n defined by the equation

$$(1-t)f_0 + tf_1 = 0.$$

The fibres in this pencil are generically smooth but they degenerate to a possibly singular projective hypersurface at $t = 0$ defined by the equation $f_0 = 0$. Given a suitable prime number p, we define, and describe a method for computing to any desired precision, a pair of matrices (F, N) such that F has entries in the p-adic field $\mathbb{Q}_p$ and N is a nilpotent matrix with entries in $\mathbb{Q}$ such that $NF = pFN$. We conjecture that the polynomial $\det(1 - TF|_{\ker N})$ has integer coefficients, and has all reciprocal roots of complex absolute value $p^{i/2}$ for $0 \leq i \leq n$. This conjecture follows from a stronger (but vaguer) one: that the polynomial is the middle Weil polynomial of some natural "semistable" limit at $t = 0$ of the family when "reduced" modulo p.

We give examples for the following: degeneration of a quartic curve to a double conic ($p = 5$); degeneration of a quartic curve to a 3-cuspidal quartic ($p = 13$); degeneration of a quintic curve to a non-reduced union of hyperplanes ($p = 31$); degeneration of a sextic curve to a sextic curve with an ordinary double point ($p = 7$); degeneration of a quartic (K3) surface to a quartic surface with two ordinary double points ($p = 5$); degeneration of a quartic surface to a quartic surface with an A_2 singularity ($p = 5, 13$); degeneration of a cubic 3-fold to a cubic 3-fold containing a pencil of planes ($p = 19$).

On the expected result for the second moment of twisted L-functions

Guillaume Ricotta

The fourth moment of Dirichlet L-functions is

$$M_4(q) := \sum_{\chi \in X^*(q)} |L(\chi, 1/2)|^4$$

where $X^*(q)$ stands for the set of primitive Dirichlet characters of modulus q whereas the second moment of twisted L-functions is

$$M_{2,f}(q) := \sum_{\chi \in X^*(q)} |L(f \times \chi, 1/2)|^2$$

where f is a *fixed* holomorphic primitive cusp form of level $D_f \geqslant 1$ coprime with q, nebentypus ψ_f of modulus D_f satisfying $\psi_f(-1) = (-1)^{k_f}$ and integer weight $k_f \geqslant 1$ (see appendix [RiRo] for the automorphic background). Note that

$$\text{card}\,(X^*(q)) := \varphi^*(q) = q \prod_{p||q} \left(1 - \frac{2}{p}\right) \prod_{p^2|q} \left(1 - \frac{1}{p}\right)^2$$

according to [IwKo, Equation (3.7) Page 46]. Finding an asymptotic formula for $M_4(q)$ as $q \to +\infty$ with a power saving in the error term should be philosophically as difficult as the corresponding question for $M_{2,f}(q)$ since

$$M_4(q) = M_{2,\left(\frac{\partial E(1/2,.)}{\partial s}\right)(1/2)}(q)$$

where $E(z,s)$ is the real-analytic Eisenstein series on the modular curve $X_0(1)$ associated to the cusp ∞. Note that $M_4(q)$ is itself the q-analog of the fourth moment of the Riemann zeta function in the t-aspect (see [In] and [Hb2]) but this analogy will not be developed here. D. Heath-Brown ([HB]) for $M_4(q)$ and T. Stefanicki ([St]) for $M_{2,f}(q)$ proved the following analogous results.

Theorem. *If q goes to infinity then*

$$M_4(q) = \frac{1}{2\pi^2} \prod_{p|q} \frac{(1-p^{-1})^3}{(1+p^{-1})} \log^4(q) \varphi^*(q) + O\left(2^{\omega(q)} q \log^3 q\right)$$

where $\omega(q)$ stands for the number of prime divisors of q and

$$M_{2,f}(q) = \frac{6(4\pi)^{k_f}}{\pi\Gamma(k)} ||f||^2 \prod_{p|q} \frac{(1-p^{-1})^2}{(1-p^{-2})} \left(1 - \frac{\lambda_f(p^2)-2}{p} + \frac{1}{p^2}\right) \log(q) \varphi^*(q) + O\left(2^{\omega(q)} q \log^\delta q\right)$$

where $||f||$ stands for Petersson's norm of f and $0 < \delta < 1$ is any real number satisfying

$$\forall \varepsilon > 0, \quad \sum_{p \leqslant x} |\lambda_f(p)| \leqslant (\delta + \varepsilon) \frac{x}{\log x}.$$

Remark 1. It is possible to choose $\delta = (\sqrt{2} + 3\sqrt{3})(5\sqrt{2})^{-1}$ according to [Ra].

Remark 2. The formula for $M_4(q)$ is an asymptotic formula for almost all integers but it turns out that if $\omega(q) > \log^{-1} 2 \log_2 q$ then the error term is not smaller than the main term. Similarly, if $\omega(q) > (1-\delta)\log^{-1} q \log_2 q$ then the error term in $M_{2,f}(q)$ is not smaller than the main term such that the formula for $M_{2,f}(q)$ is an asymptotic formula only for a set of integers of zero density according to [HR].

These results have been improved by K. Soundararajan ([So]) for $M_4(q)$ and in [GKR] for $M_{2,f}(q)$ as follows.

Theorem. *If q goes to infinity then*

$$M_4(q) = \frac{1}{2\pi^2} \prod_{p|q} \frac{(1-p^{-1})^3}{(1+p^{-1})} \log^4(q)\varphi^*(q) \left(1 + O\left(\log_2^{-1/2}(q)\right)\right)$$

and if $\omega(q) \ll \exp\left(300^{-1} \log_2 q \log_3^{-1} q\right)$ then

$$M_{2,f}(q) = \frac{6(4\pi)^{k_f}}{\pi\Gamma(k)} ||f||^2 \prod_{p|q} \frac{(1-p^{-1})^2}{(1-p^{-2})} \left(1 - \frac{\lambda_f(p^2)-2}{p} + \frac{1}{p^2}\right) \log(q)\varphi^*(q) \times \left(1 + O\left(\log_2^{-1}(q)\right)\right).$$

M. Young ([Yo]) got an asymptotic formula with a power saving in the error term for $M_4(q)$ in the prime modulus case.

Theorem. *If q goes to infinity among the prime numbers then*

$$M_4(q) = P(\log q)\varphi^*(q) + O\left(\varphi^*(q) q^{-\frac{1}{80}+\frac{\theta}{40}}\right)$$

where P is an explicit polynomial of degree 4 and $\theta = 7/64$.

Remark 3. Note that $-1/80 + \theta/40 < 0$. The same result should hold without the restriction q prime but it remains an open question so far. It should be very difficult to extend this result to any integer following the proof given in [Yo] since many technical difficulties would occur if q is composite.

Remark 4. This particular value of θ is the best currently known approximation towards Ramanujan-Petersson-Selberg's conjecture in $GL(2)$ according to [Ki] and [KH].

It turns out that the analogous result for $M_{2,f}(q)$ is still an open question and the purpose of this note is to identify the underlying analytic issue, which occurs in the second question. Let us state the expected result.

Expected Result. There exists some absolute constant $\alpha > 0$ such that if q goes to infinity then

$$M_{2,f}(q) = P(\log q)\varphi^*(q) + O\left(\varphi^*(q) q^{-\alpha}\right)$$

where P is an explicit polynomial of degree 1.

Proving this requires some new input in order to solve unbalanced shifted convolution problems. Such new input would have many other interesting applications.

Acknowledgements. The author would like to thank Karim Belabas, Hendrik W. Lenstra and Don B. Zagier for inviting him in Mathematisches Forschungsinstitut Oberwolfach on the occasion of the workshop "Explicit Methods in Number Theory".

References

[BlHaMi] Blomer V., Harcos G., Michel P.: *A Burges-like subconvex bound for twisted L-functions*, to be published in Forum Mathematicum, available at `http://www.math.univ-montp2.fr/\%7Emichel/publi.html` (2006).

[GKR] Gao P., Khan R., Ricotta G.: *The second moment of Dirichlet twists of Hecke L-functions*, preprint available at `http://arxiv.org/abs/0812.2606`, to be published in Acta Arithmetica.

[HR] Hardy G., Ramanujan S.: *The normal number of prime factors of a number n*, Quart. J. Math. 48 (1917), 76-92.

[In] Ingham A.: *On the estimation of $N(\sigma, T)$*, Quart. J. Math., Oxford Ser. 11, (1940), 291-292.

[IwKo] Iwaniec H., Kowalski E.: *Analytic number theory*, Providence R.I., Colloquium publications (American Mathematical Society) (2004).

[HB] Heath-Brown D.: *The fourth power mean of Dirichlet's L-functions*, Analysis, vol. 1, 25–32 (1981).

[Hb2] Heath-Brown D.: *The fourth power moment of the Riemann zeta function*, Proc. London Math. Soc. (3) 38 (1979), no. 3, 385-422.

[Ki] Kim H.: *Functoriality for the exterior square of* GL_4 *and the symmetric fourth of* GL_2, with appendix 1 by Dinakar Ramakrishnan and appendix 2 by Kim and Peter Sarnak, J. Amer. Math. Soc., Vol. 16 (2003) no. 1, 139–183 (electronic).

[KH] Kim H., Shahidi F., *Functorial products for* $\mathrm{GL}_2 \times \mathrm{GL}_3$ *and the symmetric cube for* GL_2, with an appendix by Colin J. Bushnell and Guy Henniart, Ann. of Math. (2), Vol. 155 (2002), no. 3, 837–893.

[KoMiVa] Kowalski E., Michel P., Vanderkam J.: *Rankin-Selberg L-functions in the level aspect*, Duke Math. J. Vol 114, No. 1 (2002).

[Ra] Rankin R.: *Sums of powers of cusp form coefficients. II*, Math. Ann. Vol. 272 (1984) no. 4, 593–600.

[Ri] Ricotta G.: *Real zeros and size of Rankin-Selberg L-functions in the level aspect*, Duke Mathematical Journal, Vol. 131, No. 2 (2006), 291–350.

[RiRo] Ricotta G., Royer E.: *Statistics for low-lying zeros of symmetric power L-functions in the level aspect*, preprint available at `http://arxiv.org/abs/math/0703760`.

[So] Soundararajan K.: *The fourth moment of Dirichlet L-functions*, preprint available at `http://front.math.ucdavis.edu/math.NT/0507150` (2005).

[St] Stefanicki T.: *Non-vanishing of L-functions attached to automorphic representations of GL*(2) *over* $\mathbb{Q}$, J. Reine Angew. Math. 474, 1–24 (1996).

[Yo] Young M.: *The fourth moment of Dirichlet L-functions*, preprint available at `http://arxiv.org/abs/math/0610335`.

Diagonal quartic surfaces

Alexei Skorobogatov

The aim of this report is to explain how to get some numerical evidence for the following conjecture.

Conjecture *The Brauer–Manin obstruction is the only obstruction to the Hasse principle and weak approximation on K3 surfaces over number fields.*

This conjecture has been discussed for some time, but probably was not taken seriously enough for lack of evidence, either numerical or theoretical. Papers [2], [13], [9] establish the Hasse principle for certain elliptic K3 surfaces, diagonal quartic surfaces, and Kummer surfaces, respectively, under specific technical conditions. These results assume the finiteness of the Tate–Shafarevich groups of elliptic curves, and the first two of these papers also assume Schinzel's Hypothesis. The author is not aware of any results on weak approximation for K3 surfaces with a rational point. We still do not know if the existence of a rational point always implies that their set is Zariski dense, or even whether it is infinite. The methods of Bogomolov and Tschinkel often allow one to prove the Zariski density of rational points over a finite extension of the ground field. In some particularly good cases, this can be achieved without enlarging the ground field, see [5]. This paper also contains results on the density of rational points in the real analytic topology.

Let X be a K3 surface over a number field k. The precise statement of the above conjecture is the density of $X(k)$ in the Brauer–Manin set

$$\big(\prod_{\text{all } v} X(k_v)\big)^{\mathrm{Br}} \subset \prod_{\text{all } v} X(k_v),$$

where the product over all completions k_v of k is equipped with the product topology, each space $X(k_v)$ having its natural local topology. The superscript Br means that we only consider the families of local points (P_v) with the zero sum of local invariants of $\mathcal{A}(P_v) \in \mathrm{Br}(k_v)$, for all $\mathcal{A} \in \mathrm{Br}(X)$, see [12] for details. Recall the notation

$$\mathrm{Br}_0(X) = \mathrm{Im}[\mathrm{Br}(k) \to \mathrm{Br}(X)], \quad \mathrm{Br}_1(X) = \mathrm{Ker}\,[\mathrm{Br}(X) \to \mathrm{Br}(\overline{X})].$$

The sum of local invariants of $\mathcal{A} \in \mathrm{Br}_0(X)$ is always zero, so the obstruction depends only on the elements of $\mathrm{Br}(X)/\mathrm{Br}_0(X)$.

Theorem [10] *Let X be a K3 surface over a field k finitely generated over $\mathbb{Q}$. Then $\mathrm{Br}(X)/\mathrm{Br}_0(X)$ is finite.*

As a consequence we see that the Brauer–Manin set is open in $\prod_{\text{all } v} X(k_v)$.

Most of the difficulties in computing, or at least estimating the order of the Brauer group $\mathrm{Br}(X)$, come from its so called 'transcendental' part $\mathrm{Br}(X)/\mathrm{Br}_1(X)$. Let $\overline{k}$ be an algebraic closure of k, and $\Gamma = \mathrm{Gal}(\overline{k}/k)$. We have a natural injective map $\mathrm{Br}(X)/\mathrm{Br}_1(X) \hookrightarrow \mathrm{Br}(\overline{X})^{\Gamma}$, where $\overline{X} = X \times_k \overline{k}$. As an abelian group $\mathrm{Br}(\overline{X})$ is isomorphic to $(\mathbb{Q}/\mathbb{Z})^{22-\rho}$, where $\rho = \mathrm{rk}\,\mathrm{Pic}\overline{X} \le 20$.

We have a good understanding of the Galois module $\mathrm{Br}(\overline{X})$ in the case when X is the (desingularized) Kummer surface associated with an abelian surface A, i.e. obtained by blowing-up the 16 double points on the quotient of A by the antipodal involution $x \mapsto -x$. In [11] we prove that $\mathrm{Br}(\overline{X})$ and $\mathrm{Br}(\overline{A})$ are isomorphic as Γ-modules. Next, for any integer $n > 1$ we show that $\mathrm{Br}(X)_n/\mathrm{Br}_1(X)_n$ is a subgroup

of $\mathrm{Br}(A)_n/\mathrm{Br}_1(A)_n$, and that this inclusion is an equality for odd n. If $A = E \times E'$ is a product of two elliptic curves, then

$$\mathrm{Br}(A)_n/\mathrm{Br}_1(A)_n = \mathrm{Hom}_\Gamma(E_n, E'_n)/\big(\mathrm{Hom}(\overline{E}, \overline{E}')/n\big)^\Gamma.$$

This can be used to prove that $\mathrm{Br}(X) = \mathrm{Br}(\mathbb{Q})$ for the Kummer surface X over $\mathbb{Q}$ given by the following affine equation:

$$z^2 = (x^3 + 1)(y^3 + 6y + 2), \tag{1}$$

and also for some other Kummer surfaces with $\rho = 18$ or $\rho = 19$.

Now let $D \subset \mathbb{P}^3_{\mathbb{Q}}$ be the quartic surface

$$x_0^4 + a_1 x_1^4 + a_2 x_2^4 + a_3 x_3^4 = 0,$$

where a_1, a_2, $a_3 \in \mathbb{Q}^*$. Using the results about the Brauer group of Kummer surfaces [11] described above, and Evis Ieronymou's thesis [3] we prove the following

Theorem [4] *The group* $\mathrm{Br}(D)/\mathrm{Br}_1(D)$ *is a subgroup of* $(\mathbb{Q}/\mathbb{Z})^2$ *killed by* $2^{12} \cdot 3 \cdot 5$. *Let* $H_D \subset \mathbb{Q}^*$ *be the subgroup generated by* -1, 4, a_1, a_2, a_3 *and the* 4*-th powers* $\mathbb{Q}^{*4}$. *If* $\{2, 3, 5\} \cap H_D = \emptyset$, *then* $\mathrm{Br}(D) = \mathrm{Br}_1(D)$.

The full list of possible values of the finite abelian group $\mathrm{Br}_1(D)/\mathrm{Br}_0(D)$ can be found in the thesis of M. Bright [1], in particular, $|\mathrm{Br}_1(D)/\mathrm{Br}_0(D)|$ divides 2^5.

Our proof is based on the crucial observation that the Fermat quartic surface $X \subset \mathbb{P}^3_{\mathbb{Q}}$ given by

$$x_0^4 + x_1^4 + x_2^4 + x_3^4 = 0$$

is a Kummer surface, at least after an appropriate extension of the ground field. This was first observed with some surprise in 1971 by I.R. Shafarevich and I.I. Piatetskii-Shapiro as an application of their global Torelli theorem for complex K3 surfaces [8]. In his thesis [6] (see also [7]) Masumi Mizukami constructed an explicit isomorphism between X and the Kummer surface associated with a certain abelian surface A over $\mathbb{Q}$. The isomorphism itself is defined over $\mathbb{Q}(\sqrt{-1}, \sqrt{2}) = \mathbb{Q}(\mu_8)$. This result allows us to control torsion of odd order in $\mathrm{Br}(D)/\mathrm{Br}_1(D)$. The 2-primary torsion subgroup of $\mathrm{Br}(D)$ was studied in the thesis of Evis Ieronymou. The result that concerns us here is [3, Thm. 5.2] which states that if $2 \notin H_D$, then the 2-primary subgroup of $\mathrm{Br}(D)/\mathrm{Br}_1(D)$ is trivial.

As an application of our results we exhibit diagonal quartic surfaces over $\mathbb{Q}$ with trivial Brauer group. By [1], Appendix A (case A161 and its subcases) we have $\mathrm{Br}_1(D) = \mathrm{Br}(\mathbb{Q})$ for the following diagonal quartics D_c:

$$x_0^4 + 4x_1^4 + cx_2^4 - cx_3^4 = 0, \tag{2}$$

where c is any non-zero rational number. By combining this with our result we see that $\mathrm{Br}(D_c) = \mathrm{Br}(\mathbb{Q})$ for many values of c, e.g. $c = 1$ or $c = 9$. The surfaces (2) have obvious $\mathbb{Q}$-points, so it is natural to test weak approximation on them.

During the workshop Martin Bright computed that any $\mathbb{Q}_2$-point of D_1 can be approximated by a rational point modulo 16 (note that 2 is the only prime of bad reduction of D_1). Similarly, any $\mathbb{Q}_2$-point of D_9 can be approximated by a rational point modulo 8, and any $\mathbb{Q}_3$-point of D_1 can be approximated modulo 9

(note that 2 and 3 are the only primes of bad reduction of D_9). It is also possible to do simultaneous approximations modulo 8 and 3. Similar experiments were done for the Kummer surface (1). I would like to thank Martin for his help.

References

[1] M. Bright. *Computations on diagonal quartic surfaces.* PhD thesis, University of Cambridge, 2002. http://www.boojum.org.uk/maths/quartic-surfaces/thesis.pdf

[2] J-L. Colliot-Thélène, A.N. Skorobogatov and Sir Peter Swinnerton-Dyer. Hasse principle for pencils of curves of genus one whose Jacobians have rational 2-division points. *Invent. Math.* **134** (1998) 579–650.

[3] E. Ieronymou. Diagonal quartic surfaces and transcendental elements of the Brauer group. Preprint, 2008.

[4] E. Ieronymou, A.N. Skorobogatov and Yu.G. Zarhin. On the Brauer group of diagonal quartic surfaces. (In preparation)

[5] A. Logan, D. McKinnon and R. van Luijk. Density of rational points on diagonal quartic surfaces. arXiv:0812.4779

[6] M. Mizukami. Master thesis, University of Tokyo, 1977. (Japanese)

[7] M. Mizukami. Fixed point free involutions on certain nonsingular quartic surfaces. In: *Proc. Int. Symp. on Algebraic Geometry* (Kyoto, 1977) Kinokuniya, Tokyo, 1978, pp. 589–593.

[8] I.I. Piatetskii-Shapiro and I.R. Shafarevich. Torelli's theorem for algebraic surfaces of type K3. *Izv. Akad. Nauk SSSR Ser. Mat.* **35** (1971) 530–572.

[9] A.N. Skorobogatov and Sir Peter Swinnerton-Dyer. 2-descent on elliptic curves and rational points on certain Kummer surfaces. *Adv. Math.* **198** (2005) 448–483.

[10] A.N. Skorobogatov and Yu.G. Zarhin. A finiteness theorem for the Brauer group of abelian varieties and K3 surfaces. *J. Alg. Geom.* **17** (2008) 481–502.

[11] A.N. Skorobogatov and Yu.G. Zarhin. The Brauer group of Kummer surfaces and torsion of elliptic curves. (In preparation)

[12] A. Skorobogatov. *Torsors and rational points.* Cambridge Univ. Press, 2001.

[13] Sir Peter Swinnerton-Dyer. Arithmetic of diagonal quartic surfaces II. *Proc. London Math. Soc.* **80** (2000) 513–544.

Rational points on higher-dimensional varieties

Bjorn Poonen

This extended abstract is based on a three-lecture miniseries given on July 14–16, 2009.

1. Existence of rational points

Throughout this article, k denotes a fixed number field, though much of what we say holds for global function fields as well. Varieties over X may be specified by giving a finite number of affine patches and explicit gluing data.

Question 1. *Does there exist an algorithm that takes as input a k-variety X, and outputs YES or NO according to whether X has a k-rational point?*

The answer to Question 1 is not known for any number field k. (But for every global function field, it is known that no such algorithm exists [23], [27], [29], [9].) See [25] for a discussion.

Question 1 is equivalent to the following variants:

(1) The same question for affine k-varieties. *Proof:* To answer the question for any arbitrary variety, it suffices to answer it for the affine patches.
(2) The same question for affine hypersurfaces $f(x_1, \ldots, x_n) = 0$ over k. *Proof:* This is equivalent to the previous question because one can combine equations: if a is any nonsquare in k, then the system $f = g = 0$ is equivalent to the single equation $f^2 - ag^2 = 0$.
(3) The same question for smooth affine k-varieties. *Proof:* Any variety is a union of locally closed smooth affine subvarieties.
(4) The same question for nice k-varieties, where *nice* means smooth, projective, and geometrically integral. *Proof:* This time, the equivalence is nontrivial: see [24].

It is not known whether these are equivalent to the corresponding question for smooth affine hypersurfaces, or the question for nice hypersurfaces.

The question for affine hypersurfaces is a restatement of Hilbert's tenth problem over k, the analogue for k of the original Hilbert's tenth problem over $\mathbb{Z}$, which asked for an algorithm for deciding whether a multivariable polynomial equation $f(x_1, \ldots, x_n) = 0$ with integer coefficients has a solution in integers. Work of M. Davis, H. Putnam, and J. Robinson [8] and Yu. Matiyasevich [18] showed that over $\mathbb{Z}$ there is no such algorithm.

Remark 2. B. Poonen and A. Shlapentokh showed in 2003 that a negative answer to Hilbert's tenth problem for the ring of integers of any fixed number field would follow from the negative answer for $\mathbb{Z}$ together with a statement about elliptic curves. The latter statement, that for every cyclic extension of number fields L/K there exists an elliptic curve E over K with $\operatorname{rank} E(K) = \operatorname{rank} E(L) = 1$, has been proved by B. Mazur and K. Rubin assuming the finiteness of Tate-Shafarevich groups of all elliptic curves over number fields, or at least the weaker statement that $\dim_{\mathbb{F}_2} Ш(E)[2]$ is even for all elliptic curves over number fields.

2. Local-global principle and weak approximation

Definition 3. Let X be a variety over a number field k. In the products below, v ranges over all nontrivial places of k.

- To say that X satisfies the local-global principle means that the implication $\prod_v X(k_v) \neq \emptyset \implies X(k) \neq \emptyset$ holds. (This is also called the Hasse principle, but we will use the more descriptive terminology.) Although the implication has a truth value for each individual X, one usually speaks of the principle holding or not for varieties in a certain class.
- To say that X satisfies weak approximation means that $X(k)$ is dense in $\prod_v X(k_v)$, where the latter is equipped with the product of the v-adic topologies, and $X(k)$ is embedded in it diagonally.

Although weak approximation is a stronger condition, it is often (but not always) the case that when the local-global principle is satisfied by all varieties in a certain class, weak approximation holds too.

For more details on weak approximation, D. Harari's survey article [11] is highly recommended.

2.1. **Examples and counterexamples.** The conditions tend to hold only for varieties that are "geometrically very simple", such as the following:

- $\mathbb{P}^n$;
- quadrics, i.e., degree 2 hypersurfaces (Hasse, Minkowski);
- smooth intersections of two quadrics in $\mathbb{P}^n$ with $n \geq 8$;
- Châtelet surfaces associated to $y^2 - az^2 = P(x)$ with $P(x)$ *irreducible* of degree 4;
- nice degree d hypersurfaces in $\mathbb{P}^n$ where $n \gg d$ (circle method);
- norm form equations $N_{L/k}(x_1e_1 + \cdots + x_ne_n) = c$; where $(e_1, \ldots, e_n)$ is a basis for L/k and $c \in k^\times$ (Hasse); and
- simply connected semisimple affine algebraic groups.

