Modular forms and elliptic curves over number fields

Paul E. Gunnells

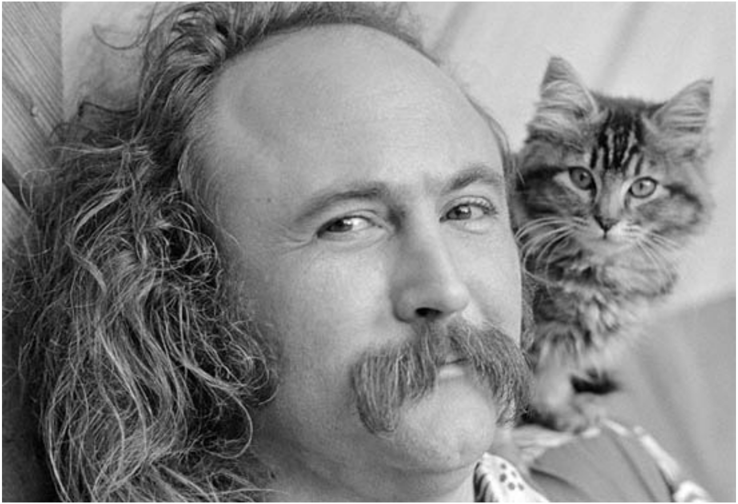
UMass Amherst

Thessaloniki 2014

Jeff

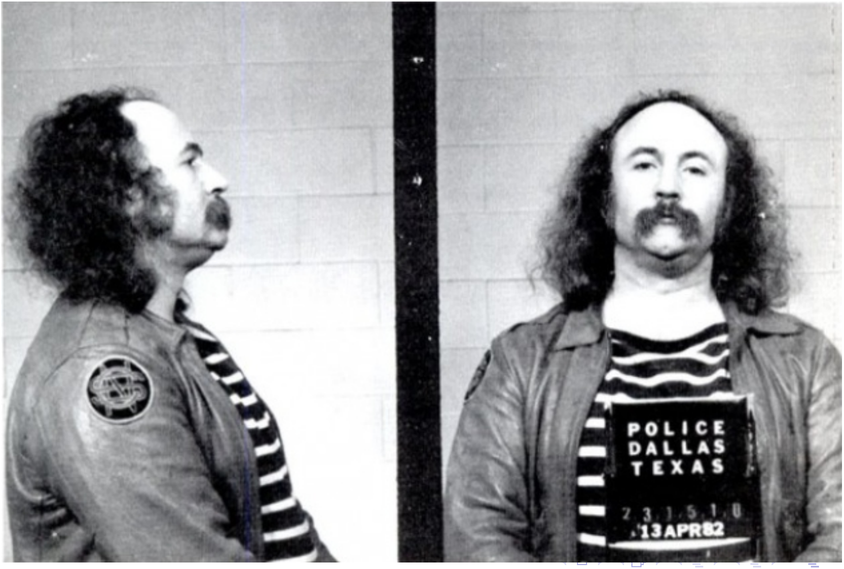
- Influential work in analytic number theory, automorphic forms (52 pubs on Mathsci, 690 citations)
- Excellent mentoring of graduate students, postdocs, other junior people (look around you!)
- Impeccable fashion sense, grooming (cf. the speaker)
- Seminal recordings with Graham Nash, Stephen Stills, and Neil Young

Jeff chillin in his crib



Jeff plays Central Park

Jeff visits Dorian at UT



Happy Birthday!

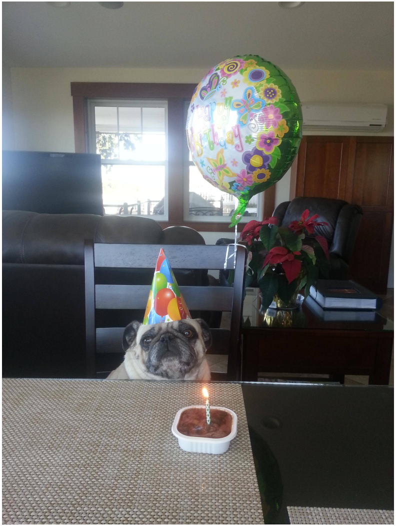
Happy Birthday Jeff!

Happy Birthday!

Happy Birthday!

Happy Birthday!

Happy Birthday!



Happy Birthday!

Goal

Our goal is computational investigation of connections between automorphic forms and elliptic curves over number fields.

