LMS J. Comput. Math. 19 (1) (2016) 155–174 © 2016 Author
doi:10.1112/S1461157016000048

Modular elliptic curves over the field of twelfth roots of unity

Andrew Jones

Abstract

In this paper we perform an extensive study of the spaces of automorphic forms for GL_2 of weight 2 and level $\mathfrak{n}$, for $\mathfrak{n}$ an ideal in the ring of integers of the quartic CM field $\mathbb{Q}(\zeta_{12})$ of twelfth roots of unity. This study is conducted through the computation of the Hecke module $H^*(\Gamma_0(\mathfrak{n}), \mathbb{C})$, and the corresponding Hecke action. Combining this Hecke data with the Faltings–Serre method for proving equivalence of Galois representations, we are able to provide the first known examples of modular elliptic curves over this field.

Supplementary materials are available with this article.

1. *Introduction*

Following the proof of the Shimura–Taniyama–Weil conjecture at the turn of the twenty-first century, it is known that all rational elliptic curves are *modular*, in the sense that for almost all primes ℓ, the representation arising from the action of the absolute Galois group $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the ℓ-adic Tate module of an elliptic curve E defined over $\mathbb{Q}$ is isomorphic to the ℓ-adic representation attached to a cuspidal modular form f of weight 2, whose level matches the conductor of E.

This notion of modularity can be viewed within the more general framework of the Langlands programme, which conjectures in particular that certain n-dimensional ℓ-adic representations of the absolute Galois group G_F (where F is a number field) should correspond to automorphic forms for the algebraic group $\mathrm{Res}_{F/\mathbb{Q}}(\mathrm{GL}_n)$, where $\mathrm{Res}_{F/\mathbb{Q}}$ denotes the Weil restriction of scalars from F to $\mathbb{Q}$. Among these Galois representations should be the two-dimensional representation arising from the action of G_F on the ℓ-adic Tate module of an elliptic curve E defined over F, so it is natural to consider modularity over an arbitrary number field.

One can approach this question from either a theoretical or a computational viewpoint. On the theoretical side, there is the search for a concrete description of the Galois representation attached to an automorphic form for the group $\mathrm{Res}_{F/\mathbb{Q}}(\mathrm{GL}_2)$ for a general number field F. Carayol [**7**], Taylor [**30**] and Blasius and Rogawski [**4**] defined these representations for the case of Hilbert modular forms over totally real fields whose weights are at least 2 (including, in particular, those forms which should correspond to elliptic curves). Subsequently, Jarvis and Manoharmayum [**23**] proved modularity of semistable elliptic curves over the real quadratic fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{17})$, and recent work by Freitas *et al.* [**13**] establishes modularity of elliptic curves over *all* real quadratic fields.

Harris, Soudry and Taylor [**22**, **31**] provided a construction in the case of automorphic forms over imaginary quadratic fields, which was later refined by Berger and Harcos [**3**]. More recently, Mok [**26**] has constructed Galois representations attached to automorphic forms defined over CM fields, subject to certain conditions on the central character of these forms (in particular, his construction covers those forms which are expected to correspond to elliptic curves). Harris *et al.* [**21**] and Scholze [**27**] have removed these restrictions, and in fact construct

Received 2 June 2015; revised 11 October 2015.

2010 Mathematics Subject Classification 11F41, 11G05, 11F80 (primary).

This work was funded by an EPSRC Scholarship at the University of Sheffield.

https://doi.org/10.1112/S1461157016000048 Published online by Cambridge University Press

Galois representations attached to regular automorphic forms for $\mathrm{Res}_{F/\mathbb{Q}}(\mathrm{GL}_n)$ for all n over CM or totally real fields (with Scholze's results extending even further to account for 'torsion automorphic forms').

As yet, there are no general modularity results over these latter fields, although examples of modular elliptic curves have been found over certain imaginary quadratic fields, such as in [12]. In this paper, the authors present an algorithm to test for isomorphism of two representations of the absolute Galois group G_F, which relies on knowledge of the traces of these representations on Frobenius elements over primes in F.

As in the classical case, these traces are determined by the action of Hecke operators on spaces of newforms, which has led to the development of methods for constructing spaces of automorphic forms defined over number fields, and for computing the Hecke action on these spaces. Classically, one can study modular forms through the use of *modular symbols* (see, for example, [29]). By the Eichler–Shimura isomorphism, one can realize cuspidal Hecke eigenforms as classes in the cohomology of modular curves, and modular symbols provide us with a means to compute this cohomology, and the corresponding Hecke action. More generally, it is known that cuspidal automorphic forms for $\mathrm{Res}_{F/\mathbb{Q}}(\mathrm{GL}_2)$ can be realized as classes in the cohomology of certain locally symmetric spaces, and so one might hope to extend the notion of modular symbols to a wider variety of number fields.

Until recently, attention had largely been focused on imaginary quadratic or totally real fields; however, the authors of [14] provide a description of a method for computing automorphic forms over the *quartic* CM field $\mathbb{Q}(\zeta_5)$, where ζ_5 denotes a primitive fifth root of unity. Moreover, they are able to compute the action of Hecke operators on these forms, and present several examples of elliptic curves which appear to be modular. In this paper, we shall extend these methods to the field $\mathbb{Q}(\zeta_{12})$, and, adapting the methodology of [12], shall combine the resulting data with our knowledge of the Galois representations constructed in [26] to give the first proven examples of modular elliptic curves over a quartic CM field.

2. *Cuspidal automorphic forms and representations*

We begin with a brief discussion of automorphic forms for the group $\mathrm{Res}_{F/\mathbb{Q}}(\mathrm{GL}_2)$, where F is a quartic CM field, before describing the attached Galois representations constructed in [26].

Let F be such a field, let $G = \mathrm{Res}_{F/\mathbb{Q}}(\mathrm{GL}_2)$, and let $G(\mathbb{A}) = G(\mathbb{A}_f) \times G(\mathbb{R})$ be a decomposition of the adelic points of G into finite and infinite parts. For simplicity, we shall assume that F has trivial class group. We can identify $G(\mathbb{R})$ with the product $\mathrm{GL}_2(\mathbb{C}) \times \mathrm{GL}_2(\mathbb{C})$ via a fixed choice of non-conjugate embeddings of F into the complex numbers, and subsequently define a compact subgroup K_∞ of $G(\mathbb{R})$ by $K_\infty = U(2) \times U(2)$.

For an ideal $\mathfrak{n}$ in the ring of integers $\mathcal{O}$ of F, let $K_0(\mathfrak{n})$ denote the product of the local subgroups $K_v(\mathfrak{n})$, where v runs through the non-archimedean places of F, and $K_v(\mathfrak{n})$ is equal to either the subgroup of $\mathrm{GL}_2(\mathcal{O}_v)$ comprising those matrices which are upper triangular modulo $\mathfrak{n}$, if $v|\mathfrak{n}$, or else is equal to $\mathrm{GL}_2(\mathcal{O}_v)$. Note that $K_0(\mathfrak{n})$ is a compact open subgroup of $G(\mathbb{A}_f)$.

An *automorphic form of level* $\mathfrak{n}$ is a function $\varphi : G(\mathbb{Q})\backslash G(\mathbb{A}) \to \mathbb{C}$ satisfying the following:

- φ acts smoothly on the real Lie group $G(\mathbb{R})$;
- φ is invariant under the right regular action of $K_0(\mathfrak{n})$ on $G(\mathbb{A}_f)$;
- the vector space spanned by the K_∞-translates of φ (under the right regular action) is finite-dimensional; and
- φ is *$\mathcal{Z}$-finite* and *of moderate growth* (in the sense of [6, § 3.2]).

Moreover, we say that φ is *cuspidal* if

$$\int_{F\backslash\mathbb{A}_F} \varphi\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} g\right) dx = 0$$

https://doi.org/10.1112/S1461157016000048 Published online by Cambridge University Press

for all $g \in G(\mathbb{A})$, and has *trivial central character*, if it is invariant under the regular action of the centre of $G(\mathbb{A})$.

Such forms lie in the space $L_0^2(G(\mathbb{Q})\backslash G(\mathbb{A}), \mathbf{1})$ of square integrable functions on $G(\mathbb{A})$ which are invariant under the action of $G(\mathbb{Q})$, and are cuspidal with trivial central character. Under the right regular action of $G(\mathbb{A})$, this space decomposes into a direct sum of irreducible Hilbert space representations,

$$L_0^2(G(\mathbb{Q})\backslash G(\mathbb{A}), \mathbf{1}) = \bigoplus_{\pi} n_\pi V_\pi,$$

where $n_\pi \in \mathbb{N}$ and V_π is a Hilbert space on which $G(\mathbb{A})$ acts by the homomorphism π, and we define a *cuspidal automorphic representation* for G to be any subrepresentation which is isomorphic to one of these summands. Cuspidal automorphic forms of level $\mathfrak{n}$ can be realized in the space of $K_0(\mathfrak{n})$-fixed vectors of some cuspidal automorphic representation, and so we may transfer our attention to these latter objects, which we are better equipped to work with.