On the other hand, counterexamples, even to the local-global principle over $\mathbb{Q}$, can be found among

- curves of genus at least 1;
- cubic surfaces;
- intersections of two quadrics in $\mathbb{P}^4$; and
- Châtelet surfaces.

(See [11] for references.)

2.2. **Known techniques.** Recently there has been an almost total "grand unification" of the diverse techniques used to construct counterexamples to the local-global principle and weak approximation. We can now say that all known counterexamples have been explained by some combination of just two methods!

The first of these is the descent obstruction (Fermat, Chevalley & Weil, Colliot-Thélène & Sansuc [4], [5], Harari & Skorobogatov [12]), which subsumes the Brauer-Manin obstruction (Manin [17]). For an introduction to these cohomological obstructions, see [28], and for recent work relating them see either [26] or the extended abstract by the author in the February 1–7, 2009 Oberwolfach report.

The second of these is the p-adic analytic method of C. Chabauty [2], which was an abelian variety analogue of an earlier idea of T. Skolem in the context of integer points on tori. A nonabelian generalization has been proposed by M. Kim [13], [14], [15], [16].

But it is expected that there are many counterexamples to the local-global principle and weak approximation that cannot be explained by any combination of these techniques. More ideas are needed!

3. Example: nice hypersurfaces in projective space

Let X be a nice degree d hypersurface $f(x_0, \ldots, x_n) = 0$ in $\mathbb{P}^n_{\mathbb{Q}}$, where f is a homogeneous polynomial of degree d with integer coefficients. How do rational points on X behave?

There is a well-known crude heuristic that suggests an answer. If $a_0, \ldots, a_n$ are integers with gcd 1, and $P := (a_0 : \cdots : a_n) \in \mathbb{P}^n(\mathbb{Q})$, then define the height of P as $H(P) := \max_i |a_i|$. The number of points in $\mathbb{P}^n(\mathbb{Q})$ of height exactly B is $\sim B^n$, where we use $f \sim g$ to denote that f/g has a positive finite limit as $B \to \infty$. For each such point, the integer $f(a_0, \ldots, a_n)$ is $O(B^d)$, so heuristically one can predict that it equals 0 with probability $\sim 1/B^d$. The previous two sentences together predict that there are $\sim B^{n-d}$ rational points of height B on X. So the total number of rational points on X should be $\sim \sum_{B \geq 1} B^{n-d}$. Thus the behavior should depend on how $n - d$ compares to -1. The heuristic suggests:

- If $d < n + 1$ (and maybe also if we are in critical case $d = n + 1$), then $X(\mathbb{Q})$ is infinite.
- If $d > n + 1$, then $X(\mathbb{Q})$ is finite.

But this is often wrong! For instance, X can fail to have points over $\mathbb{R}$ even if $d \ll n$. Also, one really should take into account congruences, to incorporate p-adic information for every prime p. Nevertheless, the crude heuristic motivates many conjectures about the behavior of rational points, even for varieties more general than hypersurfaces. We turn to some of these conjectures next.

4. Behavior of rational points in general

We have already considered the question of existence of rational points. When the set of rational points is nonempty, what questions can one ask to describe it?

4.1. **Zariski density.** First of all, one can ask whether $X(k)$ is finite or infinite.

For nice plane curves, the crude heuristic gives the right answer to this question when there are no local obstructions to rational points (i.e., when $\prod_v X(k_v) \neq \emptyset$), except that in the critical case of plane cubic curves, finiteness holds for some curves and fails for others.

For nice curves in general, the genus g plays the role played by the degree. Namely:

- If $g = 0$, and $\prod_v X(k_v) \neq \emptyset$, then $X(k)$ is infinite (and in fact, $X \simeq \mathbb{P}^1_k$).
- If $g = 1$, then $X(k)$ may be infinite, finite, or empty, even if $\prod_v X(k_v) \neq \emptyset$.
- If $g > 1$, then $X(k)$ is finite (possibly empty). This is known as the Mordell conjecture or Faltings' theorem [10].

For nice hypersurfaces of higher dimension, $X(k)$ can be infinite even when $d \gg n$: for example, the nice surface $x_0^{17} + x_1^{17} + x_2^{17} + x_3^{17} = 0$ in $\mathbb{P}^3_{\mathbb{Q}}$ has infinitely many rational points, because there are already infinitely many on the line $x_0 + x_1 = x_2 + x_3 = 0$, for instance. This suggests that perhaps the correct generalization of finiteness is "constrained to a lower-dimensional variety". One says that rational points on a k-variety X are Zariski dense if there is no closed subvariety $Z \subsetneqq X$ containing $X(k)$.

What should be the higher-dimensional analogue of the condition $g > 1$? E. Bombieri and S. Lang suggested that a sufficient condition should be that of being of general type: a nice variety X is of general type if the canonical sheaf

ω_X is such that the sections of $\omega_X^{\otimes n}$ for sufficiently positive n determine a rational map $X \dashrightarrow \mathbb{P}^N$ mapping X birationally to its image.

Conjecture 4 (Bombieri, Lang)**.** *If X is a nice variety of general type and $\dim X > 0$, then $X(k)$ is not Zariski dense in X.*

Remark 5. A nice hypersurface of degree d in $\mathbb{P}^n$ has $\omega_X \simeq \mathcal{O}_X(d-n-1)$, so X is of general type if and only if $d > n+1$. So the Bombieri-Lang conjecture is compatible with the crude heuristic.

Question 6. *Can one generalize the crude heuristic so that it predicts the Bombieri-Lang conjecture for all varieties of general type?*

4.2. **Potential density.** Some varieties that are *not* of general type also fail to have $X(k)$ Zariski dense in X. Thus the most naive converse of the Bombieri-Lang conjecture is wrong. To formulate a possibly correct converse, it is convenient to introduce a "stable" version of Zariski density:

Definition 7. Let X be a nice variety over a number field k. Say that rational points on X are potentially dense if there exists some finite extension L of k such that $X(L)$ is Zariski dense in X.

The potential density property depends only on the base extension of X to an algebraic closure of k, so one might hope that it corresponds to some simple *geometric* condition on X. For example, for a nice curve X of genus g, rational points are potentially dense if and only if $g \leq 1$.

The property of being of general type is unchanged by field extension, so the Bombieri-Lang conjecture predicts that positive-dimensional varieties of general type are among the varieties for which rational points are not potentially dense. But there are others.

If $X \dashrightarrow Y$ is a dominant rational map of nice k-varieties, then potential density for X implies potential density for Y (obviously), and the converse holds if $X \to Y$ is a finite étale morphism. So if X dominates a positive-dimensional variety of general type, or has a finite étale cover that dominates a positive-dimensional variety of general type, then again rational points on X should not be potentially dense, according to the Bombieri-Lang conjecture.

Example 8 ([6])**.** Let E be an elliptic curve. Let H be a hyperelliptic curve of genus greater than 1. Let $i_E \colon E \to E$ be translation by a 2-torsion point. Let $i_H \colon H \to H$ be the hyperelliptic involution. Let $i = (i_E, i_H)$; this is a fixed-point-free involution of $E \times H$. Let $X = (E \times H)/\langle i \rangle$. Then X has a finite étale cover (namely, $E \times H$) that dominates a positive-dimensional variety of general type (namely, H), so rational points on X are not potentially dense (we can say this unconditionally, because of Faltings' theorem for H). On the other hand, one can show that X is not of general type, and that X does not even dominate any positive-dimensional variety of general type.

Alternatively, this situation can be understood as follows. The degree 2 map $H \to \mathbb{P}^1$ factors through the stack quotient $[H/i_H]$, and X dominates $[H/i_H]$.

Moreover, $[H/i_H]$ behaves as if it were of general type: it consists of $\mathbb{P}^1$ with $2g+2$ points replaced by $\frac{1}{2}$-points, so its Euler characteristic is $2-(2g+2)\frac{1}{2}$, which is negative, like the Euler characteristic of a curve of genus greater than 1.

The fact that X dominates $[H/i_H]$ manifests itself in the fact that each component of a fiber of the composition $X \to [H/i_H] \to \mathbb{P}^1$ above any one of the $2g+2$ branch points of $H \to \mathbb{P}^1$ has multiplicity divisible by 2 (in fact, equal to 2).

Campana made the observation that when a variety X admits a morphism to $\mathbb{P}^1$ such that a fiber has two components, of multiplicity 2 and 3, then X does not map to a stacky $\mathbb{P}^1$ in the usual sense (since $\gcd(2,3)=1$), but heuristics related to the *abc* conjecture predict that its rational points should behave as if the $\mathbb{P}^1$ had only a $\frac{1}{\min\{2,3\}}$-point below that fiber. He formulates a notion of "orbifold" (not the usual notion) generalizing the notion of stack, and says that X dominates the orbifold. Then he conjectures that for a nice variety X, rational points are potentially dense if and only if X does not dominate an "orbifold of general type". See [1].

4.3. **Topological closure.** We have discussed weak approximation already, but one can also ask about the closure of $X(k)$ in the topological space $X(k_v)$ for a *single* place v. For instance, B. Mazur has conjectured the following statement [19].

Conjecture 9 (Mazur)**.** *Let X be a $\mathbb{Q}$-variety. Then the closure of $X(\mathbb{Q})$ in $X(\mathbb{R})$ with respect to the usual analytic topology has at most finitely many connected components.*

This holds for curves (by Faltings' theorem) and abelian varieties (because any closed subgroup of a compact Lie group has only finitely many connected components), but only a few other cases are known. If true, the conjecture would rule out certain approaches to proving a negative answer to Question 1: see [7].

There are also related conjectures for number fields beyond $\mathbb{Q}$ and for nonarchimedean places: see page 257 of [20].

4.4. **Counting points of bounded height.** One can define a height function $H\colon \mathbb{P}^n(k) \to \mathbb{R}$ generalizing the definition given above for $k=\mathbb{Q}$. Then, for a variety X embedded in $\mathbb{P}^n_k$, one can define a counting function

$$N(X;B) := \#\{P \in X(k) : H(P) \le B\}.$$

For certain varieties X, V. Batyrev and Yu. Manin have formulated conjectures about the asymptotic rate of growth of $N(X;B)$ as $B \to \infty$ in terms of arithmetic and geometric properties of X. So far, for every k-variety X for which $X(k)$ is nonempty and the asymptotic behavior has been determined, it has turned out that $N(X;B) \sim B^a(\log B)^b$ for some $a \in \mathbb{Q}$ and $b \in \frac{1}{2}\mathbb{Z}$ (recall that we are ignoring constant factors). For more on these conjectures, see [22].

References

[1] Frédéric Campana, *Orbifolds, special varieties and classification theory*, Ann. Inst. Fourier (Grenoble) **54** (2004), no. 3, 499–630.

[2] Claude Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, C. R. Acad. Sci. Paris **212** (1941), 882–885.
[3] C. Chevalley and A. Weil, *Un théorème d'arithmétique sur les courbes algébriques*, Comptes Rendus Hebdomadaires des Séances de l'Acad. des Sci., Paris **195** (1930), 570–572.
[4] Jean-Louis Colliot-Thélène and Jean-Jacques Sansuc, *La descente sur les variétés rationnelles*, Journées de Géometrie Algébrique d'Angers, Juillet 1979/Algebraic Geometry, Angers, 1979, pp. 223–237, Sijthoff & Noordhoff, Alphen aan den Rijn—Germantown, Md., 1980.
[5] Jean-Louis Colliot-Thélène and Jean-Jacques Sansuc, *La descente sur les variétés rationnelles II*, Duke Math. J. **54** (1987), no. 2, 375–492.
[6] J.-L. Colliot-Thélène, A. N. Skorobogatov and Peter Swinnerton-Dyer, *Double fibres and double covers: paucity of rational points*, Acta Arith. **79** (1997), no. 2, 113–135.
[7] Gunther Cornelissen and Karim Zahidi, *Topology of Diophantine sets: remarks on Mazur's conjectures*, Contemp. Math. **270** (2000), 253–260.
[8] Martin Davis, Hilary Putnam, and Julia Robinson, *The decision problem for exponential diophantine equations*, Ann. of Math. (2) **74** (1961), 425–436.
[9] Kirsten Eisenträger, *Hilbert's tenth problem for algebraic function fields of characteristic 2*, Pacific J. Math. **210** (2003), no. 2, 261–281.
[10] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366. Erratum in Invent. Math. **75** (1984), 381. Translation: *Finiteness theorems for abelian varieties over number fields*, pp. 9–27 in: Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986.
[11] David Harari, *Weak approximation on algebraic varieties*, pp. 43–60 in: Arithmetic of higher-dimensional algebraic varieties (Palo Alto, CA, 2002), Progr. Math., **226**, Birkhäuser Boston, Boston, MA, 2004.
[12] David Harari and Alexei N. Skorobogatov, *Non-abelian cohomology and rational points*, Compositio Math. **130** (2002), no. 3, 241–273.
[13] Minhyong Kim, *The motivic fundamental group of* $\mathbb{P}^1 - \{0, 1, \infty\}$ *and the theorem of Siegel*, Invent. Math. **161** (2005), no. 3, 629–656.
[14] Minhyong Kim, *The non-abelian (or non-linear) method of Chabauty*, Noncommutative geometry and number theory, 179–185, Aspects Math., E37, Vieweg, Wiesbaden, 2006.
[15] Minhyong Kim and Akio Tamagawa, *The l-component of the unipotent Albanese map*, Math. Ann. **340** (2008), no. 1, 223–235.
[16] Minhyong Kim, *The unipotent Albanese map and Selmer varieties for curves*, Publ. Res. Inst. Math. Sci. **45** (2009), no. 1, 89–133.
[17] Y. I. Manin, *Le groupe de Brauer-Grothendieck en géométrie diophantienne*, Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 1, pp. 401–411, Gauthier-Villars, Paris, 1971.
[18] Yu. Matiyasevich, *The Diophantineness of enumerable sets*, Dokl. Akad. Nauk SSSR **191** (1970), 279–282.
[19] Barry Mazur, *The topology of rational points*, Experiment. Math. **1** (1992), no. 1, 35–45.
[20] B. Mazur, *Open problems regarding rational points on curves and varieties*, Galois representations in arithmetic algebraic geometry (Durham, 1996), London Math. Soc. Lecture Note Ser. **254**, Cambridge Univ. Press, Cambridge, 1998, pp. 239–265.
[21] Barry Mazur and Karl Rubin, *Ranks of twists of elliptic curves and Hilbert's Tenth Problem*, Preprint, 25 April 2009, arXiv:0904.3709.
[22] Emmanuel Peyre, *Points de hauteur bornée et géométrie des variétés (d'après Y. Manin et al.)*, Séminaire Bourbaki, Vol. 2000/2001, Astérisque **282** (2002), Exp. No. 891, ix, 323–344.
[23] Thanases Pheidas, *Hilbert's tenth problem for fields of rational functions over finite fields*, Invent. Math., **103** (1991), 1–8.
[24] Bjorn Poonen, *Existence of rational points on smooth projective varieties*, J. Eur. Math. Soc. (JEMS) **11** (2009), 529–543.

[25] Bjorn Poonen, *Undecidability in number theory*, Notices Amer. Math. Soc. **55** (2008), no. 3, 344–350.
[26] Bjorn Poonen, *Insufficiency of the Brauer-Manin obstruction applied to étale covers*, Preprint, 4 June 2008, to appear in Annals of Math.
[27] Alexandra Shlapentokh, *Hilbert's tenth problem for rings of algebraic functions in one variable over fields of constants of positive characteristic*, Trans. Amer. Math. Soc. **333** (1992), no. 1, 275–298.
[28] Alexei Skorobogatov, Torsors and rational points, Cambridge Tracts in Mathematics **144**, Cambridge University Press, 2001.
[29] Carlos R. Videla, *Hilbert's tenth problem for rational function fields in characteristic* 2, Proc. Amer. Math. Soc. **120** (1994), no. 1, 249–253.

Visibility of Sha in abelian surfaces

Nils Bruin
(joint work with Sander Dahmen, Kevin Doerksen)

We consider Mazur's [1] concept of visibility of Shafarevich-Tate groups $Ш(E/k)$ in abelian varieties A, in the situation where E is an elliptic curve over a number field k and A is an abelian surface. In this situation, one can essentially restrict to the situation where $A = E \times E'/\Delta$, where E and E' are elliptic curves with isomorphic n-torsion, and Δ is the graph of the isomorphism $\lambda : E[n] \to E'[n]$.

We recall some standard facts that relate Galois cohomology to the arithmetic properties of covers. Suppose that $\eta \in Ш(E/k)[n] \subset H^1(Gal(\overline{k}/k), E)$. From the cohomology of the short exact sequence $0 \to E[n] \to E \xrightarrow{[n]} E \to 0$, we deduce that we can represent η using $\delta \in H^1(Gal(\overline{k}/k), E[n])$. Such a class δ also represents a degree n^2 cover $C_\delta \to E$, which over $\overline{k}$ is isomorphic to the multiplication-by-n map $[n] : E \to E$. Many of the properties of η can be recovered from C_δ. We have that η is trivial if and only if C_δ has a rational point. The fact that $\eta \in Ш(E/k)[n]$ corresponds to C_δ having points everywhere locally.

Mazur suggests the following construction to arrive at a relatively explicit model of C_δ. Suppose one can find another elliptic curve E' with an isomorphism $\lambda : E[n] \to E'[n]$, such that $C_{\lambda_*(\delta)}$ does have a rational point. We can construct A as above. The quotient $B = A/E$ is isogenous to E' and C_δ will occur as a fibre of $A \to E'$ above a rational point of E'.

Mazur also proved [2] that for $n = 3$, one can always find a suitable elliptic curve E'. It is classical that in this case, any C_δ with points everywhere locally admits a smooth plane cubic model. There is a linear family of plane cubics that share the nine flexes of C_δ. These are exactly the $C_{\lambda_*(\delta)}$ referred to above. One can simply pick a rational point in the plane and choose the cubic that goes through that point and the nine flexes.

The elliptic curves E' obtained this way have *isometric* 3-torsion. This means that the isomorphism λ preserves the Weil-pairing. This means that the abelian varieties obtained this way are generally not principally polarized over $\mathbf{C}$ and hence not jacobians of genus 2 curves. We prove the following result.

Theorem. *Any 3-torsion element of* $Ш(E/k)$*, where* E *is an elliptic curve over a number field* k*, can be made visible in the jacobian of a curve of genus* 2*.*

The situation changes drastically for $n = 4$. Since the modular curve $X(4)$ is still of genus 0, there is still an ample supply of elliptic curves E' with isometric or anti-isometric 4-torsion. Let s be a parameter for the appropriate twist $X_E(4)$, let E'_s be the universal elliptic curve over $X_E(4)$ and let $C_{\delta,s} \to E_s$ be the corresponding cover. Over k, the curves $C_{\delta,s}$ describe a $K3$-surface. Therefore, the fact that a fibre of it over $X_E(4)$ has points everywhere locally, does not guarantee rational points on the surface (although in many practical cases, there are points).

If one is interested in making $Ш(E/k)[4]$ visible in a jacobian, a novel obstruction arises. Given E, one obtains an elliptic curve with anti-isometric 4-torsion by twisting with the discriminant of E. As it turns out, in order to obtain a suitable model of $C_{\lambda_*(\delta)}$ in this case, one needs to find a solution to a certain quartic norm equation that becomes a square upon adjuction of the square root of the discriminant of E. Such solutions turn out to generally not exist. This means that order 4 elements of $Ш(E/k)$ are almost never visible in jacobians of curves of genus 2.

References

[1] John E. Cremona, Barry Mazur, *Visualizing elements in the Shafarevich-Tate group.* Experiment. Math. **9** (2000), no. 1, 13–28.

[2] Barry Mazur, *Visualizing elements of order three in the Shafarevich-Tate group. Sir Michael Atiyah: a great mathematician of the twentieth century.* Asian J. Math. **3** (1999), no. 1, 221–232.

The reflection principle for 4–ranks of class groups

Jürgen Klüners

(joint work with Étienne Fouvry)

Let $d \in \mathbb{Z}$ be not a square number. We denote by C_d the narrow class group of the field $\mathbb{Q}(\sqrt{d})$. For a prime number p the p–rank of C_d is denoted by $\mathrm{rk}_p(\mathrm{C}_d) := \dim_{\mathbb{F}_p}(\mathrm{C}_d \,/\, \mathrm{C}_d^p)$. Furthermore we denote by $\mathrm{rk}_4(\mathrm{C}_d) := \mathrm{rk}_2(\mathrm{C}_d^2)$ the 4–rank of C_d.

In 1932 Scholz proved the Spiegelungssatz for 3–ranks:

Theorem 1 (Scholz, 1932 [7])**.** *Assume* $d > 1$*. Then*

$$\mathrm{rk}_3(\mathrm{C}_d) \le \mathrm{rk}_3(\mathrm{C}_{-3d}) \le \mathrm{rk}_3(\mathrm{C}_d) + 1.$$

In the same spirit we get the corresponding result for 4–ranks:

Theorem 2 (Damey-Payan, 1970 [2])**.** *Assume* $d > 1$*. Then*

$$\mathrm{rk}_4(\mathrm{C}_d) \le \mathrm{rk}_4(\mathrm{C}_{-4d}) \le \mathrm{rk}_4(\mathrm{C}_d) + 1.$$

Note that $\mathrm{C}_{-4d} = \mathrm{C}_{-d}$. There are also reflection theorems for $p \ge 5$, but in those cases the reflected field of a quadratic extension is not quadratic. We are interested in the following question:

How often is $\mathrm{rk}_4(\mathrm{C}_d) = \mathrm{rk}_4(\mathrm{C}_{-d})$?

We can also ask the corresponding question for the 3–rank. These questions are closely related to the behavior of the class groups of quadratic number fields. There are well know conjectures of Cohen and Lenstra how these class groups should behave. E.g. in [3] it was shown that the reflection principle and Conjecture 3 for 3–ranks are compatible.

We will cite the version in [1, 6] concerning the density of fundamental discriminants D such that $\mathrm{rk}_\ell(C_D^2) = r$ for a given integer $r \geq 0$.

Conjecture 3. *Let ℓ be a prime and $r \geq 0$. Then the density of fundamental discriminants D such that $\mathrm{rk}_\ell(C_D^2) = r$ is equal to*

- $\ell^{-r^2}\eta_\infty(\ell)\eta_r(\ell)^{-2}$ *for negative D's,*
- $\ell^{-r(r+1)}\eta_\infty(\ell)\eta_r(\ell)^{-1}\eta_{r+1}(\ell)$ *for positive D's,*

where we define

$$\eta_k(t) := \prod_{j=1}^{k}(1 - t^{-j}) \text{ for } k \in \mathbb{N} \text{ or } k = \infty.$$

We proved the following theorem in [4].

Theorem 4. *Let $\ell = 2$. Then Conjecture 3 is true all $r \geq 0$. Furthermore we get the same densities when we restrict the discriminants to the congruence classes $a \bmod q$, where $(a, q) \in \{(1, 4), (4, 8), (0, 8)\}$.*

By applying this theorem, we are able to completely answer the above question for the 4–rank. Let us denote by $A^-(X)$ the set of negative fundamental discriminants D bounded by X, i.e. $-D < X$. Then we can prove:

Theorem 5.

$$\lim_{X\to\infty} \frac{\#\{D \in A^-(X) \mid \mathrm{rk}_4(C_D) = \mathrm{rk}_4(C_{-D}) = r\}}{\#\{D \in A^-(X) \mid \mathrm{rk}_4(C_D) = r\}} = 2^{-r}.$$

Note that in the above theorem D is negative and $-D$ is positive. We are also able to derive the following result:

Theorem 6.

$$\lim_{X\to\infty} \frac{\#\{D \in A^-(X) \mid \mathrm{rk}_4(C_D) = \mathrm{rk}_4(C_{-D})\}}{\#\{D \in A^-(X)\}} = \sum_{r=0}^{\infty} 2^{-r}2^{-r^2}\eta_\infty(2)/\eta_r(2)^{-2}.$$

We remark that the number on the right hand side is about 0.61032. The proofs of these results can be found in [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] P. Damey and J–J. Payan, *Existence et construction des extensions galoisiennes et non–abéliennes de degré* 8 *d'un corps de caractéristique différente de* 2., J. für reine Angew. Math, **244**, (1970), 37–54.

[3] P. Dutarte, *Compatibilité avec le Spiegelungssatz de propabilités conjecturales sur le p–rang du groupe de classes.* Théorie des Nombres (Besançon), 1983 – 1984, Exp. No. 4, 11 pp., Publ. Math. Fac. Sci. Besançon, Univ. Franche-Comté, Besançon, 1984.
[4] É. Fouvry and J. Klüners, *On the 4–rank of class groups of quadratic number fields*, Inv. Math. **167**, (2007), 455–513.
[5] É. Fouvry and J. Klüners, *On the Spiegelungssatz for the* 4*–rank*, submitted.
[6] F. Gerth, III, *Extension of conjectures of Cohen and Lenstra*, Exposition. Math. **5(2)**, (1987) 181–184.
[7] A. Scholz, *Über die Beziehung der Klassenzahlen quadratischer Körper zueinander.* J. für reine Angew. Math.,**166**, (1932), 201–203.

