2010

Modular forms and elliptic curves over the field of fifth roots of unity

PE Gunnells
University of Massachusetts - Amherst, gunnells@math.umass.edu

F Hajir
University of Massachusetts - Amherst, hajir@math.umass.edu

Dan Yasaki

MODULAR FORMS AND ELLIPTIC CURVES OVER THE FIELD OF FIFTH ROOTS OF UNITY

PAUL E. GUNNELLS, FARSHID HAJIR, AND DAN YASAKI

ABSTRACT. Let F be the cyclotomic field of fifth roots of unity. We computationally investigate modularity of elliptic curves over F.

1. Introduction

Let ζ be a primitive fifth root of unity, and let $F = \mathbb{Q}(\zeta)$. In this paper we describe 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 $\mathfrak{n}$ there should exist an automorphic form f on GL_2, also of conductor $\mathfrak{n}$, 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 $\mathfrak{n}$. 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 [9, 10, 14, 24] for complex quadratic fields, and of Socrates–Whitehouse [25] and Dembélé [15] 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. A main motivation for this is the Eichler–Shimura isomorphism, which identifies the cohomology of subgroups of $\mathrm{SL}_2(\mathbb{Z})$ with spaces of modular forms. More precisely, let $N \geq 1$ be an integer and let $\Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$ be the usual congruence subgroup of matrices upper triangular mod N. The group cohomology $H^*(\Gamma_0(N); \mathbb{C})$ is isomorphic to the cohomology $H^*(\Gamma_0(N)\backslash\mathfrak{H}; \mathbb{C})$, where $\mathfrak{H}$ is the upper halfplane. We have an isomorphism

$$H^1(\Gamma_0(N); \mathbb{C}) \simeq S_2(N) \oplus \overline{S}_2(N) \oplus \mathrm{Eis}_2(N), \tag{1}$$

Date: 14 May 2010.

1991 *Mathematics Subject Classification.* Primary 11F75; Secondary 11F67, 11G05, 11Y99.

Key words and phrases. Automorphic forms, cohomology of arithmetic groups, Hecke operators, elliptic curves.

We thank Mark Watkins for writing the appendix to this paper. PG thanks the NSF for support. FH thanks the NSA for support. This manuscript is submitted for publication with the understanding that the United States government is authorized to produce and distribute reprints. DY thanks UNC Greensboro for support through a UNC Greensboro New Faculty Grant.

where $S_2(N)$ 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 of level N, and the bar denotes complex conjugation.

Moreover (1) is an isomorphism of Hecke modules: there are Hecke operators defined on the cohomology $H^1(\Gamma_0(N);\mathbb{C})$ that parallel the usual operators defined on modular forms, and the two actions respect the isomorphism. This means that the cohomology of $\Gamma_0(N)$ provides a concrete way to compute with the modular forms of interest in the study of elliptic curves over $\mathbb{Q}$.

Further motivation is provided by Franke's proof of Borel's conjecture [16]. Franke's work shows that the cohomology of arithmetic groups can always be computed in terms of certain automorphic forms. Although the forms that occur in cohomology are a small subset of all automorphic forms, they are widely believed to have deep connections with arithmetic geometry. In particular, let $\Gamma_0(\mathfrak{n}) \subset \mathrm{GL}_2(\mathcal{O})$ be the congruence subgroup of matrices upper triangular modulo $\mathfrak{n}$. There is a subspace of the cohomology $H^*(\Gamma_0(\mathfrak{n});\mathbb{C})$ called the *cuspidal cohomology* that corresponds to cuspidal automorphic forms. This subspace provides a natural place to realize the "appropriate" automorphic forms above. Thus instead of defining what a "weight 2 modular form over F of level $\mathfrak{n}$" means, we work with the cuspidal cohomology with trivial coefficients of the congruence subgroup $\Gamma_0(\mathfrak{n})$.

We now give an overview of the contents of this paper and summarize our main results. In §2 we give the geometric background of our cohomology computations and describe the Hecke operators and how they act on cohomology. The next two sections give details about how we performed the cohomology computations. In §3 we explain the explicit reduction theory we need for the group $\mathrm{GL}_2(\mathcal{O})$, and in §4 we discuss how we compute the action of the Hecke operators on cohomology. Next we turn to the elliptic curve side of the story, and in §5 we examine various methods for writing down elliptic curves over F. Here the methods are more ad hoc than on the cohomology side. We describe the straightforward method of searching "in a box," and a trick using S-unit equations and the Frey–Hellegouarch construction. Finally in §6 we present our computational data. We give tables of cohomology data, including the levels where we found cuspidal cohomology and the dimensions, as well as some eigenvalues of Hecke operators $T_{\mathfrak{q}}$ for a range of primes $\mathfrak{q}$. We then give "motivic" explanations for the cuspidal cohomology classes with rational Hecke eigenvalues — either by identifying them as arising from weight 2 modular forms on $\mathbb{Q}$ or parallel weight 2 Hilbert modular forms on $F^+ = \mathbb{Q}(\sqrt{5})$, or by finding elliptic curves over F — that apparently match the eigenvalue data.

We were able to motivically account for every rational Hecke eigenclass we computed. All eigenclasses that appeared to come from classes over $\mathbb{Q}$ and F^+ were found using tables computed by Cremona [12] and tables/software due to Dembélé [15]. Of the eigenclasses that do not come from $\mathbb{Q}$ and F^+, for all but one our searches found elliptic curves over $\mathbb{Q}(\zeta_5)$ whose point counts matched the eigenvalue data. We also

note that one rational eigenclass we found corresponds to a "fake elliptic curve" in the sense of Cremona [11]. Details can be found in §6. The only form we were unable to account for occured at norm level 3641. After this paper was first distributed, Mark Watkins conducted a successful targeted search for the missing curve by modifying techniques of Cremona–Lingham [13]. We thank him for writing an appendix describing his result.

Conversely, within the range of our computations we were able to cohomologically account for all the elliptic curves over F that we found. That is, we found no elliptic curve over F that was not predicted by a rational Hecke eigenclass.

Acknowledgements. We thank Avner Ash, Kevin Buzzard, John Cremona, and Lassina Dembélé for helpful conversations and correspondence. We especially thank Dinakar Ramakrishnan for suggesting this project and for his encouragement. Finally, we thank Mark Watkins for finding the missing curve at norm level 3641 and for writing the appendix.

2. Geometric background

2.1. Let $\mathbf{G}$ be the reductive $\mathbb{Q}$-group $\mathrm{Res}_{F/\mathbb{Q}}(\mathrm{GL}_2)$, where Res denotes restriction of scalars. We have $\mathbf{G}(\mathbb{Q}) \simeq \mathrm{GL}_2(F)$. Let $G = \mathbf{G}(\mathbb{R})$ be the group of real points. We have $G \simeq \mathrm{GL}_2(\mathbb{C}) \times \mathrm{GL}_2(\mathbb{C})$, where the two factors corresponding to the two non-conjugate pairs of complex embeddings of F. Let $K \simeq \mathrm{U}(2) \times \mathrm{U}(2)$ be the maximal compact subgroup of G, and let $A_G \simeq \mathbb{C}^\times$ be the identity component of the real points of the maximal $\mathbb{Q}$-split torus in the center of G. Fix an ideal $\mathfrak{n} \subset \mathcal{O}$, and let Γ be the congruence subgroup $\Gamma_0(\mathfrak{n})$ defined in the introduction.

Let X be the global symmetric space $G/A_G K$. We have an isomorphism

$$X \simeq \mathfrak{H}_3 \times \mathfrak{H}_3 \times \mathbb{R}, \tag{2}$$

where $\mathfrak{H}_3$ is hyperbolic 3-space; thus X is 7-dimensional.

The space X should be compared with the product of upper halfplanes $\mathfrak{H} \times \mathfrak{H}$ one sees when studying Hilbert modular forms over quadratic fields. Indeed, if we were to work instead with $\mathbf{G}' = R_{F/\mathbb{Q}}(\mathrm{SL}_2)$, the appropriate symmetric space would be $\mathfrak{H}_3 \times \mathfrak{H}_3$, which makes the analogy clear. The extra flat factor $\mathbb{R}$ in (2) accounts for the difference between the centers of $\mathrm{GL}_2(\mathcal{O})$ and $\mathrm{SL}_2(\mathcal{O})$. As we will see in §3, it is much more convenient computationally to work with GL_2 instead of SL_2.