Each cuspidal automorphic representation π admits a decomposition $\pi = \bigotimes \pi_v$, where v runs over the places of F. For each non-archimedean place v, π_v is an irreducible *admissible* complex representation $\pi_v : \mathrm{GL}_2(F_v) \to \mathrm{GL}(V_v)$, in the sense that the stabilizer of each point $v \in V_v$ is open, and, given a compact open subgroup K_v of $\mathrm{GL}_2(F_v)$, the space of K_v-fixed vectors in V_v is finite-dimensional.

We recall that a representation π_v is *unramified* if the space of $\mathrm{GL}_2(\mathcal{O}_v)$-fixed vectors is non-trivial. Since π is automorphic, each unramified component π_v is a *principal series*, and is parameterized by a pair (χ_1, χ_2) of characters of $F_v^\times$. To each such representation we can assign a semisimple conjugacy class t_{π_v} in $\mathrm{GL}_2(\mathbb{C})$, known as the *Langlands class* of π_v, a representative of which is given by the matrix $\left(\begin{smallmatrix} \chi_1(\varpi) & 0 \\ 0 & \chi_2(\varpi) \end{smallmatrix}\right)$, where ϖ is a uniformizer for $\mathcal{O}_v$.

As intimated previously, we can realize automorphic forms (or, as we shall consider, the corresponding automorphic representations) as classes in the cohomology of certain locally symmetric spaces. An in-depth discussion of this can be found in [**28**, Chapter 3], of which we shall present a brief précis, tailored to our particular case.

For a fixed ideal $\mathfrak{n}$, we define the locally symmetric space

$$X_0(\mathfrak{n}) = A_G^0(\mathbb{R})G(\mathbb{Q})\backslash G(\mathbb{A})/K_\infty K_0(\mathfrak{n}),$$

where the *split component* $A_G^0(\mathbb{R})$ is isomorphic to $\mathbb{R}_+$, embedded diagonally into the two components of $G(\mathbb{R}) \simeq \mathrm{GL}_2(\mathbb{C}) \times \mathrm{GL}_2(\mathbb{C})$. We then define $H^*(X_0(\mathfrak{n}), \mathbb{C})$ to be the cohomology of $\Omega(X_0(\mathfrak{n}), \mathbb{C})$, where the latter denotes the de Rham complex of smooth, complex-valued differentials on $X_0(\mathfrak{n})$.

Let $\mathfrak{m}_G$ be the Lie algebra of $A_G^0(\mathbb{R})\backslash G(\mathbb{R})$, and denote by $\mathcal{A}(K_0(\mathfrak{n}))$ the space of automorphic forms of level $\mathfrak{n}$ on which $A_G^0(\mathbb{R})$ acts trivially. There is then an isomorphism of $K_0(\mathfrak{n})$-modules,

$$H^*(X_0(\mathfrak{n}), \mathbb{C}) \simeq H^*(\mathfrak{m}_G, K_\infty; \mathcal{A}(K_0(\mathfrak{n}))),$$

where $H^*(\mathfrak{m}_G, K_\infty; \mathcal{A}(K_0(\mathfrak{n})))$ denotes the Lie algebra cohomology with respect to $(\mathfrak{m}_G, K_\infty)$ (in the sense of [**28**, § 3.2]).

There is a decomposition

$$H^*(X_0(\mathfrak{n}), \mathbb{C}) = H^*_{\mathrm{Eis}}(X_0(\mathfrak{n}), \mathbb{C}) \oplus H^*_{\mathrm{cusp}}(X_0(\mathfrak{n}), \mathbb{C})$$

of $H^*(K_0(\mathfrak{n}), \mathbb{C})$ into *Eisenstein* and *cuspidal* parts, the latter of which is connected to cuspidal automorphic representations. Denoting by $V_\pi = V_{\pi_f} \otimes V_{\pi_\infty}$ the space on which a cuspidal automorphic representation π acts, we have a decomposition of $K_0(\mathfrak{n})$-modules

$$H^*_{\mathrm{cusp}}(X_0(\mathfrak{n}), \mathbb{C}) \simeq \bigoplus_{\pi} H^*(\mathfrak{m}_G, K_\infty; V_{\pi_\infty}) \otimes V_{\pi_f}^{K_0(\mathfrak{n})},$$

https://doi.org/10.1112/S1461157016000048 Published online by Cambridge University Press

where the sum ranges over all cuspidal automorphic subrepresentations of the space $\mathcal{A}(K_0(\mathfrak{n}))$ with trivial central character, and $V_{\pi_f}^{K_0(\mathfrak{n})}$ denotes the space of $K_0(\mathfrak{n})$-fixed vectors in V_{π_f} (see [**28**, Theorem 4.1]). We shall say that a representation π is *of cohomological type* and *weight two* if $H^*(\mathfrak{m}_G, K_\infty; V_{\pi_\infty})$ is non-zero.

With this in mind, we can now state a version of the main result in [**26**].

THEOREM 2.1. *Let F be a CM field, and let π be a cuspidal automorphic representation of $\mathrm{Res}_{F/\mathbb{Q}}(\mathrm{GL}_2)$ of cohomological type, with trivial central character, and fix a prime ℓ. Then there exists an ℓ-adic Galois representation*

$$\rho_\pi : G_F \to \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$$

such that, for each place v of F not dividing ℓ, we have the local-to-global compatibility statement, up to semisimplification,

$$\mathrm{WD}(\rho_{\pi,v})^{ss} \simeq \mathscr{L}_v(\pi_v \otimes |\det|_v^{-1/2})^{ss}.$$

Furthermore, if π_v is not a twist of Steinberg (for example, is an unramified principal series) then we have the full local-to-global compatibility statement, up to Frobenius semisimplification,

$$\mathrm{WD}(\rho_{\pi,v})^{\mathrm{Frob}} \simeq \mathscr{L}_v(\pi_v \otimes |\det|_v^{-1/2}).$$

Here $\mathscr{L}_v(\pi_v)$ denotes the representation of the Weil–Deligne group W_v' of F_v assigned to π_v by the local Langlands correspondence for GL_2, and WD denotes the Weil–Deligne functor taking representations of G_{F_v} to representations of W_v'.

We shall say that an elliptic curve E over F is *modular* if, for some rational prime ℓ, the ℓ-adic Galois representation ρ_E defined by the action on the ℓ-adic Tate module of E is, up to semisimplification, isomorphic to ρ_π for some cohomological cuspidal automorphic representation π of weight 2 and level $\mathfrak{n}_E$, where $\mathfrak{n}_E$ denotes the conductor of E. Note that, since such representations form a compatible family ranging over all rational primes ℓ, isomorphism for some prime implies isomorphism for all but finitely many primes.

We note some important details concerning these representations. Firstly, since the Frobenius semisimplification of a Weil–Deligne representation agrees with the original representation on inertia, $\mathrm{WD}(\rho_{\pi,v})$ is unramified at a place v of F if, and only if, $\rho_{\pi,v}$ is too. Similarly, under the local Langlands correspondence, $\mathscr{L}_v(\pi_v)$ and π_v are unramified at the same set of places. In particular, if the representation π occurs in the cohomology of the locally symmetric space $X_0(\mathfrak{n})$, then $\rho_{\pi,v}$ is unramified at all primes not dividing $\mathfrak{n}$.

Secondly, the determinant of $\mathscr{L}_v(\pi_v)$ corresponds to the central character of π_v, and thus is trivial, so in particular the determinant of $\rho_{\pi,v}$ is equal to $|\det|_v^{-1/2}$. Observing that, for a uniformizer ϖ, we have $\det(\rho_{\pi,v}(\mathrm{Frob_v})) = |\det(\varpi)|_v^{-1/2} = q$, where q is the cardinality of the residue field of F_v, we see that $\det(\rho_{\pi,v})$ is equivalent to the local cyclotomic character.

Finally, the trace of $\mathscr{L}_v(\pi_v)(\mathrm{Frob_v})$ is equal to the trace of the Langlands class t_{π_v} of π_v, and so $\mathrm{Tr}(\rho_{\pi,v}(\mathrm{Frob_v})) = q^{1/2}\,\mathrm{Tr}(t_{\pi_v})$. If the representation π_v is unramified, the space of $\mathrm{GL}_2(\mathcal{O}_v)$-fixed vectors of π_v is known to be one-dimensional, on which the Hecke operator T_v (defined as the normalized characteristic function of the double coset $\mathrm{GL}_2(\mathcal{O}_v)\left(\begin{smallmatrix}\varpi & 0\\ 0 & 1\end{smallmatrix}\right)\mathrm{GL}_2(\mathcal{O}_v)$) acts via scalar multiplication by precisely this value.