- Test modularity of E: Given E/F, can we find a suitable automorphic form f on GL_2/F such that $L(s,f) = L(s,E)$?
- Test converse: Given f that appears to come from an elliptic curve over F (i.e. has rational Hecke eigenvalues), can one find an elliptic curve E/F such that $L(s,E) = L(s,f)$?
- Use input from automorphic forms to build tables of elliptic curves over F (up to isomorphism).

Note this work is purely computational, although in some cases one can computationally prove that a given curve E is modular (Faltings–Serre method).

Prior work

- Antwerp IV (Swinnerton-Dyer, Atkin, Velú, . . .). Tables of elliptic curves over $\mathbb{Q}$, weight 2 modular forms and their Hecke eigenvalues. Conductors up to 200.
- Cremona. Extensive table of elliptic curves over $\mathbb{Q}$ (currently up to conductor 350000 as of 5/14). Gold standard.
- Cremona, Whitley, Bygott, Lingham. Imaginary quadratic fields.
- Socrates–Whitehouse, Dembele. Certain real quadratic fields. Note: we now know all such elliptic curves are modular (Freitas–Le Hung–Siksek).
- Bober et. al. Database of curves over $\mathbb{Q}(\sqrt{5})$.

Our work

We treat two different fields that are in some sense as unlike each other as possible.

- G–Hajir–Yasaki (2013). $\mathbb{Q}(\zeta_5)$.
- G–Yasaki (2013). Cubic field of discriminant -23.
- Donnelly–G–Klages-Mundt–Yasaki (almost done). Cubic field of discriminant -23.

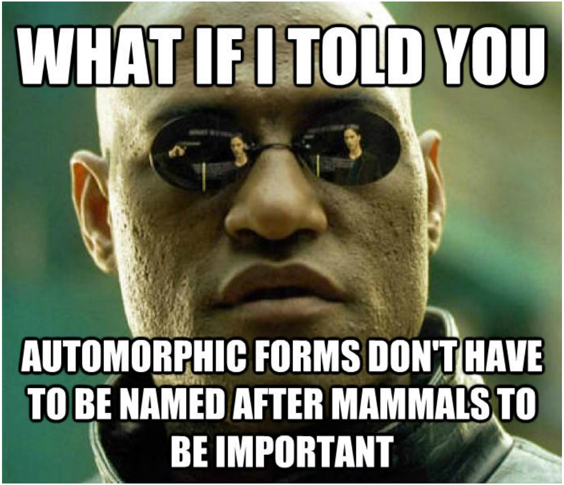
The fields

$\mathbb{Q}(\zeta_5)$ is totally complex quartic, Galois, CM, even cyclotomic. Much more symmetric than it should be.

The cubic field F of discriminant -23 is a nonreal cubic field, so not Galois. No symmetry. However it is not without charm.

- First in list of cubic fields ordered by $|\mathrm{disc}|$.
- Galois closure is Hilbert class field of $\mathbb{Q}(\sqrt{-23})$.
- Minimal volume of a closed hyperbolic 3-manifold is $3 \cdot 23^{3/2}\zeta_F(2)/4\pi^4$ (Gabai–Meyerhoff–Milley).
- Contains the *plastic number* $\rho = \sqrt[3]{1+\sqrt[3]{1+\sqrt[3]{1+\cdots}}}$.

What kinds of automorphic forms are these?


WHAT IF I TOLD YOU
AUTOMORPHIC FORMS DON'T HAVE TO BE NAMED AFTER MAMMALS TO BE IMPORTANT

$\mathbb{Q}$

Recall what happens over $\mathbb{Q}$. First the automorphic side.

- $\Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$
- $M_2(N) \supset S_2(N) \supset S_2^{\mathrm{new}}(N)$
- Given $f = \sum_{n>0} a(n)q^n$, $q = \exp(2\pi iz)$, we can make its L-function $L(s,f) = \sum a(n)n^{-s}$.
- Have action of Hecke operators T_p (for $p \nmid N$), U_p (for $p|N$). Simultaneously diagonalizable on $S_2^{\mathrm{new}}(N)$.

$\mathbb{Q}$

Now the elliptic curve side.

- E is given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathbb{Z}.$$

- Conductor N_E.
- For $p \nmid N_E$, put $b(p) = p + 1 - \#E(\mathbb{F}_p)$. If $p|N_E$, then $b(p) \in \{-1, 0, 1\}$ depending on singularity type mod p.
- L-function

$$L(s, E) = \prod_{p \nmid N_E} (1 - b(p)p^{-s} + p^{1-2s})^{-1} \prod_{p|N_E} (1 - b(p)p^{-s})^{-1}.$$

$\mathbb{Q}$

The correspondence is as perfect as one could hope.