2.2. We are interested in the complex group cohomology $H^*(\Gamma; \mathbb{C})$, which can be identified with $H^*(\Gamma\backslash X; \mathbb{C})$. As mentioned in the introduction, there is a precise way to compute these cohomology spaces in terms of automorphic forms, and there is a distinguished subspace $H^*_{\mathrm{cusp}}(\Gamma\backslash X; \mathbb{C})$ corresponding to the cuspidal automorphic forms. We will not make this explicit here, and instead refer to [6, 7, 20, 23] for more information. Our goal now is to pin down exactly which cohomology group we want to study. In other words, which cohomology space $H^i(\Gamma\backslash X; \mathbb{C})$, where $0 \le i \le 7$, plays the role of H^1 of the modular curve?

First, although we a priori have cohomology in degrees 0 to 7, a result of Borel–Serre [5] implies that H^7 vanishes identically. Moreover, standard computations from representation theory (cf. [23]) show that $H^i_{\text{cusp}}(\Gamma\backslash X;\mathbb{C}) = 0$ unless $2 \leq i \leq 5$. One also knows that if a cuspform contributes to any of these degrees, it does to all, and in essentially the same way. For computational reasons it is much easier to work with cohomology groups of higher degree, and so we choose to work with $H^5(\Gamma\backslash X;\mathbb{C})$.

2.3. Next we consider the Hecke operators. Let $\tilde{\Gamma} \subset \mathbf{G}(\mathbb{Q})$ be the commensurator of Γ. By definition $\tilde{\Gamma}$ consists of all $g \in \mathbf{G}(\mathbb{Q})$ such that both Γ and $\Gamma^g := g^{-1}\Gamma g$ have finite index in $\Gamma' := \Gamma \cap \Gamma^g$. The inclusions $\Gamma' \to \Gamma$ and $\Gamma' \to \Gamma^g$ determine a diagram

$$\begin{array}{ccc} & \Gamma'\backslash X & \\ {\scriptstyle s}\swarrow & & \searrow{\scriptstyle t} \\ \Gamma\backslash X & & \Gamma\backslash X \end{array}$$

Here $s(\Gamma' x) = \Gamma x$ and t is the composition of $\Gamma' x \mapsto \Gamma^g x$ with left multiplication by g. This diagram is the *Hecke correspondence* associated to g. It can be shown that, up to isomorphism, the Hecke correspondence depends only on the double coset $\Gamma g \Gamma$.

Because the maps s and t are proper, they induce a map on cohomology:

$$t_* s^* \colon H^*(\Gamma\backslash X;\mathbb{Z}) \to H^*(\Gamma\backslash X;\mathbb{Z}).$$

We denote the induced map by T_g and call it the *Hecke operator* associated to g.

In our application we consider g of the form $\left(\begin{smallmatrix} 1 & 0 \\ 0 & a \end{smallmatrix}\right)$, where a is a generator of any prime ideal $\mathfrak{q}$ coprime with $\mathfrak{n}$ (note every ideal in $\mathcal{O}$ is principal since F has class number 1). Thus we are led to the main computational issue on the modular side: for each $\mathfrak{n}$ compute the space $H^5_{\text{cusp}}(\Gamma_0(\mathfrak{n})\backslash X;\mathbb{C})$ together with the action of the Hecke operators

$$\left\{ T_{\mathfrak{q}} \;\middle|\; \mathfrak{q} \text{ prime}, \, \mathfrak{q} \nmid \mathfrak{n} \right\}.$$

3. Reduction theory

3.1. In this section we explain the connection between our symmetric space X and a cone of Hermitian forms. This connection is exactly the reason we prefer to work with $\mathrm{GL}_2(\mathcal{O})$ instead of $\mathrm{SL}_2(\mathcal{O})$. Let $\iota = (\iota_1, \iota_2)$ denote the (non complex conjugate) embeddings

$$\iota : F \to \mathbb{C} \times \mathbb{C}$$

given by sending ζ to (ζ, ζ^3). We abbreviate the second embedding by $\cdot'$, and for $\alpha \in F$ write (α, α') for $\iota(\alpha)$.

First let V be the real vector space of 2×2 Hermitian matrices over $\mathbb{C}$. Let $C \subset V$ be the cone of positive-definite Hermitian matrices. The cone C is preserved by homotheties (scaling by $\mathbb{R}_{>0}$), and the quotient is isomorphic to $\mathrm{GL}_2(\mathbb{C})/A{\cdot}\mathrm{U}(2) \simeq \mathfrak{H}_3$, where A denotes the diagonal subgroup of $\mathrm{GL}_2(\mathbb{C})$.

Our symmetric space X is then built from two copies of C, reflecting the structure of ι. More precisely, let $\mathcal{V} = V \times V$ and $\mathcal{C} = C \times C$. Again $\mathcal{C}$ is preserved by homotheties, and we have an diffeomorphism

$$\mathcal{C}/\mathbb{R}_{>0} \xrightarrow{\sim} X = G/A_G K, \tag{3}$$

where G, A_G, K are as in §2.1.

3.2. Now we introduce an F-structure into the picture. Let $F^+ \subset F$ be the real quadratic subfield $\mathbb{Q}(\sqrt{5})$. Then a *binary Hermitian form over* F is a map $\phi\colon F^2 \to F^+$ of the form

$$\phi(x, y) = ax\bar{x} + bx\bar{y} + \bar{b}\bar{x}y + cy\bar{y},$$

where $a, c \in F^+$ and $b \in F$. Note that $\hat{\phi} = \phi + \phi'$ takes values in $\mathbb{Q}$. Indeed, $\hat{\phi}$ is precisely the composition $\mathrm{Tr}_{F^+/\mathbb{Q}} \circ \phi$, and by choosing a $\mathbb{Q}$-basis for F, $\hat{\phi}$ can be viewed as a quaternary quadratic form over $\mathbb{Q}$. In particular, it follows that $\hat{\phi}(\mathcal{O}^2)$ is discrete in $\mathbb{Q}$.

The *minimum of* ϕ is

$$m(\phi) = \inf_{v \in \mathcal{O}^2 \setminus \{0\}} \hat{\phi}(v).$$

A vector $v \in \mathcal{O}^2$ is *minimal vector* for ϕ if $\phi(v) = m(\phi)$. The set of minimal vectors for ϕ is denoted $M(\phi)$. A Hermitian form over F is *perfect* if it is uniquely determined by $M(\phi)$ and $m(\phi)$.

3.3. We now recall the explicit reduction theory of Koecher [22] and Ash [1] that generalizes work of Voronoï on rational positive-definite quadratic forms [26]. Although these constructions can be done in more generality, we only work with GL_2 over our field F.

Recall that $\mathcal{V} = V \times V$ and $\mathcal{C} = C \times C$. Let $q\colon F^2 \to \mathcal{V}$ be the map defined by

$$q(v) = (vv^*, v'v'^*). \tag{4}$$

Here we view v as a column vector, and $*$ means complex conjugate transpose. The restriction of q to $\mathcal{O}^2 \smallsetminus \{0\}$ defines a discrete subset Ξ of $\bar{\mathcal{C}}$, the closure of $\mathcal{C}$ in $\mathcal{V}$. Let Π be the closed convex hull in $V \times V$ of Ξ. Then Π is an infinite polyhedron known as the *Voronoï polyhedron*. It comes equipped with a natural action of $\mathrm{GL}_2(\mathcal{O})$. Modulo this action Π has finitely many faces, and the top-dimensional faces are in bijection with the perfect quadratic forms over F.

Let Σ be the collection of cones on the faces of Π. The set Σ forms a Γ-*admissible polyhedral decomposition* in the sense of [1]; in particular Σ is a fan and admits an action of $\mathrm{GL}_2(\mathcal{O})$. When intersected with the cone $\mathcal{C}$, the cones in Σ provide an explicit reduction theory for $\mathrm{GL}_2(\mathcal{O})$ in the following sense. Any point $x \in \mathcal{C}$ is contained in a unique $\sigma(x) \in \Sigma$, and the set

$$\{\gamma \in \mathrm{GL}_2(\mathcal{O}) \mid \gamma \cdot \sigma(x) = \sigma(x)\}$$

is finite. There is also an explicit algorithm to determine $\sigma(x)$ given x, the *Voronoï reduction algorithm* [17, 26].

3.4. Every cone $\sigma \in \Sigma$ is preserved by homotheties, and thus defines a subset in X via (3). We call these subsets *Voronoï cells*. One can think of the Voronoï cells as providing a polytopal tessellation of X, although some faces of the polytopes might be at infinity. Because of this latter point it is somewhat awkward to use Σ directly to compute cohomology, although there is a workaround.