3. *Comparing Galois representations*

Armed with our knowledge of these representations, we shall use the following method, described in [**12**] for imaginary quadratic fields, to determine whether an elliptic curve E

https://doi.org/10.1112/S1461157016000048 Published online by Cambridge University Press

defined over a quartic CM field is modular. We shall denote by ρ_E and ρ_π the Galois representations corresponding to a curve E and a cuspidal automorphic representation π, respectively.

We begin with a definition. Let ρ be an arbitrary ℓ-adic Galois representation. Up to isomorphism, we may assume that the image of ρ is defined over a finite extension of $\mathbb{Z}_\ell$, and thus we may compose ρ with the reduction map to the residue field of this valuation ring to obtain a representation $\bar{\rho} : G_F \to \mathrm{GL}_2(\mathbb{F}_{\ell^r})$ for some r. The *residual representation* $\widetilde{\rho} : G_F \to \mathrm{GL}_2(\mathbb{F}_{\ell^r})$ is defined to be the semisimplification of any such $\bar{\rho}$ (which is well defined up to isomorphism).

Each Galois representation that we shall consider is *rational*, in the sense that, for each non-archimidean place v, the coefficients of the characteristic polynomial of Frob_v are rational. The following result (which is no doubt well known to the experts, but for which we could find no reference) shows that, for any such representation, the corresponding residual representation can be assumed to have image in $\mathrm{GL}_2(\mathbb{F}_\ell)$.

Lemma 3.1. *Let $\rho : G_F \to \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$ be a rational Galois representation, and let $\widetilde{\rho} : G_F \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the corresponding residual representation. Then there exists an element $t \in \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ such that $t\widetilde{\rho}(g)t^{-1} \in \mathrm{GL}_2(\mathbb{F}_\ell)$ for all $g \in G_F$.*

Proof. Let the image of $\widetilde{\rho}$ lie in $\mathrm{GL}_2(\mathbb{F}_{\ell^r})$, let σ generate the cyclic group $\mathrm{Gal}(\mathbb{F}_{\ell^r}/\mathbb{F}_\ell)$, and consider the representations $\widetilde{\rho}$ and $\sigma \circ \widetilde{\rho}$. Since σ fixes $\mathbb{F}_\ell$, the characteristic polynomials of these two representations on Frobenius elements coincide, and, since both representations are semisimple by definition, a theorem of Brauer and Nesbitt implies that they are isomorphic. Thus there exists some $s \in \mathrm{GL}_2(\mathbb{F}_{\ell^r})$ such that $\sigma(\widetilde{\rho}(g)) = s^{-1}\widetilde{\rho}(g)s$ for all $g \in G_F$.

Define an element

$$\pi_s = \prod_{i=1}^{r} \sigma^i(s) \in \mathrm{GL}_2(\mathbb{F}_{\ell^r}).$$

Since $\mathrm{GL}_2(\mathbb{F}_{\ell^r})$ is finite, π_s must have finite order, m, say.

Let $n = mr$, and let τ be a generator of the cyclic group $G = \mathrm{Gal}(\mathbb{F}_{\ell^n}/\mathbb{F}_\ell)$, so that, in particular, $\tau|_{\mathbb{F}_{\ell^r}} = \sigma$. A straightforward check shows that the map

$$\gamma : G \to \mathrm{GL}_2(\mathbb{F}_{\ell^n}); \quad \tau^k \mapsto \gamma_{\tau^k} := \prod_{i=0}^{k-1} \tau^i(s)$$

defines a G-cocycle. By Hilbert's Theorem 90, the first cohomology group $H^1(G, \mathrm{GL}_2(\mathbb{F}_{\ell^n}))$ is trivial, and thus there exists some $t \in \mathrm{GL}_2(\mathbb{F}_{\ell^n})$ such that $t\gamma_{\tau^k}\tau^k(t)^{-1} = \mathrm{Id}$ for all k. In particular, since $\gamma_\tau = s$, we have $s = t^{-1}\tau(t)$.

Viewing $\mathrm{GL}_2(\mathbb{F}_{\ell^r})$ as a subgroup of $\mathrm{GL}_2(\mathbb{F}_{\ell^n})$ on which $\tau \in \mathrm{Gal}(\mathbb{F}_{\ell^n}/\mathbb{F}_{\ell^r})$ acts as the element $\sigma \in \mathrm{Gal}(\mathbb{F}_{\ell^r}/\mathbb{F}_\ell)$, we observe that, for each $g \in G_F$,

$$\tau(t\widetilde{\rho}(g)t^{-1}) = \tau(t)\sigma(\widetilde{\rho}(g))\tau(t)^{-1} = \tau(t)s^{-1}\widetilde{\rho}(g)s\tau(t)^{-1} = t\widetilde{\rho}(g)t^{-1},$$

and thus $t\widetilde{\rho}(g)t^{-1} \in \mathrm{GL}_2(\mathbb{F}_\ell)$ for all $g \in G_F$, as required. □

Remark. There is nothing special about our restriction to rational representations. The same argument shows that, if the coefficients of the characteristic polynomial of $\widetilde{\rho}(\mathrm{Frob}_\mathfrak{p})$ lie in $\mathbb{F}_{\ell^r}$ for all primes $\mathfrak{p}$, then we can define $\widetilde{\rho}$ over the field $\mathbb{F}_{\ell^r}$.

We restrict our attention to the case $\ell = 2$. Thus, for any rational 2-adic representation ρ, the residual representation $\widetilde{\rho}$ has image in $\mathrm{GL}_2(\mathbb{F}_2)$, which is isomorphic to S_3. It is straightforward

https://doi.org/10.1112/S1461157016000048 Published online by Cambridge University Press

to see that, up to semisimplification, $\widetilde{\rho}$ has only three possible images; it can be trivial, have cyclic image isomorphic to C_3, or be isomorphic to S_3 itself.

Using class field theory, it is possible to determine isomorphism of the residual representations $\widetilde{\rho_E}$ and $\widetilde{\rho_\pi}$ by checking certain parity conditions on the traces of these representations at Frobenius elements above a finite set $\mathcal{S}_1$ of prime ideals of F (a discussion of this method may be found in [**24**, Chapter 6.3]). Henceforth, we shall assume that these residual representations are indeed isomorphic. It is then known that one can produce a second set $\mathcal{S}_2$ of prime ideals of F such that the full representations ρ_E and ρ_π are isomorphic if, and only if, the traces of $\rho_E(\mathrm{Frob}_\mathfrak{p})$ and $\rho_\pi(\mathrm{Frob}_\mathfrak{p})$ for all primes $\mathfrak{p} \in \mathcal{S}_2$ are equal. A suitable set $\mathcal{S}_2$ can be constructed by the *Faltings–Serre method* in the case that the residual representations are absolutely irreducible, or by a result of Livné in all other cases.

For reference, we state these results here, beginning with the absolutely irreducible case.

THEOREM 3.2. *Let ρ_1, $\rho_2 : G_F \to \mathrm{GL}_2(\mathbb{Z}_2)$ be two representations which have the same determinant, are unramified outside a finite set of prime ideals of F, and whose residual representations are absolutely irreducible and isomorphic. Then there exists a finite set $\mathcal{S}$ of prime ideals of F such that ρ_1 and ρ_2 have isomorphic semisimplifications if, and only if, $\mathrm{Tr}(\rho_1(\mathrm{Frob}_\mathfrak{p})) = \mathrm{Tr}(\rho_2(\mathrm{Frob}_\mathfrak{p}))$ for all $\mathfrak{p} \in \mathcal{S}$.*

For a detailed account of the proof, we refer the reader to [**12**, § 4]. The requirement that both representations have image in $\mathrm{GL}_2(\mathbb{Z}_2)$, which *a priori* could be problematic, is in fact easily dealt with. Indeed, absolute irreducibility of the residual representations, combined with the rationality of the traces of the full representations, means that we can use a result of Carayol (see [**8**, Theorem 2]) to find that ρ_π (and indeed ρ_E, although this is well known) is in fact equivalent to a representation which takes values in $\mathrm{GL}_2(\mathbb{Z}_2)$.

If the images of ρ_π and ρ_E are not absolutely irreducible, then we require the following result of Livné, whose statement we borrow from the thesis of Chênevert [**9**, Theorem 5.4.9].