Cycles on modular varieties and rational points on elliptic curves

Henri Darmon

This is a summary of a three-part lecture series given at the meeting on "Explicit methods in number theory" that was held in Oberwolfach from July 12 to 18, 2009. The theme of this lecture series was the explicit construction of algebraic points on elliptic curves from cycles on *modular varieties*. Given a fixed elliptic curve E over $\mathbb{Q}$, the goal is to better understand the group $E(\bar{\mathbb{Q}})$ of algebraic points on E by focusing on the following question:

Which points in $E(\bar{\mathbb{Q}})$ can be accounted for by a "modular construction"?

Heegner points arising from CM points on modular curves are the prototypical example of such a modular construction. While we do not dispose of a completely satisfactory general definition of modular points, fulfilling the conflicting requirements of flexibility and mathematical precision, several "test cases" that go beyond the setting of Heegner points have been studied over the last 10 years (cf. [Da01], [DL], [BDG], [Da04], [Tr], [Gre], [BDP2]). Three illustrative examples were touched upon in these lectures:

(1) [BDP1], [BDP2]. "Chow-Heegner points" arising from algebraic cycles on higher dimensional varieties. The existence and key properties of Chow-Heegner points are typically conditional on the Hodge or Tate conjectures on algebraic cycles.
(2) [DL], [BDG], [CD]. "Stark-Heegner points" arising from ATR ("Almost Totally Real") cycles on Hilbert modular varieties parametrising elliptic curves over totally real fields. These ATR cycles are not algebraic, and the expected algebraicity properties of the associated Stark-Heegner points do not seem (for now) to be part of a systematic philosophy.
(3) [Da01], [DP]. Stark-Heegner points attached to real quadratic cycles on the "mock Hilbert modular surface" $\mathbf{SL}_2(\mathbb{Z}[1/p])\backslash(\mathcal{H}_p \times \mathcal{H})$ parametrising an elliptic curve E over $\mathbb{Q}$ of prime conductor p. These real quadratic cycles are indexed by ideal classes of orders in a real quadratic field K, and are topologically isomorphic to $\mathbb{R}/\mathbb{Z}$. By an analytic process that combines complex and p-adic integration, they can be made to yield p-adic points on E which are expected to be defined over class fields of K.

This setting leads to convincing experimental evidence for the existence of a theory of "complex multiplication for real quadratic fields".

1. Heegner Points

We begin with a brief sketch of the classical picture which we aim to generalize.

Modular parametrisations. Let E be an elliptic curve over $\mathbb{Q}$, and let N be its conductor. The classical construction of Heegner points is based on the modularity theorem of [Wi], [TW], as completed in [BCDT]. It asserts that

$$L(E,s) = L(f,s), \tag{1}$$

where $f(z) = \sum a_n e^{2\pi i n z}$ is a cusp form of weight 2 on the Hecke congruence group $\Gamma_0(N)$. The modularity of E is established by showing that the p-adic Galois representation

$$V_p(E) = \left(\lim_{\leftarrow,n} E[p^n]\right) \otimes \mathbb{Q}_p = H^1_{\mathrm{et}}(\bar{E}, \mathbb{Q}_p)(1) \tag{2}$$

is a constituent of the first p-adic étale cohomology of the modular curve $X_0(N)$. The surjective $G_{\mathbb{Q}}$-equivariant projection of Galois representations

$$H^1_{\mathrm{et}}(\overline{X_0(N)}, \mathbb{Q}_p) \longrightarrow H^1_{\mathrm{et}}(\bar{E}, \mathbb{Q}_p) \tag{3}$$

gives rise to a non-trivial *Tate cycle*

$$\Pi_p \in H^2_{\mathrm{et}}(\overline{X_0(N) \times E}, \mathbb{Q}_p)(1)^{G_{\mathbb{Q}}}. \tag{4}$$

By the Tate conjecture for curves over number fields that was proved by Faltings, there is therefore a non-constant morphism over $\mathbb{Q}$

$$\Phi : J_0(N) \longrightarrow E, \tag{5}$$

where $J_0(N)$ is the Jacobian of $X_0(N)$. This stronger, "geometric" form of modularity is crucial for the Heegner point construction.

CM points. The modular curve $X_0(N)$ is equipped with a distinguished supply of 0-dimensional cycles $\mathrm{CM}_K \subset \mathrm{Div}^0(X_0(N)(K^{\mathrm{ab}}))$ attached to any imaginary quadratic field K. The group CM_K consists of degree zero divisors supported on CM points attached to the moduli of elliptic curves with complex multiplication by an order in K. It is not hard to show that $\Phi(\mathrm{CM}_K)$ is an infinitely generated subgroup of $E(K^{\mathrm{ab}})$; it will be referred to as the group of *Heegner points* on E attached to K. The importance of Heegner points can be justified on (at least) three grounds.

(1) The Gross-Zagier formula [GZ] relates the heights of certain points in $\Phi(\mathrm{CM}_K)$ to the central critical derivatives of the Hasse-Weil L-series of E over K, twisted by abelian characters of K, and thus supplies a link between the arithmetic of E and its Hasse-Weil L-series.
(2) Following a method of Kolyvagin (cf. [Gr2]), the non-triviality of certain Heegner points can be used to bound the Selmer group of E (and therefore, its rank and Shafarevich-Tate group). Combined with the Gross-Zagier

formula, this has led to the strongest known results on the Birch and Swinnerton-Dyer conjecture, most notably the theorem that

$$\mathrm{rank}(E(\mathbb{Q})) = \mathrm{ord}_{s=1} L(E,s) \text{ and } \#Ш(E/\mathbb{Q}) < \infty, \quad \text{when } \mathrm{ord}_{s=1}(L(E,s)) \leq 1.$$

(3) Heegner points can be computed efficiently in practice by analytic methods. After identifying the set $Y_0(N)(\mathbb{C})$ of complex points on the open modular curve with the quotient $\Gamma_0(N)\backslash\mathcal{H}$, and replacing $E(\mathbb{C})$ by the isogenous torus $\mathbb{C}/\Lambda_f$ for an appropriate period lattice Λ_f attached to f, one has

$$\Phi(\tau) = \int_{i\infty}^{\tau} 2\pi i f(z)dz = \sum_{n=1}^{\infty} \frac{a_n}{n} e^{2\pi i n\tau} \pmod{\Lambda_f}.$$

This formula leads to efficient algorithms for computing Heegner points numerically, which have been implemented in software systems like Pari-GP, Magma, and SAGE.

2. Chow-Heegner points

Chow Groups. Given a variety V of dimension d defined over a field F, let

$$\begin{aligned} \mathrm{CH}^j(V)(F) &= \left\{ \begin{array}{c} \text{Codimension } j \text{ algebraic cycles on } V \text{ over } F \\ \text{modulo rational equivalence} \end{array} \right\}, \\ \mathrm{CH}^j(V)_0(F) &= \text{the subgroup of null-homologous cycles.} \end{aligned}$$

Modular parametrisations. Any element Π of the Chow group $\mathrm{CH}^{d+1-j}(V \times E)(\mathbb{Q})$ induces homomorphisms

$$\Phi_F : \mathrm{CH}^j(V)_0(F) \longrightarrow E(F) \tag{6}$$

for any $F \supset \mathbb{Q}$, by the rule

$$\Phi_F(\Delta) := \pi_E(\pi_V^{-1}(\tilde{\Delta}) \cdot \tilde{\Pi}), \tag{7}$$

where π_V and π_E denote the natural projections from $V \times E$ to V and E respectively and $\tilde{\Delta}$ and $\tilde{\Pi}$ are representatives of the class of Δ and Π, chosen so that $\pi_V^{-1}(\tilde{\Delta})$ and $\tilde{\Pi}$ intersect transversally. The assignment $\Phi : F \mapsto \Phi_F$ is a natural transformation from $\mathrm{CH}^j(V)_0$ to E, viewed as functors on $\mathbb{Q}$-algebras. This leads to the following informal definition:

Definition 1. A *modular parametrisation* of E is a triple (V, Π, j) where

(1) V is a "modular variety" of dimension d;
(2) Π is a cycle class in $\mathrm{CH}^{d+1-j}(V \times E)(\mathbb{Q})$;
(3) the induced morphism $\Phi : \mathrm{CH}^j(V)_0 \longrightarrow E$ is *non trivial*.

The non-triviality condition on Φ merits some clarification. The most obvious notion of non-triviality is to require the existence of a cycle $\Delta \in \mathrm{CH}^j(V)_0(\bar{\mathbb{Q}})$ for

which $\Phi(\Delta)$ is non-zero in $E(\bar{\mathbb{Q}}) \otimes \mathbb{Q}$. A second notion rests on the fact that the correspondence Π induces a functorial map on deRham cohomology:

$$\Phi^*_{\mathrm{dR}} : H^1_{\mathrm{dR}}(E/\mathbb{Q}) \longrightarrow H^{2d-2j+1}_{\mathrm{dR}}(V/\mathbb{Q}).$$

The modular parametrisation Φ will be said to be non-trivial if the class of $\Phi^*_{\mathrm{dR}}(\omega_E)$ is non-zero, where ω_E is a non-zero regular differential on E. We will henceforth work with this cohomological notion of non-triviality.

Modular varieties. Definition 1 above falls short of being mathematically precise because we have not explained what is meant by "modular variety". Loosely speaking, such a variety is one which can be related to a Shimura variety in a reasonably direct way. For instance, a Shimura variety is a modular variety, as is the universal object or the r-fold fiber product of the universal object over a Shimura variety of PEL type. Examples include modular and Shimura curves, Kuga-Sato varieties, Hilbert modular varieties, Siegel modular varieties, Shimura varieties attached to the the orthogonal group $O(2, n)$ or the unitary group $U(p, q)$, etc. For the purposes of these lectures, the term "modular variety" is best interpreted informally in the broadest possible sense, as any variety whose cohomology is related to modular forms.

Chow-Heegner points. Modular varieties frequently contain a plentiful supply of arithmetically interesting algebraic cycles. The images in $E(\bar{\mathbb{Q}})$ of such special cycles under a modular parametrisation can be viewed as "higher-dimensional" analogues of Heegner points: they will be referred to as *Chow-Heegner points*.

The general program. Given an elliptic curve E, it would be of interest to construct modular parametrisations to E in the greatest possible generality, study their basic properties, and explore the relations (if any) between the resulting systems of Chow-Heegner points and values of L-series attached to E.

3. Generalised Heegner cycles

We flesh out the loosely formulated program of the previous paragraph in a simple but non-trivial setting, in which $E = A$ is an elliptic curve with complex multiplication by an imaginary quadratic field K, and V is a suitable family of $2r$-dimensional abelian varieties fibered over a modular curve. This construction (to which two of the lectures in the series ended up being devoted to) is part of a work in progress with Massimo Bertolini and Kartik Prasanna [BDP1], [BDP2].

The setting. Fix a quadratic imaginary field K, and let A be an elliptic curve with complex multiplication by the maximal order in K. In order to simplify the presentation of the main results, we make the following assumptions:

Assumption 2. (1) *The field K has class number one, unit group of order two, and odd discriminant. This implies that $D := -\mathrm{Disc}(K)$ is one of the following 6 primes:*

$$D = 7, 11, 19, 43, 67, \text{ or } 163.$$

(2) *The elliptic curve A is defined over $\mathbb{Q}$ and has conductor D^2.*

These assumptions are of course very restrictive; they are only made to ease the exposition, and the main results of [BDP1] and [BDP2] are obtained under more general conditions in which K is not assumed to have class number one.

Let $\epsilon_D : (\mathbb{Z}/D\mathbb{Z})^\times \longrightarrow \pm 1$ be the quadratic Dirichlet character of conductor D attached to K. Because A has complex multiplication, its modularity follows from the fact (known much before the work of Wiles, of course) that

$$L(A, s) = L(\psi, s),$$

where ψ is the Hecke character of K of infinity type $(1, 0)$ defined on (principal) ideals by the rule

$$\psi((a)) = \epsilon_D(a \bmod \sqrt{D})a.$$

The theta-series

$$\theta_\psi := \frac{1}{2}\sum_{a\in\mathcal{O}_K} \psi(a)q^{a\bar{a}} \in S_2(\Gamma_0(D^2)) \qquad (q = e^{2\pi i\tau})$$

is the weight two normalised eigenform of level D^2 attached to A.

Fix an integer $r \geq 0$, and consider the higher weight theta series

$$\theta_{\psi^{r+1}} := \frac{1}{2}\sum_{a\in\mathcal{O}_K} \psi(a)^{r+1}q^{a\bar{a}} = \sum_{n=1}^{\infty} a_n q^n \in \begin{cases} S_{r+2}(\Gamma_0(D^2)) \text{ if } r \text{ is even;} \\ S_{r+2}(\Gamma_0(D), \epsilon_K) \text{ if } r \text{ is odd.} \end{cases} \tag{8}$$

Set

$$\Gamma = \begin{cases} \Gamma_0(D) \text{ if } r \text{ is odd,} \\ \Gamma_0(D^2) \text{ if } r \text{ is even,} \end{cases}$$

and write C for the modular curve attached to Γ. Let W_r be the Kuga-Sato variety obtained by taking a canonical desingularisation of the r-fold fiber product

$$\mathcal{E} \times_C \mathcal{E} \times_C \cdots \times_C \mathcal{E}$$

of the universal (generalised) elliptic curve $\mathcal{E}$ over C. The locus $W_r^0 \subset W_r$ that lies over the open modular curve admits an explicit complex uniformisation

$$W_r^0(\mathbb{C}) = (\mathbb{Z}^{2r} \rtimes \Gamma)\backslash(\mathbb{C}^r \times \mathcal{H}).$$

The theta series $\theta_{\psi^{r+1}}$ has a geometric interpretation as a regular $(r+1)$-form on W_r given on $W_r^0(\mathbb{C})$ by

$$\omega_{\psi^{r+1}} = (2\pi i)^{r+1}\theta_{\psi^{r+1}}(\tau)dz_1 \cdots dz_r d\tau,$$

where $(z_1, \ldots, z_r, \tau)$ are the standard coordinates on $\mathbb{C}^r \times \mathcal{H}$. The q-expansion principle implies that

$$\omega_{\psi^{r+1}} \text{ belongs to } \Omega^{r+1}(W_r/\mathbb{Q}) = \mathrm{Fil}^{r+1} H^{r+1}_{\mathrm{dR}}(W_r/\mathbb{Q}).$$

The Deligne-Scholl motive associated to ψ^{r+1} corresponds to the piece of the $(r+1)$-st cohomology of W_r on which the nth Hecke correspondence T_n acts (for each n) as multiplication by the Fourier coefficient a_n of (8). It can be shown that the

étale realisations of this motive are isomorphic to a specific piece of the middle cohomology of A^{r+1}:

$$H^{r+1}_{\mathrm{et}}(\bar{W}_r, \mathbb{Q}_p)^{\theta_{\psi^{r+1}}} = H^{r+1}_{\mathrm{et}}(\bar{A}^{r+1}, \mathbb{Q}_p)^{\psi^{r+1}}.$$

This isomorphism gives a non-trivial Tate cycle

$$\Pi_p \in H^{2r+2}(\overline{W_r \times A^{r+1}}, \mathbb{Q}_p)(r{+}1)^{G_{\mathbb{Q}}}.$$

The existence of this Tate cycle suggests the following conjecture which is the basis for the definition of Chow-Heegner points on A.

Conjecture 3. *There is an algebraic cycle class* $\Pi^? \in \mathrm{CH}^{r+1}(W_r \times A^{r+1})(K) \otimes \mathbb{Q}$ *satisfying*

$$\Pi^{?*}_{\mathrm{dR}}([\omega_A^{r+1}]) \sim [\omega_{\psi^{r+1}}], \qquad \Pi^{?*}_{\mathrm{dR}}([\omega_A^j \bar{\omega}_A^{r+1-j}]) = 0, \qquad \text{for all } 1 \leq j \leq r,$$

where

$$\Pi^{?*}_{\mathrm{dR}} : H^{r+1}_{\mathrm{dR}}(A^{r+1}/\mathbb{C}) \longrightarrow H^{r+1}_{\mathrm{dR}}(W_r/\mathbb{C})$$

is the map on deRham cohomology induced by $\Pi^?$*, and the symbol* $\sim$ *denotes equality up to multiplication by a non-zero scalar of* $\mathbb{Q}^\times$*.*

Notice that the putative cycle $\Pi^?$ is also an element of $\mathrm{CH}^{r+1}(X_r \times A)$, where X_r is the $(2r{+}1)$-dimensional variety

$$X_r := W_r \times A^r.$$

Viewed in this way, the cycle $\Pi^?$ gives rise to a modular parametrisation

$$\Phi^? : \mathrm{CH}^{r+1}(X_r)_0 \longrightarrow A$$

defined over K. It is not hard to see that $\Phi^?$ is non-trivial. More precisely, a direct calculation reveals that

$$\Phi^{?*}_{\mathrm{dR}}(\omega_A) = \omega_{\psi^{r+1}} \wedge \eta_A^r, \tag{9}$$

where η_A is a suitably normalised class in $H^{0,1}_{\mathrm{dR}}(A/\mathbb{C})$. (The fact that A has complex multiplication implies that the class η_A can be chosen to belong to $H^1_{\mathrm{dR}}(A/K)$.)

Generalised Heegner cycles on X_r. The article [BDP1] introduces and studies a collection of null-homologous, r-dimensional algebraic cycles on X_r, referred to as *generalised Heegner cycles*. These cycles, which extend the notion of Heegner cycles on Kuga-Sato varieties considered in [Scho], [Ne] and [Zh], are indexed by isogenies $\varphi : A \longrightarrow A'$, and are defined over abelian extensions of K. The cycle Δ_φ attached to φ is essentially equal to the r-fold product of the graph of φ:

$$\Delta_\varphi := \epsilon_r(\mathrm{Graph}(\varphi)^r) \subset (A \times A')^r = (A')^r \times A^r \overset{(*)}{\subset} W_r \times A^r = X_r, \tag{10}$$

where the inclusion (*) arises by embedding $(A')^r$ in W_r as a fiber for the natural projection $W_r \longrightarrow C$. The projector ϵ_r that appears in (10) is a suitable idempotent in the ring of algebraic correspondences on X_r, which has the effect of making the cycle Δ_φ homologically trivial.

It can be shown, by adapting an argument of Schoen [Scho], that the cycles Δ_φ generate a subgroup of $\mathrm{CH}^{r+1}(X_r)_0(K^{\mathrm{ab}})$ of infinite rank. The conjectural map $\Phi^?_{K^{\mathrm{ab}}}$ sends these generalised Heegner cycles to points in $A(K^{\mathrm{ab}})$. The resulting collection

$$\{\Phi^?_{K^{\mathrm{ab}}}(\Delta_\varphi)\}_{\varphi:A\longrightarrow A'} \tag{11}$$

of Chow-Heegner points should generate an infinite rank subgroup of $A(K^{\mathrm{ab}})$, and should give rise to an "Euler system" in the sense of Kolyvagin. In the classical situation where $r = 0$, the variety X_r is just a modular curve and the existence of $\Pi^?$ follows from Faltings' proof of the Tate conjecture for curves. When $r \geq 1$, the very existence of the collection of Chow-Heegner points relies, ultimately, on producing the algebraic cycle $\Pi^?$ unconditionally.

Complex calculations. Since this is a workshop about explicit methods, we hasten to point out that even when the modular parametrisation $\Phi^?$ cannot be shown to exist, *it can still be computed efficiently in practice*, by complex analytic means.

The numerical calculation of $\Phi^?$ rests on the complex Abel-Jacobi map

$$\mathrm{AJ}_{X_r} : \mathrm{CH}^{r+1}(X_r)_0(\mathbb{C})\longrightarrow \frac{\mathrm{Fil}^{r+1}\, H^{2r+1}_{\mathrm{dR}}(X_r/\mathbb{C})^{\mathrm{dual}}}{\mathrm{Im}H_{2r+1}(X_r(\mathbb{C}),\mathbb{Z})} \tag{12}$$

of Griffiths and Weil, which is defined by the rule:

$$\mathrm{AJ}_{X_r}(\Delta)(\omega) = \int_{\tilde{\Delta}} \omega, \qquad \text{(for any } (2r{+}1)\text{-chain } \tilde{\Delta} \text{ with } \partial\tilde{\Delta} = \Delta). \tag{13}$$

This is a natural generalisation of the usual Abel-Jacobi map for elliptic curves:

$$\mathrm{AJ}_A : A(\mathbb{C}) = \mathrm{CH}^1(A)_0(\mathbb{C})\longrightarrow \frac{\Omega^1(A/\mathbb{C})^{\mathrm{dual}}}{\mathrm{Im}H_1(A(\mathbb{C}),\mathbb{Z})}, \tag{14}$$

which one recovers from (12) after replacing X_r by A and setting $r = 0$. The image of the Chow-Heegner point $\Phi^?(\Delta_\varphi)$ under the Abel-Jacobi map (14) is computed by noting that:

$$\mathrm{AJ}_A(\Phi^?(\Delta_\varphi))(\omega_A) = \mathrm{AJ}_{X_r}(\Delta_\varphi)(\Phi^{?*}_{\mathrm{dR}}(\omega_A)) = \mathrm{AJ}_{X_r}(\Delta_\varphi)(\omega_{\psi^{r+1}} \wedge \eta_A^r), \tag{15}$$

where the first equality follows from the functorial properties of the Abel-Jacobi maps, and the second follows from (9).

Let $N = D$ or D^2 (depending on whether r is odd or even) and let $\varphi : A\longrightarrow A'$ be an isogeny from A to some elliptic curve A'. Suppose that $A'(\mathbb{C})$ is described as $A' = \mathbb{C}/\langle 1, \tau\rangle$, and that $(A')^r$ is embedded in W_r as the fiber above the point of C corresponding to the pair $(\mathbb{C}/\langle 1, \tau\rangle, 1/N)$. Suppose also that

$$\varphi^*(2\pi i dz) = \omega_A,$$

where z is the standard coordinate on $\mathbb{C}/\langle 1, \tau\rangle = A'(\mathbb{C})$. The last expression in (15) can be calculated from the following proposition, which is established in [BDP1], Thm. 3.14:

Proposition 4. *Let $0 \leq j \leq r$ be an integer. For a complex isogeny φ as above, modulo the appropriate period lattice,*

$$\mathrm{AJ}_{X_r}(\Delta_\varphi)(\omega_{\theta_{\psi^{r+1}}} \wedge \omega_A^j \eta_A^{r-j}) = \frac{(-d_\varphi)^j (2\pi i)^{j+1}}{(\tau - \bar{\tau})^{r-j}} \int_{i\infty}^{\tau} (z-\tau)^j (z-\bar{\tau})^{r-j} \theta_{\psi^{r+1}}(z) dz.$$

Setting $j = 0$, we find that $\Phi_{\mathbb{C}}^? = \Phi_{\mathbb{C}}$, where

$$\Phi_{\mathbb{C}} : \mathrm{CH}^{r+1}(X_r)_0(\mathbb{C}) \longrightarrow A(\mathbb{C})$$

is given by the explicit formula

$$\Phi_{\mathbb{C}}(\Delta_\varphi) = \frac{2\pi i}{(\tau - \bar{\tau})^r} \int_{i\infty}^{\tau} (z-\bar{\tau})^r \theta_{\psi^{r+1}}(z) dz \pmod{\Lambda_A},$$

for an appropriate period lattice Λ_A attached to the elliptic curve A. Conjecture 3 on the existence of the modular parametrisation $\Phi^?$ implies the following explicit algebraicity statement:

Conjecture 5. *Let H be a subfield of K^{ab} and let $\Delta_\varphi \in \mathrm{CH}^{r+1}(X_r)_0(H)$ be a generalised Heegner cycle defined over H. Then (after fixing an an embedding of K^{ab} into $\mathbb{C}$),*

$$\Phi_{\mathbb{C}}(\Delta_\varphi) \text{ belongs to } A(H) \otimes \mathbb{Q},$$

and

$$\Phi_{\mathbb{C}}(\Delta_\varphi^\sigma) = \Phi_{\mathbb{C}}(\Delta_\varphi)^\sigma \quad \text{for all } \sigma \in \mathrm{Gal}(H/K).$$

While ostensibly weaker than Conjecture 3, Conjecture 5 has the virtue of being more readily amenable to experimental verification. A number of such verifications–which can be viewed as indirect numerical "tests" of the Tate conjectures for $W_r \times A^{r+1}$–are documented in [BDP2]. In these experiments, the complex points $\Phi_{\mathbb{C}}(\Delta_\varphi)$ attached to a few generalised Heegner cycles Δ_φ are calculated to high accuracy and recognized as algebraic points defined over the predicted class fields.

p-adic methods. Aside from such numerical explorations, the main theoretical evidence for the existence of the modular parametrisation $\Phi^?$ arises from p-adic methods.