- Given f rational 2 weight newform of level N, we can find a matching elliptic curve E_f. Eichler–Shimura construction.
- Given an elliptic curve $E/\mathbb{Q}$, one can find a weight 2 newform f_E with matching L-function. Wiles–Taylor–Breuil–Diamond.

Cohomology of the modular curve

How do we compute with modular forms? We use cohomology instead. Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$, $Y_\Gamma = \Gamma\backslash\mathfrak{H}$. Then

$$H^*(\Gamma;\mathbb{C}) \simeq H^*(Y_\Gamma;\mathbb{C}) \simeq S_2(\Gamma) \oplus \overline{S}_2(\Gamma) \oplus \mathrm{Eis}_2(\Gamma).$$

Moreover these isomorphisms are compatible with Hecke actions.

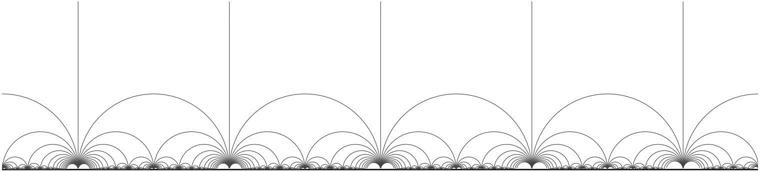
Modular symbols

For explicit computations we can use *modular symbols*. Let $\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{Q} \cup \infty$ and $X_\Gamma = \Gamma \backslash \mathfrak{H}^*$. Let $\alpha, \beta \in \mathfrak{H}^* \smallsetminus \mathfrak{H}$ be cusps of $\mathfrak{H}$. Then we can take an ideal geodesic from α to β and take its image in X_Γ. We get a class $\{\alpha, \beta\}_\Gamma \in H_1(X_\Gamma, \partial X_\Gamma; \mathbb{C})$.

These classes span. We can write down all the relations between them and can get a concrete model for the relative H_1, which is dual to H^1. The Hecke operators act on these symbols.

Unimodular symbols

Unfortunately this is not yet computable, because this model is infinitely presented. Instead one works with the *unimodular symbols*.



There are finitely many unimodular symbols mod Γ, and finitely many relations, but the Hecke operators don't act directly. However, Manin showed (with an algorithm) that any modular symbol can be written as a finite linear combination of unimodular symbols, so one can act by the Hecke operators.

General case

What to do in general? Instead of studying automorphic forms directly, we work with cohomology of arithmetic groups.

- Franke: these cohomology spaces can be computed in terms of certain automorphic forms. (Borel's conjecture.)
- Scholze: in many cases one can attach families of Galois representations to these cohomology classes. This had been known before for certain fields. For instance $\mathbb{Q}(\zeta_5)$ had been treated by Ramakrishnan. But for -23 we have no such result.

Geometric setup

$\mathbf{G}$	reductive connected algebraic group $/\mathbb{Q}$
$G = \mathbf{G}(\mathbb{R})$	group of real points (Lie group)
$K \subset G$	maximal compact subgroup
$A_G \subset G$	connected component of group of real points of maximal $\mathbb{Q}$-split torus in the center of G
$X = G/A_G K$	global symmetric space
$\Gamma \subset \mathbf{G}(\mathbb{Q})$	arithmetic subgroup

We want to compute $H^*(\Gamma; \mathbb{C}) = H^*(\Gamma\backslash X; \mathbb{C})$.

$\mathbb{Q}$

$\mathbf{G}$	$\mathrm{SL}_2/\mathbb{Q}$
G	$\mathrm{SL}_2(\mathbb{R})$
K	$\mathrm{SO}(2)$
A_G	trivial
X	the upper halfplane $\mathfrak{H}$
$\Gamma \subset \mathbf{G}(\mathbb{Q})$	congruence subgroup $\Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$

$F = \mathbb{Q}(\zeta_5)$

$\mathbf{G}$	$R_{F/\mathbb{Q}}\mathrm{GL}_2$
G	$\mathrm{GL}_2(\mathbb{C}) \times \mathrm{GL}_2(\mathbb{C})$
K	$\mathrm{U}(2) \times \mathrm{U}(2)$
A_G	$\mathbb{R}_+$
X	$\mathfrak{H}_3 \times \mathfrak{H}_3 \times \mathbb{R}$ (7 dimensional)
$\Gamma \subset \mathbf{G}(\mathbb{Q})$	congruence subgroup $\Gamma_0(\mathfrak{n}) \subset \mathrm{GL}_2(\mathscr{O})$

Note the flat factor in X. SL_2 vs GL_2.