THEOREM 3.3. *Let F be a number field, and V_λ a finite extension of $\mathbb{Q}_2$ with ring of integers $\mathcal{O}_\lambda$ and maximal ideal λ. Let*

$$\rho_1, \rho_2 : G_F \to \mathrm{GL}_2(V_\lambda)$$

be two continuous representations unramified outside a finite set $\mathcal{S}$ of places of F, such that

$$\mathrm{Tr}(\widetilde{\rho_1}) \equiv \mathrm{Tr}(\widetilde{\rho_2}) \equiv 0 \pmod{\lambda} \quad \text{and} \quad \det(\widetilde{\rho_1}) \equiv \det(\widetilde{\rho_2}) \equiv 1 \pmod{\lambda}.$$

Let $F_{2,\mathcal{S}}$ denote the compositum of all quadratic extensions of F unramified outside $\mathcal{S}$, and suppose that there exists a set of prime ideals $\mathcal{T}$ of F, disjoint from $\mathcal{S}$, such that:

(i) *$\{\mathrm{Frob}_\mathfrak{p}, \mathfrak{p} \in \mathcal{T}\}$ surjects onto $\mathrm{Gal}(F_{2,\mathcal{S}}/F)$; and*

(ii) *the characteristic polynomials of ρ_1 and ρ_2 at the elements $\{\mathrm{Frob}_\mathfrak{p}, \mathfrak{p} \in \mathcal{T}\}$ are equal.*

Then ρ_1 and ρ_2 have isomorphic semisimplifications.

If the residual representations are trivial, then this suffices to prove isomorphism (up to semisimplification) of the full representations, and indeed this is all we require for our examples, which have either trivial or full residual image. For completeness, we note that if the residual representations have C_3-image, then the hypotheses of the theorem do not hold (since the traces of the elements in $\mathrm{GL}_2(\mathbb{F}_2)$ of order 3 are odd), and we must take an additional step.

Let $\widetilde{\rho_E} \simeq \widetilde{\rho_\pi} \simeq \widetilde{\rho}$, say, and define the fixed field $L = \overline{F}^{\ker(\widetilde{\rho})}$, so that L/F is a cubic Galois extension, and G_L is a normal subgroup of G_F. Denoting by ρ'_E and ρ'_π the restrictions of ρ_E and ρ_π to G_L, it is clear that the corresponding residual representations are trivial, so we can use Theorem 3.3 to determine isomorphism of ρ'_E and ρ'_π (as usual, up to semisimplification).

https://doi.org/10.1112/S1461157016000048 Published online by Cambridge University Press

For the following argument, we impose an additional restriction on the elliptic curve E, namely that the base change of E to the field L does not possess complex multiplication. If this restriction is satisfied, then the representation ρ'_E (and thus also ρ'_π) is in fact irreducible. By Schur's lemma, $\mathrm{Hom}_{G_L}(\rho'_E, \rho'_\pi)$ contains a copy of V_λ on which G_L acts trivially, and so $\mathrm{Hom}_{G_L}(\mathbf{1}, (\rho_E \otimes \rho_\pi^\vee)|_{G_L})$ is non-trivial. By Frobenius reciprocity, the latter group is isomorphic to $\mathrm{Hom}_{G_F}(\mathrm{Ind}_{G_L}^{G_F}(\mathbf{1}), \rho_E \otimes \rho_\pi^\vee)$, which decomposes as a direct sum

$$\mathrm{Hom}_{G_F}(\mathrm{Ind}_{G_L}^{G_F}(\mathbf{1}), \rho_E \otimes \rho_\pi^\vee) \simeq \bigoplus_{\chi|_{G_L}=\mathbf{1}} \mathrm{Hom}_{G_F}(\rho_\pi \otimes \chi, \rho_E).$$

Invoking Schur's lemma once more, we observe that one of these summands must be non-trivial, and that $\rho_E \simeq \rho_\pi \otimes \chi$ for some character χ of G_F whose restriction to G_L is non-trivial. One can then determine whether this character is trivial, by finding a prime $\mathfrak{p}$ of F which is inert in L. In this case, $\mathrm{Frob}_\mathfrak{p}$ is non-trivial, and so χ is completely determined by the value it takes on this Frobenius element. In particular, if $\mathrm{Tr}(\rho_\pi(\mathrm{Frob}_\mathfrak{p})) = \mathrm{Tr}(\rho_E(\mathrm{Frob}_\mathfrak{p}))$, then $\chi(\mathrm{Frob}_\mathfrak{p}) = 1$, χ is trivial, and ρ_π and ρ_E have isomorphic semisimplifications, as required.

4. *Computing the Hecke action on cohomology*

To utilize the method described in the previous section, we require knowledge of the representation ρ_E, and the values $\mathrm{Tr}(\rho_\pi(\mathrm{Frob}_\mathfrak{p}))$ for a finite set of primes $\mathfrak{p}$ of F. The former is straightforward to find, given an elliptic curve E, as the action of G_F on the 2-adic Tate module $\mathrm{Ta}_2(E)$ of E is well understood. We therefore require a method to compute the trace of ρ_π on Frobenius elements.

From § 2, we know that, for a place v of F, dividing $\mathfrak{p}$, at which π is unramified, this is given by the action of the Hecke operator T_v on the space of $\mathrm{GL}_2(\mathcal{O}_v)$-fixed vectors of π_v. Moreover, this Hecke action translates to the cohomological setting mentioned previously, where it is described in terms of the action of a double coset operator on the de Rham cohomology of differential forms on $X_0(\mathfrak{n})$.

At this juncture, we note an important observation: one could, instead, work with the *rational* cohomology, $H^*_{\mathrm{cusp}}(X_0(\mathfrak{n}), \mathbb{Q})$. By [19, Chapter III, Proposition 2.2], this is also a $K_0(\mathfrak{n})$-module, and so admits a Hecke action. Moreover, the identification

$$H^*_{\mathrm{cusp}}(X_0(\mathfrak{n}), \mathbb{C}) \simeq H^*_{\mathrm{cusp}}(X_0(\mathfrak{n}), \mathbb{Q}) \otimes \mathbb{C}$$

is an isomorphism of Hecke modules, and so, in particular, the action of the Hecke operators T_v on the *complex* cohomology can be defined rationally, a fact which shall prove useful later.

We shall now provide a more concrete realization of this cohomology and the corresponding Hecke operators, which we can use to compute the desired information about the Galois representations ρ_π. Key to this is the fact that we may reinterpret the locally symmetric space $X_0(\mathfrak{n})$ as a quotient of some *globally* symmetric space X by an arithmetic subgroup $\Gamma_0(\mathfrak{n})$ of $G(\mathbb{Q})$, which in turn allows us to compute $H^*(X_0(\mathfrak{n}), \mathbb{C})$ by considering the group cohomology $H^*(\Gamma_0(\mathfrak{n}), \mathbb{C})$.

More precisely, define the globally symmetric space

$$X = G(\mathbb{R})/A_G^0(\mathbb{R})K_\infty,$$

and let $\Gamma_0(\mathfrak{n})$ denote the arithmetic subgroup of $G(\mathbb{Q})$, which we identify with $\mathrm{GL}_2(F)$, comprising those matrices in $\mathrm{GL}_2(\mathcal{O})$ which are upper-triangular modulo the ideal $\mathfrak{n}$. Recalling that we have restricted our attention to fields F with trivial class group, we have an identification

$$X_0(\mathfrak{n}) \simeq \Gamma_0(\mathfrak{n})\backslash X.$$

https://doi.org/10.1112/S1461157016000048 Published online by Cambridge University Press

A standard argument (an example of which can be found in the appendix of [20]) then states that we have an equivalence of cohomology groups:

$$H^*(X_0(\mathfrak{n}), \mathbb{C}) \simeq H^*(\Gamma_0(\mathfrak{n}), \mathbb{C}).$$

We may therefore choose to work with the group cohomology appearing on the right-hand side, but we require a little extra work before we can compute it effectively.

Recall that the *cohomological dimension* ν of a torsion-free arithmetic subgroup Γ of $G(\mathbb{Q})$ is defined to be the smallest integer such that $H^{\nu+1}(\Gamma, \mathcal{M}) = 0$ for *all* coefficient systems $\mathcal{M}$. Since $\Gamma_0(\mathfrak{n})$ is not torsion-free, we need a more general definition, that of the *virtual cohomological dimension* (which we also denote by ν) of an arbitrary arithemtic subgroup Γ of $G(\mathbb{Q})$, which is defined to be the cohomological dimension of any finite-index torsion-free subgroup of Γ.