If F is any field, then the Abel-Jacobi map admits an analogue in étale cohomology:

$$\mathrm{AJ}_F^{\mathrm{et}} : \mathrm{CH}^{r+1}(X_r)_0(F) \longrightarrow H^1(F, H_{\mathrm{et}}^{2r+1}(\bar{X}_r, \mathbb{Q}_p)(r+1)). \tag{16}$$

The image of the conjectural algebraic cycle $\Pi^?$ under the étale cycle class map is a Tate cycle

$$\Pi_{\mathrm{et}} \in H_{\mathrm{et}}^{2r+2}(\overline{X_r \times A}, \mathbb{Q}_p)(r+1)^{G_{\mathbb{Q}}},$$

which in turn gives rise to a surjective, $G_{\mathbb{Q}}$-equivariant projection

$$\pi_r : H_{\mathrm{et}}^{2r+1}(\bar{X}_r, \mathbb{Q}_p)(r+1) \longrightarrow H_{\mathrm{et}}^1(\bar{A}, \mathbb{Q}_p)(1) = V_p(A).$$

Applying π_r to the target of (16) gives a map

$$\pi_r \circ \mathrm{AJ}_F^{\mathrm{et}} : \mathrm{CH}^{r+1}(X_r)_0(F) \longrightarrow H_{\mathrm{Sel}}^1(F, V_p(A)), \tag{17}$$

where $H^1_{\mathrm{Sel}}(F, V_p(A))$ is the pro-p *Selmer group* of A over F. This Selmer group consists cohomology classes whose restrictions to each completion F_v of F belongs to the image of the local connecting homomorphism

$$\delta_v : (\lim_{\leftarrow} A(F_v)/p^n A(F_v)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \longrightarrow H^1(F_v, V_p(A))$$

arising from the p-power descent exact sequence of Kummer theory for A over F_v. When F is a global field, this is the "usual" pro-p Selmer group of A over F, and when F is a local field of residue characteristic p, the $\mathbb{Q}_p$-vector space $H^1_{\mathrm{Sel}}(F, V_p(A))$ is identified with the Lie algebra $A^1(F) \otimes \mathbb{Q}_p$ of the p-adic Lie group $A(F)$.

Remark: The system $\{\mathrm{AJ}^{\mathrm{et}}_{F_\varphi}(\Delta_\varphi)\}_\varphi$ (as φ ranges over all isogenies from A, and F_φ is the field of definition of φ) is an infinite collection of global cohomology classes defined over finite abelian extensions of K, satisfying various norm compatibility and Selmer conditions. This collection obeys (a simple variant of) the axioms of an Euler system, as they are spelled out in [Ru] for example.

In the case where F is a finite extension of $\mathbb{Q}_p$, equation (17) can be used to define a p-adic parametrisation

$$\Phi_F := \pi_r \circ \mathrm{AJ}^{\mathrm{et}}_F : \mathrm{CH}^{r+1}(X_r)_0(F) \longrightarrow A(F) \otimes \mathbb{Q},$$

which is a p-adic counterpart of the map $\Phi_{\mathbb{C}}$, is defined *independently* of the Hodge or Tate conjectures, and agrees with $\Phi^?_F$ when the latter exists. The main theorem of [BDP2] is the following p-adic analogue of Conjecture 5, which shows that the images of generalised Heegner points under Φ_F have the expected algebraicity properties, and can be related to the L-series of A. Assume for simplicity that the integer r is odd.

Theorem 6. *Let $p = \mathfrak{p}\bar{\mathfrak{p}}$ be a rational prime which splits in $K/\mathbb{Q}$. Let $H \subset K^{\mathrm{ab}}$ be a finite extension of $\mathbb{Q}$ which is unramified at p, let $\Delta \in \mathrm{CH}^{r+1}(X_r)_0(H)$ be a generalised Heegner cycle defined over this field, and let $H_{\mathfrak{p}} \supset H$ be the completion of H at a prime above $\mathfrak{p}$. Then*

$$\Phi_{H_{\mathfrak{p}}}(\Delta) \text{ belongs to } A(H) \otimes \mathbb{Q}.$$

In particular, the cycle $\Delta_1 \in \mathrm{CH}^{r+1}(X_r)_0(K)$ attached to the identity isogeny $1 : A \longrightarrow A$ maps to a rational point on $A(K) \otimes \mathbb{Q}$ under $\Phi_{K_{\mathfrak{p}}}$. This point is of infinite order if and only if

$$L(\psi^{2r+1}, r+1) \neq 0, \quad \text{and} \quad L'(\psi, 1) \neq 0.$$

The idea of the proof of Theorem 6 is to express the local points $\Phi_{H_{\mathfrak{p}}}(\Delta_\varphi)$ in terms of special values of the p-adic L-functions studied in [BDP1] which are attached to the Rankin convolution of $\theta_{\psi^{r+1}}$ with Hecke characters of K. The resulting formulae for the local points $\Phi_F(\Delta_\varphi)$ (for F any p-adic field over which Δ_φ can be defined) allows one to *compare* these points for different values of r, and thereby reduce the case $r > 0$ of Theorem 6 to the case $r = 0$, where it follows from the Tate conjecture for curves proved by Faltings.

The very possibility of such a proof reveals that the Chow-Heegner points constructed in this setting are not *genuinely new*, since they can ultimately be related to CM points on modular curves. The set-up involving the CM elliptic curve A and the variety X_r—a simple but non-trivial "toy model" for the notion of Chow-Heegner points—is perhaps most noteworthy for bringing the Hodge and Tate conjectures on algebraic cycles, which are notoriously difficult to test numerically, in the realm of "explicit methods".

4. ATR cycles

Of course, the hope is that higher-dimensional cycles will lead to points on E that cannot already be obtained by more classical approaches based on Heegner points. We will take a first step in this direction by considering certain *non-algebraic* cycles on Hilbert modular varieties.

The setting. Let F be a totally real field of degree $r+1$, and fix an ordering $v_0, v_1, \ldots, v_r$ of the r+1 distinct real embeddings of F. Let E be an elliptic curve over F, and let

$$E_j := E \otimes_{v_j} \mathbb{R} \qquad (0 \leq j \leq r)$$

be the r+1 elliptic curves over $\mathbb{R}$ obtained by taking the base change of E to $\mathbb{R}$ via the embedding v_j. To ease the exposition, we will make the following inessential assumptions:

(1) The field F has narrow class number one;
(2) the conductor of E/F is equal to 1 (i.e., E has everywhere good reduction).

Remark 7. These hypotheses, although very restrictive, are satisfied in some examples. For example, when $D = 29, 37$ and 41, the real quadratic field $F = \mathbb{Q}(\sqrt{D})$ has narrow class number one, and there is an elliptic curve E of conductor one over F. This elliptic curve cannot be defined over $\mathbb{Q}$, but it is isogenous to its Galois conjugate, and is a quotient of the Jacobian $J_1(D)$. The elliptic modular form thus associated to E belongs to $S_2(\Gamma_0(D), \epsilon_D)$, where ϵ_D is the quadratic Dirichlet character of conductor D attached to F.

In general, the modularity conjecture asserts that E gives rise to a *Hilbert modular form* f on $\mathbf{SL}_2(\mathcal{O}_F)$. Such a form is a holomorphic function on the product $\mathcal{H}_0 \times \mathcal{H}_1 \times \cdots \times \mathcal{H}_r$ of r+1 copies of the complex upper half plane, which is of parallel weight $(2, 2, \ldots, 2)$ under the action of the Hilbert modular group $\mathbf{SL}_2(\mathcal{O}_F)$. The latter group acts discretely on $\mathcal{H}_0 \times \cdots \times \mathcal{H}_r$ by Möbius transformations via the embedding

$$(v_0, \ldots, v_r) : \mathbf{SL}_2(\mathcal{O}_F) \longrightarrow \mathbf{SL}_2(\mathbb{R})^{r+1}.$$

Because of this trasformation property, the Hilbert modular form f can be interpreted geometrically as a holomorphic differential $(r+1)$-form on the complex analytic quotient

$$X(\mathbb{C}) := \mathbf{SL}_2(\mathcal{O}_F) \backslash (\mathcal{H}_0 \times \mathcal{H}_1 \times \cdots \times \mathcal{H}_r), \tag{18}$$

by setting

$$\omega_f^{\mathrm{hol}} := (2\pi i)^{r+1} f(\tau_0, \ldots, \tau_r) d\tau_0 \cdots d\tau_r.$$

This quotient in (18) is identified with the complex points of the (open) *Hilbert modular variety* X attached to $\mathrm{GL}(2)_{/F}$, but this algebraic structure will not be exploited in our construction of Stark-Heegner points attached to ATR cycles.

It will be useful to replace ω_f^{hol} by a closed, but non-holomorphic differential $(r{+}1)$-form ω_f on $X(\mathbb{C})$. When $r = 1$, the differential ω_f is defined by choosing a unit $\epsilon \in \mathcal{O}_F^\times$ of norm -1 satisfying

$$\epsilon_0 := v_0(\epsilon) > 0, \qquad \epsilon_1 := v_1(\epsilon) < 0,$$

and setting

$$\omega_f = (2\pi i)^2 \left(f(\tau_0, \tau_1) d\tau_0 d\tau_1 - f(\epsilon_0 \tau_0, \epsilon_1 \bar{\tau}_1) d\tau_0 d\bar{\tau}_1 \right).$$

For general r, one defines ω_f similarly, but this time summing over the subgroup of $\mathcal{O}_F^\times / (\mathcal{O}_F^+)^\times$ of cardinality 2^r consisting of units ϵ with $v_0(\epsilon) > 0$. Note that the closed $(r{+}1)$-form ω_f is holomorphic in τ_0, but only harmonic in the remaining variables $\tau_1, \ldots, \tau_r$. The justification for working with ω_f rather than ω_f^{hol} lies in the following statement which is a reformulation of a conjecture of Oda [Oda].

Conjecture 8 (Oda)**.** *Let*

$$\Lambda_f := \left\{ \int_\gamma \omega_f, \quad \gamma \in H_r(X(\mathbb{C}), \mathbb{Z}) \right\}.$$

Then Λ_f is a lattice in $\mathbb{C}$ and the elliptic curve $\mathbb{C}/\Lambda_f$ is isogenous to E_0.

This conjecture is known to hold for Hilbert modular forms which are base change lifts of classical elliptic modular forms. For example, in the setting of Remark 7, the Hilbert modular form attached to E is the Doi-Naganuma lift of an elliptic modular form in $S_2(\Gamma_1(D), \epsilon_D)$ and Conjecture 8 is known to hold in this case.

Let

$$\mathcal{Z}_r(X(\mathbb{C})) := \left\{ \begin{array}{c} \text{Null-homologous cycles} \\ \text{of real dimension } r \\ \text{on } X(\mathbb{C}) \end{array} \right\}.$$

Conjecture 8 makes it possible to define an "Abel-Jacobi map"

$$\mathrm{AJ}_f : \mathcal{Z}_r(X(\mathbb{C})) \longrightarrow E_0(\mathbb{C}), \tag{19}$$

by choosing an isogeny $\iota : \mathbb{C}/\Lambda_f \longrightarrow E_0(\mathbb{C})$, and setting

$$\mathrm{AJ}_f(\Delta) := \iota \left(\int_{\tilde{\Delta}} \omega_f \right), \qquad (\text{for any } \tilde{\Delta} \text{ with } \partial \tilde{\Delta} = \Delta). \tag{20}$$

Note that the domain $\mathcal{Z}_r(X(\mathbb{C}))$ of AJ_f has no natural algebraic structure, and that the map AJ_f bears no obvious relation (beyond an analogy in its definition) with the Griffiths-Weil Abel-Jacobi map on the Hilbert modular variety X.

ATR Cycles. A quadratic extension K of F is called an ATR extension if

$$K \otimes_{F, v_0} \mathbb{R} \simeq \mathbb{C}, \qquad K \otimes_{F, v_j} \mathbb{R} \simeq \mathbb{R} \oplus \mathbb{R}, \quad (1 \leq j \leq r).$$

The acronym ATR stands for "Almost Totally Real"; an ATR extension of F is "as far as possible" from being a CM extension, without being totally real.

Fix an ATR extension K of F, and let $\Psi : K \longrightarrow M_2(F)$ be an F-algebra embedding. Then

(1) Since $K \otimes_{F,v_0} \mathbb{R} \simeq \mathbb{C}$, the torus $\Psi(K^\times)$ has a unique fixed point $\tau_0 \in \mathcal{H}_0$.
(2) For each $1 \leq j \leq r$, the fact that $K \otimes_{F,v_j} \mathbb{R} \simeq \mathbb{R} \oplus \mathbb{R}$ shows that $\Psi(K^\times)$ has two fixed points τ_j and τ_j' on the boundary of $\mathcal{H}_j$. Let $\Upsilon_j \subset \mathcal{H}_j$ be the hyperbolic geodesic joining τ_j to τ_j'.

An embedding $\Psi : K \longrightarrow M_2(F)$ has a *conductor*, which is defined to be the unique $\mathcal{O}_F$-ideal c_Ψ for which

$$\Psi(K) \cap M_2(\mathcal{O}_F) = \Psi(\mathcal{O}_F + c_\Psi \mathcal{O}_K).$$

The $\mathcal{O}_F$-order $\mathcal{O}_\Psi := \mathcal{O}_F + c_\Psi \mathcal{O}_K$ is called the *order associated to* Ψ. By the Dirichlet unit theorem, the group

$$\Gamma_\Psi := \Psi((\mathcal{O}_\Psi^+)^\times) \subset \mathbf{SL}_2(\mathcal{O}_F)$$

is of rank r and preserves the region

$$R_\Psi := \{\tau_0\} \times \Upsilon_1 \times \cdots \times \Upsilon_r.$$

The ATR cycle associated to the embedding Ψ is defined to be the quotient

$$\Delta_\Psi := \Gamma_\Psi \backslash R_\Psi.$$

It is a closed cycle on $X(\mathbb{C})$ which is topologically isomorphic to an r-dimensional real torus. In many cases, one can show that Δ_Ψ is null-homologous, at least after tensoring with $\mathbb{Q}$. (This is the case, for instance, when $r = 1$, and it follows from the fact that the group cohomology $H^r(\mathbf{SL}_2(\mathcal{O}_F), \mathbb{C})$ is trivial.) Assume from now on that Δ_Ψ is homologically trivial, and therefore that it belongs to $\mathcal{Z}_r(X(\mathbb{C}))$.

The following conjecture lends arithmetic meaning to the Abel-Jacobi map AJ_f and to the ATR cycles Δ_Ψ.

Conjecture 9. *Let $\Psi : K \longrightarrow M_2(F)$ be an F-algebra embedding of an ATR extension K of F. Then the complex point $\mathrm{AJ}_f(\Delta_\Psi) \in E_0(\mathbb{C})$ is algebraic. More precisely, the isogeny ι in the definition (20) of AJ_f can be chosen so that, for all Ψ,*

$$\mathrm{AJ}_f(\Delta_\Psi) \text{ belongs to } E(H_{c_\Psi}),$$

where H_{c_Ψ} is the ring class field of K of conductor c_Ψ.

This conjecture has been tested numerically in [DL], for the three elliptic curves mentionned in Remark 7. A key ingredient in [DL] is the formulation of an efficient algorithm for calculating AJ_f numerically. This algorithm relies on group cohomology, and involves the manipulation of certain $(r+1)$-cochains on Γ which are defined by integrating ω_f over appropriate regions. The algorithm described in [DL] also exploits the fact that the real quadratic field $K = \mathbb{Q}(\sqrt{D})$ for $D = 29, 37$, and 41, is Euclidean. It would be of interest to have algorithms to calculate AJ_f in more general settings, particularly in cases where $r > 1$.

Conjecture 9 is poorly understood at present. For instance, it is not clear whether the Tate conjecture sheds any light on it. On the positive side, the ATR points that are produced by Conjecture 9 are "genuinely new" and go beyond what

can be obtained using only CM points on Shimura curves. Indeed, the former are defined over abelian extensions of ATR extensions of totally real fields, while the latter are defined over abelian extensions of CM fields.

5. Real quadratic cycles on $\mathbf{SL}_2(\mathbb{Z}[1/p])\backslash(\mathcal{H}_p \times \mathcal{H})$

The construction based on ATR cycles fails to cover some of the most basic settings where a modular construction might be expected to exist. The simplest non-trivial such setting arises when E is an elliptic curve over $\mathbb{Q}$ of prime conductor p, and K is a *real* quadratic field in which p is inert. In that case, a study of signs in functional equations reveals that

$$\mathrm{ord}_{s=1} L(E/H, s) \geq [H : K],$$

for any abelian extension H of K which is unramified at p and for which $\mathrm{Gal}(H/K)$ is isomorphic to a (generalised) dihedral group. (See the discussion in the introduction of [Da01] for example.) The Birch and Swinnerton-Dyer conjecture therefore predicts that

$$\mathrm{rank}(E(H)) \overset{?}{\geq} [H : K].$$

It is natural to ask whether this predicted systematic growth in Mordell-Weil rank can be accounted for by a modular construction.

Such a modular construction does appear to exist. It rests on the formal analogy between the Hilbert modular surface $\mathbf{SL}_2(\mathcal{O}_F)\backslash(\mathcal{H}_0 \times \mathcal{H}_1)$ (corresponding to the case $r = 1$ of the ATR construction described in the previous paragraph) and the quotient

$$\mathbf{SL}_2(\mathbb{Z}[1/p])\backslash(\mathcal{H}_p \times \mathcal{H}),$$

where $\mathcal{H}_p := \mathbb{P}_1(\mathbb{C}_p) - \mathbb{P}_1(\mathbb{Q}_p)$ is the p-adic upper half plane. Some of the terms that make up the analogy are listed in the table below.

ATR cycles	Real quadratic cycles
F real quadratic	$\mathbb{Q}$
v_0, v_1	p, ∞
Elliptic curve E/F of conductor 1	Elliptic curve $E/\mathbb{Q}$ of conductor p
$\mathbf{SL}_2(\mathcal{O}_F)\backslash(\mathcal{H}_0 \times \mathcal{H}_1)$	$\mathbf{SL}_2(\mathbb{Z}[1/p])\backslash(\mathcal{H}_p \times \mathcal{H})$
K/F ATR	$K/\mathbb{Q}$ real quadratic, with p inert
$\Psi : K \longrightarrow M_2(F)$	$\Psi : K \longrightarrow M_2(\mathbb{Q})$
$\langle\gamma\rangle := \Psi((\mathcal{O}_\Psi^+)^\times)$	$\langle\gamma\rangle := \Psi((\mathcal{O}_\Psi^+)^\times)$
$\Delta_\Psi = \{\tau_0\} \times (\Upsilon_1/\gamma), \quad \tau \in \mathcal{H}_0$	$\Delta_\Psi = \{\tau\} \times (\Upsilon_1/\gamma), \quad \tau \in \mathcal{H}_p.$
$\Downarrow \mathrm{AJ}_f$	$\Downarrow \mathrm{AJ}_f^{(p)}$
Points in $\mathbb{C}/\Lambda_f = E_0(\mathbb{C})$, defined over abelian extensions of K	Points in $K_p^\times/q^{\mathbb{Z}} = E(K_p)$, defined over abelian extensions of K.

The "real quadratic cycles" Δ_Ψ in $\mathbf{SL}_2(\mathbb{Z}[1/p])\backslash(\mathcal{H}_p \times \mathcal{H})$ are topologically isomorphic to $\mathbb{R}/\mathbb{Z}$, and $\mathrm{AJ}_f^{(p)}(\Delta_\Psi)$ belongs to $K_p^\times/q^{\mathbb{Z}} = E(K_p)$, where $q \in \mathbb{Q}_p^\times$ is the p-adic Tate period of E. Since the symmetric space $\mathcal{H}_p \times \mathcal{H}$ mixes a rigid analytic topology on the first factor with a complex analytic topology on the second, one cannot define $\mathrm{AJ}_f^{(p)}$ by directly integrating an appropriate differential on a two-dimensional region having Δ_Ψ as boundary, as in equation (20) defining AJ_f. The main steps that make it possible to define the p-adic analogue of AJ_f are:

(1) To reinterpret the elliptic modular form $f \in S_2(\Gamma_0(p))$ attached to E as a "mock Hilbert modular form" on $\mathbf{SL}_2(\mathbb{Z}[1/p])\backslash\mathcal{H}_p \times \mathcal{H}$. This reinterpretation gives a precise meaning to certain 2-cochains on Γ with values in $\mathbb{C}_p^\times$ which are the direct p-adic analogues of the corresponding cochains considered in the ATR setting in the algorithms of [DL].
(2) With these cochains in hand, the algorithms of [DL] can be precisely mimicked, yielding invariants $\mathrm{AJ}_f^{(p)}(\Delta_\Psi) \in K_p^\times/q^{\mathbb{Z}}$.

For more details on this construction, and the precise definition of $\mathrm{AJ}_f^{(p)}$, see [Da01], [Da04]. The article [DP] describes the most efficient algorithms for computing the Stark-Heegner points $\mathrm{AJ}_f^{(p)}(\Delta_\Psi)$ attached to real quadratic fields. These algorithms have been implemented in MAGMA and can be downloaded from the web site

http://www.math.mcgill.ca/darmon/programs/shp/shp.html

References

[BCDT] Breuil, C., Conrad, B., Diamond, F., and Taylor, R., *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises.* J. Amer. Math. Soc. 14 (2001), no. 4, 843–939.

[BDG] Bertolini, M., Darmon, H., and Green, P. *Periods and points attached to quadratic algebras.* Heegner points and Rankin L-series, 323–367, Math. Sci. Res. Inst. Publ., 49, Cambridge Univ. Press, Cambridge, 2004.

[BDP1] Bertolini, M., Darmon, H., and Prasanna, K. *Generalised Heegner cycles and p-adic Rankin L-series*, submitted.

[BDP2] Bertolini, M., Darmon, H., and Prasanna, K., *Chow-Heegner points on CM elliptic curves and values of p-adic L-series*, in progress.

[CD] Charollois, P., Darmon, H. *Arguments des unités de Stark et périodes de séries d'Eisenstein.* Algebra Number Theory 2 (2008), no. 6, 655–688.

[Da01] Darmon, H., *Integration on* $\mathcal{H}_p \times \mathcal{H}$ *and arithmetic applications.* Ann. of Math. (2) 154 (2001), no. 3, 589–639.

[Da04] Darmon, H. Rational points on modular elliptic curves. CBMS Regional Conference Series in Mathematics, 101. Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 2004. xii+129 pp.

[Da06] Darmon, H., *Heegner points, Stark-Heegner points, and values of L-series.* International Congress of Mathematicians. Vol. II, 313–345, Eur. Math. Soc., Zürich, 2006.

[DG] Darmon, H., Green, P. Elliptic curves and class fields of real quadratic fields: algorithms and evidence. Experiment. Math. 11 (2002), no. 1, 37–55.

[DL] Darmon, H. and Logan, A. *Periods of Hilbert modular forms and rational points on elliptic curves.* Int. Math. Res. Not. 2003, no. 40, 2153–2180.

[DP] Darmon, H., Pollack, R. *Efficient calculation of Stark-Heegner points via overconvergent modular symbols*. Israel J. Math. 153 (2006), 319–354.
[Gre] Greenberg, Matthew. *Stark-Heegner points and the cohomology of quaternionic Shimura varieties*. Duke Math. J. 147 (2009), no. 3, 541–575.
[Gr2] Gross, B.H., *Kolyvagin's work on modular elliptic curves*. in L-functions and arithmetic (Durham, 1989), 235–256, London Math. Soc. Lecture Note Ser., 153, Cambridge Univ. Press, Cambridge, 1991.
[GZ] Gross, Benedict H. and Zagier, Don B. *Heegner points and derivatives of L-series*. Invent. Math. 84 (1986), no. 2, 225–320.
[Ne] Nekovar, Jan. *On the p-adic height of Heegner cycles*. Math. Ann. 302 (1995), no. 4, 609–686.
[Oda] Oda, Takayuki. Periods of Hilbert modular surfaces. Progress in Mathematics, 19. Birkhuser, Boston, Mass., 1982.
[Ru] Rubin, K., Euler systems. Annals of Mathematics Studies, 147. Hermann Weyl Lectures. The Institute for Advanced Study. Princeton University Press, Princeton, NJ, 2000. xii+227 pp.
[Scho] Schoen, Chad. *Complex multiplication cycles on elliptic modular threefolds*. Duke Math. J. 53 (1986), no. 3, 771–794.
[Tr] Trifkovic, M., *Stark-Heegner points on elliptic curves defined over imaginary quadratic fields*, Duke Math. J. 135 (2006), no. 3, 415–453.
[TW] Taylor, Richard; Wiles, Andrew Ring-theoretic properties of certain Hecke algebras. Ann. of Math. (2) 141 (1995), no. 3, 553–572.
[Wi] Wiles, A., *Modular elliptic curves and Fermat's last theorem*. Ann. of Math. (2) 141 (1995), no. 3, 443–551.
[Zh] Zhang, Shouwu. *Heights of Heegner cycles and derivatives of L-series*. Invent. Math. 130 (1997), no. 1, 99–152.