According to [2], there is a deformation retraction $\mathcal{C} \to \mathcal{C}$ that is equivariant under the actions of both $\mathrm{GL}_2(\mathcal{O})$ and the homotheties. Its image modulo homotheties is the *well-rounded retract* W in X. The well-rounded retract is contractible, and we have $H^*(\Gamma\backslash X; \mathbb{C}) \simeq H^*(\Gamma\backslash W; \mathbb{C})$. Moreover, the quotient $\Gamma\backslash W$ is compact.

The well-rounded retract W is naturally a locally finite cell complex. The group $\mathrm{GL}_2(\mathcal{O})$ preserves the cell structure, and the stabilizer of each cell in $\mathrm{GL}_2(\mathcal{O})$ is finite. One can show that the cells in W are in a one-to-one, inclusion-reversing correspondence with the cones in the Voronoï fan Σ and thus with the Voronoï cells. This makes it possible to use either the cells in W or the Voronoï cells to compute cohomology. Section 3 of [4] gives a very detailed description of how to use W to compute $H^*(\Gamma\backslash W; \mathbb{C})$.[1]

3.5. The structure of Π in our case has been explicitly determined by one of us (DY) [27].

Modulo the action of $\mathrm{GL}_2(\mathcal{O})$, there is one perfect form ϕ, represented by the matrix

$$A_\phi = \frac{1}{5}\begin{pmatrix} \zeta^3+\zeta^2+3 & \zeta^3-\zeta^2+\zeta-1 \\ -2\zeta^3-\zeta-2 & \zeta^3+\zeta^2+3 \end{pmatrix}.$$

The perfect form ϕ has 240 minimal vectors. It is clear that if $v \in M(\phi)$ then $\tau v \in M(\phi)$ for any torsion unit $\tau \in \mathcal{O}$; modulo torsion units there are 24 minimal vectors. Let ω denote the unit $\zeta + \zeta^2$. Then modulo torsion the minimal vectors for ϕ are

(5)
$$\begin{pmatrix} -\zeta+1 \\ \zeta^3+1 \end{pmatrix}, \begin{pmatrix} -\zeta^3+1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -\omega \end{pmatrix}, \begin{pmatrix} 1 \\ -\zeta^2 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ \zeta^3 \end{pmatrix}, \begin{pmatrix} 1 \\ -\zeta^2+1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ \zeta^3+1 \end{pmatrix},$$
$$\begin{pmatrix} 1 \\ \zeta+1 \end{pmatrix}, \begin{pmatrix} 1 \\ \zeta^3+\zeta+1 \end{pmatrix}, \begin{pmatrix} 1 \\ -\zeta^4 \end{pmatrix}, \begin{pmatrix} \omega^{-1} \\ \zeta^4 \end{pmatrix}, \begin{pmatrix} \omega^{-1} \\ \zeta^4-1 \end{pmatrix}, \begin{pmatrix} \omega^{-1} \\ -1 \end{pmatrix}, \begin{pmatrix} \omega^{-1} \\ -\zeta^3-1 \end{pmatrix},$$
$$\begin{pmatrix} \omega^{-1} \\ -\zeta^3-\zeta^2-1 \end{pmatrix}, \begin{pmatrix} \omega \\ \omega+1 \end{pmatrix}, \begin{pmatrix} \omega \\ -\zeta^3 \end{pmatrix}, \begin{pmatrix} \omega \\ 0 \end{pmatrix}, \begin{pmatrix} \omega \\ \zeta^2 \end{pmatrix}, \begin{pmatrix} \omega \\ \omega \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ \omega \end{pmatrix}.$$

[1] More precisely, in [4, §3] the authors work with the equivariant cohomology $H^*_\Gamma(W; \mathbb{C})$, but this is isomorphic to $H^*(\Gamma\backslash W; \mathbb{C})$ since $\mathbb{C}$ has characteristic zero.

In $\bar{\mathcal{C}}$ these become 24 points defining an 8-cone, which represents the unique top-dimensional cone in Σ modulo $\mathrm{GL}_2(\mathcal{O})$. Moreover, one can compute the rest of the cones in Σ modulo $\mathrm{GL}_2(\mathcal{O})$. One finds 5 $\mathrm{GL}_2(\mathcal{O})$-classes of 7-cones, 10 classes of 6-cones, 11 classes of 5-cones, 9 classes of 4-cones, 4 classes of 3-cones, and 2 classes of 2-cones. We refer to [27] for details.

4. Hecke operators

4.1. The Voronoï fan Σ gives us a convenient model to compute cohomology, but unfortunately one cannot use it directly to compute the action of the Hecke operators. The problem is that the Hecke operators, when thought of as Hecke correspondences acting geometrically on the locally symmetric space $\Gamma\backslash X$, do not preserve the tessellation corresponding to Σ. To address this problem, we introduce another complex computing the cohomology, the *sharbly complex* S_* [3].

Given any nonzero $v \in F^2$, let $R(v) \subset \mathcal{V}$ be the ray through the point $q(v)$ from (4). Let S_k, $k \geq 0$, be the Γ-module A_k/C_k, where (i) A_k is the set of formal $\mathbb{Z}$-linear sums of symbols $\mathbf{v} = [v_1, \cdots, v_{k+2}]$, (ii) each v_i is a nonzero element of F^2, and (iii) C_k is the submodule generated by

(1) $[v_{\sigma(1)}, \cdots, v_{\sigma(k+2)}] - \mathrm{sgn}(\sigma)[v_1, \cdots, v_{k+2}]$, where σ is a permutation on $k+2$ letters,
(2) $[v, v_2, \cdots, v_{k+2}] - [w, v_2, \cdots v_{k+2}]$ if $R(v) = R(w)$, and
(3) $[v]$, if v is *degenerate*, i.e., if $v_1, \cdots, v_{k+2}$ are contained in a hyperplane.

We define a boundary map $\partial\colon S_{k+1} \to S_k$ by

$$\partial[v_1, \cdots, v_{k+2}] = \sum_{i=1}^{k+2} (-1)^i [v_1, \cdots, \hat{v}_i, \cdots, v_{k+2}]. \tag{6}$$

This makes S_* into a complex. Note that S_* is indexed as a homological complex, i.e. the boundary map has degree (-1). We remark that the our definition is slightly different from that of [3]. In particular the complex in [3] uses unimodular vectors over $\mathcal{O}^2$ and does not include the relation (2). However it is easy to see that the complexes are quasi-isomorphic.

The basis elements $\mathbf{v} = [v_1, \cdots, v_{k+2}]$ are called *k-sharblies*. Our field F has class number 1, and so using the relations in C_k one can always find a representative for $\mathbf{v}$ with each v_i a primitive vector in $\mathcal{O}^2$. In particular, one can always arrange that each $q(v_i)$ is a vertex of Π. When such a representative is chosen, the v_i are unique up to multiplication by a torsion unit in F. In this case the v_i—or by abuse of notation the $q(v_i)$—are called the *spanning vectors* for $\mathbf{v}$. We say a sharbly is *Voronoï-reduced* if its spanning vectors are a subset of the vertices of a Voronoï cone.

The geometric meaning of this notion is the following. Each sharbly $\mathbf{v}$ with spanning vectors v_i determines a closed cone $\sigma(\mathbf{v})$ in $\bar{\mathcal{C}}$, by taking the cone generated by the points $q(v_i)$. Then $\mathbf{v}$ is Voronoï-reduced if and only if $\sigma(\mathbf{v})$ is contained in some Voronoï cone. It is clear that there are finitely many Voronoï-reduced sharblies

modulo Γ. Not every cone $\sigma(\mathbf{v})$ is actually a cone in the fan Σ, and not every cone in Σ has the form $\sigma(\mathbf{v})$. However, as we will see, this causes no difficulty in our computations.

We can also use the spanning vectors to measure how "big" a 0-sharbly $\mathbf{v}$ is: we define the *size of* $\mathbf{v}$ $\mathrm{size}(\mathbf{v})$ to be the absolute value of the norm determinant of the 2×2 matrix formed by spanning vectors for $\mathbf{v}$. By construction size takes values in $\mathbb{Z}_{>0}$. In the classical picture for $\mathbf{G} = \mathrm{GL}_2/\mathbb{Q}$, there is only one (up to conjugation and scaling) perfect form, and it has minimal vectors e_1, e_2, e_1+e_2. Thus for $F = \mathbb{Q}$, a 0-sharbly is Voronoï-reduced if and only if it has size 1, and a 1-sharbly is Voronoï-reduced if and only if its boundary is consists of 0-sharblies of size 1. For GL_2 over general number fields, the size of a 0-sharbly $\mathbf{v}$ is related to whether or not $\mathbf{v}$ is Voronoï-reduced, but in general there exist Voronoï-reduced 0-sharblies with size > 1.