By *Borel–Serre duality* (see [5, § 11.4]) we have an equivalence of Hecke modules

$$H^{\nu-k}(\Gamma_0(\mathfrak{n}), \mathbb{C}) \simeq H_k(\Gamma_0(\mathfrak{n}), \mathrm{St}_2 \otimes_{\mathbb{Z}} \mathbb{C}),$$

where the *Steinberg module* St_2 for $\mathrm{GL}_2(F)$ is defined by the short exact sequence

$$0 \to \mathrm{St}_2 \to \mathbb{Z}[\mathbb{P}^1(F)] \xrightarrow{\epsilon} \mathbb{Z} \to 0$$

(here ϵ denotes the augmentation map sending $\sum n_P P$ to $\sum n_P$).

The group homology of $\Gamma_0(\mathfrak{n})$ with coefficients in $\mathrm{St}_2 \otimes_{\mathbb{Z}} \mathbb{C}$ can in turn be computed by constructing an appropriate resolution of the Steinberg module. Our preferred example of such a resolution is given by the *sharbly complex* $\mathscr{S}_*$, which we define as follows: for each non-negative integer k, let $\mathscr{S}_k$ denote the space of $\mathbb{Z}$-linear combinations of k-*sharblies*, $(k+2)$-tuples $\mathbf{u} = [u_1, \ldots, u_{k+2}]$ with each $u_i \in \mathcal{O}^2$, subject to the following relations:

- $[u_1, \ldots, u_{k+2}] = \mathrm{sgn}(\sigma)[u_{\sigma(1)}, \ldots, u_{\sigma(k+2)}]$ for any permutation $\sigma \in S_{k+2}$;
- $[u, u_2, \ldots, u_{k+2}] = [v, u_2, \ldots, u_{k+2}]$ if there exists $\lambda \in \mathbb{R}_+$ such that for each embedding $\iota : F \hookrightarrow \mathbb{C}$ we have $\iota(uu^*) = \lambda\iota(vv^*)$;
- $[u_1, \ldots, u_{k+2}] = 0$ if $u_1, \ldots, u_{k+2}$ span a ine-dimensional F-vector space (we call such sharblies *degenerate*).

To give $\mathscr{S}_*$ the form of a simplicial complex, we define a boundary map $\partial_k : \mathscr{S}_k \to \mathscr{S}_{k-1}$ by

$$\partial_k[u_1, \ldots, u_{k+2}] = \sum_{i=1}^{k} (-1)^{i+1}[u_1, \ldots, \hat{u}_i, \ldots, u_{k+2}],$$

where $\hat{u}_i$ indicates that we omit the vector u_i from the resulting sharbly. The sharbly complex admits an obvious action of $\mathrm{GL}_2(\mathcal{O})$, given by

$$g \cdot [u_1, \ldots, u_{k+2}] = [gu_1, \ldots, gu_{k+2}], \quad g \in \mathrm{GL}_2(\mathcal{O}),$$

which commutes with the boundary map, and thus in particular we can define the subcomplex of $\Gamma_0(\mathfrak{n})$-invariants, which we denote by $(\mathscr{S}_*)_{\Gamma_0(\mathfrak{n})}$, by imposing the additional relation that

- $[u_1, \ldots, u_{k+2}] = \gamma[u_1, \ldots, u_{k+2}]$ for all $\gamma \in \Gamma_0(\mathfrak{n})$.

It is known (see, for example, [1, Theorem 5]) that the sharbly complex provides an acyclic resolution of the Steinberg module, and thus we have an identification

$$H_k(\Gamma_0(\mathfrak{n}), \mathrm{St}_2 \otimes_{\mathbb{Z}} \mathbb{C}) \simeq H_k((\mathscr{S}_*)_{\Gamma_0(\mathfrak{n})}, \mathbb{C})$$

of homology groups. Moreover, the identifications we have established are all Hecke equivariant (see, for example, [2, Theorem 2.4]), and so we have a Hecke action on the sharbly homology.

https://doi.org/10.1112/S1461157016000048 Published online by Cambridge University Press

One can see without too much difficulty that, for a non-archimedean place v of F, corresponding to the prime ideal $\mathfrak{p}$ of F, the action of the Hecke operator T_v on $\mathscr{S}_*$ is given by

$$T_v(u) = \sum g_i \mathbf{u},$$

where we have a decomposition of the double coset space

$$\Gamma_0(\mathfrak{n}) \begin{pmatrix} 1 & 0 \\ 0 & \nu \end{pmatrix} \Gamma_0(\mathfrak{n}) = \coprod \Gamma_0(\mathfrak{n}) g_i,$$

for a generator ν of the ideal $\mathfrak{p}$.

Thus we can, in theory at least, use the homology of the sharbly complex to compute the Hecke action on cuspidal automorphic forms of level $\mathfrak{n}$. Moreover, as we are interested in classes which correspond to cuspidal automorphic forms, we can restrict our attention to homology whose degree lies within a specified range.

Indeed, one can show (using a slight adaptation of [**28**, Theorem 6.2]) that the cuspidal cohomology $H^i_{\mathrm{cusp}}(X_0(\mathfrak{n}), \mathbb{C})$ is non-trivial only if $2 \leqslant i \leqslant 5$. Combined with the fact that the virtual cohomological dimension of $\Gamma_0(\mathfrak{n})$ is 6 (which can be found by applying [**5**, Theorem 11.4.4] to our specific case), this means that we need only consider homology in degrees 1 to 4. Furthermore, it is known that any cuspidal automorphic form which appears as a homology class in one of these degrees in fact appears in *every* degree, so we lose nothing by specializing to a single degree.

The sharbly complex is intrinsically linked with the symmetric space X defined previously, and so we shall spend some time discussing the geometry of this space in greater detail. Recall that

$$X = G(\mathbb{R})/A^0_G(\mathbb{R})K_\infty,$$

and moreover that $G(\mathbb{R}) \simeq \mathrm{GL}_2(\mathbb{C}) \times \mathrm{GL}_2(\mathbb{C})$, $K_\infty \simeq \mathrm{U}(2) \times \mathrm{U}(2)$, and $A^0_G(\mathbb{R}) \simeq \mathbb{R}_+$. Using the standard identification of $\mathrm{SL}_2(\mathbb{C})/\mathrm{SU}(2)$ with the hyperbolic 3-space $\mathcal{H}_3$, we therefore find that

$$X \simeq \mathcal{H}_3 \times \mathcal{H}_3 \times \mathbb{R}_+,$$

a seven-dimensional space.

We can identify X with a cone of binary Hermitian forms. More precisely, let v_1 and v_2 be two non-conjugate embeddings of F into $\mathbb{C}$, and define $\mathrm{Herm}_2(F_{v_i})$ to be the space of 2×2 Hermitian matrices with entries in F_{v_i}. Then we can define an inner product space

$$\mathcal{V} = \mathrm{Herm}_2(F_{v_1}) \times \mathrm{Herm}_2(F_{v_2}),$$

with inner product $\langle\, , \rangle$ defined by

$$\langle \Phi, \Psi \rangle = 2\,\mathrm{Tr}(\Phi_1\Psi_1 + \Phi_2\Psi_2)$$

(the factor of 2 is largely irrelevant in this case, but comes into play if we extend these ideas to fields of mixed signature; see [**17**] for an example of this).

Note that any point $\Phi \in \mathcal{V}$ defines a Hermitian form on F^2 (which, through abuse of notation, we shall also denote by Φ) given by

$$\Phi(x, y) = 2\,\mathrm{Tr}(\Phi_1 x_1 y_1^* + \Phi_2 x_2 y_2^*),$$

where x_i and y_i denote the images of x and y under the embedding v_i, and * denotes the complex conjugate transpose. We shall henceforth refer to points in $\mathcal{V}$ and their corresponding Hermitian forms interchangeably, dependent on the context.

https://doi.org/10.1112/S1461157016000048 Published online by Cambridge University Press

We denote by $\mathcal{C}$ the cone of positive definite forms in $\mathcal{V}$, whose closure $\overline{\mathcal{C}}$ is the cone of positive semidefinite forms. It can be shown that a form Φ belongs to $\mathcal{C}$ (respectively, $\overline{\mathcal{C}}$) if, and only if, each matrix Φ_i is positive definite (respectively, positive semidefinite). The group $G(\mathbb{R})$ acts on $\mathcal{V}$ via the map

$$g \cdot \Phi = (g_1 \Phi_1 g_1^*, g_2 \Phi_2 g_2^*),$$

and this action preserves $\mathcal{C}$. Moreover, it can easily be seen that $G(\mathbb{R})$ acts *transitively* on $\mathcal{C}$, and that the stabilizer of any point is isomorphic to K_∞. Thus we obtain an isomorphism

$$\mathcal{C}/\mathbb{R}_+ \simeq X.$$

The usefulness of this isomorphism lies in the fact that the cone $\mathcal{C}$ is an example of a *positivity domain*, in the sense of Koecher's work in [**25**]. Such structures possess many desirable properties: in particular, $\mathcal{C}$ admits a decomposition into polyhedral cones, which will provide us with a cellular decomposition of our symmetric space X.