F disc -23

$\mathbf{G}$	$R_{F/\mathbb{Q}}\mathrm{GL}_2$
G	$\mathrm{GL}_2(\mathbb{R}) \times \mathrm{GL}_2(\mathbb{C})$
K	$\mathrm{O}(2) \times \mathrm{U}(2)$
A_G	$\mathbb{R}_+$
X	$\mathfrak{H} \times \mathfrak{H}_3 \times \mathbb{R}$ (6 dimensional)
$\Gamma \subset \mathbf{G}(\mathbb{Q})$	congruence subgroup $\Gamma_0(\mathfrak{n}) \subset \mathrm{GL}_2(\mathscr{O})$

Which cohomology spaces?

Our spaces have more than one nontrivial cohomology group, so it's not clear which we want to study. Let d be the dimension of X.

Borel–Serre: We have $H^i = 0$ unless $i \leq \nu := d - 1$, the *virtual cohomological dimension*.

The *cuspidal cohomology*, that is the cohomology built from cuspidal automorphic forms via Franke's theorem, can only appear in a limited range.

Cuspidal range

Field	$\mathbb{Q}$	Imag quadratic	$\mathbb{Q}(\zeta_5)$	-23
$\dim X$	2	3	7	6
ν	1	2	6	5
top degree of H^*_{cusp}	1	2	5	4
bottom degree of H^*_{cusp}	1	1	2	2

Note that for our examples, the cuspidal cohomology doesn't appear in the top nonvanishing degree H^ν. This makes our computations a lot more difficult than the classical case.

Explicit reduction theory

For explicit computations we need good models for the locally symmetric spaces $\Gamma\backslash X$. In particular we want to apply tools from combinatorial topology, so we need analogues of the Farey tessellation (the ideal triangulation of $\mathfrak{H}$ with edges the unimodular geodesics).

We use generalizations of Voronoi's work on reduction theory for positive definite quadratic forms due to Ash and Koecher.

- $\mathbb{Q}(\zeta_5)$: Ash, as part of the team constructing toroidal compactifications of locally symmetric varieties (Kempf–Knudsen–Mumford–Rapaport–St. Donat–Tai) developed a very explicit reduction theory. CM is important here.
- -23: Koecher gave a very general construction that works for any number field. Not as easy to work with, but gives a practical method to find cell decompositions.

Cones and perfect forms

We model X via an appropriate cone C of positive definite forms.

- For $F = \mathbb{Q}(\zeta_5)$, we use positive definite binary hermitian forms over $F \otimes \mathbb{R}$, i.e. a product of two 4-dimensional real hermitian cones in two variables.
- For -23, we have to take a "mixed" cone. We take the product of the cone of positive definite binary quadratic forms/$\mathbb{R}$ and the cone of positive definite binary hermitian forms.

Cones and perfect forms

In both cases $\mathrm{GL}_2(\mathscr{O})$ acts, and we can finite an equivariant decomposition of C into finitely generated polyhedral cones with finitely many mod $\mathrm{GL}_2(\mathscr{O})$. The top-dimensional cones are called *perfect cones*.

We have $X \simeq C/\mathbb{R}_+$, and the perfect cones and their faces pass to cells in X. We can use complexes built on these cones to replace unimodular symbols.

Hecke operators

There is a natural action of the Hecke operators on cohomology, but they do not act directly on the complex built from the perfect cones.

As for the classical case, one needs a bigger complex, the analogue of the modular symbols. This is easy to define (*sharbly complex*). But the problem then becomes, given a Hecke image of a cycle, how do you rewrite it as a sum of unimodular cycles (i.e. cycles induced from the faces of the perfect cones)?

Hecke operators

This is much more challenging than the classical case. The complexity of the problem is governed by the gap between the top of the cuspidal range and the virtual cohomological dimension.

For our fields this gap is 1. That is, the cusp classes don't show up in the top degree but in degree one below. This also happens for $\mathrm{SL}_4(\mathbb{Z})$. In prior work with Ash–McConnell we developed an algorithm to treat this case. The ideas underlying this algorithm were extended by G–Yasaki to handle $\mathbb{Q}(\zeta_5)$, -23. Also GL_2/real quadratic and GL_3/imaginary quadratic.

New phenomena occur that reflect the presence of the flat factor.

Need to hear more? Ask me . . .