We now consider our field $\mathbb{Q}(\zeta)$. The vertices of a fixed top-dimensional Voronoï cone are given in (5). Using this data one can check that a non-degenerate 0-sharbly is Voronoï-reduced if and only if it has size 1 or 5. For $k > 1$, the relationship between size and Voronoï-reduced k-sharblies is more subtle, but a necessary condition is that each of the sub 0-sharblies must have size 1 or 5.

The boundary map (6) commutes with the action of Γ, and we let $S_*(\Gamma)$ be the homological complex of coinvariants. Note that $S_*(\Gamma)$ is infinitely generated as a $\mathbb{Z}\Gamma$-module. One can show, using Borel–Serre duality [5], that

$$H_k((S_* \otimes \mathbb{C})(\Gamma)) \xrightarrow{\sim} H^{6-k}(\Gamma; \mathbb{C}) \tag{7}$$

(cf. [3]). Moreover, there is a natural action of the Hecke operators on $S_*(\Gamma)$ (cf. [18]). We note that the Voronoï-reduced sharblies form a *finitely generated* subcomplex of $S_*(\Gamma)$ that also computes the cohomology of Γ as in (7). This is our finite model for the cohomology of Γ.

4.2. The complex of Voronoï-reduced sharblies is not stable under the action of Hecke operators. Thus in order to use the subcomplex of Voronoï-reduced sharblies to compute Hecke operators, one needs a "reduction algorithm" for representing the class of a sharbly that is not Voronoï-reduced as a sum of Voronoï-reduced sharblies. We employ a method analogous to the one described in [19] for real quadratic fields, adapted for the field $F = \mathbb{Q}(\zeta)$.

For the convenience of the reader, we recall some of the key points. By (7), in order to compute cohomology classes in $H^5(\Gamma; \mathbb{C})$, we need to reduce 1-sharblies. Specifically, a cohomology class can be thought of as a linear combination of Voronoï-reduced 1-sharblies, and the Hecke action sends a Voronoï-reduced 1-sharbly to a 1-sharbly that is no longer Voronoï-reduced. The reduction algorithm an iterative process which proceeds by replacing a 1-sharbly that is not Voronoï-reduced by a sum of 1-sharblies that are closer (in a sense described below) to being Voronoï-reduced.

As described above, the boundaries of Voronoï-reduced sharblies have boundaries components of size 0, 1, or 5, and so size gives a coarse measure of how bad, or far

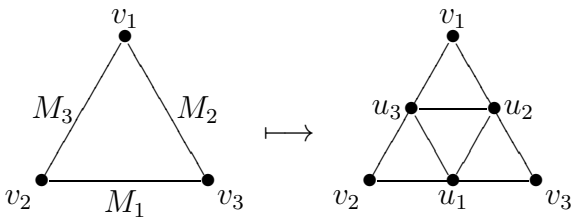

FIGURE 1. Reduction of generic 1-sharbly.

from Voronoï-reduced, a 1-sharbly is. We describe the reduction of a generic bad 1-sharbly here; the other special cases are treated with analogous modifications of [19].

A generic 1-sharbly $\mathbf{v}$ that is not Voronoï-reduced has boundary components that have large size, and so can be thought of as a triangle $\mathbf{v} = [v_1, v_2, v_3]$ such that $\text{size}([v_i, v_j]) \gg 0$. We split each edge by choosing *reducing points* u_1, u_2, and u_3 and forming three additional edges $[u_1, u_2], [u_2, u_3]$, and $[u_3, u_1]$. We then replace T by the four 1-sharblies

$$[v_1, v_2, v_3] \longmapsto [v_1, u_3, u_2] + [u_3, v_2, u_1] + [u_2, u_1, v_3] + [u_1, u_2, u_3] \tag{8}$$

as seen in Figure 4.2. Choosing the reducing points uses the Voronoï polyhedron. Specifically, the spanning vectors of the 0-sharbly $[v_i, v_j]$ are points in the 8-dimensional vector space $\mathcal{V}$. The barycenter b of the line joining these points lies in a Voronoï cone σ. The cone σ lies between the cone containing v_i and the cone containing v_j, and so the vertices of σ form the candidates for reducing points for the 0-sharbly $[v_i, v_j]$. We choose the reducing point u so that the sum $\text{size}([v_i, u]) + \text{size}([u, v_j])$ is minimized. Note that we have not proved that this process decreases size, so we are not guaranteed that

$$\text{size}([v_i, v_j]) > \max(\text{size}([v_i, u]), \text{size}([u, v_j])). \tag{9}$$

Nor are we guaranteed that the 1-sharbly at the far right of (8) is closer to being Voronoï-reduced than the original 1-sharbly $[v_1, v_2, v_3]$. However, in practice we find that both of these problems do not arise. Indeed, the sizes of the 0-sharblies on the right of (9) are typically much smaller than the size of $[v_i, v_j]$, and the 1-sharbly $[u_1, u_2, u_3]$ is usually quite close to being Voronoï-reduced.

Eventually one produces a 1-sharbly cycle with all edges Voronoï-reduced. Unfortunately this is not enough the guarantee that the cycle *itself* is Voronoï-reduced. This situation does not occur when one works over $\mathbb{Q}$ as in [4], and reflects the presence of units of infinite order. Some additional reduction steps are needed to deal with this problem. The technique is very similar to reduction step (IV) in [19, §3.5].

5. Elliptic curves

5.1. In this section we describe how we constructed the elliptic curve table at the end of the paper (Table 7). The method itself is the most naive and straightforward one can imagine. Recall that $\mathcal{O} = \mathbb{Z}[\zeta]$ and for a positive integer B, let

$$S_B = \big\{ c_0 + c_1\zeta + c_2\zeta^2 + c_3\zeta^3 \;\big|\; |c_i| \leq B, 0 \leq i \leq 3 \big\},$$

be a boxed grid of size $16B^4$ inside the lattice of algebraic integers in F, centered at the origin. For each positive integer N, there exists a bound $B = B(N)$ such that every elliptic curve E over F of conductor having norm at most N has a Weierstrass model

$$E : y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6, \qquad \text{with} \qquad a_1, a_2, a_3, a_4, a_6 \in S_{B(N)}.$$

With $N = 10^4$, for example, having found all modular forms which should correspond to elliptic curves having conductor of norm at most N, we could in principle produce a proof that no elliptic curves not predicted to exist from the cohomology data up to that level exist as well as finding the predicted curves. The bound $B(N)$, however, is so large as to make this not a practical exercise at the moment. Under the assumption of certain conjectures (the ABC conjecture, for example), one can obtain a much smaller conditional bound $B^*(N)$, but even this would be far too large to carry out the proof.

The question we posed for ourselves, therefore, was much a more practical one: (i) can we perform a reasonable search that finds an elliptic curve of the predicted conductor matching each rational cuspidal eigenclass that was found, and (ii) can we in the process show that though the search is not exhaustive, no unpredicted elliptic curves appear?

5.2. We therefore sifted through curves whose coefficients a_i lie in the box S_1, keeping only those whose discriminants have modestly sized norm, then filtering those remaining for having conductor of small norm. Every curve that was found with conductor having norm less than 10^4, matched up with a rational cuspidal eigenclass from Tables 3 and 5. For each of these curves, we then computed the coefficients $a_{\mathfrak{q}} = \mathrm{Norm}(\mathfrak{q}) + 1 - |E(\mathbb{F}_{\mathfrak{q}})|$ and found that these matched the Fourier coefficients of the corresponding form for as many $\mathfrak{q}$ as were computed on the cohomology side. Of course the computation of $a_{\mathfrak{q}}$ on the elliptic curve side is very rapid, so in this way we are able to produce predicted Frobenius eigenvalues of the modular forms for quite large primes.

5.3. Before proceeding with the box search above—which in the end was the most effective method we could find—we applied another technique. Although this technique is less systematic, it provides a strategy for answering a slightly different question: Suppose F is a number field with class number 1, and an oracle predicts the existence of an elliptic curve over F of a certain conductor $\mathfrak{n}$, where $\mathfrak{n}$ is a square-free ideal of fairly small norm, assumed to be odd for simplicity. What are some ways in which one

can attempt to find a Weierstrass model for this putative curve and thereby confirm the prediction of the oracle? Though we did not need to use it to find the curves we needed, we discuss a method for answering this question in case it may serve in another context.