This decomposition is straightforward to describe. For each vector $x \in \mathcal{O}^2$, we can define a point $q(x) \in \mathcal{V}$ by setting

$$q(x) = (x_1 x_1^*, x_2 x_2^*).$$

Note that, using this definition, we can rewrite the second relation defining the sharbly complex as

$$[u, u_2, \ldots, u_{k+2}] = [v, u_2, \ldots, u_{k+2}] \text{ if } q(u) = \lambda q(v) \text{ for some } \lambda \in \mathbb{R}_+.$$

We may (and henceforth shall) therefore assume that each vector $u_i \in \mathcal{O}^2$ appearing in a sharbly $\mathbf{u}$ is *primitive*, in the sense that no point of Ξ lies on the line segment joining $q(u_i)$ and the origin (that is, if $q(v_i) = \lambda q(u_i)$ for some $v_i \in \mathcal{O}^2$ and $\lambda \in \mathbb{R}_+$, then $\lambda \geqslant 1$).

Each matrix $x_i x_i^*$ is positive semidefinite, and so $q(x)$ lies in $\overline{\mathcal{C}}$. The set $\Xi := \{q(x);\ x \in \mathcal{O}^2\}$ is an example of what Koecher refers to as an *admissible subset* of $\overline{\mathcal{C}}$. For each form $\Phi \in \mathcal{C}$, the set of values $\{\langle \Phi, q(x) \rangle :\ q(x) \in \Xi\}$ forms a discrete subset of $\mathbb{R}$, and in particular we may define the *minimum* of Φ to be

$$m(\Phi) := \inf_{q(x) \in \Xi} \{\langle \Phi, q(x) \rangle\}.$$

The points $q(x)$ in Ξ for which $\langle \Phi, q(x) \rangle$ attains this minimum are called *minimal vectors* of Φ, and we denote by $M(\Phi)$ the set of minimal vectors of Φ. If the set of minimal vectors of a form Φ span the vector space $\mathcal{V}$, then we call Φ *perfect*. Note that, if Φ is perfect, then so too is $\lambda\Phi$ for any $\lambda \in \mathbb{R}_+$, so we may assume without loss of generality that $m(\Phi) = 1$ for all perfect forms Φ.

The perfect forms provide us with our desired decomposition. To each perfect form Φ, we can assign a convex polytope $\mathcal{F}_\Phi$ in $\overline{\mathcal{C}}$ by taking the convex hull of the minimal vectors of Φ. We can then define a polyhedral cone, known as a *perfect pyramid*, by taking the cone above $\mathcal{F}_\Phi$ (that is, the set of half-lines passing through both the origin and a point in $\mathcal{F}_\Phi$). Koecher's work then shows that the set of perfect pyramids provides a decomposition of the cone $\mathcal{C}$, in the sense that every point in $\mathcal{C}$ lies in some perfect pyramid, and any two perfect pyramids have disjoint interiors. Moreover, the action of $\mathrm{GL}_2(\mathcal{O})$ on $\mathcal{O}^2$ clearly induces an action on the set of points Ξ, which preserves the set of perfect pyramids, and under this action there are only finitely many equivalence classes of perfect pyramids. For a more detailed description of these ideas, we refer the reader to the excellent exposition in [**16**, § 7].

Recalling our earlier identification of the symmetric space X with $\mathcal{C}/\mathbb{R}_+$, the set of polytopes $\mathcal{F}_\Phi$ provides us with a cellular decomposition of X. At this juncture, we note that one *can* use the corresponding cell complex to compute the cohomology $H^*(X_0(\mathfrak{n}), \mathbb{C})$ directly. More precisely, there is a retract W of the space X, known as the *well-rounded retract*, from which

https://doi.org/10.1112/S1461157016000048 Published online by Cambridge University Press

one can obtain a cell complex using the decomposition induced by that on X, and then one can compute $H^*(X_0(\mathfrak{n}), \mathbb{C})$ by considering the $\Gamma_0(\mathfrak{n})$-*equivariant* cohomology $H^*_{\Gamma_0(\mathfrak{n})}(W, \mathbb{C})$.

Since $\Gamma_0(\mathfrak{n})$ has finite index in $\mathrm{GL}_2(\mathcal{O})$, there are only finitely many cells of a given dimension up to $\Gamma_0(\mathfrak{n})$-equivalence, and thus one can compute the cohomology using standard techniques for finite cell complexes (as is done in [**17**], for example).

We prefer to work completely with the sharbly complex, but still make use of the cellular decomposition of X that we have just described. Note that any k-sharbly $\mathbf{u} = [u_1, \ldots, u_{k+2}]$ defines a convex polytope $\mathcal{P}(\mathbf{u})$ in $\mathcal{V}$ by taking the convex hull of the points $q(u_i)$. We define a k-sharbly $\mathbf{u}$ to be *reduced* if $\mathcal{P}(\mathbf{u})$ is contained in $\mathcal{F}_\Phi$ for some perfect form Φ, and *totally reduced* if $\mathcal{P}(\mathbf{u})$ defines a $(k+1)$-dimensional face of $\mathcal{F}_\Phi$ for some perfect form Φ. Clearly, the set of totally reduced k-sharblies is a subset of the set of reduced k-sharblies.

Since there are only finitely many perfect pyramids under the action of $\Gamma_0(\mathfrak{n})$, it follows that there are only finitely many reduced and totally reduced sharblies up to $\Gamma_0(\mathfrak{n})$-equivalence. In [**14**], the authors use the subcomplex of reduced sharblies to compute the homology of the sharbly complex. We choose to work instead with the smaller subcomplex of totally reduced sharblies, which our data suggests also computes the homology of $(\mathscr{S}_*)_{\Gamma_0(\mathfrak{n})}$ in practice.

It soon becomes apparent that the subcomplex of totally reduced sharblies is not preserved by the action of the Hecke operators T_v defined previously. Thus we would like to find a means for rewriting an arbitrary k-sharbly chain in terms of totally reduced sharblies, in order to be able to compute this action. While this is not possible in general, it turns out that if $k \in \{0, 1\}$ then, given a k-sharbly *cycle* representing a class in $H_k((\mathscr{S}_*)_{\Gamma_0(\mathfrak{n})}, \mathbb{C})$, we can in practice find another representative of the same class whose support consists entirely of totally reduced sharblies, using an algorithm described in [**15**], which we shall now briefly describe.

To begin with, suppose that we are given a generic 0-sharbly $\mathbf{u} = [u_1, u_2]$, and consider the point $\mathcal{B}(\mathbf{u}) = \frac{1}{2}(q(u_1) + q(u_2))$. Since $\overline{\mathcal{C}}$ is a convex cone, $\mathcal{B}(\mathbf{u})$ lies inside it and, in particular, is contained in some perfect pyramid $\mathcal{F}_\Phi$, say. We define the *size* $N(\mathbf{u})$ of $\mathbf{u}$ to be the inner product $\langle \Phi, \mathcal{B}(\mathbf{u}) \rangle$. Note that this definition of size is well defined; this is clear if $\mathcal{B}(\mathbf{u})$ lies in the interior of $\mathcal{F}_\Phi$, as in this case Φ is uniquely determined. If, on the other hand, $\mathcal{B}(\mathbf{u})$ lies in some face $\mathcal{E}$ on the boundary of a perfect pyramid $\mathcal{F}_\Phi$, then it is a convex combination of the vertices of $\mathcal{E}$. If Φ' is another perfect form, with the intersection $\mathcal{F}_{\Phi'} \cap \mathcal{F}_\Phi$ containing $\mathcal{E}$, then $M(\Phi) \cap M(\Phi')$ contains the vertices of $\mathcal{E}$, and so $\langle \Phi, \mathcal{B}(\mathbf{u}) \rangle = \langle \Phi', \mathcal{B}(\mathbf{u}) \rangle$.

By definition, $N(\mathbf{u}) \geqslant 1$, with equality if, and only if, the points $q(u_1), q(u_2) \in M(\Phi)$ for some perfect form Φ, which occurs if, and only if, $\mathbf{u}$ is reduced. The size of a 0-sharbly therefore seems an appropriate measure for how far it is from being reduced.

Now suppose that $\mathbf{u}$ is not reduced, and note that for any point $x \in \mathcal{O}^2$ we have

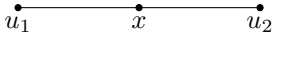
$$\mathbf{u} + \partial[u_2, u_1, x] = [u_1, x] + [x, u_2],$$

and thus $\mathbf{u}$ is homologous to $[u_1, x] + [x, u_2]$. We call a point $x \in \mathcal{O}^2$ a *reducing point* for $\mathbf{u}$ if

$$\mathrm{Max}\{N([u_1, x]), N([x, u_2])\} < N(\mathbf{u}).$$

One can prove (independently of the field F) that, if Φ denotes the perfect form corresponding to the perfect pyramid containing the point $\mathcal{B}(\mathbf{u})$, then there exists a reducing point x for $\mathbf{u}$ such that $q(x)$ is a minimal vector for Φ.