Computing Frobenius elements in Galois groups

Tim Dokchitser
(joint work with Vladimir Dokchitser)

Suppose $f(t) \in \mathbb{Z}[t]$ is a polynomial of degree n. Write $\alpha_i \in \mathbb{C}$ for its roots,

$$K = \mathbb{Q}(\alpha_1, ..., \alpha_n)$$

for the splitting field and $G = \mathrm{Gal}(K/\mathbb{Q}) \subset S_n$ for the Galois group. At almost all primes p (e.g. those not dividing the discriminant Δ_f of f) there is a well-defined conjugacy class in G, the *class of Frobenius* $[\mathrm{Frob}_p]$.

Problem. *Suppose we are given f, and we know its Galois group G as a permutation group in S_n. How to compute* Frob_p *at a given prime p?*

In the 'maximal' case $G = S_n$ the conjugacy classes in G are in one-to-one correspondence with possible cycle types of n-cycles. Then the (well-known) solution is to factor $\bar{f} = f \mod p$, and the degrees of the irreducible factors determine the cycle type. On the other hand, if G is e.g. alternating or dihedral, the situation is more subtle as the cycle type does not determine the conjugacy class uniquely. For example in A_5 there are two conjugacy classes of 5-cycles, so when $f \mod p$ is irreducible it is not clear which one of them is $[\mathrm{Frob}_p]$.

This problem has been studied by Serre and Buhler for A_5 and generalized by Roberts for A_n, and the solution is that the values of the square root of the discriminant of f distinguish the conjugacy classes.

In this joint work, we try to address the problem for a general group $G \subset S_n$. The idea is as follows:

Suppose G has several conjugacy classes with the same cycle type, and fix $g_0 \in S_n$ of this type.

Pick a polynomial $F \in \mathbb{Q}[x_1, ..., x_n]$ and compute, say, the set of all possible values $F(\sigma(\underline{\alpha})) \in K$ for $\sigma \in S_n$, i.e. the values of F on all permutations of the roots. The group G acts on this set, and write $m_1(x), ...m_t(x) \in \mathbb{Z}[x]$ for the minimal polynomials of these values. Now suppose $\bar{f}$ factors according to our cycle type. Compute the roots of $\bar{f}$,

$$\bar{f}(x) = (x - \beta_1) \cdots (x - \beta_n) \in \bar{\mathbb{F}}_p[x],$$

choosing the ordering of β_j in such a way that Frobenius $x \mapsto x^p$ acts on them as g_0. Then $F(\beta)$ is a root of one (and in general only one) of the reductions of the polynomials m_j. If we are lucky, the index j determines the conjugacy class uniquely, in which case we found the Frobenius class.

For instance, for $G = A_n \subset S_n$,

$$F = \prod_{1 \le i < j \le n} (x_i - x_j)$$

can take two distinct values $\pm\sqrt{\Delta_f}$ on the permutations of the roots α_j, both rational. In this case $m_1 = x - \sqrt{\Delta_f}$ and $m_2 = x - \sqrt{\Delta_f}$. Now

$$\prod_{1 \le i < j \le n} (\beta_i - \beta_j)$$

is a root of either m_1 or m_2, and this precisely determines the conjugacy class of Frobenius at p.

For general G, whether or not this method works or not for a given F turns out to be a purely group-theoretic question about subgroups of S_n. I discussed several reasonable choices for these subgroups and the invariants F, and the efficiency of the algorithms that they lead to. In particular, the method does work efficiently for cyclic, dihedral and alternating groups.

On the extremality of an 80-dimensional lattice

Mark Watkins

Joint work with Zachary Abel, Steve Donnelly, Noam D. Elkies, Scott Kominers, and Damien Stehlé.

We show the extremality of a specific even unimodular 80-dimensional lattice. This lattice comes about by a general construction of Quebbemann [2] and is specifically derived by Schulze-Pillot [4]. It has an automorphism group that contains $\mathbf{SL}_2(\mathbf{F}_{79})$, which comes about naturally via a relation to coding theory. It was the "first candidate" for an extremal lattice of dimension 80, though Bachoc

and Nebe [1] found two others (with automorphism group related to that of the Mathieu group M_{22}) for which it proved easier to show extremality. Our method of showing extremality (which means that the minimum length of a nonzero vector is 8) is to use the positivity of the Θ-series of the lattice, and find all 7541401190400 vectors of norm 10. This idea was previously used by Abel, Elkies, and Kominers in exploring similar questions in dimension 72.

The lattice can be described as a sublattice of the direct sum of two lattices. One of these is simply a 2-dimensional lattice M_2 with determinant p. The other is a 78-dimensional lattice constructed from $E = \mathbf{Q}(\zeta_{79})$. Here we take an ideal $\mathfrak{A} \subseteq O_E$ such that $\mathfrak{A}\bar{\mathfrak{A}} = (d)$ with $d \in E^+$ totally positive. This ideal induces a (positive definite) lattice U_{78} of dimension 78 via a basis for the ring of integers $\mathbf{Z}[\zeta_{79}]$, with the quadratic form given by $Q_1(u) = \mathrm{tr}_{\mathbf{Q}}^E(u\bar{u}d^{-1})$. A computation with the different gives the determinant to be 79^{77}.

Writing $Q_0(m)$ for the quadratic form on M_2, we then take the sublattice of index p of $M_2 \oplus U_{78}$ given by the pairs (m, u) such that $Q_0(m) + Q_1(u)$ is a multiple of 79. A calculation with projection maps shows that this subset is indeed actually a sublattice. The determinant here is $79 \cdot 79^{77} \cdot 79^2$, and every vector has norm divisible by 79; upon dividing this lattice by 79, we thus obtain an integral unimodular lattice of dimension 80. It will be even when Q_0 is even.

Schulze-Pillot relates this construction to coding theory, from which one can more easily obtain the automorphism group. However, he chooses Q_0 to be odd for simplicity on that side of the argument, and then has to pass to an even lattice via Kneser's neighbouring argument. He works in $K = \mathbf{Q}(\sqrt{-79})$, and takes $d = 19$ as an auxiliary prime that splits in K, which gives $\mathfrak{A}$ by passing up to E. The import of $d = 19$ here is its location in the class group of K; we could obtain five distinct (even) lattices by this method, one for each ideal class.

The relation to coding theory then allows Schulze-Pillot to find a scaled root system (of type $80A_1$, that is, 80 vectors all of the same norm that are mutually orthogonal) in the lattice, from which a standard construction yields a unimodular lattice whose automorphism group contains $\mathbf{SL}_2(\mathbf{F}_{79})$. A calculation shows this to be identical to our lattice, and as mentioned above, a 2-neighbour of this is our candidate for an even unimodular extremal lattice in dimension 80.

We now turn to showing that this lattice is extremal, that is, that it has no vectors of norm 2, 4, or 6. One can make a direct argument to show that neither of the first two possibilities occur. For vectors of norm 6, we use the Θ-series of the lattice. This is a modular form of weight 40 and level 1. The space of such modular forms has dimension 4, and a triangular basis is

$$\begin{aligned}
f_0 &= 1 + 1250172000q^4 + 7541401190400q^5 + O(q^6),\\
f_1 &= q + 19291168q^4 + 37956369150q^5 + O(q^6),\\
f_2 &= q^2 + 156024q^4 + 57085952q^5 + O(q^6),\\
f_3 &= q^3 + 168q^4 - 12636q^5 + O(q^6).
\end{aligned}$$

We know that $\Theta_{80} = f_0 + a_1 f_1 + a_2 f_2 + a_3 f_3$ for some integers a_i, and as noted above, can show that $a_1 = a_2 = 0$ directly. So we can write

$$\Theta_{80} = 1 + a_3 q^3 + (\cdots) q^4 + (7541401190400 - 12636 a_3) q^5 + O(q^6),$$

and by positivity we have $a_3 \geq 0$. By finding 7541401190400 vectors of norm 10 in the lattice, we will show that $a_3 = 0$, which in turn implies that the lattice is extremal as claimed.

The capability to find all vectors of norm 10 is made possible via use of the automorphism group, which reduces the problem by a factor of about 492960 (its order). Contrariwise, a search for vectors of length 6 would take much longer, as such a search must be exhaustive.

Upon cataloguing vectors with nontrivial stabiliser (of which there are 483 orbits of vectors of norm 10, most with stabiliser of size 3), we are left to find 15298043 orbits (of norm 10) with nontrivial stabiliser. A probabilistic analysis of the situation (which turns out to be the same as that for the "coupon-collecting" problem) leads us to a harmonic sum, and so we estimate that about 250 million vectors of norm 10 will need to be generated to hit each orbit at least once, at least if the vectors found are suitably random.

We then used the standard lattice vector searching algorithms, augmented by an idea of pruning. The idea here, first mentioned by Schnorr and Hörner [3], is to truncate the hyperspheres (or hyperellipsoids) in which the iterative search is performed, as locations closer to boundaries are somewhat less likely to contain lattice points. Viewed in a different way, pruning demands that the first coordinates considered (in the Gram-Schmidt basis) be small in size, as the latter coordinates will also need to be small if a sufficiently short vector is to be found. Furthermore, by periodically switching the lattice basis via a small perturbation, we can reduce ourselves to only searching in the first 60 or so (of 80) layers of the pruning tree (with but one choice, the most central, being considered for the final coordinates), and this also has a noticeable impact on the number of norm 10 vectors found per unit time. In this idea, we again exploit the irrelevance of exhaustivity.

Changing the basis is not totally cost-free, as lattice reduction must be applied to the new perturbed basis (this takes 2-3 minutes). However, due to the large dimension of the problem, it is unlikely that LLL will return an identical reduced basis to one that had previously been found via such randomisation. Also, all such bases should be similar in their enumeration efficacy.

In practise, we switched the basis every 10^5 vectors, which typically took about 20-30 minutes to find. Our whole run took about 2 cpu-months, or about 4 days of real time on 12-16 CPUs, due to the obvious parallelisation of running a different basis on each CPU. Without pruning, our estimate is that it would have taken about 1000 times longer (or more). We did indeed find the expected 15298043 free orbits of norm 10 vectors, and conclude that the lattice is thus extremal.

References

[1] C. Bachoc, G. Nebe, *Extremal lattices of minimum 8 related to the Mathieu group M_{22}*. J. Reine Angew. Math. **494** (1998), 155–171.

[2] H.-G. Quebbemann, *Zur Klassifikation unimodularer Gitter mit Isometrie von Primzahlordnung.* (German) [On the classification of unimodular lattices with an isometry of prime order]. J. Reine Angew. Math. **326** (1981), 158–170.
[3] C. P. Schnorr and H. H. Hörner, *Attacking the Chor-Rivest cryptosystem by improved lattice reduction.* In *Advances in Cryptology – EUROCRYPT 1995*, Lecture Notes in Computer Science **921**, Springer-Verlag, Berlin (1995), 1–12.
[4] R. Schulze-Pillot, *Quadratic residue codes and cyclotomic lattices.* Arch. Math. (Basel) **60** (1993), no. 1, 40–45.

Intersecting curves on a torus

Arjen Stolk

This talk is about a problem in algebraic geometry that arises when studying certain questions of discrete tomography. Tomography is concerned with reconstructing images from sets of projections.

The images we consider are finite sets of numbers placed on a square lattice. The space of such images can be represented by the Laurent polynomial ring $\mathbb{Q}[u, u^{-1}, v, v^{-1}]$. The monomials represent grid positions, the coefficients the numbers placed at these positions.

The projections are made as follows. For a finite set of distinct directions, take the sum of the numbers placed on the points along each straight line in that direction. The ring homomorphism

$$\sigma_{a,b} : \mathbb{Q}[u, u^{-1}, v, v^{-1}] \longrightarrow \mathbb{Q}[w, w^{-1}]$$

sending u to w^{-b} and v to w^a precisely identifies those monomials which are on the same line in direction (a, b). For a finite set of directions one considers the map

$$\sigma : \mathbb{Q}[u, u^{-1}, v, v^{-1}] \longrightarrow \mathbb{Q}[w, w^{-1}]^n,$$

where $\sigma = (\sigma_{a_1,b_1}, \ldots, \sigma_{a_n,b_n})$.

Of interest is the computation of linear *dependencies* between the line sums of images. These are linear maps $d : \mathbb{Q}[w, w^{-1}]^n \to \mathbb{Q}$ such that $d \circ \sigma = 0$, i.e. linear combinations of the line sums that are zero for all images. The space of such dependencies is $\mathrm{Hom}(\mathrm{cok}(\sigma), \mathbb{Q})$. Satisfying all dependencies is clearly necessary for a vector of line sums to come from an image. One can show that it is also sufficient. Thus the dependencies provide a way to identify which line sums arise from images.

Geometrically, the map $\sigma_{a,b}$ embeds a one-dimensional torus as a closed subgroup of a two-dimensional torus. The map σ takes a disjoint union of such one-dimensional tori and maps it to their union inside the two-dimensional torus. From this it is clear that the cokernel, which measures the difference between the rings of functions of these objects, consists of local contributions coming from the intersection points of the one-dimensional tori.

These intersection points can be explicitly computed for any given set of directions. Each local contribution can then also be described explicitly by locally 'taking logarithms', which turns the problem into some finite linear algebra. When

combined these provide an explicit way to compute generators for the space of dependencies.

Algorithms for automorphic forms on Shimura curves

John Voight

Modular symbols allow a detailed investigation of classical modular forms. Automorphic forms on more general Shimura varieties have proved no less interesting to study, and yet many aspects of the theory are not as well understood. In joint work with Matthew Greenberg, we describe below an algorithm to compute automorphic forms on Shimura curves working with explicit group cohomology; via the Jacquet-Langlands correspondence, these methods also allow the computation of Hilbert modular forms over totally real fields of odd degree. Remarkably, our methods work without reference to cusps or a canonical moduli interpretation of the Shimura curve, as these features of the classical situation are absent.

Let F be a totally real field of degree $n = [F : \mathbb{Q}]$ and let $\mathbb{Z}_F$ denote its ring of integers. Let $S_2(\mathfrak{N})$ denote the Hecke module of (classical) Hilbert modular cusp forms over F of parallel weight 2 and level $\mathfrak{N} \subset \mathbb{Z}_F$. Our main result is as follows.

Theorem. *There exists an algorithm which, given a totally real field F of strict class number 1 and odd degree n, and an ideal $\mathfrak{N}$ of $\mathbb{Z}_F$, computes the system of Hecke eigenvalues associated to Hecke eigenforms in the space $S_2(\mathfrak{N})$ of Hilbert modular forms of parallel weight 2 and level $\mathfrak{N}$.*

We now sketch the method of the above algorithm. Let B be the quaternion algebra ramified at all but one real place of F and at no finite place. Let $\mathcal{O}$ be an Eichler order of level $\mathfrak{N}$, let $\mathcal{O}_1^*$ denote the units of norm 1 in $\mathcal{O}$, and let $\Gamma = \Gamma_0^B(\mathfrak{N}) = \mathcal{O}_1^*/\{\pm 1\}$. Let $S_2^B(\mathfrak{N})$ denote the space of modular forms of weight 2 on the Shimura curve $X = X_0^{\mathfrak{D}}(\mathfrak{N})$ associated to $\mathcal{O}$. By the Jacquet-Langlands correspondence, there is an isomorphism

$$S_2^B(\mathfrak{N}) \xrightarrow{\sim} S_2(\mathfrak{N})$$

of Hecke modules.

Note this is only possible when n has *odd* degree, since the number of ramified places of B must be even. When n has even degree, Jacquet-Langlands relates the space $S_2(\mathfrak{N})$ to a space of modular forms on a zero-dimensional Shimura variety, corresponding to a definite quaternion algebra; this avenue has been pursued by Dembélé and his coauthors.

We compute with these spaces in cohomology, by using the analogue of the Eichler-Shimura theorem: there is an isomorphism of Hecke modules

$$H^1(\Gamma_0^{\mathfrak{D}}(\mathfrak{N}), \mathbb{C}) \xrightarrow{\sim} S_2^B(\mathfrak{N}) \oplus \overline{S_2^B(\mathfrak{N})},$$

where $\overline{\ }$ denotes complex conjugation. The group $H^1(\Gamma, \mathbb{Q}) = \mathrm{Hom}(\Gamma, \mathbb{Z})$ is 'just' group cohomology: it is a free $\mathbb{Z}$-module of rank $2g$, where g is the genus of X.

The above results extend to higher weight k by an appropriate modification of the coefficient module.

The Hecke operators act on $H^1(\Gamma, \mathbb{Z})$ via double cosets as follows. Let $\mathfrak{l} \subset \mathbb{Z}_F$ be a prime and choose a splitting $\iota_\mathfrak{l} : \mathcal{O} \hookrightarrow M_2(\mathbb{Z}_{F,\mathfrak{l}})$. For $(x : y) \in \mathbb{P}^1(\mathbb{F}_\mathfrak{l})$, let $\lambda_{(x:y)} \in \mathcal{O}$ be an element such that

$$\iota_\mathfrak{l}(\lambda_{(x:y)}) \equiv \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \pmod{\mathfrak{l}}$$

and the reduced norm of $\lambda_{(x:y)}$) is a totally positive generator of $\mathfrak{l}$.

Then for $f \in H^1(\Gamma, \mathbb{Z})$, we define $f \mid T_\mathfrak{l} : \Gamma \to \mathbb{Z}$ as follows: for all $\gamma \in \Gamma$ and $a \in \mathbb{P}^1(\mathbb{F}_\mathfrak{l})$, there is a unique $b \in \mathbb{P}^1(\mathbb{F}_\mathfrak{l})$ and $\delta_a \in \Gamma$ such that

$$\lambda_a \gamma = \delta_a \lambda_b.$$

We then define

$$(f \mid T_\mathfrak{l})(\gamma) = \sum_{a \in \mathbb{P}^1(k_\mathfrak{l})} f(\delta_a).$$

Therefore, to effectively compute systems of Hecke eigenvalues on $S_2^{\mathfrak{D}}(\mathfrak{N})$, we need algorithms to:

(1) Compute an explicit finite presentation of Γ;
(2) Compute a generator (with totally positive norm) of a left ideal $I \subset \mathcal{O}$; and
(3) Given $\delta \in \Gamma$, write δ as an explicit word in the generators for Γ, i.e., solve the word problem in Γ.

In Problem 3, we are really finding a replacement for the *Manin trick* for modular symbols, which gives a kind of substitute for the Euclidean algorithm in this context.

We address Problems 1 and 3 by the computation of a fundamental domain. Let $p \in \mathcal{H}$ be a point with trivial stabilizer $\Gamma_p = \{1\}$. We define the *Dirichlet domain* centered at p to be

$$D(p) = \{z \in \mathcal{H} : d(z, p) \leq d(gz, p) \text{ for all } g \in \Gamma\}.$$

The set $D(p)$ is a closed, connected, and hyperbolically convex fundamental domain whose boundary consists of finitely many geodesic segments. The key result is then as follows:

Proposition. *There exists an algorithm which, given Γ and $p \in \mathcal{H}$, returns the Dirichlet domain $D(p)$, a finite presentation for Γ with a minimal set of generators, and a solution to the word problem for Γ.*

In Problem 2, we define the structure of a lattice on I in a natural way and use a variation of the LLL-reduction algorithm to find an element in I of small reduced norm.

As an application of our results, we have proven the following result, in joint work with Lassina Dembélé and Matthew Greenberg.

Theorem. *There exists a finite, nonsolvable Galois extension K of $\mathbb{Q}$ which is ramified only at $p = 3$ and one ramified only at $p = 5$.*

This answers a conjecture of Gross (for $p = 3$ and $p = 5$). For $p \geq 11$, Serre constructed such extensions ramified only at p using the Galois representation associated to a classical cusp form of level 1. Recently, Dembélé has constructed such an extension ramified only at $p = 2$ arising from a Hilbert modular form of level 1 and parallel weight 2 over the totally real field $\mathbb{Q}(\zeta_{32})^+$. Using our techniques, we settle Gross' conjecture by exhibiting a Hilbert modular form of level 1 and parallel weight 2 over $\mathbb{Q}(\zeta_{27})^+$ (for $p = 3$) and level $\mathfrak{p}_5 \mid 5$ and parallel weight 2 over $F \subset \mathbb{Q}(\zeta_{25})$ with $[F : \mathbb{Q}] = 5$ (for $p = 5$). For $p = 3$, our field K has Galois group $PGL_2(\mathbb{F}_{3^{27}}) \cdot 9$ and so has degree

$$3^{29}(3^{54} - 1) = 39908383941873399295342466069419716703 44.$$

The root discriminant of F satisfies $\delta_F < 76.21$, which is remarkably small in comparison, and similar results hold for $p = 5$.

The case $p = 7$ seems difficult to reach using these methods, owing to the fact that there are no interesting forms over $\mathbb{Q}(\zeta_7)^+$ but the genus of the Shimura curve for the field of degree 7 inside $\mathbb{Q}(\zeta_{49})$ has genus 22684 which places it beyond the realm of computational feasibility at the moment.

Solving quadratic equations over number fields

Denis Simon

The following are latex notes by Bjorn Poonen, taken in real time during the talk:

Over $\mathbb{Q}$: Given $a, b, c \in \mathbb{Z}$, to find $x_1, x_2, x_3 \in \mathbb{Z}$ not all zero such that $ax_1^2 + bx_2^2 + cx_3^2 = 0$, use the following two steps:

(1) Minimization (find a minimal integral model): Factor a, b, c, and eliminate the bad primes by local computations.
(2) Reduction (LLL).

Today we'll generalize the minimization step to number fields.

First let us describe minimization over $\mathbb{Q}$. Let $Q \in M_3(\mathbb{Q})$ be symmetric with $\det Q \neq 0$.

(1) Clear denominators, to make $Q \in M_3(\mathbb{Z})$.
(2) Divide by $\gcd(a, b, c)$.
(3) For $p | \det Q$, compute the kernel of $Q \bmod p$. Find $U \in \mathrm{SL}_3(\mathbb{Z})$ such that $QU \bmod p$ has first two columns zero.
(4) If $\dim \ker(Q \bmod p) = 2$, then ${}^tUQU \bmod p$ has zero entries except in the lower right corner. Multiply Q on left and right by the matrix $\begin{pmatrix} 1 & & \\ & 1 & \\ & & p \end{pmatrix}$ to get pQ' with $\det Q' = (\det Q)/p$. (Legendre: make a, b, c pairwise coprime.)
(5) If $\dim \ker(Q \bmod p) = 1$ and $p^2 | \det Q$, ${}^tUQU \bmod p$ has nonzero entries only in the upper left 2×2 block, and the lower right entry is $0 \bmod p^2$.

Multiply Q on left and right by the matrix $\begin{pmatrix} p & & \\ & p & \\ & & 1 \end{pmatrix}$ to get pQ' with $\det Q' = p^{-2}(\det Q)$. (Legendre: make a, b, c squarefree.)

(6) If $\dim \ker(Q \bmod p) = 1$ and $p | \det Q$ and $p^2 \nmid \det Q$. Choose U as before to get upper left 2×2 block mod p; then the existence of a p-adic solution implies that the determinant of this block is a square mod p.

$$\begin{pmatrix} p & & \\ & 1 & \\ & & 1 \end{pmatrix} \begin{pmatrix} * & * & 0 \\ * & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} p & & \\ & 1 & \\ & & 1 \end{pmatrix}$$

Get pQ' with $\det Q' = p^{-1} \det Q$. (Legendre: compute square root of $-b/a$ mod c.)

Over number fields:

(1) OK (gp: nfinit).
(2) Just store the gcd as an ideal I_0.

View Q as a function $I_1 \oplus I_2 \oplus I_3 \to I_0$. Define

$$\det(Q; I_0, I_1, I_2, I_3) := (\det Q) I_0^{-3} (I_1 I_2 I_3)^2.$$

Integral model: $Q_{ij} \in I_0 I_i^{-1} I_j^{-1}$ for all i and j; in this case $\det(Q; I_0, I_1, I_2, I_3)$ is an integral ideal.