The idea is to use the Frey–Hellegouarch construction of elliptic curves. Namely, suppose $u + v = w$ is an equation of S-units where S is the set of primes of $\mathcal{O}_F$ dividing $\mathfrak{n}$; this means that $u, v, w \in \mathcal{O}_F$ are not divisible by primes outside S. Let S' be the union of S with the set of $\mathcal{O}_F$-primes dividing 2. Then, the curve $E_{u,v}$ given by the model $y^2 = x(x-u)(x+v)$ has good reduction away from S'. By imposing congruences on u and v, we may guarantee that $E_{u,v}$ has good reduction outside S. To speed up the computation, we note that if ξ is an S-unit, then $E_{\xi u,\xi v}$ is a quadratic twist by $\sqrt{\xi}$ of $E_{u,v}$. It's also easily seen that curves obtained from re-orderings such as $E_{v,u}$, $E_{u,-w}$ etc. are also at most quadratic twists by $\sqrt{-1}$. Thus, it's convenient to search over curves $E_{1,\varepsilon}$ and its quadratics twists by square roots of S-units. In the case of $F = \mathbb{Q}(\zeta)$, $\mathcal{O}_F^\times/\mathcal{O}_F^{\times 2}$ is generated by $\langle -1, 1+\zeta\rangle$, so for each S-unit equation $1 + \varepsilon = \rho$, we get four curves $E_{1,\varepsilon}$, $E_{-1,-\varepsilon}$, $E_{1+\zeta,(1+\zeta)\varepsilon}$, and $E_{-(1+\zeta),-(1+\zeta)\varepsilon}$.

One can experimentally search for S-unit equations via a similar grid search as above. Namely, one finds a basis $\xi_1, \ldots, \xi_r$ for the group of S-units and for a given bound B searches over integer r-tuples $(m_i)_{i=1}^r$ satisfying $|m_i| \leq B$ to see if $\varepsilon = \prod \xi_i^{m_i}$ yields an S-unit equation $1 + \varepsilon = \rho$ by first filtering out those with unsuitable $\mathrm{Norm}(1+\varepsilon)$. For example, if $\mathfrak{n} = (\nu)$ is a principal prime ideal, we can take a basis $\xi_1, \ldots \xi_r$ of $\mathcal{O}_F^\times$ and check whether $\mathrm{Norm}(\nu - \prod_i \xi_i^{m_i}) = \pm 1$.

As an example over $F = \mathbb{Q}(\zeta)$, the unit group is generated by $-\zeta, 1+\zeta$. If we take $1 + \varepsilon = \rho$ where $\varepsilon = -\zeta^3(1+\zeta)^{24}$, then the curve $E_{1,\varepsilon}$ has discriminant $\Delta = 2^{12}3^4 5\zeta^4(1+\zeta)^{72}$, conductor $\mathfrak{n} = (3 - 3\zeta)$ of norm 405, which is the second conductor listed in Table 2.

As another example, the 5-unit equation $u + v = w$ where $u = \zeta^3(1+\zeta)^{-1} = \zeta + \zeta^{-1}$ and $v = \zeta^2(1+\zeta)$ is especially nice because $v - u = 1, -uv = -1$ yields that the curve $E_{u,v}$ is $y^2 = x^3 + x^2 - x$ which descends to $\mathbb{Q}$. It has conductor of norm 1280, the sixth conductor listed in Table 2.

6. Results

6.1. In this section we present our computational data, both on the cohomology and elliptic curve sides. Our programs were implemented in Magma [8]. We remark that in the cohomology computations, following a standard practice (cf. [4]) we did not work over the complex numbers $\mathbb{C}$, but instead computed cohomology with coefficients in a large finite field $\mathbb{F}_{12379}$. This technique was used to avoid the precision problems in floating-point arithmetic. Since we do not expect $\Gamma_0(\mathfrak{n})$ to have 12379-torsion, we expect that the Betti numbers we report coincide with those one would compute for the group cohomology with $\mathbb{C}$-coefficients. As a check, we reran some computations with coefficients in finite fields over other large primes, and found the same Betti

numbers each time. Thus we believe we are actually reporting the dimensions of $H^5(\Gamma_0(\mathfrak{n})\backslash X;\mathbb{C})$.

6.2. **Cuspidal cohomology.** Our first task was to identify those levels with nonzero cuspidal cohomology. We first experimentally determined the dimensions of the subspace H^5_{Eis} spanned by *Eisenstein cohomology classes* [21]. Such classes are closely related to Eisenstein series. In particular the eigenvalue of $T_{\mathfrak{q}}$ on these classes equals $\mathrm{Norm}(\mathfrak{q})+1$. We expect that for a given level $\mathfrak{n}$, the dimension of the Eisenstein cohomology space depends only the factorization type of $\mathfrak{n}$. Thus initially we used some Hecke operators applied to cohomology spaces of small level norm to compute the expected Eisenstein dimension for small levels with different factorization types. The result can be found in Table 1.

After compiling Table 1, we computed cohomology for a larger range of levels and looked for Betti numbers in excess of that in Table 1. We were able to compute H^5 for all levels $\mathfrak{n}$ with $\mathrm{Norm}(\mathfrak{n}) \leq 4941$. For $\mathfrak{n}=\mathfrak{p}$ prime we were able to carry the computations further to $\mathrm{Norm}(\mathfrak{p}) \leq 7921$. Table 2 shows the norms of the levels $\mathfrak{n}$ with nonzero cuspidal cohomology and generators of $\mathfrak{n}$ we used. It turns out that modulo the action of Galois each cuspidal space can be uniquely identified by the norm of the level, except when $\mathrm{Norm}(\mathfrak{n})=3641$. In this case there are two levels up to Galois with nonzero cuspidal cohomology; we call them 3641a and 3641b. The dimensions of the cuspidal subspaces H^5_{cusp} are given in Table 3.

6.3. **Hecke operators.** Next we computed the Hecke operators and looked for eigenclasses with rational eigenvalues. These computations were quite intensive. For all levels we were able to compute at least up to $T_{\mathfrak{q}}$ with $\mathfrak{q}\subset\mathcal{O}$ prime satisfying $\mathrm{Norm}(\mathfrak{q})\leq 41$; at some smaller levels, such as $\mathrm{Norm}(\mathfrak{n})=701$, we computed much further. At the largest levels ($\mathrm{Norm}(\mathfrak{n})=4455, 4681, 6241, 7921$) the computation was so big that our implementation could not compute any Hecke operators. Table 4 gives our choices of generators for the ideals $\mathfrak{q}$.

For all levels except for one, the cuspidal cohomology split into 1-dimensional rational eigenspaces. We give some eigenvalues for the rational eigenclasses in Table 5. The remaining level — norm 3721 — is 2-dimensional with Hecke eigenvalues generating the field $F^+=\mathbb{Q}(\sqrt{5})$. The characteristic polynomials can be seen in Table 6.

6.4. **Elliptic curves over F.** Now we give motivic explanations for all the cuspidal cohomology we found.

Thirteen of the eigenclasses in Table 5 have the property that their eigenvalues $a_{\mathfrak{q}}$ differ for at least two primes $\mathfrak{q},\mathfrak{q}'$ lying over the same prime in the subfield F^+. Hence we expect these classes to correspond to elliptic curves over F. Using the techniques described in §5, we were able to find elliptic curves E/F such that for all primes $\mathfrak{q}$ of good reduction, the identity $a_{\mathfrak{q}}=\mathrm{Norm}(\mathfrak{q})+1-|E(\mathbb{F}_{\mathfrak{q}})|$ held for every Hecke operator we computed. Equations for these curves are given in Table 7.

Although we were unable to match the remaining eigenclass, namely the second labelled 3641b, to an elliptic curve over F, a curve matching this class was found by Mark Watkins (Appendix A).

6.5. **The remaining eigenclasses.** All the other eigenclasses Tables 5 and 6 can be accounted for either by elliptic curves over $\mathbb{Q}$, elliptic curves over F^+, "old" cohomology classes coming from lower levels, or other Hilbert modular forms over F^+. We indicate briefly what happens.

6.5.1. *Elliptic curves over* $\mathbb{Q}$. The eigenclasses at 400, 405, 1280, 1296, 4096, and one of the eigenclasses at 2025, correspond to elliptic curves over $\mathbb{Q}$ that can readily be found in Cremona's tables [12]. In all cases, there are actually *two* rational elliptic curves that are not isogenous over $\mathbb{Q}$ but produce the same eigenvalue data when considered as curves over F; the curves in these pairs are quadratic twists by 5 of each other that become isomorphic over F^+. For instance, at 400 the two curves are 50A1 and 50B3 (in the notation of [12]).