One can visualize this process by means of the following diagram. Here a 0-sharbly is represented by a straight line, with shorter lines representing sharblies of smaller size:



If $\mathbf{u}$ is reduced, but not totally reduced, we take a slightly different approach. One can define an alternative notion of the size of $\mathbf{u}$ (as in [**14**]) which we shall denote by $n(\mathbf{u})$, by

https://doi.org/10.1112/S1461157016000048 Published online by Cambridge University Press

setting $n(\mathbf{u}) = \mathrm{Norm}_{F/\mathbb{Q}}(\det(u_1|u_2))$. There appears to be a correlation between the values $N(\mathbf{u})$ and $n(\mathbf{u})$, with small values of $N(\mathbf{u})$ typically corresponding to small values of $n(\mathbf{u})$; for example, over the field $\mathbb{Q}(\zeta_{12})$, we observe that a non-degenerate 0-sharbly $\mathbf{u}$ is reduced if, and only if, $n(\mathbf{u}) \in \{1, 4, 9\}$, and is totally reduced if, and only if, $n(\mathbf{u}) = 1$. We therefore call a point $x \in \mathcal{O}^2$ a *reducing point* for a reduced 0-sharbly $\mathbf{u}$ if $\mathrm{Max}\{n([u_1, x]), n([x, u_2])\} < n(\mathbf{u})$. Over the field $\mathbb{Q}(\zeta_{12})$, one can always find such a reducing point (as there are only finitely many reduced 0-sharblies up to $\mathrm{GL}_2(\mathcal{O})$-equivalence, this can be confirmed by checking a finite number of possibilities).

We now consider the case of 1-sharblies, which is considerably more involved. Our original notion of size can be extended to a 1-sharbly $\mathbf{u} = [u_1, u_2, u_3]$ by defining $N(\mathbf{u})$ to be $\langle \Phi, \mathcal{B}(\mathbf{u})\rangle$, where $\mathcal{B}(\mathbf{u}) = \frac{1}{3}(q(u_1)+q(u_2)+q(u_3))$, and Φ once again denotes the perfect form corresponding to the perfect pyramid within which $\mathcal{B}(\mathbf{u})$ lies. Once again, $\mathbf{u}$ is reduced if, and only if, $N(\mathbf{u}) = 1$. (We note that one can similarly extend the definition of $n(\mathbf{u})$ to cater to 1-sharblies by setting $n(\mathbf{u}) = \mathrm{Max}\{n([u_i, u_j])\}$).

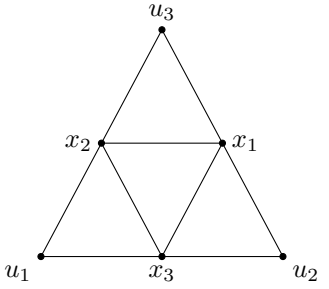
Now suppose we are given a generic 1-sharbly $\mathbf{u} = [u_1, u_2, u_3]$, none of whose edges are totally reduced, and choose reducing points x_1, x_2 and x_3 for the edges $[u_2, u_3]$, $[u_3, u_1]$ and $[u_1, u_2]$, respectively. Define a 2-sharbly chain

$$\nu := [u_1, u_2, u_3, x_1] + [u_3, u_1, x_1, x_2] + [u_1, u_2, x_1, x_3] + [u_1, x_1, x_2, x_3],$$

so that

$$\mathbf{u} + \partial\nu = [u_1, x_3, x_2] + [u_2, x_1, x_3] + [u_3, x_2, x_1] + [x_1, x_2, x_3] + \sum_{\sigma \in A_3} [u_{\sigma(1)}, u_{\sigma(2)}, x_{\sigma(3)}].$$

By definition, $\mathbf{u} + \partial\nu$ is homologous to $\mathbf{u}$. If we were able to neglect the final terms $[u_{\sigma(1)}, u_{\sigma(2)}, x_{\sigma(3)}]$, then we could represent the process of replacing $\mathbf{u}$ with $\mathbf{u} + \partial\nu$ by the following diagram, with 1-sharblies represented by triangles, where a smaller triangle corresponds to a sharbly of smaller size (we note that, unlike in the case of 0-sharblies, we cannot prove whether these sharblies are indeed smaller than $\mathbf{u}$, although in practice they seem to be):



In general, we cannot neglect the terms $[u_{\sigma(1)}, u_{\sigma(2)}, x_{\sigma(3)}]$. However, if $\mathbf{u}$ lies in the support of some 1-sharbly cycle ξ, then through careful choice of reducing points we can ensure that, when we perform this procedure over the entire chain, all such terms vanish. To provide a brief justification of this statement, let $\mathbf{u} \in \mathrm{Supp}(\xi)$, and consider the single edge $[u_1, u_2]$ of $\mathbf{u}$. Since the boundary of ξ vanishes in $(\mathscr{S}_*)_{\Gamma_0(\mathfrak{n})}$, one can show that there must exist some $\mathbf{v} = [v_1, v_2, v_3] \in \mathrm{Supp}(\xi)$ and some edge $[v_i, v_j]$ of $\mathbf{v}$ such that

$$[u_1, u_2] + [v_i, v_j] = 0 \pmod{\Gamma_0(\mathfrak{n})},$$

or equivalently that

$$[v_i, v_j] = \gamma[u_2, u_1]$$

https://doi.org/10.1112/S1461157016000048 Published online by Cambridge University Press

for some $\gamma \in \Gamma_0(\mathfrak{n})$. Let x be a reducing point for $[u_1, u_2]$, and assign to $[v_i, v_j]$ the reducing point γx. Then

$$[u_1, u_2, x] + [v_1, v_2, \gamma x] = [u_1, u_2, x] + \gamma[u_2, u_1, x] = 0 \pmod{\Gamma_0(\mathfrak{n})}.$$

Thus, as long as we can choose our reducing points in this manner, the term

$$\sum_{\mathbf{u} \in \mathrm{Supp}(\xi)} \sum_{\sigma \in A_3} [u_{\sigma(1)}, u_{\sigma(2)}, x_{\sigma(3)}]$$

vanishes in $(\mathscr{S}_1)_{\Gamma_0(\mathfrak{n})}$ for any 1-sharbly cycle ξ, so we need a means of ensuring that these points are chosen appropriately. We do this as follows. For any 0-sharbly $\mathbf{v}$, define a *lift* of $\mathbf{v}$ to be a matrix $M_{\mathbf{v}} \in M_2(\mathcal{O})$ such that, if m_1 and m_2 denote the columns of $M_{\mathbf{v}}$, then $[m_1, m_2] = \pm\mathbf{v}$, subject to the relations defining the sharbly complex. Now, to each 1-sharbly in $\mathrm{Supp}(\xi)$, we assign three lift matrices, one for each edge, such that if $\mathbf{v}$ and $\mathbf{w}$ are two edges, satisfying $\mathbf{v} = -\gamma\mathbf{w}$ for some $\gamma \in \Gamma_0(\mathfrak{n})$, then $M_{\mathbf{v}} = \gamma M_{\mathbf{w}}$.

Now suppose we wish to choose a reducing point for an edge $\mathbf{v}$ of $\mathbf{u} \in \mathrm{Supp}(\xi)$. If $M_{\mathbf{v}} = \gamma M_{\mathbf{w}}$, where $\gamma \in \Gamma_0(\mathfrak{n})$ and $\mathbf{w}$ is an edge for which we have already chosen a reducing point $x_{\mathbf{w}}$, then we assign to $\mathbf{v}$ the reducing point $\gamma x_{\mathbf{w}}$. Otherwise, we choose an arbitrary reducing point $x_{\mathbf{v}}$ for $\mathbf{v}$, and record both $M_{\mathbf{v}}$ and $x_{\mathbf{v}}$. In particular, if $\mathbf{v} = -\gamma\mathbf{w}$, then $M_{\mathbf{v}} = \gamma M_{\mathbf{w}}$, and so $x_{\mathbf{v}} = \gamma x_{\mathbf{w}}$, as we have required.

In practice, repeated applications of this procedure (with some minor adjustments to cater for certain exceptional cases, for which we refer the reader to the expositions in [**16**] or [**24**]) eventually produce a sharbly chain supported entirely by totally reduced 1-sharblies. In particular, given a basis for the homology group $H_1((\mathscr{S}_*)_{\Gamma_0(\mathfrak{n})}, \mathbb{C})$ and a non-archimedean place v of F, we can compute the action of the Hecke operator T_v on the sharbly homology.

