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

PAUL E. GUNNELLS
(joint work with Farshid Hajir, Dinakar Ramakrishnan, Dan Yasaki)

Let ζ_5 be a primitive fifth root of unity, and let $F = \mathbf{Q}(\zeta_5)$. 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 $\mathrm{SL}_2(\mathbf{Z})$ with a space of modular forms. More precisely, if $N \geq 1$ is an integer and if $\Gamma_0(N) \subset \mathrm{SL}_2(\mathbf{Z})$ is the usual congruence subgroup of matrices upper triangular mod N, then we have $H^1(\Gamma_0(N); \mathbf{C}) \simeq H^1(X_0(N); \mathbf{C}) \simeq S_2(N) \oplus \overline{S}_2(N) \oplus \mathrm{Eis}_2(N)$, 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 $\mathbf{Q}(\zeta_5)$" in the title.

Now we explain the setting for our computations. For our field we begin with the algebraic group $\mathbf{G} = R_{F/\mathbf{Q}}(\mathrm{GL}_2)$ (R denotes restriction of scalars), which satisfies $\mathbf{G}(\mathbf{Q}) = \mathrm{GL}_2(F)$. We replace the upper halfplane $\mathfrak{H}$ with the symmetric space X for the group $G = \mathbf{G}(\mathbf{R}) \simeq \mathrm{GL}_2(\mathbf{C}) \times \mathrm{GL}_2(\mathbf{C})$. We have $X \simeq \mathfrak{H}_3 \times \mathfrak{H}_3 \times \mathbf{R}$, where $\mathfrak{H}_3$ is hyperbolic 3-space; thus X is 7-dimensional. We remark that if we were to work with $\mathbf{G}' = R_{F/\mathbf{Q}}(\mathrm{SL}_2)$ instead, the appropriate symmetric space would be $\mathfrak{H}_3 \times \mathfrak{H}_3$. The extra flat factor $\mathbf{R}$ 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 $H^*(\Gamma_0(N); \mathbf{C}) = H^*(\Gamma_0(N)\backslash X; \mathbf{C})$, 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 $\mathrm{SL}_4(\mathbf{Z})$, and [13], which treats the Hilbert modular case, we developed an method to compute the cohomology space $H^5(\Gamma_0(N); \mathbf{C})$ 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 $H^5(\Gamma_0(N); \mathbf{C})$ 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 $\mathbf{Q}(\sqrt{5})$ to F.[1]

[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.

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.