6.5.2. *Elliptic curves over* F^+. The eigenclasses at 605, 961, 1681, 1805, 2401, and 4205 correspond to elliptic curves over F^+. The class at 2401 already appears in [15]; the others were verified using software written by Dembélé. As an example, the three eigenclasses at 4205 correspond to three cuspidal parallel weight 2 Hilbert modular newforms of level $\mathfrak{p}_5\mathfrak{p}_{29} \subset \mathcal{O}_{F^+}$. Although we were unable to compute Hecke operators at 6241 and 7921, we expect that these classes correspond to elliptic curves given in [15].

6.5.3. *Old classes.* There are two-dimensional eigenspaces at 2000, 2025, 3025, 3505, 4400, and 4455 on which the Hecke operators we computed act by scalars. These subspaces correspond to curves appearing at lower levels. For example, the classes at 2000 and 4400 correspond to the classes that already appeared at 400. We note that 2000, 2025, 4400, and 4455 correspond to elliptic curves over $\mathbb{Q}$, while 3025 corresponds to an elliptic curve over F^+ (seen in Table 5 at 605) and 3505 to a curve over F (seen in Table 5 at 701).

6.5.4. *Other Hilbert modular forms.* There are two eigenclasses remaining, namely the class at 3721 with eigenvalues in F^+ and the third eigenclass ξ at 3025 with eigenvalues in $\mathbb{Q}$. Both can be attributed to Hilbert modular forms of parallel weight 2 attached to abelian surfaces.

For 3721, the characteristic polynomials match those of a parallel weight 2 Hilbert modular newform of level $\mathfrak{p}_{61} \subset \mathcal{O}_{F^+}$.

The class ξ at 3025 is perhaps the most interesting of all, other than the classes matching elliptic curves over F, since it gives an example of a *fake elliptic curve* in the sense of [11]. Let $\mathfrak{m} \subset \mathcal{O}_{F^+}$ be the ideal $\mathfrak{p}_5^2\mathfrak{p}_{11}$. The space of parallel weight 2 Hilbert modular newforms of level $\mathfrak{m}$ contains an eigenform g with Hecke eigenvalues

$a_{\mathfrak{q}}$ in the field F^+. For any prime $\mathfrak{q} \subset \mathcal{O}_{F^+}$, let $q \in \mathbb{Z}$ be the prime under $\mathfrak{q}$. Then we have $a_{\mathfrak{q}}(g) = 0$ if $q = 5$, and

$$a_{\mathfrak{q}}(g) \in \begin{cases} \mathbb{Z} & \text{if } q = 1 \bmod 5, \\ \mathbb{Z} \cdot \sqrt{5} & \text{if } q = 2, 3, 4 \bmod 5. \end{cases} \tag{10}$$

Table 8 gives some eigenvalues of g. The conditions (10) imply that there is a quadratic character ε of $\mathrm{Gal}(F/F^+)$ such that the L-series $L(s, g)L(s, g \otimes \varepsilon)$ agrees with the L-series attached to our eigenclass ξ. Indeed, following [11], if $\mathfrak{q} \subset \mathcal{O}_{F^+}$ splits in F as $\mathfrak{r} \cdot \bar{\mathfrak{r}}$ (respectively, remains inert in F), then we should expect the Hecke eigenvalues of g and ξ to be related by

$$a_{\mathfrak{r}}(\xi) = a_{\bar{\mathfrak{r}}}(\xi) = a_{\mathfrak{q}}(g) \quad \text{(split)}$$

and

$$a_{\mathfrak{q}}(\xi) = a_{\mathfrak{q}}(g)^2 - 2\,\mathrm{Norm}_{F^+/\mathbb{Q}}(\mathfrak{q}) \quad \text{(inert)}.$$

Comparison of Tables 5 and 8 shows that this holds.

Appendix A. Elliptic curves with good reduction outside a given set (Mark Watkins)

The method to find a curve with good reduction outside a finite set is outlined in Cremona–Lingham [13], though much of this was well-known to experts in prior times. In our specific case, we can make some additional simplifications and/or modifications.

Since the primes $S = \{\mathfrak{p}_{11}, \mathfrak{p}_{331}\}$ that divide the level are exactly the same as the primes that divide the discriminant of the elliptic curve, we immediately have that $\Delta = (-1)^a u^b e_{11}^c e_{331}^d$ where $u = 1 + \zeta_5^2 + \zeta_5^3$ is a unit, $\mathfrak{p}_{11} = (e_{11})$ and $\mathfrak{p}_{331} = (e_{331})$ are principalisations, and $a \in \{0, 1\}$, $0 \le b \le 11$, and $c, d \ge 1$.

The formulæ $j = c_4^3/\Delta$ and $j - 1728 = c_6^2/\Delta$ then give us various divisibility conditions. For instance, upon noting the triviality of the class group of $\mathbf{Q}(\zeta_5)$, Proposition of 3.2 of [13] implies that $w = j^2(j - 1728)^3$ must have $6|v_{\mathfrak{p}}(w)$ for all primes $\mathfrak{p}$ other than $\mathfrak{p}_{11}$ and $\mathfrak{p}_{331}$. It is a standard problem in algorithmic number theory to list all possible such $w \in \mathbf{Q}(\zeta_5)$ up to 6th powers, and then for each w we are left to find S-integral points on the curve $E(w) : Y^2 = X^3 - 1728w$.

We can work more directly in our case, and note that $j = c_4^3/\Delta = 1728 + c_6^2/\Delta$ gives an elliptic curve $E(\Delta) : c_6^2 = c_4^3 - 1728\Delta$ in the unknowns c_4 and c_6. We can note that two curves with Δ differing by a 6th power will give isomorphic $E(\Delta)$, though in making such a passage we may need to find S-integral points on the resulting curves rather than just integral points. Also, this allows us to restrict to $0 \le b \le 5$ without loss. We are unable to find the full Mordell–Weil group for most of the $E(\Delta)$ curves in any event, and so completeness is impractical.

It turns out that $(a, b, c, d) \in \{(1, 3, 2, 1), (1, 5, 2, 1)\}$ will give the first and second curves corresponding to 3641b. To find these, we tried all possibilities for (a, b) with $(c, d) = (1, 1)$, and then $(c, d) = (2, 1)$. Thus we had to try to find the Mordell–Weil

group for 24 different elliptic curves (we were succesful for only 7). The curves $E(\Delta)$ all have a 3-isogeny, but this does not seem to be of much use.

We used the Magma package of Nils Bruin to try to search for points on the $E(\Delta)$. We can get an upper bound on the rank using `TwoSelmerGroup`, though this is not strictly necessary. We then search for points on the elliptic curves using the function `PseudoMordellWeilGroup` with a `SearchBound` of 100. This took about 5 minutes per curve (the search bound is about the 4th power of this in terms of the norm, as the field is quartic). In Table 9 we list the data for the upper bound on the rank and the number of generators found.

It is natural that we can find more points when the rank is large, as the points are more likely to be of smaller height. Once we have some linearly independent points in the Mordell–Weil group, we can find all integral points that they generate. Again a provable version of this is rather technical, and largely unneeded. We simply took all linear combinations with coefficients of size not more than 5. This then gives a set of integral points (X, Y) on $E(\Delta)$, and from each we can obtain an elliptic curve with the correct j-invariant via

$$j = X^3/\Delta \quad \text{and} \quad E_\Delta(X) : y^2 = x^3 - \frac{3j}{j-1728}x - \frac{2j}{j-1728}.$$

We can then try to twist away ramification at places outside $\mathfrak{p}_{11}$ and $\mathfrak{p}_{331}$. However, we can also perform a preliminary check on the traces of Frobenius of the curves $E_\Delta(X)$, as they must match those from the Hecke operators up to sign if the twisting is to be successful.

We are fortunate in the end, since even though Table 9 contains many missing Mordell–Weil groups, we are still able to find the two desired curves. In Table 9, the (a, b, c, d) column gives the choice of these parameters in the discriminant, the s-column gives the upper bound on the rank from `TwoSelmerGroup`, the g-column gives the number of generators we found via a search up to naïve height 100, and I-column gives the number of integral points we obtained from these when taking small linear combinations of the generators.

We conclude by giving the Weierstrass equation for the second curve labelled 3641b:

$$\begin{aligned}(11)\quad y^2 + (\zeta^2+1)xy + \zeta^2 = x^3 &+ (-\zeta^3+\zeta^2+\zeta+1)x^2 \\ &+ (-\zeta^3 - 82\zeta^2 + 52\zeta - 84)x + (310\zeta^3 - 366\zeta^2 + 418\zeta - 175).\end{aligned}$$

References

[1] A. Ash, *Deformation retracts with lowest possible dimension of arithmetic quotients of self-adjoint homogeneous cones*, Math. Ann. **225** (1977), no. 1, 69–76.