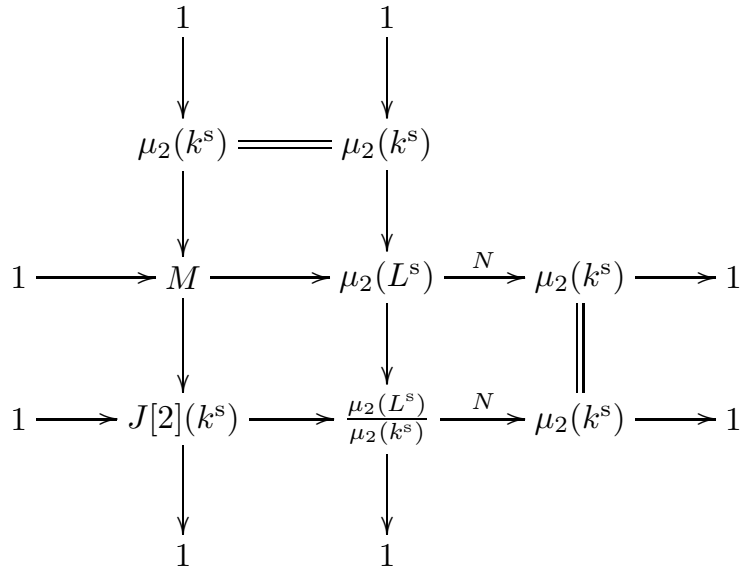
Two-coverings of Jacobians

Ronald van Luijk

Let k be a field of characteristic different from 2, and let k^{s} be a separable closure of k. Let C be a curve of genus 2 defined over k, with Jacobian variety J. A two-covering of J is a variety X over k, together with a morphism $\pi\colon X \to J$, such that there exists an isomorphism $g\colon X_{k^{\mathrm{s}}} \to J_{k^{\mathrm{s}}}$ satisfying $\pi = [2] \circ g$, where $[2]$ is the multiplication-by-2 map. Given a choice of g, we obtain a cocycle $\sigma \to g \circ \sigma(g^{-1})$, where the composition of isomorphisms is translation by some 2-torsion point P_σ. This determines a well-defined cocycle class in $H^1(J[2]) = H^1\big(\mathrm{Gal}(k^{\mathrm{s}}/k), J[2](k^{\mathrm{s}})\big)$ that does not depend on the choice of g. We thus get a bijection between isomorphism classes of two-coverings of J and elements of $H^1(J[2])$. In this talk, we show that the two-coverings corresponding to elements of a large subgroup of $H^1(J[2])$ (containing the Selmer group when k is a global field) can be embedded as intersection of 72 quadrics in $\mathbb{P}^{15}_k$, just as the Jacobian J itself. Moreover, we can give explicit equations for the models of these twists in the generic case, extending the work of Gordon and Grant which applied only to the case when all Weierstrass points are rational. In addition, we can describe elegant equations on the Jacobian itself.

The key idea is as follows. Let C be given as $y^2 = f(x)$, where $f \in k[x]$ is a separable polynomial of degree 6. Set $L = k[x]/f$ and $L^{\mathrm{s}} = L \otimes_k k^{\mathrm{s}} \cong k^{\mathrm{s}}[x]/f$.

Denote the norm from L to k by $N = N_{L/k}$. The following diagram exists.



Here M is by definition the kernel of the induced map $N\colon \mu_2(L^s) \to \mu_2$. The Weil-pairing extends to a pairing on $\mu_2(L^s)$ and a pairing on $M \times \mu_2(L^s)/\mu_2$, making the diagram is self-dual around its diagonal.

The action of $J[2]$ on J induces a linear action of $J[2]$ on the model of J in $\mathbb{P}^{15}$, and thus on $\mathbb{P}^{15}$ itself. The corresponding projective representation $J[2] \to \mathrm{PSL}(16)$ lifts to a linear representation $M \to \mathrm{SL}(16)$. Since M is abelian, this representation is the direct sum of 16 characters of M. It turns out they are those elements of $\mu_2(L^s)/\mu_2$, the dual of M, that are not contained in the image of $J[2]$. These characters give a set of coordinates on $\mathbb{P}^{15}$. This gives the homogeneous coordinate ring of $\mathbb{P}^{15}$ a natural grading by the group $\mu_2(L^s)/\mu_2$. The most important ingredient in our work is the fact that the ideal that determines the model of J in $\mathbb{P}^{15}$ is homogeneous with respect to this grading.

Higher descents on elliptic curves with a rational 2-torsion point

Tom Fisher

Let E/K be an elliptic curve over a number field. Descent calculations on E can be used to find upper bounds on the rank of the Mordell-Weil group $E(K)$, and to compute covering curves that assist in the search for generators of $E(K)$. The general method of 4-descent, developed in the PhD theses of Siksek [4], Womack [7] and Stamminger [6], has been implemented in MAGMA [3] (when $K = \mathbb{Q}$) and works well for curves of sufficiently small discriminant. However the method can be improved when E has a rational 2-torsion point. In this case we follow Bremner and Cassels [1], see also Siksek [4].

We recall that E has a Weierstrass equation of the form

$$y^2 = x(x^2 + ax + b)$$

with 2-torsion point $T = (0, 0)$. Let $\phi : E \to E'$ be the 2-isogeny with kernel $\{\mathcal{O}, T\}$ and let $\widehat{\phi} : E' \to E$ be the dual isogeny. There is an injective group homomorphism $\delta : E(K)/\widehat{\phi}E'(K) \to K^\times/(K^\times)^2$ given (for $P \neq \mathcal{O}, T$) by $P = (x, y) \mapsto x$. Suppose $P = (x, y) \in E(K)$ with $\delta(P) = \xi_1 \mod (K^\times)^2$. Then $x = \xi_1(s/t)^2$ and $y = \xi_1(rs/t^3)$ where

$$r^2 = \xi_1 s^4 + as^2t^2 + (b/\xi_1)t^4. \tag{1}$$

Parametrising a conic over K gives

$$(s^2 : t^2 : r) = (f(l, m) : g(l, m) : h(l, m))$$

where f, g and h are binary quadratic forms. Then

$$f(l, m) = \xi_2 s^2 \quad \text{and} \quad g(l, m) = \xi_2 t^2 \tag{2}$$

for some $\xi_2 \in K^\times$. Parametrising each of these conics over K gives

$$(l : m : s) = (p_1(c, d) : p_2(c, d) : p_3(c, d))$$
$$(l : m : t) = (q_1(\theta, \psi) : q_2(\theta, \psi) : q_3(\theta, \psi))$$

where the p_i and q_i are binary quadratic forms. Then

$$p_1(c, d) = \xi_3 q_1(\theta, \psi) \quad \text{and} \quad p_2(c, d) = \xi_3 q_2(\theta, \psi) \tag{3}$$

for some $\xi_3 \in K^\times$. The singular fibres in the pencil of quadrics spanned by (3), are defined over $L = K(\sqrt{b/\xi_1})$ and $L' = K(\sqrt{\xi_1})$. We write

$$p_1(c, d) - \varepsilon p_2(c, d) = \xi_3 \alpha(c + \gamma d)^2$$

for some $\varepsilon, \alpha, \gamma \in L$. Then by (3) we have

$$q_1(\theta, \psi) - \varepsilon q_2(\theta, \psi) = \alpha(c + \gamma d)^2.$$

Parametrising a conic over L gives

$$(\theta : \psi : c + \gamma d) = (Q_1(\lambda, \mu) : Q_2(\lambda, \mu) : Q_3(\lambda, \mu))$$

where Q_1, Q_2 and Q_3 are binary quadratic forms. Then

$$\theta = \pi Q_1(\lambda, \mu) \quad \text{and} \quad \psi = \pi Q_2(\lambda, \mu)$$

for some $\pi \in L^\times$. Let $1, \beta$ be a basis for L over K. Writing $\lambda = x + \beta y$ and $\mu = u + \beta v$ we expand to give

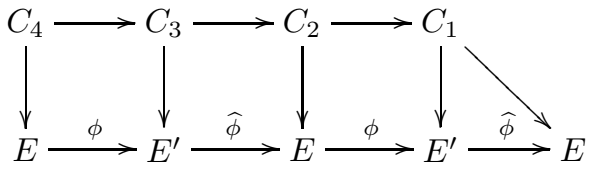
$$\pi Q_1(\lambda, \mu) = F_1(x, y, u, v) + \beta F_2(x, y, u, v)$$
$$\pi Q_2(\lambda, \mu) = G_1(x, y, u, v) + \beta G_2(x, y, u, v)$$

where F_1, F_2, G_1 and G_2 are quadratic forms with coefficients in K. Since $\theta, \psi \in K$ it follows that

$$F_2(x, y, u, v) = G_2(x, y, u, v) = 0. \tag{4}$$

Up to linear changes of co-ordinates over K, this quadric intersection depends only on the image of π in $L^\times/K^\times(L^\times)^2$, and hence only on $\xi_4 := N_{L/K}(\pi) \in K^\times/(K^\times)^2$. We recover π from ξ_4 by again solving a conic over K.

The equations (1), (2), (3), (4) define covering curves C_1, C_2, C_3, C_4 that fit in a commutative diagram



where the vertical maps are isomorphisms defined over $\overline{K}$, and all other maps are morphisms of degree 2 defined over K. At each stage ($j = 1, 2, 3, 4$) there are only finitely many $\xi_j \in K^\times/(K^\times)^2$ for which the corresponding covering curve C_j is everywhere locally soluble. Thus each rational point on E lifts to one of only finitely many 4-coverings C_4 of E, and these can be computed explicitly.

We recall that the general method of 4-descent requires that we compute the class group and units of a degree 4 extension of K. In contrast (assuming the class group and units of K itself are known) the above method only requires that we solve conics over K and over L. We make the following improvements.

- We use the Cassels pairing to efficiently compute upper bounds for the rank. (This was not required in [1], since for the curves considered there, descent by 2-isogeny already shows that the rank is at most 1.)
- By solving conics over both L and L' we can write C_4 as a quadric interesection in two different ways. It is then easy to compute one further covering curve. The same idea gives two further covering curves when all the 2-torsion points of E are K-rational. This corresponds to a full 8-descent on E.
- We replace the problem of solving a conic over L with that of solving a quadratic form of rank 4 over K. Taking $K = \mathbb{Q}$ the latter can be solved efficiently using an algorithm of Simon [5].

We are in the process of writing a program in MAGMA to compute rank bounds by this method (when $K = \mathbb{Q}$). Initial versions of this program have assisted in finding an elliptic curve $E/\mathbb{Q}$ with $E(\mathbb{Q}) \cong \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}^4$ (the previous largest known rank for this torsion subgroup was 3) and in finding 10 new examples of elliptic curves $E/\mathbb{Q}$ with $E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}^3$, including one where every point of infinite order has canonical height greater than 100. The examples are listed on Dujella's website [2]. The main reason we need higher descents to make these searches is that we would otherwise be swamped by examples which, while appearing to be candidates for large rank, are in fact accounted for by elements of 2-power order in the Tate-Shafarevich group.

The universal family of elliptic curves with torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ is $E_\lambda : y^2 = x(x^2 + Ax + B)$ where

$$A = (\lambda^2 - 1)^4 - 32\lambda^4$$
$$B = -16\lambda^4(\lambda^2 + 1)^2(\lambda^4 - 6\lambda^2 + 1).$$

In addition to the 10 new rank 3 examples mentioned above, we have found 7 examples that conjecturally have rank 3, in the sense that our best upper bound

for the rank is 3 and we have found two independent points of infinite order. The corresponding values of λ and heights of the known generators are as follows.

λ	$\widehat{h}(P_1)$	$\widehat{h}(P_2)$	$\widehat{h}(P_3)$
15/272	15.49	71.16	?
9/296	18.03	51.62	?
303/520	14.67	159.65	?
672/689	106.64	185.69	?
101/770	55.31	219.37	?
865/888	109.63	206.01	?
581/922	41.38	68.39	?

These points were found by searching on 4-coverings. We are presently unable to compute the 8-coverings (as curves of degree 8), since the method in [6] requires that we solve a conic over a degree 4 number field, and this seems out of reach for examples of this size. The curves are also far too large for any sort of L-value computation, so we do not know any (even conjectural) upper bound on the heights of the missing generators.

References

[1] A. Bremner and J.W.S. Cassels, On the equation $Y^2 = X(X^2 + p)$, *Math. Comp.* **42** (1984), no. 165, 257–264.

[2] A. Dujella, High rank elliptic curves with prescribed torsion, `http://web.math.hr/~duje/tors/tors.html`

[3] MAGMA is described in W. Bosma, J. Cannon and C. Playoust, The MAGMA algebra system I: The user language, *J. Symb. Comb.* **24**, 235-265 (1997). (See also the MAGMA home page at `http://magma.maths.usyd.edu.au/magma/`.)

[4] S. Siksek, *Descent on curves of genus one*, PhD thesis, University of Exeter, 1995. See `http://www.warwick.ac.uk/staff/S.Siksek/papers/phdnew.pdf`

[5] D. Simon, *Quadratic equations in dimensions 4, 5 and more*, preprint (2005).

[6] S. Stamminger, *Explicit 8-descent on elliptic curves*, PhD thesis, International University Bremen, 2005.

[7] T.O. Womack, *Explicit descent on elliptic curves*, PhD thesis, University of Nottingham, 2003. See `http://www.warwick.ac.uk/staff/J.E.Cremona/theses/`

Non-split Cartan modular curves

Burcu Baran

For any positive integer n, let $X_{ns}^+(n)$ denote the modular curve associated to the normalizer of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbf{Z}/\mathbf{nZ})$. The curve $X_{ns}^+(n)$ classifies isomorphism classes of elliptic curves with a certain type of "non-split" level n structure. Historically, both the integral points and the rational points of $X_{ns}^+(n)$ play crucial roles in two different problems. The integral points are closely related to the class number one problem and the rational points are described by Serre's uniformity conjecture. In this talk, after a brief introduction to $X_{ns}^+(n)$ we focus on all $X_{ns}^+(n)$ whose genus is less than or equal to 2 and has finitely many integral

points. We discuss their equations and integral points. We also discuss $X_{ns}^{+}(13)$ which is a genus 3 curve and is defined by a quartic in $\mathbf{P}^2$.

The unit-residue group

Gabriele Dalla Torre

The Tate pairing of curves over finite fields is a non-degenerate paring from a subgroup and a quotient group of the divisor class group onto a quotient group of the multiplicative group of the finite field. The goal of this talk is to study the unit-residue group, which is an obstruction to a similar pairing on number fields.

Given a positive integer m and a local field F which contains a primitive m-th root ζ_m of unity, it is possible to define the norm-residue symbol, an antisymmetric bilinear map of $F^* \times F^*$ into the group $\langle \zeta_m \rangle$. This definition can be extended to ideles J of any global field K which contains a primitive m-th root of unity and we obtain a non-degenerate pairing on $J/J^m \times J/J^m$.

Definition 1. Let K be a global field containing a primitive m-th root of unity and let U be the unit idele group of K. The *unit-residue group* is the quotient $\overline{U}/\overline{U}^{\perp}$, where $\overline{U} = UJ/J^m$ and $\overline{U}^{\perp}$ is the annihilator of $\overline{U}$ with respect to the inner product defined by the norm-residue symbol.

The unit-residue group is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^{2\cdot|S_\infty|}$, where S_∞ is the set of infinite primes, and hence is trivial when K is a function field. Moreover the norm-residue symbol induces a non-degenerate pairing on $\overline{U}/\overline{U}^{\perp} \times \overline{U}/\overline{U}^{\perp}$.

Definition 2. Let K be a number field containing a primitive m-th root of unity. Let J be the idele group of K and U be the unit idele group of K. The *virtual subgroup* V is the group $V = \mathcal{V}/\overline{U}^{\perp}$, where $\mathcal{V} = (\overline{K^*} \cap \overline{U}) \cdot \overline{U}^{\perp} = (\overline{K^*} \cdot \overline{U}^{\perp}) \cap \overline{U}$.

The virtual subgroup is a maximal self-annihilating subgroup of the unit-residue group, but it is not generally a free $\mathbb{Z}/m\mathbb{Z}$-module.

We give examples and, in some cases, a complete description of the unit-residue group and the virtual subgroup. Our results include the following theorem.

Theorem 1. *Let K be a cyclic cubic or quintic number field where 2 splits and let $m = 2$. Then the virtual subgroup induces a bijection between the set of primes above 2 and the set of infinite primes.*

Computing Igusa Class Polynomials

Marco Streng

The *Hilbert class polynomial* $H_K \in \mathbb{Z}[X]$ of an imaginary quadratic number field K has as roots the j-invariants of complex elliptic curves having complex multiplication (CM) by the ring of integers of K. These roots generate the Hilbert class field of K, and Weber [9] computed H_K for many small K. The CM method uses the reduction of H_K modulo large primes p to construct elliptic curves over $\mathbb{F}_p$ with a prescribed number of points, for example for cryptography. The bit size of H_K grows exponentially with K, like $\widetilde{O}(\Delta)$, and so does the runtime of the algorithms that compute it.

If we go from elliptic curves (genus 1) to genus 2 curves, we get the *Igusa class polynomials* $H_{K,n} \in \mathbb{Q}[X]$ $(n = 1, 2, 3)$ of a *quartic CM field* K. Their roots are the *Igusa invariants* of all complex genus 2 curves having CM by the ring of integers of K. As in the case of genus 1, these roots generate class fields and the reduction modulo large primes p yields cryptographic curves of genus 2. Computing Igusa class polynomials is considerably more complicated, in part because of their denominators. Recently, various algorithms have been developed [1, 2, 6, 8], but as these algorithms use approximations to an unspecified precision, no runtime bound or proof of correctness was given.

In [7], we describe a complete and correct algorithm that computes Igusa class polynomials $H_{K,n} \in \mathbb{Q}[X]$ of *quartic CM fields* $K = \mathbb{Q}(\sqrt{\Delta_0}, \sqrt{-a + b\sqrt{\Delta_0}})$, where Δ_0 is a real quadratic fundamental discriminant and $a, b \in \mathbb{Z}$ are such that $-a + b\sqrt{\Delta_0}$ is totally negative. Our algorithm is based on the complex analytic approach of [6] and [8]. This is the first proof of correctness and the first runtime bound of any algorithm that computes these polynomials. The discriminant Δ of K is of the form $\Delta = \Delta_1\Delta_0^2$ for a positive integer Δ_1. We may and will assume $0 < a < \Delta$, as each quartic CM field has such a representation. We disregard the degenerate case of *non-primitive* quartic CM fields, i.e., those that can be given with $b = 0$, as abelian varieties with CM by non-primitive quartic CM fields are isogenous to products of CM elliptic curves, which are given already by the Hilbert class polynomial. We have the following runtime bound.

Main Theorem. *The algorithm in [7] computes $H_{K,n}$ $(n = 1, 2, 3)$ for any primitive quartic CM field K in which 2 and 3 do not ramify. It has a runtime of $\widetilde{O}(\Delta_1^{7/2}\Delta_0^{11/2})$, and the bit size of the output is $\widetilde{O}(\Delta_1^2\Delta_0^3)$.*

An essential part of the proof is the denominator bound, as provided by Goren and Lauter [5] and Goren [3, 4]. As the results of [3, 4] assume ramification bounds on the primes 2 and 3, we have a similar restriction. This restriction will disappear as soon as Goren's results are extended to this case.

Yang's [10] denominator bounds are tighter than those of Goren and Lauter, but are proven only for a small class of CM fields. For that class of CM fields, we get an improvement from $\widetilde{O}(\Delta_1^{7/2}\Delta_0^{11/2})$ to $\widetilde{O}(\Delta_1^{3/2}\Delta_0^{7/2}) + \widetilde{O}(\Delta_1^{5/2}\Delta_0^{5/2})$.

We do not claim that our runtime is optimal, but an exponential runtime is unavoidable, because the degree of the Igusa class polynomials (as with Hilbert class polynomials) is already bounded from below by a power of the discriminant.

References

[1] K. Eisenträger and K. Lauter, *A CRT algorithm for constructing genus 2 curves over finite fields*, To appear in *Arithmetic, Geometry and Coding Theory*, proceedings of AGCT-10 Marseille, 2005, arXiv:math/0405305v2

[2] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng, *The 2-Adic CM Method for Genus 2 Curves with Application to Cryptography*, in Advances in Cryptology - ASIACRYPT 2006, Lecture Notes in Computer Science **4284**, 2006, 114 – 129, Springer-Verlag, arXiv:math/0503148

[3] E. Goren, Personal communication, 2007.

[4] E. Goren, *Class invariants for genus 2 curves, part II*, Fourth spring conference on Siegel modular forms and abelian varieties, Lake Hamana, Japan, 2007, slides available at `http://research.microsoft.com/~klauter/JapanTalk2007CombinedV2.pdf`

[5] E. Goren and K. Lauter, *Class Invariants for Quartic CM Fields*, Annales de l'Institut Fourier **57** (2), 2007, 457–480, arXiv:math/0404378v2

[6] A.-M. Spallek, *Kurven vom Geschlecht* 2 *und ihre Anwendung in Public-Key-Kryptosystemen*, PhD thesis, Institut für Experimentelle Mathematik, Universität GH Essen, 2008, `http://www.iem.uni-due.de/zahlentheorie/AES-KG2.pdf`

[7] M. Streng, *Computing Igusa Class Polynomials*, preprint, 2009, arXiv:0903.4766

[8] P. van Wamelen, *Examples of Genus two CM Curves Defined over the Rationals*, Mathematics of Computation **68** (225), 1999, 307–320.

[9] H. Weber, *Algebraische Zahlen*, volume 3 of Lehrbuch der Algebra, Braunschweig, Friedrich Vieweg, 1908.

[10] T. Yang, *Arithmetic intersection on a Hilbert modular surface and the Faltings height*, preprint, 2007, `http://www.math.wisc.edu/~thyang/RecentPreprint.html`

Rings associated to binary forms and the class groups of those rings

Melanie Wood

The association of algebraic objects to forms has had many important applications in number theory. Gauss, over two centuries ago, studied quadratic rings and ideals associated to binary quadratic forms, and found that ideal classes of quadratic rings are exactly parametrized by equivalence classes of integral binary quadratic forms. Delone and Faddeev, in 1940, showed that cubic rings are parametrized by equivalence classes of integral binary cubic forms. Birch, Merriman, Nakagawa, Corso, Dvornicich, and Simon have all studied rings associated to binary forms of degree n for any n, but it has not previously been known which rings, and with what additional structure, are associated to binary forms. Rings and certain ideals have been associated to classes of binary forms, by writing the bases and multiplication tables in terms of the coefficients of the form.

In this talk, we describe a geometric construction for rings and ideals associated to binary forms, which gives Gauss composition, the theorem of Delone and Faddeev, and the rings and ideals associated to higher forms. We describe briefly what algebraic structures are parametrized by binary n-ic forms, for all n. The algebraic data associated to an integral binary n-ic form includes a rank n ring,

an ideal class for that ring, and a condition on the ring and ideal class that comes naturally from geometry. We further explain that classes of pairs of n by n matrices parametrize the ideal classes of rings associated to binary n-ic forms. We give a geometric construction for the rings and ideals from a pair of matrices, and show how to use the Eagon-Northcott complex to make this geometric construction for all matrices, even the pair of zero matrices. These parametrizations work when any base scheme replaces the integers, and the correspondences between forms and the algebraic data are functorial in the base scheme. The proofs of these statements are all included in the author's PhD thesis.

An integral version of Shimura's conjecture on Petersson inner products

Kartik Prasanna

The aim of this talk is to motivate and outline an integral version of Shimura's conjecture on Petersson inner products of quaternionic modular forms. Let F be a totally real field and f a Hilbert modular newform over F of weights $(k_1, \ldots, k_d)$ with $k_1 \equiv \cdots \equiv k_d \mod 2$. Let B be a quaternion algebra over F such that f admits a Jacquet-Langlands transfer to B. Shimura studied the question of how the Petersson inner products $\langle f, f\rangle$ and $\langle f_B, f_B\rangle$ are related to each other, when f and f_B arithmetically normalized. (See below for an explanation of this term.) In particular, he made the following conjecture:

Conjecture 1. *(Shimura) Let Σ_∞ denote the set of infinite places of F. Then for each $v \in \Sigma_\infty$, there exists a complex number c_v such that (for varying B)*

$$\langle f_B, f_B\rangle \sim_{\bar{\mathbb{Q}}^\times} \prod_{v\in\Sigma_\infty, v\nmid \operatorname{disc} B} c_v. \tag{1}$$

Remark 2. *(Arithmetic normalizations)* The form f_B may be thought of as a section of a vector bundle over a quaternionic Shimura variety. The variety and this bundle admit canonical models over a suitable number field K_f, and even integral models at good primes p, using which f_B can be normalized up to a p-unit in K_f.

Towards this conjecture, Shimura [5] showed that if B_1 and B_2 are *complementary* quaternion algebras i.e. such that $\Sigma_\infty = \{v \in \Sigma_\infty : v \mid \operatorname{disc} B_1\} \sqcup \{v \in \Sigma_\infty : v \mid \operatorname{disc} B_2\}$, then

$$\langle f, f\rangle \sim_{\bar{\mathbb{Q}}^\times} \langle f_{B_1}, f_{B_1}\rangle\langle f_{B_2}, f_{B_2}\rangle.$$

In later work, Michael Harris [1] proved Shimura's conjecture under the technical hypothesis that the automorphic representation π attached to f admits at least one finite place at which it is discrete series.

We would like to make a more precise version of Shimura's conjecture, that is valid up to p-units for good primes p. To motivate this, we look at the simplest case, that of $F = \mathbb{Q}$ and f a form of weight 2 with rational Fourier coefficients. Then f corresponds to an isogeny class $\mathcal{C}$ of elliptic curves over $\mathbb{Q}$. Suppose that

the conductor of f is (a square-free integer) N so that f may be viewed as a differential on the modular curve $X := X_0(N)$. Let B be an indefinite quaternion algebra with $N^- = \operatorname{disc} B | N$. Then f admits a Jacquet-Langlands transfer f_B to the Shimura curve $X_B := X_0^{N^-}(N^+)$ where $N = N^+N^-$. Further, if E and E' denote the *strong* elliptic curves in $\mathcal{C}$ corresponding to X and X_B respectively, φ and φ_B the corresponding modular parametrizations, and p is a non-Eisenstein prime for f (i.e. such that the Galois representation $E[p]$ is irreducible), then one can show that

$$\frac{\langle f, f\rangle}{\langle f_B, f_B\rangle} \sim \frac{\deg \varphi}{\deg \varphi_B} \sim \prod_{q|N^-} c_q, \tag{2}$$

where c_q is the order of the component group (over the algebraic closure) of the Neron model of E at q, and $\sim$ now denotes equality up to p-adic units. The first $\sim$ above follows from an analysis of the Manin constant for f and f_B and using that E and E' are isogenous by an isogeny of degree prime to p; the second $\sim$ is a theorem of Ribet-Takahashi [4]. (See [2], Sec. 2.2.1 for more details.) The constants c_q are arithmetically interesting, since they measure *level-lowering* congruences satisfied by the form f at q.