Elliptic curves

Now suppose we've computed various Hecke eigenclasses that appear to be attached to elliptic curves. We can then take their levels and attempt to find elliptic curves $/F$ that agree (i.e., have the same conductor and match the Hecke eigenvalues). We have several techniques at our disposal:

- Search over box of Weierstrass equations.

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathscr{O}.$$

- Torsion families. Have explicit families of curves with prescribed torsion (Kubert). If $l | \# E(\mathscr{O}/\mathfrak{p}\mathscr{O})$ for certain (infinitely many) $\mathfrak{p}$ then $l | \# E(F)_{tors}$. So we can look in such families for curves $/F$ (note that this requires knowledge of the Hecke eigenvalues).

Elliptic curves

Over -23, we found the curve

$$\begin{gathered} y^2 + (a^2+1)xy + ay \\ = x^3 + (-a^2+a+1)x^2 + (-249910a^2 + 438560a - 331055)x \\ +86253321a^2 - 151364024a + 114261323 \end{gathered}$$

with conductor $(3a^2 - 14a + 1)$ of norm 2065 by searching for curves with F-rational 6-torsion. Here $a^3 - a^2 + 1 = 0$.

Elliptic curves

- Twisting. We can construct new curves via quadratic twists. If the twist $d \in \mathscr{O}$ is small enough, the conductor of E^d might be within our search region. For instance this is how we found the curve

  $$y^2 + (a^2 + a)xy + a^2 y$$

  $$= x^3 + (-a^2 - a)x^2 + (-212a^2 + 305a - 181)x - 1422a^2 + 2466a - 2087$$

  with conductor $(-15a^2 + 8a - 1)$ and norm conductor 3025.

Elliptic curves

The most powerful technique is that of Cremona–Lingham. Their algorithm expresses searching for elliptic curves of a given conductor in terms of finding S-integral points on certain elliptic curves $/\mathbb{Q}$.

This exchanges one hard problem for another. Nevertheless it's a useful algorithm.

The current best implementation of this is in MAGMA by Steve Donnelly. In fact he extended this algorithm substantially in the course of this work.

$F = \mathbb{Q}(\zeta_5)$

Over this field we found excellent agreement between the cohomology and elliptic curves.

- For every elliptic curve over F within the range of our computation (all ideals of norm ≤ 4941, and prime ideals of norm ≤ 7921), we found a matching cohomology class.
- For every cohomology class, we were able to find a matching elliptic curve except in one case. At level norm 3025 there is an abelian surface over $F^+ = \mathbb{Q}(\sqrt{5})$ such that when we base change its automorphic form to F, the Euler factors become rational. This phenomenon was already observed by Cremona over imaginary quadratic fields.

$F = \mathbb{Q}(\zeta_5)$

- The curve of smallest conductor norm is

$$[a_1, a_2, a_3, a_4, a_6] = [-\zeta - 1, \zeta^2 - 1, 1, -\zeta^2, 0], \qquad (1)$$

which has conductor norm 701. In his thesis, Andrew Jones (Sheffield) extended Faltings–Serre to this setting and has proved that this curve is modular. He also produced examples for other complex quartic fields.

F disc -23

Over this field we've gone much further.

- Not only have we computed cohomology much further, we've also enumerated curves up to isomorphism in isogeny classes (using work of Billerey).
- We've also applied heuristics for dimensions of the subspace of Eisenstein cohomology and for old/newclasses to make predictions about conductors of elliptic curves should exist.
- Printed out, the resulting table has 171 pages and goes up to conductor norm 19987.
- We're (reasonably) confident that the table is complete up to norm 11575 is complete. Namely we have 212 levels with nontrivial unexplained newspace (all of dimension ≥ 2, none of dimension 1). Looking hard for curves at these levels found nothing.

Highlights

We finish with some examples over the cubic field.

- The first curve occurs at level norm 89:

$$[a+1, 2a^2+2a+2, 2a^2+a, 8a^2+2a-3, 6a^2-2a-5].$$

  It has 10-torsion and rank 0. There are three other curves in its isogeny class.

- The first curve with nontrivial rank occurs at level norm 719:

$$[a^2+1, 2a^2+2a+2, -a, 12a^2+a-5, 7a^2-7a-9].$$

  It has rank 1 and no torsion. It is alone in its isogeny class.

- The first curve of rank 2 occurs at level norm 9173:

$$[1, a^2+2, -a^2+1, a^2+2a-1, a^2].$$

  Again it is alone in its isogeny class.

The End

Thank you!