[2] ———, *Small-dimensional classifying spaces for arithmetic subgroups of general linear groups*, Duke Math. J. **51** (1984), no. 2, 459–468.

[3] ———, *Unstable cohomology of* $\mathrm{SL}(n, \mathscr{O})$, J. Algebra **167** (1994), no. 2, 330–342.

[4] A. Ash, P. E. Gunnells, and M. McConnell, *Cohomology of congruence subgroups of* $\mathrm{SL}_4(\mathbb{Z})$, J. Number Theory **94** (2002), no. 1, 181–212.
[5] A. Borel and J.-P. Serre, *Corners and arithmetic groups*, Comment. Math. Helv. **48** (1973), 436–491, Avec un appendice: Arrondissement des variétés à coins, par A. Douady et L. Hérault.
[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] A. Borel, *Introduction to the cohomology of arithmetic groups*, Lie groups and automorphic forms, AMS/IP Stud. Adv. Math., vol. 37, Amer. Math. Soc., Providence, RI, 2006, pp. 51–86.
[8] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993).
[9] J. Bygott, *Modular forms and modular symbols over imaginary quadratic fields*, Ph.D. thesis, Exeter, 1999.
[10] J. E. Cremona, *Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields*, Compositio Math. **51** (1984), no. 3, 275–324.
[11] ———, *Abelian varieties with extra twist, cusp forms, and elliptic curves over imaginary quadratic fields*, J. London Math. Soc. (2) **45** (1992), no. 3, 404–416.
[12] ———, *The elliptic curve database for conductors to 130000*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 11–29.
[13] J. E. Cremona and M. P. Lingham, *Finding all elliptic curves with good reduction outside a given set of primes*, Experiment. Math. **16** (2007), no. 3, 303–312.
[14] 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.
[15] L. Dembélé, *Explicit computations of Hilbert modular forms on* $\mathbb{Q}(\sqrt{5})$, Experiment. Math. **14** (2005), no. 4, 457–466.
[16] J. Franke, *Harmonic analysis in weighted* L_2*-spaces*, Ann. Sci. École Norm. Sup. (4) **31** (1998), no. 2, 181–279.
[17] P. E. Gunnells, *Modular symbols for* $\mathbf{Q}$*-rank one groups and Voronoĭ reduction*, J. Number Theory **75** (1999), no. 2, 198–219.
[18] ———, *Computing Hecke eigenvalues below the cohomological dimension*, Experiment. Math. **9** (2000), no. 3, 351–367.
[19] 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.
[20] G. Harder, *Cohomology of arithmetic groups*, book in preparation available from Harder's website.
[21] ———, *Eisenstein cohomology of arithmetic groups. The case* GL_2, Invent. Math. **89** (1987), no. 1, 37–118.
[22] M. Koecher, *Beiträge zu einer Reduktionstheorie in Positivitätsbereichen. I*, Math. Ann. **141** (1960), 384–432.
[23] J.-S. Li and J. Schwermer, *Automorphic representations and cohomology of arithmetic groups*, Challenges for the 21st century (Singapore, 2000), World Sci. Publ., River Edge, NJ, 2001, pp. 102–137.
[24] M. Lingham, *Modular forms and elliptic curves over imaginary quadratic fields*, Ph.D. thesis, Nottingham, 2005.
[25] J. Socrates and D. Whitehouse, *Unramified Hilbert modular forms, with examples relating to elliptic curves*, Pacific J. Math. **219** (2005), no. 2, 333–364.

[26] G. Voronoĭ, *Sur quelques propriétés des formes quadratiques positives parfaites*, J. Reine Angew. Math. **133** (1908), 97–178.
[27] D. Yasaki, *Binary Hermitian forms over a cyclotomic field*, J. Algebra **322** (2009), 4132–4142.

Factorization of $\mathfrak{n}$	$\mathfrak{p}$	$\mathfrak{p}^2$	$\mathfrak{p}^3$	$\mathfrak{p}^4$	$\mathfrak{p}^5$	$\mathfrak{pq}$	$\mathfrak{p}^2\mathfrak{q}$	$\mathfrak{p}^3\mathfrak{q}$	$\mathfrak{p}^2\mathfrak{q}^2$	$\mathfrak{pqr}$	$\mathfrak{p}^2\mathfrak{qr}$
$\dim H^5_{\mathrm{Eis}}(\Gamma_0(\mathfrak{n}))$	3	5	7	9	11	7	11	15	17	15	23

TABLE 1. Expected dimension of Eisenstein cohomology $H^5_{\mathrm{Eis}}(\Gamma_0(\mathfrak{n}))$ in terms of the prime factorization of $\mathfrak{n}$. Prime ideals are denoted by $\mathfrak{p}$, $\mathfrak{q}$, $\mathfrak{r}$.

N($\mathfrak{n}$)	generator of $\mathfrak{n}$	N($\mathfrak{n}$)	generator of $\mathfrak{n}$	N($\mathfrak{n}$)	generator of $\mathfrak{n}$
400	$2\zeta^2 - 4\zeta + 2$	405	$-3\zeta^3 - 3\zeta^2 - 3\zeta - 6$	605	$-\zeta^3 + 4\zeta^2 - 4\zeta + 1$
701	$-2\zeta^3 - \zeta^2 - 3\zeta - 6$	961	$-2\zeta^3 - 2\zeta^2 + 5$	1280	$-4\zeta + 4$
1296	6	1681	$-6\zeta^3 - 7\zeta^2 - 7\zeta - 6$	1805	$-3\zeta^3 - 4\zeta^2 - 5\zeta - 8$
2000	$-2\zeta^3 + 6\zeta^2 - 6\zeta + 2$	2025	$-3\zeta^3 - 3\zeta^2 - 9$	2201	$-2\zeta^3 - 6\zeta^2 - 7\zeta - 8$
2351	$-2\zeta^3 - 6\zeta^2 - \zeta - 9$	2401	7	3025	$-6\zeta^3 + 7\zeta^2 - 6\zeta$
3061	$-6\zeta^3 - 7\zeta^2 - 5\zeta - 10$	3355	$5\zeta^3 - 5\zeta^2 + 2\zeta + 3$	3505	$-2\zeta^3 - 8\zeta^2 + \zeta - 11$
3571	$-4\zeta^2 - 6\zeta - 9$	3641a	$-2\zeta^3 - 5\zeta^2 + 4\zeta - 10$	3641b	$-\zeta^3 + 7\zeta^2 - 4\zeta + 1$
3721	$7\zeta^3 + 7\zeta^2 + 3$	4096	8	4205	$-4\zeta^3 - 5\zeta^2 - 6\zeta - 10$
4400	$4\zeta^3 + 10\zeta^2 - 2\zeta + 8$	4455	$-6\zeta^2 - 9$	4681	$\zeta^3 - 8\zeta^2 - 7$
5081	$-2\zeta^3 - 5\zeta^2 - 5\zeta - 10$	5101	$-6\zeta^3 - 2\zeta^2 - 11$	6241	$3\zeta^3 + 11\zeta^2 + 3\zeta$
6961	$-8\zeta^3 - 6\zeta^2 - 5\zeta - 14$	7921	$-11\zeta^3 - \zeta^2 - \zeta - 11$		

TABLE 2. Levels $\mathfrak{n}$ with nontrivial cuspidal cohomology. Only one representative of each level up to Galois is given.

N($\mathfrak{n}$)	dimension	N($\mathfrak{n}$)	dimension	N($\mathfrak{n}$)	dimension
400	1	405	1	605	1
701	1	961	1	1280	1
1296	1	1681	1	1805	1
2000	2	2025	3	2201	1
2351	1	2401	1	3025	3
3061	1	3355	1	3505	2
3571	1	3641a	1	3641b	2
3721	2	4096	1	4205	3
4400	2	4455	2	4681	1
5081	1	5101	1	6241	1
6961	1	7921	1		

TABLE 3. Dimensions of cuspidal cohomology.