Example 3. The elliptic curve

$$y^2 + y = x^3 - x^2 - 2174x - 151262$$

has conductor $N = 291 = 3 \cdot 97$. For this curve, $c_3 = 23$ and $c_{97} = 1$.

Combining (1) and (2), we are lead to the following refined version of Shimura's conjecture for arbitrary totally real fields F, which appeared in [3]. (We assume here that p is a good prime for f i.e. such that $p \nmid \operatorname{disc} F$, $\operatorname{cond} f$, $[F : \mathbb{Q}]$ and the class number of F and further that p is not Eisenstein for f.)

Conjecture 4. *([3], 4.2) Let $\pi = \otimes_v \pi_v$ denote the automorphic representation of $\mathrm{GL}_2(\mathbb{A}_F)$ corresponding to f. For each place v of F such that π_v is discrete series, there exists a complex number c_v such that*

$$\langle f_B, f_B\rangle \sim \frac{\langle f, f\rangle}{\prod_{v|\operatorname{disc} B} c_v}, \tag{3}$$

where $\sim$ denotes equality up to a p-adic unit.

Naturally, one would expect that for infinite places v, c_v is transcendental, while for finite places v, c_v is an algebraic integer and measures level-lowering congruences satisfied by f at v.

References

[1] Harris, Michael, *L-functions of 2×2 unitary groups and factorization of periods of Hilbert modular forms*, J. Amer. Math. Soc. **6** (1993), no. 3, 637–719.

[2] Prasanna, Kartik, *Integrality of a ratio of Petersson norms and level-lowering congruences*, Ann. of Math., **163** (2006), 901-967.

[3] Prasanna, Kartik, *Arithmetic aspects of the theta correspondence and periods of modular forms*, Eisenstein series and applications, 251–269, Progr. Math., **258**, Birkhäuser Boston, Boston, MA, 2008.
[4] Ribet, Kenneth A.; Takahashi, Shuzo, *Parametrizations of elliptic curves by Shimura curves and by classical modular curves*, Elliptic curves and modular forms (Washington, DC, 1996). Proc. Nat. Acad. Sci. U.S.A. **94** (1997), no. 21, 11110–11114.
[5] Shimura, Goro, *Algebraic relations between critical values of zeta functions and inner products*, Amer. J. Math. **105** (1983), no. 1, 253–285.

Towards Cohen-Lenstra heuristics for orders

Manjul Bhargava

We determine the mean number of 3-torsion elements in the ideal groups and class groups of quadratic orders. In fact, we are able to determine these means for any family of quadratic orders defined by suitable sets of local conditions.

As a consequence, we show that the difference between the average number of order 3 ideals and the average number of order 3 ideal classes, in any such family of complex quadratic orders, is independent of the family!

Complete addition laws for all elliptic curves over finite fields

Daniel J. Bernstein
(joint work with Tanja Lange)

This talk reports the latest news from a joint project with Tanja Lange to find, for each elliptic curve E, the fastest possible complete addition law for E.

Quaternionic Shimura varieties and Stark-Heegner points

Matthew Greenberg

Let F be a totally real number field of narrow class number one with ring of integers $\mathcal{O}_F$. Let N be a squarefree ideal of $\mathcal{O}_F$ and let E be an elliptic curve over F with conductor N. Let $\mathcal{O}$ be a $\mathcal{O}_F$-order in a non-CM quadratic extension K such that $(\operatorname{disc}\mathcal{O}, N) = 1$. Let $H_{\mathcal{O}}^+$ be the narrow ring class field of K associated to $\mathcal{O}$. Under the assumption that the sign in the functional equation of $L(E/K, s)$ is -1, one has

$$\operatorname{ord}_{s=1} L(E/H_{\mathcal{O}}^+, s) \geq [H_{\mathcal{O}}^+ : K]. \tag{1}$$

In this case, the conjecture of Birch and Swinnerton-Dyer predicts that the rank of $E(H_{\mathcal{O}}^+)$ is at least $[H_{\mathcal{O}}^+ : K]$. Our goal is to present, under the assumption that the sign in the functional equation of $L(E/K, s)$ is -1, analytic constructions of conjecturally algebraic points on E which should generate a finite index subgroup of $E(H_{\mathcal{O}}^+)$ under the assumption that equality holds in (1). Our constructions generalize constructions of Darmon for the following special cases:

(1) K is an ATR (almost totally real) extension of F and all primes $\ell|N$ split in K.

(2) $F = \mathbb{Q}$, K is real quadratic and there is a prime $p|N$ which is inert in K and all $\ell|N$, $\ell \neq p$, split in K.

Let

$$\Sigma = \{\ell|N : \ell \text{ is inert in } K\} \cup \{\text{infinite places of } K\}.$$

Our assumption that the sign in the functional equation of $L(E/K, s)$ is -1 implies that $|\Sigma|$ is odd. Assume that Σ contains a nonarchimedean place $\mathfrak{p}$. Let B be the quaternion F-algebra ramified precisely at the primes in $\Sigma - \{\mathfrak{p}\}$. Assuming the modularity of E/F, the Jacquet-Langlands correspondence implies that $L(E/F, s) = L(\pi, s)$, where π is an automorphic representation of $B^\times(\mathbb{A}_F)$.

Let $R_0(N^+)$ be an Eichler $\mathcal{O}_F$-order in B of level N^+, where N^+ is the product of the primes dividing N which are not in Σ. Let $R = R_0(N^+) \otimes_{\mathcal{O}_F} \mathcal{O}_{F,\{\mathfrak{p}\}}$, where $\mathcal{O}_{F,\{\mathfrak{p}\}}$ denotes the ring of $\{\mathfrak{p}\}$-integers of F. Let $\Gamma_0(N^+)$ and Γ be the groups of norm one units of the orders $R_0(N^+)$ and R, respectively.

Using p-adic integration, we associate a cohomology class

$$\varphi \in H^{n+1}(\Gamma, K_{\mathfrak{p}}^\times)$$

to π, where n is the number of infinite places of F at which B is split. There is a natural pairing

$$\langle \cdot, \cdot \rangle : H^{n+1}(\Gamma, K_{\mathfrak{p}}^\times) \times H_{n+1}(\Gamma, \mathbb{Z}) \longrightarrow K_{\mathfrak{p}}^\times$$

The subgroup $\Lambda_\varphi := \langle \varphi, H_{n+1}(\Gamma, \mathbb{Z}) \rangle$ is a lattice in $K^\times$, the *lattice of periods of* φ,and we obtain an induced *Abel-Jacobi map*

$$\mathrm{AJ}_\varphi : B_n(\Gamma, \mathbb{Z}) \longrightarrow K_{\mathfrak{p}}^\times / \Lambda_\varphi,$$

where $B_n(\Gamma, \mathbb{Z})$ is group of n-boundaries on Γ with coefficients in $\mathbb{Z}$.

Conjecture [4, Conjecture 2]. Λ_φ is commensurable with the Tate lattice of $E/K_{\mathfrak{p}}$.

In [3], this conjecture is proved using Hida theory in the case $F = \mathbb{Q}$. The case $F = \mathbb{Q}$ and $B = M_2(\mathbb{Q})$ was previously known by work of Darmon [2]. Let $q_E \in F_{\mathfrak{p}}$ be the Tate period of E. Assuming the above conjecture, we may find an isogeny

$$\beta : K_{\mathfrak{p}}/\Lambda_\varphi \longrightarrow K_{\mathfrak{p}}/q_E^{\mathbb{Z}} = E(K_{\mathfrak{p}}).$$

To each optimal embedding $\psi : \mathcal{O} \to R_0(N^+)$, we may naturally associate an n-boundary $\Delta_\psi \in B_n(\Gamma, \mathbb{Z})$ and set

$$P_\psi = \beta\, \mathrm{AJ}_\varphi(\Delta_\varphi) \in E(K_{\mathfrak{p}})$$

Conjecture [4, Conjecture 3]. The point P_ψ belongs to $E(H_{\mathcal{O}}^+)$.

We present the following result, proved in [5], as evidence for this conjecture.

Theorem. Suppose $F = \mathbb{Q}$. Let χ be an unramified quadratic character of $\mathrm{Gal}(\bar{K}/K)$ and let H_χ be the extension of K cut out by χ. Then

$$\sum_{\sigma \in \mathrm{Gal}(H_{\mathcal{O}}^+/K)} \chi(\sigma) P_{\psi^\sigma} \in E(H_\chi).$$

This theorem in the case $B = M_2(\mathbb{Q})$ was previously known by work of Bertolini and Darmon [1], and our techniques of proof are based on theirs.

References

[1] M. Bertolini, H. Darmon, *The rationality of Stark-Heegner points over genus fields of real quadratic fields*, Ann. of Math., to appear.

[2] H. Darmon, *Integration on $\mathcal{H}_p \times \mathcal{H}$ with arithmetic applications*, Ann. of Math. 154 (2001) 589-639.

[3] S. Dasgupta, M. Greenberg, *L-invariants and Shimura curves*, in preparation.

[4] M. Greenberg *Stark-Heegner points and the cohomology of quaternionic Shimura varieties*, Duke Math. J. 147 (2009), no. 3, 541–575.

[5] M. Greenberg, S. Shahabi *p-adic deformation of Shintani cycles on Shimura curves and rational points on elliptic curves*, in preparation.

Un survol de l'obstruction de Brauer–Manin entière

Jean-Louis Colliot-Thélène

Soient k un corps de nombres, Ω l'ensemble de ses places, k_v le complété de k en une place v. Soit Ω_∞ l'ensemble des places archimédiennes de k. Soit X une k-variété algébrique. On note $X(A_k)$ l'espace des adèles de X. On a l'application diagonale $X(k) \to X(A_k)$.

Lorsque X/k est propre, $X(A_k)$ coïncide avec le produit topologique des $X(k_v)$. Dans ce cas, l'image de $X(k)$ dans $X(A_k)$ est dense si et seulement si le principe de Hasse et l'approximation faible valent pour X.

On s'intéresse ici au cas où X/k n'est pas nécessairement propre, par exemple au cas des variétés affines. On note $X_\bullet(A_k)$ l'espace des adèles de X, modifié de la façon suivante : pour chaque place archimédienne v de k, on remplace l'espace topologique $X(k_v)$ par l'ensemble de ses composantes connexes.

Si l'ensemble $X(k)$ des k-points de X est dense dans $X_\bullet(A_k)$, on dit que X satisfait l'approximation forte.

Deux exemples classiques de variétés satisfaisant cette propriété sont :
1) La droite affine. Dans ce cas l'approximation forte est une généralisation du théorème du reste chinois.
2) Tout groupe semisimple simplement connexe G tel que le produit $\prod_{v\in\Omega_\infty} G(k_v)$ n'est pas compact : c'est là un théorème de Martin Kneser et de V. P. Platonov.

Soit Br X le groupe de Brauer de X. On dispose de l'accouplement de Brauer–Manin

$$X_\bullet(A_k) \times \text{Br } X/\text{Br } k \to \mathbf{Q}/\mathbf{Z}.$$

On note $X_\bullet(A_k)^{\text{Br}} \subset X_\bullet(A_k)$ l'espace des adèles modifiées qui sont orthogonales au groupe de Brauer de X. L'image de l'application diagonale $X(k) \to X_\bullet(A_k)$ est dans le fermé $X_\bullet(A_k)^{\text{Br}}$. Des exemples de variétés affines X pour lesquelles $X_\bullet(A_k)^{\text{Br}}$ est un sous-ensemble propre de $X_\bullet(A_k)$ se trouvent dans la littérature, parfois sous une forme quelque peu cachée, comme dans l'étude des représentations

"spinorielles" ou des "exceptions spinorielles" dans la théorie des formes quadratiques entières (voir [1], Prop. 7.3 et §7.4). On peut aussi construire des exemples en partant de la définition ci-dessus ([6]).

Si l'image de $X(k)$ est dense dans $X_\bullet(A_k)^{\mathrm{Br}}$, on dit que l'obstruction de Brauer–Manin entière est la seule obstruction à l'approximation forte sur X.

Théorème 1 (JLCT et Fei Xu [1]) *Soient k un corps de nombres et G un k-groupe semisimple simplement connexe tel que le produit $\prod_{v\in\Omega_\infty} G(k_v)$ ne soit pas compact. Soit X/k une k-variété espace homogène de G. Si les groupes d'isotropies géométriques sont connexes, alors l'obstruction de Brauer–Manin entière est la seule obstruction à l'approximation forte sur X.*

Théorème 2 (JLCT et Fei Xu [1]) *Soient k un corps de nombres et G un k-groupe semisimple simplement connexe tel que le produit $\prod_{v\in\Omega_\infty} G(k_v)$ ne soit pas compact. Soit X/k une k-variété espace homogène de G. Si les groupes d'isotropies géométriques sont abéliens finis, alors l'obstruction de Brauer–Manin entière est la seule obstruction à l'approximation forte sur X.*

La démonstration de ces théorèmes utilise le théorème d'approximation forte pour G, le principe de Hasse pour les espaces principaux homogènes sous G (théorème de Kneser, Harder et Chernousov), ainsi que diverses formes de la théorie du corps de classes (suites exactes de Tate–Nakayama, de Poitou–Tate, de Kottwiz).

Lorsque $G = Spin(q)$ est le groupe des spineurs d'une forme quadratique de rang au moins 3, isotrope en une place archimédienne, un cas particulier est le théorème classique (Eichler, Kneser): *Soit q une forme quadratique entière q indéfinie, en au moins 4 variables. Si un entier $n \in \mathbf{Z}$ est représenté par q sur chaque anneau p-adique $\mathbf{Z}_p$, alors il est représenté par q sur $\mathbf{Z}$.*

Pour les formes de rang 3, il peut y avoir une obstruction de Brauer–Manin entière à la validité d'un tel énoncé (cela donne lieu à des "exceptions spinorielles"). L'analyse de cette obstruction donne naissance à un algorithme ([1], §5.8) permettant de décider si une équation $n = q(x, y, z)$, avec $n \in \mathbf{Z}$ entier et q une forme quadratique entière indéfinie, admet une solution en entiers $x, y, z \in \mathbf{Z}$ (mais cet algorithme ne permet pas de déterminer explicitement une solution). L'algorithme requiert la connaissance explicite d'une solution de $n = q(x, y, z)$ avec $(x, y, z) \in \mathbf{Q}$ (à ce sujet voir l'article de D. Simon [7]).

Le problème de la représentation d'un entier par une forme quadratique binaire est aussi très intéressant, comme on peut le voir en lisant le livre [3] de D. Cox, et aussi diverses notes de F. Lemmermeyer. Dans ce cas, la $\mathbf{Q}$-variété algébrique sous-jacente X est un espace principal homogène d'un tore algébrique. Le groupe $\mathrm{Br}\, X/\mathrm{Br}\, \mathbf{Q}$ associé est en général infini.

Théorème 3 (D. Harari [5]). *Soient k un corps de nombres et T un k-tore algébrique. L'obstruction de Brauer–Manin entière est la seule obstruction à l'approximation forte sur tout espace homogène de T.*

C. Demarche [4] vient d'établir un énoncé général qui recouvre les théorèmes 1, 2 et 3.

Soit n un entier positif. Dans [3], Cox donne un algorithme pour décider si un nombre premier p est représentable sous la forme $x^2 + ny^2$. On peut montrer que cet algorithme revient à calculer l'obstruction de Brauer–Manin. De façon générale, on peut se demander si le théorème 3 peut être rendu algorithmique. Cette question vient de faire l'objet d'un travail de Dasheng Wei et Fei Xu [8].

Si l'on quitte le monde des espaces homogènes de groupes, y a-t-il des classes intéressantes de variétés algébriques pour lesquelles on peut espérer que l'obstruction de Brauer–Manin entière soit la seule obstruction ?

Soit $n \neq 0$ un entier. Si n n'est pas congru à ± 4 modulo 9, peut-on écrire n comme somme de trois cubes d'entiers ? C'est là un problème diophantien célèbre. Notons X_n le $\mathbf{Z}$-schéma défini par

$$n = x^3 + y^3 + z^3.$$

La condition de congruence assure que X_n a des points dans tous les anneaux p-adiques $\mathbf{Z}_p$.

Théorème 4 (JLCT et O. Wittenberg [2]) *Sous les hypothèses ci-dessus, pour tout n non congru à ± 4 modulo 9, il existe un point dans $\prod_p X_n(\mathbf{Z}_p)$ qui est orthogonal à $\mathrm{Br}(X_n \times_{\mathbf{Z}} \mathbf{Q})$.*

En d'autres termes, l'obstruction de Brauer–Manin entière ne saurait donner une réponse négative au problème. De façon informelle : aucune utilisation de lois de réciprocité ne permettra de montrer l'existence d'un tel entier n non somme de trois cubes.

Des arguments généraux de nature arithmétique montrent que le groupe quotient $\mathrm{Br}(X_n \times_{\mathbf{Z}} \mathbf{Q})/\mathrm{Br}(\mathbf{Q})$ est fini. Mais il faut des arguments arithmétiques *ad hoc* pour déterminer ce groupe et en expliciter des représentants dans $\mathrm{Br}(X_n \times_{\mathbf{Z}} \mathbf{Q})$, ce qui est requis pour la démonstration du théorème 4.

Des arguments géométriques suggèrent que l'étude des points entiers sur les surfaces cubiques est du même ordre de difficulté que celle des points rationnels sur les surfaces quartiques.

References

[1] J.-L. Colliot-Thélène et F. Xu, Brauer–Manin obstruction for integral points of homogeneous spaces and representation of integral quadratic forms, Compositio Mathematica, **145** (2009) 309–363.

[2] J.-L. Colliot-Thélène et O. Wittenberg, Sommes de trois cubes, en préparation.

[3] D. A. Cox, Primes of the form $x^2 + ny^2$, John Wiley and Sons, 1989.

[4] C. Demarche, Le défaut d'approximation forte dans les groupes linéaires connexes, prépublication (2009) arXiv:0906.3456v1.

[5] D. Harari, Le défaut d'approximation forte pour les groupes algébriques commutatifs, Algebra and Number Theory **2** (2008) 595–611.

[6] A. Kresch et Yu. Tschinkel, Two examples of Brauer–Manin obstruction to integral points, Bull. Lond. Math. Soc. **40** (2008) 995–1001.

[7] D. Simon, Solving quadratic equations using reduced unimodular quadratic forms, Math. Comp. **74** (2005), 1531-1543.
[8] Dasheng Wei et Fei Xu, Integral points for multi-norm tori, prépublication (2009).

Constructing explicit isogenies of hyperelliptic Jacobians in genus ≥ 3

Benjamin Smith

We survey a range of constructions of explicit isogenies of Jacobians of curves of genus ≥ 3. This forms part of a program aimed at generalizing, where possible, the work of Vélu for elliptic curves and the well-known Richelot isogeny in genus 2.

Theorem 1. *There exists an efficient algorithm which takes as input a hyperelliptic curve H of genus 3 over a field K (of characteristic not 2 or 3) and a maximal 2-Weil isotropic subgroup S of $J_H[2]$ generated by differences of Weierstrass points, and returns an extension L/K, a curve X/L of genus 3, and a correspondence $C \subset H_L \times X$ such that the induced homomorphism $\phi_C = (\pi_X^C)_* \circ (\pi_{H_L}^C)^* : J_{H_L} \to J_X$ is an isogeny with kernel S.*

In general, the curve X of the algorithm in Theorem 1 is *not* hyperelliptic. This leads us to an application of Theorem 1 in cryptology, where it can be used to move instances of the Discrete Logarithm Problem from hyperelliptic to non-hyperelliptic Jacobians, which are vulnerable to faster index calculus algorithms.

We draw attention to the recent work of Mestre, which constructs for each $g \geq 2$ a $(g+1)$-parameter family of pairs of hyperelliptic curves of genus g with explicitly isogenous Jacobians. In each case, the isogeny has kernel isomorphic to $(\mathbb{Z}/2\mathbb{Z})^g$.

Finally, we construct some new families of isogenies of hyperelliptic Jacobians based on factorizations of separated-variable polynomials. These include the first families (to our knowledge) of nontrivial non-endomorphism isogenies of Jacobians where the degree of the isogenies is odd.

Theorem 2. *For each row of the following table, there exists an n-dimensional family of pairs (X, Y) of hyperelliptic curves of genus g defined over K, together with a correspondence $C \subset X \times Y$ inducing an explicit isogeny $\phi : J_X \to J_Y$ splitting multiplication by m on J_X; further, the kernel of ϕ is isomorphic to G.*

g	n	$[m]$	G	K
3	2	[2]	$(\mathbb{Z}/2\mathbb{Z})^3$	$\mathbb{Q}(\sqrt{-7})$
5	1	[3]	$(\mathbb{Z}/3\mathbb{Z})^5$	$\mathbb{Q}(\sqrt{-11})$
6	3	[2]	$(\mathbb{Z}/2\mathbb{Z})^6$	$\mathbb{Q}(\sqrt{-7})$
6	2	[3]	$(\mathbb{Z}/3\mathbb{Z})^6$	$\mathbb{Q}(\sqrt{-3\sqrt{13}+1})$
7	2	[4]	$(\mathbb{Z}/4\mathbb{Z})^4 \times (\mathbb{Z}/2\mathbb{Z})^6$	$\mathbb{Q}(\sqrt{-15})$
10	2	[3]	$(\mathbb{Z}/3\mathbb{Z})^{10}$	$\mathbb{Q}(\sqrt{-11})$
10	1	[4]	$(\mathbb{Z}/4\mathbb{Z})^9 \times (\mathbb{Z}/2\mathbb{Z})^2$	$\mathbb{Q}(\sqrt{-7})$
12	3	[3]	$(\mathbb{Z}/3\mathbb{Z})^{12}$	$\mathbb{Q}(\sqrt{-3\sqrt{13}+1})$
14	3	[4]	$(\mathbb{Z}/4\mathbb{Z})^9 \times (\mathbb{Z}/2\mathbb{Z})^{10}$	$\mathbb{Q}(\sqrt{-15})$
15	1	[8]	$(\mathbb{Z}/8\mathbb{Z})^5 \times (\mathbb{Z}/4\mathbb{Z})^{10} \times (\mathbb{Z}/2\mathbb{Z})^{10}$	*sextic CM-field*
20	2	[4]	$(\mathbb{Z}/4\mathbb{Z})^{19} \times (\mathbb{Z}/2\mathbb{Z})^2$	$\mathbb{Q}(\sqrt{-7})$
30	2	[8]	$(\mathbb{Z}/8\mathbb{Z})^{11} \times (\mathbb{Z}/4\mathbb{Z})^{19} \times (\mathbb{Z}/2\mathbb{Z})^{19}$	*sextic CM-field*

References

[1] J.-F. Mestre, *Couples de jacobiennes isogénes de courbes hyperelliptiques de genre arbitraire.* Preprint `arXiv:0902.3470v1 [math.AG]`

[2] B. Smith, *Families of explicit isogenies between hyperelliptic Jacobians*, In preparation.

[3] B. Smith, *Isogenies and the discrete logarithm problem in Jacobians of genus 3 hyperelliptic curves.* In N. Smart (ed.), *EUROCRYPT 2008*, Springer LNCS **4965** (2008) 163–180.

Progress report: curves with many points via high-rank K3 surfaces

Noam D. Elkies

We briefly review the theory of K3 surfaces X in characteristic zero and their moduli, and how one might use models of X as an elliptic K3 surface, double plane, quartic surface, "etc." to obtain explicit formulas for certain modular varieties, and to search for curves $C/\mathbb{Q}$ of small genus $g > 0$ with many points. We then recount some of the latest findings of this project.

Genus 1. For $g = 1$, "many points" means large Mordell–Weil rank given the torsion group T. In the case $T = \mathbb{Z}/2\mathbb{Z}$, our previous rank records over $\mathbb{Q}$ of 17 and 18 (announced in 2005 and 2006 respectively) used an elliptic K3 surface with Mordell–Weil group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^9$ parametrized by a sporadic rational point[1] on the modular curve $X_0(191)/w_{191}$. Recently we found that the same Mordell–Weil group can be obtained using K3 surfaces parametrized by the Shimura curve $X(10, 23)/w_{230}$ which is rational. This gives a wider selection of candidate curves, a few of which turned out to have rank 19. This is the current record for torsion $\mathbb{Z}/2\mathbb{Z}$. As J. Cremona pointed out when this record was 15 (Dujella 2002) or 14 (Fermigier 1996), this record is also the largest r for which we have a curve $E/\mathbb{Q}$ that is *proved* to have rank exactly r. Thanks to the 2-torsion point, a 2-descent is

[1] That is, a rational point that is neither cusp nor CM; We had found the simple model $y^2 - (x^3 + x - 1)y = x^3 + x^2 - x$ for the genus-2 curve $X_0(191)/w_{191}$, and the sporadic point with $x = 2$, back in 1989.

feasible, and implemented in Cremona's MWRANK, even for curves as complicated as the rank-19 curve

$$\begin{aligned} y^2 &= x^3 - 78643789435835792130621 75x^2/4 \\ &\quad + 13198775193181875109436919806563798708790790144 00x; \end{aligned}$$

whereas in the absence of torsion we have no feasible way to check whether the group generated by 28 independent points is of finite index in the Mordell–Weil group. The use of a rational moduli space $X(10,23)/w_{230}$ also lets us use biquadratic base changes to find nonconstant curves over $\mathbb{Q}(t)$ with a 2-torsion point and Mordell–Weil rank at least 11; our earlier family already gave infinitely many $C/\mathbb{Q}$ whose group of rational points contains $(\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}^{11}$, but it was a much sparser collection, parametrized by elliptic curves of positive rank rather than rational curves.

[We also incremented the rank record for $T = (\mathbb{Z}/2\mathbb{Z})^2$ from 14 to 15, for the curve

$$y^2 = x(x - 16305880494794397409378471875)(x + 25789944353867828597179055913 6);$$

but the only new ingredient here was more patience with MWRANK.]

Genus 2. Once $g > 1$, Faltings' theorem (= Mordell's conjecture) guarantees that the number of rational points on any given curve C is finite, but the bound on $\#C(\mathbb{Q})$ is not uniform as we vary C over all genus-g curves. Caporaso, Harris, and Mazur proved (c.1994) that, assuming the Bombieri–Lang conjecture (the rational points on a variety of general type are not Zariski dense), the number of rational points on genus-g curves over $\mathbb{Q}$ is uniformly bounded given g. But the bound is not effective even for $g = 2$.[2]

In addition to $\#C(\mathbb{Q})$, one can ask for large orbit counts $\#(C(\mathbb{Q})/\mathrm{Aut}(\mathbb{Q}))$. For genus 2, $\mathrm{Aut}_{\mathbb{Q}}(C)$ is always nontrivial but its size can be as small as 2 and as large as 12. For over a decade the record for the number of points of a genus-2 curve was 588,[3] for the Keller–Kulesz curve

$$y^2 = 278271081x^2(x^2 - 9)^2 - 229833600(x^2 - 1)^2$$

(1995); but this curve has 12 automorphisms, so "only" 49 orbits, whereas Stahlke (1997) found a curve with fewer points (≥ 366) but minimal symmetry, and thus many more orbits (≥ 183). In 2007 we searched through linear sections of a suitable "double plane" model of the singular K3 surface with Néron–Severi discriminant 163, finding several examples that broke Stahlke's record, the best of which had at least $2 \cdot 268 = 536$ points. Finally in December 2008 Stoll searched our double

[2]For both Faltings and CHM (Caporaso–Harris–Mazur), $\mathbb{Q}$ can be replaced by any fixed number field K. The bound may depend on K as well as g, but CHM also show that for each $g > 1$ there is an upper bound N_g on $\limsup_{C/K} \#C(K)$ independent of K, assuming a further Bombieri–Lang conjecture that a variety V of general type contains a closed subvariety V_0, smaller than V itself, such that $V(K) - V_0(K)$ is finite for every number field K.

[3]Here and later it is not feasible to prove that a set of rational points is complete, so the counts reported are lower bounds.

plane models more systematically, finding several examples with even more points than the 588 of the Keller–Kulesz curve; the largest count was $2 \cdot 321 = 642$, for

$$\begin{aligned} y^2 &= 82342800x^6 - 470135160x^5 + 52485681x^4 \\ &\quad + 2396040466x^3 + 567207969x^2 - 985905640x + 15740^2. \end{aligned}$$

(The techniques used to find the largest few point pairs also found four more pairs on Stahlke's curve, raising its count to $2 \cdot 187 = 374$, but this is still well below the new records.)

For $\limsup_C \#C(\mathbb{Q})$ we had obtained a lower bound of 150. This was for infinite families each of whose Zariski closures in $\mathcal{M}_2$ (the moduli space of genus-2 curves) has dimension 1. (The previous record of 48, due to Mestre, also had 1-dimensional closure in $\mathcal{M}_2$.) For a family whose Zariski closure has dimension 2, we can show that some lines on our double planes yield curves with at least 120 rational points. For a family of curves that is Zariski-dense in $\mathcal{M}_2$, we use a one-dimensional family of double planes parametrized by the rational Shimura curve $X(146,1)/w_{146}$ that parametrizes smooth sextics with 49 tritangents to get a lower bound of $2(49+6) = 110$.

Several other genus-2 curves C coming from our double planes have absolutely simple Jacobians J_C of rank at least 26, incrementing Dreier's 1995 record of 25; an example is

$$\begin{aligned} y^2 &= 80878009x^6 - 236558406x^5 - 1018244179x^4 \\ &\quad + 4436648480x^3 + 6445563464x^2 - 13620761544x + 68406^2. \end{aligned}$$

Stoll found several more such examples. [NB if we do not require that the Jacobian be simple then it is easy to use rank records for elliptic curves to get bielliptic curves of genus 2 whose Jacobian has rank 30+.]

These high Jacobian ranks all come from divisors supported on rational points. In another direction, we use plane sections of quartic K3 surfaces with high Néron–Severi rank but no lines to find infinite families of genus-2 curves that probably have *no* rational points, but whose Jacobians are simple of rank at least 19. Alas these curves are much too complicated to hope for a proof that any of them has $C(\mathbb{Q}) = \emptyset$.

Coming attractions. We have already used these techniques to find curves of genus 2 with a rational Weierstrass point that have a large point count or Jacobian rank. The condition that C have a rational Weierstrass point is equivalent to a restriction on the image of the representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $J_C[2]$. The technique can be adapted to produce curves satisfying other such restrictions, such as a nontrivial subgroup of $J_C(\mathbb{Q})[2]$ or $J_C(\mathbb{Q})[3]$. Naturally the resulting ranks and point counts will not be as impressive as for unrestricted curves, but the special Galois structure could make such curves more amenable to descent techniques for finding exact values, not just lower bounds, for $\#C(\mathbb{Q})$ or the rank of $J_C(\mathbb{Q})$.

We'll also explore analogous constructions of curves of genus 3, using quartic K3 surfaces. For each $g > 2$ there is a similar approach using K3's embedded in $\mathbf{P}^g$ via a complete linear series of sections of a divisor of self-intersection $2g-2$.

For large enough g this method will not do as well as more elementary approaches using polynomial identities; but $g = 3$ is still promising: there are infinite families (not yet computed explicitly) of smooth plane quartics with at least 52 rational points, and some individual curves in these families will likely have much larger counts.

Modular forms and elliptic curves over $\mathbb{Q}(\zeta_5)$

Paul E. Gunnells
(joint work with Farshid Hajir, Dinakar Ramakrishnan, Dan Yasaki)

Let ζ_5 be a primitive fifth root of unity, and let $F = \mathbb{Q}(\zeta_5)$. In this talk we describe recent computational work that investigates the modularity of elliptic curves over F. Here by *modularity* we mean that for a given elliptic curve E over F with conductor N there should exist an automorphic form f on GL_2, also of conductor N, such that we have the equality of partial L-functions $L_S(s, f) = L_S(s, E)$, where S is a finite set of places including those dividing N. We are also interested in checking a converse to this notion, which says that for an appropriate automorphic form f on GL_2, there should exist an elliptic curve E/F again with matching of partial L-functions. Our work is in the spirit of that of Cremona and his students [7–9, 15] for complex quadratic fields, and of Socrates–Whitehouse [16] and Dembélé [10] for real quadratic fields.

Instead of working with automorphic forms, we work with the cohomology of congruence subgroups of $\mathrm{GL}_2(\mathcal{O})$, where $\mathcal{O}$ is the ring of integers of F. There are several reasons for this. First, we have the Eichler–Shimura isomorphism, which identifies the cohomology of subgroups of $\mathrm{SL}_2(\mathbb{Z})$ with a space of modular forms. More precisely, if $N \geq 1$ is an integer and if $\Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$ is the usual congruence subgroup of matrices upper triangular mod N, then we have $H^1(\Gamma_0(N); \mathbb{C}) \simeq H^1(X_0(N); \mathbb{C}) \simeq S_2(N) \oplus \overline{S}_2(N) \oplus \mathrm{Eis}_2(N)$, where $X_0(N)$ is the open modular curve $\Gamma_0(N)\backslash\mathfrak{H}$, $S_2(N)$ is the space of weight two holomorphic cusp forms of level N, the summand $\mathrm{Eis}_2(N)$ is the space of weight two holomorphic Eisenstein series, and the bar denotes complex conjugation.

Moreover, this reason generalizes. Borel conjectured, and Franke proved [11], that all the complex cohomology of any arithmetic group can be computed in terms of certain automorphic forms, namely those with "nontrivial $(\mathfrak{g}, K)$-cohomology" [6, 18]. Although this is a small subset of all automorphic forms (Maass forms, for instance, can never show up in this way), all such automorphic forms are widely believed to be connected with arithmetic geometry (Galois representations, motives, ...).

Finally, working with cohomology also has the advantage that computations can be done very explicitly using tools of combinatorial topology. In a sense the cohomology provides a concrete incarnation of exactly the automorphic forms we want. These are the automorphic forms that account for the "modular forms over $\mathbb{Q}(\zeta_5)$" in the title.

Now we explain the setting for our computations. For our field we begin with the algebraic group $\mathbf{G} = R_{F/\mathbb{Q}}(\mathrm{GL}_2)$ (R denotes restriction of scalars), which satisfies $\mathbf{G}(\mathbb{Q}) = \mathrm{GL}_2(F)$. We replace the upper halfplane $\mathfrak{H}$ with the symmetric space X for the group $G = \mathbf{G}(\mathbb{R}) \simeq \mathrm{GL}_2(\mathbb{C}) \times \mathrm{GL}_2(\mathbb{C})$. We have $X \simeq \mathfrak{H}_3 \times \mathfrak{H}_3 \times \mathbb{R}$, where $\mathfrak{H}_3$ is hyperbolic 3-space; thus X is 7-dimensional. We remark that if we were to work with $\mathbf{G}' = R_{F/\mathbb{Q}}(\mathrm{SL}_2)$ instead, the appropriate symmetric space would be $\mathfrak{H}_3 \times \mathfrak{H}_3$. The extra flat factor $\mathbb{R}$ accounts for the fact that $\mathrm{SL}_2(\mathcal{O})$ has infinite index in $\mathrm{GL}_2(\mathcal{O})$.

One might ask why we prefer GL_2 to SL_2. First, one knows that the same cusp forms contributing to the cohomology of subgroups of $\mathrm{SL}_2(\mathcal{O})$ also appear in the cohomology of subgroups of $\mathrm{GL}_2(\mathcal{O})$, so there is no reason not to work with GL_2. But a more compelling reason for our choice is that there is a natural model of X in terms of the cone of positive-definite binary hermitian forms over F [1, 14]. In fact, using GL_2 is essential, since this linear model plays a key role in our computations of cohomology and the Hecke action; more details (for the analogous Hilbert modular case) can be found in [13].

Now let N be an ideal in $\mathcal{O}$. We consider the cohomology spaces $H^*(\Gamma_0(N); \mathbb{C}) = H^*(\Gamma_0(N)\backslash X; \mathbb{C})$, which contain classes corresponding to the cusp forms we want to study (the analogue of "weight two" modular forms). A priori we have cohomology in degrees 0 to 7, but thanks to a vanishing theorem of Borel–Serre [5] we know that the cohomology vanishes in degree 7 (the *virtual cohomological dimension* is 6). Furthermore, standard computations from representation theory show that the only degrees where cuspidal automorphic forms can contribute to the cohomology are 2 through 5, and that a given cusp form will contribute to all of these groups. Thus it suffices to investigate only one degree. Generalizing techniques of [2–4, 12], which treat $\mathrm{SL}_4(\mathbb{Z})$, and [13], which treats the Hilbert modular case, we developed an method to compute the cohomology space $H^5(\Gamma_0(N); \mathbb{C})$ and its structure as a Hecke module. The technique is similar to the modular symbol method, although the combinatorics are more involved (cf. [17, Appendix]).

We conclude by discussing our results and giving an example. We have computed the cuspidal subspace of $H^5(\Gamma_0(N); \mathbb{C})$ for all levels N with $\mathrm{Norm}(N) \leq 4800$, and for prime levels N with $\mathrm{Norm}(N) \leq 7921$. We have simultaneously compiled a list of elliptic curves over F of small norm conductor, essentially by carefully searching over the space of coefficients for Weierstrass equations. For each rational cuspidal Hecke eigenform we identified, we found an elliptic curve E over F whose number of points modulo primes not dividing the conductor N_E agreed with the Hecke eigenvalues for operators away from N_E, as far as we could compute both sides. Conversely, for any level N where we found no rational eigenclasses, we did not find any elliptic curve over F of that conductor. In other words, our data totally supports a generalization of a modularity conjecture connecting elliptic curves over F with rational Hecke eigenclasses.

The first prime level (up to Galois) where we found a rational eigenclass was the prime in $\mathcal{O}$ dividing 701. The corresponding elliptic curve has Weierstrass parameters $(a_1, a_2, a_3, a_4, a_6) = (-\zeta_5^2 - \zeta_5 - 1, \zeta_5^3 - \zeta_5, -\zeta_5^4, -\zeta_5^4, 0)$. We computed

the Hecke operators T_ℓ for primes ℓ with $\mathrm{Norm}(\ell) \leq 751$. Note that this curve is not a base change form $\mathbb{Q}(\sqrt{5})$ to F.[1]

References

[1] A. Ash, *Deformation retracts with lowest possible dimension of arithmetic quotients of self-adjoint homogeneous cones*, Math. Ann. **225** (1977), 69–76.

[2] A. Ash, P. E. Gunnells, and M. McConnell, *Cohomology of congruence subgroups of $SL_4(\mathbf{Z})$. III*, Math. Comp. (to appear).

[3] ———, *Cohomology of congruence subgroups of $SL_4(\mathbf{Z})$*, J. Number Theory **94** (2002), 181–212.

[4] ———, *Cohomology of congruence subgroups of $SL_4(\mathbf{Z})$. II*, J. Number Theory **128** (2008), no. 8, 2263–2274.

[5] A. Borel and J.-P. Serre, *Corners and arithmetic groups*, Comm. Math. Helv. **48** (1973), 436–491.

[6] A. Borel and N. Wallach, *Continuous cohomology, discrete subgroups, and representations of reductive groups*, second ed., Mathematical Surveys and Monographs, vol. 67, American Mathematical Society, Providence, RI, 2000.

[7] J. Bygott, *Modular forms and modular symbols over imaginary quadratic fields*, Ph.D. thesis, Exeter, 1999.

[8] J. E. Cremona, *Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields*, Compositio Math. **51** (1984), no. 3, 275–324.

[9] J. E. Cremona and E. Whitley, *Periods of cusp forms and elliptic curves over imaginary quadratic fields*, Math. Comp. **62** (1994), no. 205, 407–429.

[10] L. Dembélé, *Explicit computations of Hilbert modular forms on $\mathbb{Q}(\sqrt{5})$*, Experiment. Math. **14** (2005), no. 4, 457–466.

[11] J. Franke, *Harmonic analysis in weighted L_2-spaces*, Ann. Sci. École Norm. Sup. (4) **31** (1998), no. 2, 181–279.

[12] P. E. Gunnells, *Computing Hecke eigenvalues below the cohomological dimension*, Experiment. Math. **9** (2000), no. 3, 351–367.

[13] P. E. Gunnells and D. Yasaki, *Hecke operators and Hilbert modular forms*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, pp. 387–401.

[14] M. Koecher, *Beiträge zu einer Reduktionstheorie in Positivitätsbereichen. I*, Math. Ann. **141** (1960), 384–432.

[15] M. Lingham, *Modular forms and elliptic curves over imaginary quadratic fields*, Ph.D. thesis, Nottingham, 2005.

[16] J. Socrates and D. Whitehouse, *Unramified Hilbert modular forms, with examples relating to elliptic curves*, Pacific J. Math. **219** (2005), no. 2, 333–364.

[17] W. Stein, *Modular forms, a computational approach*, Graduate Studies in Mathematics, vol. 79, American Mathematical Society, Providence, RI, 2007, With an appendix by P. E. Gunnells.

[18] D. A. Vogan, Jr. and G. J. Zuckerman, *Unitary representations with nonzero cohomology*, Compositio Math. **53** (1984), no. 1, 51–90.

[1] In real time, as the talk concluded, Nils Bruin and Mark Watkins checked that the L-function of this curve doesn't vanish at the critical point and that its Mordell–Weil rank is zero.

Selmer Groups and Galois representations

Alex Bartel

In this talk, we present a technique for extracting information about certain integral Galois modules from other number theoretic quantities. This technique exploits the compatibility of standard conjectures or theorems about special values of L-functions with so-called Artin formalism. We will briefly explain the main idea below but first we give some examples of the results that can be proved using it:

Theorem 1 ([1], Theorem 1.1)**.** *Let p be a prime number. As $E/\mathbb{Q}$ ranges over elliptic curves and $F/\mathbb{Q}$ ranges over Galois extensions with Galois group D_{2p}, the order of the p-Selmer group $S_p(E/F)$ is unbounded.*

Theorem 2 ([2], Theorem 1.1)**.** *Let p be an odd prime, F/k a Galois extension of number fields with Galois group D_{2p}, S a finite Galois stable set of places of F including all the archimedean ones, K the intermediate quadratic extension and L, L' two distinct intermediate extensions of degree p over k. Then*

$$\frac{h_S(F)h_S(k)^2}{h_S(K)h_S(L)^2} = p^{\alpha}[\mathcal{O}_{S,F}^{\times} : \mathcal{O}_{S,L}^{\times}\mathcal{O}_{S,L'}^{\times}\mathcal{O}_{S,K}^{\times}]$$

for an easily computable explicit number α depending e.g. on the numbers of embeddings of the intermediate fields lying below those in S.

The technique for proving these results is essentially representation theoretic and will now be explained. Let F/K be a finite Galois extension of number fields with Galois group G and suppose that H_i and H'_j are two sets of subgroups such that there is an isomoprhism of permutation representations

$$\bigoplus_i \mathbb{C}[G/H_i] \cong \bigoplus_j \mathbb{C}[G/H'_j].$$

Write $L_i = F^{H_i}$, $L_j = F^{H'_j}$ and let E/K be an elliptic curve. Then, a set of identities between twisted L-functions of E, called Artin formalism implies that there is an equality of products of L-functions of E over corresponding fixed subfields of F:

$$\prod_i L(E/L_i, s) = \prod_j L(E/L'_j, s).$$

The conjecture of Birch and Swinnerton-Dyer then predicts that there should be an equality of the conjectural interpretations of leading coefficients of the Taylor expansions around $s = 1$, which after various cancellations reads

$$\prod_i \frac{\#Ш(E/L_i)\mathrm{Reg}(E/L_i)C(E/L_i)}{|E(L_i)_{\mathrm{tors}}|^2} \stackrel{?}{=} \prod_j \frac{\#Ш(E/L'_j)\mathrm{Reg}(E/L'_j)C(E/L'_j)}{|E(L'_j)_{\mathrm{tors}}|^2}, \tag{1}$$

where C denotes Tamagawa number, renormalised in a certain way but we will suppres that in the rest of the discussion, and Reg is the determinant of the Néron-Tate height pairing evaluated on a basis for the free part of the elliptic curve. This number is in general transcendental, but in the above situation we see that

$$\frac{\prod_i \mathrm{Reg}(E/L_i)}{\prod_j \mathrm{Reg}(E/L'_j)} \stackrel{?}{\in} \mathbb{Q}^\times.$$

In fact, equation (1) can be shown to be true only under the assumption that all the relevant Tate-Shafarevich groups are finite, but without assuming the full conjecture of Birch and Swinnerton-Dyer (see [3, Theorem 2.3]). Moreover, one can derive a very similar formula unconditionally, where the size of the Tate-Shafarevich group is replaced by a suitable expression of its torsion and its divisible part (see [3, Theorem 4.3] and [1, Section 4]).

The conceptual explanation for the rationality of the above regulator quotient was discovered by Tim and Vladimir Dokchitser. Namely the value of the regulator quotient does not depend on the particular choice of pairing with respect to which the determinants are evaluated and instead of the Néron-Tate height pairing any other bilinear non-degenerate G-invariant pairing on $E(F)$ could be chosen. In particular, if this pairing is $\mathbb{Q}$-valued then the value of the quotient is rational, therefore it always is. The regulator quotient can be regarded as a purely representation theoretic quantity, dependant only on the Galois module structure of $E(F)$ and if we understand its representation theoretic nature then we can infer properties of the Galois module $E(F)$ from other quantities present in equation (1). For example, to prove Theorem 1, one constructs elliptic curves over $\mathbb{Q}$ and Galois extensions $F/\mathbb{Q}$ with galois group D_{2p} such that the p-part of the Tamagawa number quotient gets arbitrarily large. One then needs to show that if (the p-part of) the regulator quotient gets arbitrarily large then the rank of the Galois module must get arbitrarily large.

The idea at the heart of Theorem 2 is very similar. This time, the Birch and Swinnerton-Dyer conjecture is replaced by the analytic class number formula. The main representation theoretic difficulty is that the regulator of a number field is defined differently from the regulator of an elliptic curve and to reduce the situation to a representation theoretic consideration one needs to be able to relate the quotient of regulators of number fields to the representation theoretic invariant we have encountered before.

References

[1] A. Bartel, *Large Selmer groups over number fields*, Math. Proc. Cambridge Philos. Soc. (to appear), arXiv:0805.1231v3 [math.NT], 2008.

[2] A. Bartel, *On Brauer-Kuroda type relations of S-class numbers in dihedral extensions*, arXiv: 0904.2416 [math.NT], 2009.

[3] T. Dokchitser and V. Dokchitser. *On the Birch-Swinnerton-Dyer quotients modulo squares*, Annals of Math. (to appear), arXiv:math/0610290v3 [math.NT], 2007.

Reporter: Alex Bartel

Participants

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

Alex Bartel
St. John's College
Department of Mathematics
GB-Cambridge CB2 1TP

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

Prof. Dr. Daniel J. Bernstein
2506 N.Clark #309
Chicago IL 60614
USA

Prof. Dr. Massimo Bertolini
Dipartimento di Matematica
Universita di Milano
Via C. Saldini, 50
I-20133 Milano

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

Dr. Martin Bright
Department of Mathematics
University of Bristol
University Walk
GB-Bristol BS8 1TW

Prof. Dr. Nils Bruin
Dept. of Mathematics and Statistics
Simon Fraser University
Burnaby 2 , B.C. V5A 1S6
CANADA

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-Louis Colliot-Thelene
Laboratoire de Mathematiques
Universite Paris Sud (Paris XI)
Batiment 425
F-91405 Orsay Cedex

Prof. Dr. Jean-Marc Couveignes
Departement de Mathematiques et
Informatique; UFR S.E.S.
Universite Toulouse II
5, Allee Antonio Machado
F-31058 Toulouse Cedex 9

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

Gabriele Dalla Torre
Mathematisch Instituut
Universiteit Leiden
P.O. Box 9512
NL-2300 RA Leiden

Prof. Dr. Henri Rene Darmon
Dept. of Mathematics and Statistics
McGill University
805, Sherbrooke Street West
Montreal , P.Q. H3A 2K6
CANADA

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

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

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

Prof. Dr. Eugene Victor Flynn
New College
University of Oxford
GB-Oxford OX1 3BN

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

Dr. Matthew Greenberg
Department of Mathematics and
Statistics
University of Calgary
2500 University Drive N.W.
Calgary Alberta T2N 1N4
CANADA

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

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

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

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

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
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
NL-2300 RA Leiden

Melanie Matchett Wood
Department of Mathematics
Stanford University
Building 380
Serra Mall
Stanford CA 94305-2125
USA

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

Dr. Kartik Prasanna
Department of Mathematics
University of Maryland
College Park , MD 20742-4015
USA

Jens Putzka
Max-Planck-Institut für Mathematik
Postfach 7280
53072 Bonn

Dr. Guillaume Ricotta
Institut de Mathematiques
Universite de Bordeaux I
351 Cours de la Liberation
F-33405 Talence Cedex

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
The 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

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

Denis Simon
Dept. de Mathematiques et Mecanique
Universite de Caen
F-14032 Caen Cedex

Prof. Dr. Alexei N. Skorobogatov
Imperial College
Department of Mathematics
Huxley Building
180 Queen's Gate
GB-London SW7 2AZ

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

Dr. Benjamin Smith
Laboratoire d'Informatique (LIX)
Ecole Polytechnique
F-91128 Palaiseau Cedex

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

Arjen Stolk
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
NL-2300 RA Leiden

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

Marco Streng
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
NL-2300 RA Leiden

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

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

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

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