Prime under $\mathfrak{q}$	Generator of $\mathfrak{q}$
2	2
5	$-\zeta+1$
11	$-\zeta^3-\zeta+1$
	$\zeta^3-\zeta+1$
	$-\zeta^2+\zeta+1$
	$2\zeta^2+\zeta+1$
31	$-2\zeta+1$
	$-2\zeta^2+1$
	$-2\zeta^3+1$
	$2\zeta^3+2\zeta^2+2\zeta+3$
41	$-\zeta^3-3\zeta^2-\zeta-2$
	$-\zeta^3-\zeta^2-2\zeta-3$
	$-\zeta^3-2\zeta^2-2\zeta-3$
	$2\zeta^3+3\zeta^2+\zeta+2$

TABLE 4. Choice of primes $\mathfrak{q}$ for Hecke operators.

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF MASSACHUSETTS, AMHERST, MA 01003-9305
E-mail address: gunnells@math.umass.edu

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF MASSACHUSETTS, AMHERST, MA 01003-9305
E-mail address: hajir@math.umass.edu

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF NORTH CAROLINA AT GREENSBORO, GREENSBORO, NC 27402-6170
E-mail address: d_yasaki@uncg.edu

N($\mathfrak{n}$)	2	5	11	11	11	11	31	31	31	31	41	41	41	41
400	•	•	−3	−3	−3	−3	2	2	2	2	−3	−3	−3	−3
405	1	•	−4	−4	−4	−4	0	0	0	0	10	10	10	10
605	−7	•	•	•	•	•	8	−4	−4	8	−6	6	6	−6
701	−1	−3	3	3	−6	3	−4	5	−4	−4	6	−3	6	−12
961	1	−2	4	4	−4	−4	•	•	•	•	−6	−6	−6	−6
1280	•	•	0	0	0	0	−4	−4	−4	−4	6	6	6	6
1296	•	−4	2	2	2	2	−8	−8	−8	−8	2	2	2	2
1681	−4	−1	5	5	−2	−2	−10	4	4	−10	•	•	•	•
1805	−7	•	0	0	0	0	−4	8	8	−4	−6	−6	−6	−6
2000	•	•	−3	−3	−3	−3	2	2	2	2	−3	−3	−3	−3
2000	•	•	−3	−3	−3	−3	2	2	2	2	−3	−3	−3	−3
2025	1	•	−4	−4	−4	−4	0	0	0	0	10	10	10	10
2025	1	•	−4	−4	−4	−4	0	0	0	0	10	10	10	10
2025	−8	•	2	2	2	2	−3	−3	−3	−3	−8	−8	−8	−8
2201	1	−4	−3	−6	−5	−2	•	•	•	•	4	−3	−6	0
2351	3	−1	−2	5	−2	−2	4	−3	4	4	0	0	0	7
2401	−8	−4	−3	−3	−3	−3	2	2	2	2	2	2	2	2
3025	−7	•	•	•	•	•	8	−4	−4	8	−6	6	6	−6
3025	−7	•	•	•	•	•	8	−4	−4	8	−6	6	6	−6
3025	−3	•	•	•	•	•	−8	2	2	−8	2	−8	−8	2
3061	−3	−4	−4	−3	−1	−2	−2	−2	−9	−6	6	−4	−5	3
3355	5	•	•	•	•	•	−4	−4	−4	8	−6	−6	−6	−6
3505	−1	•	3	3	−6	3	−4	5	−4	−4	6	−3	6	−12
3505	−1	•	3	3	−6	3	−4	5	−4	−4	6	−3	6	−12
3571	−5	−3	−6	−2	−3		−8	−5	−2	0	−2	8	10	−3
3641a	−7	−3	•	•	•	•	−1	−6	3	11	0	−2	−9	−2
3641b	−1	−3	•	•	•	•	−1	8	−7	−7	−12	0	9	0
3641b	7	1	•	•	•	•	7	−8	−3	−3	12	−8	−3	−8
4096	•	−2	−4	−4	−4	−4	0	0	0	0	2	2	2	2
4205	−4	•	5	5	−2	−2	−10	−3	−3	−10	0	7	7	0
4205	−4	•	−3	−3	−6	−6	2	5	5	2	0	−9	−9	0
4205	−7	•	−4	−4	4	4	8	0	0	8	−6	10	10	−6
4400	•	•	•	•	•	•	2	2	2	2	−3	−3	−3	−3
4400	•	•	•	•	•	•	2	2	2	2	−3	−3	−3	−3
5081	3	−4	−4	0	0	−6	0	0	−8	0	−6	6	−6	−4
5101	−3	−3	−1	0	−3	−5	7	−10	1	−8	10	4	−12	−10
6961	1	−2	0	−6	−4	0	−10	4	−8	−2	−10	−8	0	−2

TABLE 5. Eigenvalues of cuspidal $\mathbb{Q}$-eigenclasses. For each Hecke operator $T_{\mathfrak{q}}$ we give the rational prime lying under $\mathfrak{q}$. The order of the columns corresponds to Table 4.

Prime under $\mathfrak{q}$	Characteristic polynomial of $T_{\mathfrak{q}}$
2	$x^2+4x-16$
5	x^2+x-11
11	x^2-20
	x^2-20
	x^2+x-1
	x^2+x-1
31	$x^2-14x+44$
	$x^2-14x+44$
	$x^2+3x-29$
	$x^2+3x-29$
41	$x^2-10x+20$
	$x^2-10x+20$
	$x^2+16x+44$
	$x^2+16x+44$

TABLE 6. Characteristic polynomials for Hecke operators on the cuspidal subspace with norm level 3721. The order corresponds to Table 4.

Norm($\mathfrak{n}$)	a_1	a_2	a_3	a_4	a_6
701	$-\zeta-1$	ζ^2-1	1	$-\zeta^2$	0
2201	$-\zeta^2-2$	$\zeta^3+\zeta^2$	ζ	0	0
2351	1	$\zeta^2+\zeta+2$	ζ	ζ^2+1	0
3061	$2\zeta^3+\zeta+2$	1	$-\zeta^2$	0	0
3355	$\zeta^3-\zeta+1$	$-\zeta$	0	1	0
3571	$-\zeta^3-\zeta$	$\zeta-1$	ζ^3+1	0	0
3641a	$-2\zeta^2-\zeta-1$	ζ^2	$\zeta+1$	0	0
3641b	ζ^3-1	$2\zeta^3+\zeta+2$	ζ^2+1	ζ	0
4681	ζ^3	$-\zeta^3+1$	ζ^3	$-\zeta^3$	0
5081	$-\zeta^2+\zeta+1$	$\zeta^3+\zeta+1$	$\zeta+1$	0	0
5101	$-\zeta^3-2\zeta$	-1	ζ	0	0
6961	ζ^3-1	$-\zeta-2$	0	$\zeta+1$	0

TABLE 7. Equations for elliptic curves over F. The curve 3641b corresponds to the first eigenclass labelled 3641b in Table 5. (We did not find a curve corresponding to the second eigenclass labelled 3641b.)

q	$a_{\mathfrak{q}}$	q	$a_{\mathfrak{q}}$	q	$a_{\mathfrak{q}}$	q	$a_{\mathfrak{q}}$
2	$\sqrt{5}$	11	1	29	$4\sqrt{5}$	41	-8
3	$-2\sqrt{5}$	11	2	29	$-2\sqrt{5}$	41	2
5	0	19	$-2\sqrt{5}$	31	-8	59	$-2\sqrt{5}$
7	$2\sqrt{5}$	19	0	31	2	59	$4\sqrt{5}$

TABLE 8. Hecke eigenvalues of the Hilbert modular newform g corresponding to the third eigenclass at 3025.

(a,b,c,d)	s	g	I	(a,b,c,d)	s	g	I	(a,b,c,d)	s	g	I	(a,b,c,d)	s	g	I
(0,0,1,1)	3	**3**	12	(1,0,1,1)	3	1	2	(0,0,2,1)	3	0	-	(1,0,2,1)	1	0	-
(0,1,1,1)	0	-	-	(1,1,1,1)	2	0	-	(0,1,2,1)	0	-	-	(1,1,2,1)	2	1	2
(0,2,1,1)	3	**3**	8	(1,2,1,1)	1	0	-	(0,2,2,1)	2	0	-	(1,2,2,1)	2	1	2
(0,3,1,1)	1	0	-	(1,3,1,1)	1	0	-	(0,3,2,1)	3	1	2	(1,3,2,1)	1	**1**	**4**
(0,4,1,1)	2	0	-	(1,4,1,1)	0	-	-	(0,4,2,1)	2	1	2	(1,4,2,1)	2	1	2
(0,5,1,1)	1	0	-	(1,5,1,1)	1	0	-	(0,5,2,1)	2	0	-	(1,5,2,1)	4	**4**	**22**

TABLE 9. Data concerning Mordell–Weil groups of elliptic curves $E(\Delta)$