5. *Results*

The following pages give details of cuspidal Hecke eigenclasses defined over the field $F = \mathbb{Q}(\zeta_{12})$, for which we investigated the cohomology $H^5(X_0(\mathfrak{n}), \mathbb{C})$ for all levels $\mathfrak{n}$ with norm at most 5500. In order to detect non-trivial cuspidal cohomology, we required data regarding the rank of the corresponding Eisenstein cohomology. This is provided in the following table, which collates heuristic data from [**14**] (to determine these ranks, one observes that the Hecke operator T_v, where v does not divide the level $\mathfrak{n}$, acts on the Eisenstein subspace via multiplication by $\mathrm{Norm}_{F/\mathbb{Q}}(v) + 1$):

Factorization type	$\mathfrak{p}$	$\mathfrak{p}^2$	$\mathfrak{p}^3$	$\mathfrak{p}^4$	$\mathfrak{p}^5$	$\mathfrak{p}^6$	$\mathfrak{p}\mathfrak{q}$	$\mathfrak{p}^2\mathfrak{q}$	$\mathfrak{p}^3\mathfrak{q}$	$\mathfrak{p}^4\mathfrak{q}$	$\mathfrak{p}^2\mathfrak{q}^2$	$\mathfrak{p}^3\mathfrak{q}^2$	$\mathfrak{p}\mathfrak{q}\mathfrak{r}$	$\mathfrak{p}^2\mathfrak{q}\mathfrak{r}$
$\dim H^5_{\mathrm{Eis}}(X_0(\mathfrak{n}), \mathbb{C})$	3	5	7	9	11	13	7	11	15	19	17	23	15	23

Up to Galois conjugation, there are 544 levels whose norm lies within the studied range. We discovered non-Eisenstein cohomology at 55 of these levels, with a total of 99 non-Eisenstein Hecke eigenclasses spread across these levels. Table 1 lists a set of generators for the levels studied, together with their factorization type and the discrepancy d between the rank of $H_1((\mathscr{S}_*)_{\Gamma_0(\mathfrak{n})}, \mathbb{C})$ and the expected rank of the Eisenstein cohomology (here $t = \zeta_{12}$ denotes a primitive twelfth root of unity):

Of the 99 non-Eisenstein Hecke eigenclasses we detected:

- 68 admitted rational eigenvalues;
- 18 admitted eigenvalues lying in a quadratic extension of $\mathbb{Q}$, which we list in Table 8;
- 9 admitted eigenvalues lying in a cubic extension of $\mathbb{Q}$, which we list in Table 9; and
- 4 admitted eigenvalues lying in a quartic extension of $\mathbb{Q}$, which we also list in Table 10.

https://doi.org/10.1112/S1461157016000048 Published online by Cambridge University Press

Of the 68 eigenclasses which admitted rational Hecke eigenvalues:

- 31 had eigenvalues matching an eigenclass appearing at a lower level, which we list in Table 4;
- 16 had eigenvalues matching those expected from the base change of an automorphic form defined over a quadratic subfield of F, which we list in Tables 5 and 6;
- 2 had eigenvalues matching those from the Eisenstein cohomology, up to sign, which we list in Table 7; and
- 19 classes could not be attributed to any of these phenomena, and we were able to find elliptic curves defined over F whose local data matched the eigenvalue data for each of these classes, and whose conductor was equal to the level $\mathfrak{n}$ at which this eigenclass appeared. We list these classes in Table 2, while the corresponding elliptic curves are listed in Table 10.

For each Hecke eigenclass, we list the corresponding Hecke eigenvalues for a number of primes of small norm. We indicate with a $*$ those primes which divide the level $\mathfrak{n}$.

Table 3 lists generators for the prime ideals of norm up to 25.

The classes listed in Table 4 are 'old', in the sense that the Hecke eigenvalues of this class match those of a non-Eisenstein class appearing at a level $\mathfrak{d}$ dividing $\mathfrak{n}$. Lower-case Roman numerals are used to denote each eigenclass.

The classes listed in Table 5 correspond to the base change of an automorphic representation π' defined over a subfield F' of F, such that the Hecke eigenvalues $a_{\mathfrak{q}}(\pi')$ are rational. If π is

TABLE 1. *Levels with non-Eisenstein cohomology classes.*

Level	Generator	Type	d	Level	Generator	Type	d
169	$2t^3-3t^2-3t+2$	$\mathfrak{pq}$	1	$3721a$	$7t^3-6t^2-t-1$	$\mathfrak{pq}$	3
441	$5t^2-1$	$\mathfrak{pq}$	1	$3721b$	$6t^2-5t-6$	$\mathfrak{pq}$	1
484	t^3+4t^2-4t-1	$\mathfrak{pq}$	1	3844	$5t^3-t^2+t+6$	$\mathfrak{pq}$	1
576	$2t^3+2t^2+2t-4$	$\mathfrak{p}^3\mathfrak{q}$	1	3969	$9t^2-6$	$\mathfrak{p}^2\mathfrak{q}$	2
625	5	$\mathfrak{pq}$	2	$4033a$	$-8t^3+9t-9$	$\mathfrak{pq}$	1
676	$3t^3-t^2+3t$	$\mathfrak{pqr}$	2	$4033b$	$-11t^3+6t^2+5t-9$	$\mathfrak{pq}$	1
1089	$-t^3+2t-6$	$\mathfrak{pq}$	2	4057	$6t^3+2t^2-9t-2$	$\mathfrak{p}$	1
1156	$3t^2+5t-3$	$\mathfrak{pq}$	1	4069	$-7t^3-6t^2+6t+2$	$\mathfrak{pq}$	1
1369	$2t^3+2t^2+3t-5$	$\mathfrak{pq}$	2	4096	8	$\mathfrak{p}^6$	1
1521	$4t^3+4t^2-5t+1$	$\mathfrak{pqr}$	2	$4225a$	$-5t^3+3t^2+9t-3$	$\mathfrak{pqr}$	2
1764	t^3+4t^2+4t-5	$\mathfrak{pqr}$	2	$4225b$	$-9t^3+3t^2+6t-1$	$\mathfrak{p}^2\mathfrak{q}$	1
1936	$4t^3-4t^2-6t-2$	$\mathfrak{p}^2\mathfrak{q}$	2	$4225c$	$-4t^3+7$	$\mathfrak{pqr}$	1
2041	$-t^3+6t^2-t-7$	$\mathfrak{pq}$	1	4356	$5t^3+3t^2+5t$	$\mathfrak{pqr}$	6
2116	$5t^3-5t^2+t+6$	$\mathfrak{pq}$	2	4516	$-4t^3-3t^2+9t+1$	$\mathfrak{pq}$	1
$2197a$	t^3-2t^2+3t+7	$\mathfrak{pqr}$	2	4624	$-8t^3-2$	$\mathfrak{p}^2\mathfrak{q}$	2
$2197b$	t^3+2t^2-7t-2	$\mathfrak{p}^2\mathfrak{q}$	2	4672	$8t^3+6t^2-6t-2$	$\mathfrak{p}^3\mathfrak{q}$	1
2209	$4t^3-8t-1$	$\mathfrak{p}$	1	4761	$-7t^3+5t^2+2t+2$	$\mathfrak{pq}$	3
2257	$-2t^3+6t^2+5t+1$	$\mathfrak{pq}$	1	4852	$-4t^3+7t^2+3t+1$	$\mathfrak{pq}$	1
2304	$8t^3-4t$	$\mathfrak{p}^4\mathfrak{q}$	2	5041	$-8t^3+3t^2+3t-8$	$\mathfrak{p}$	2
2401	7	$\mathfrak{pq}$	3	5184	$-6t^2+6t+6$	$\mathfrak{p}^3\mathfrak{q}^2$	2
2452	$-7t^3+t^2+t+2$	$\mathfrak{pq}$	1	5317	$-7t^3+3t^2-2t-4$	$\mathfrak{pq}$	1
$2500a$	$-t^3-7t^2+t$	$\mathfrak{p}^2\mathfrak{q}$	1	$5329a$	t^3+5t^2+3t-9	$\mathfrak{p}^2$	2
$2500b$	$5t^2+5t-5$	$\mathfrak{pqr}$	4	$5329b$	$3t^3-8t^2-3t$	$\mathfrak{pq}$	2
2704	$-2t^3-6t^2+6t+2$	$\mathfrak{p}^2\mathfrak{qr}$	4	$5329c$	$3t^3-6t-10$	$\mathfrak{pq}$	4
2916	$3t^3-3t^2+3t+6$	$\mathfrak{p}^3\mathfrak{q}$	2	$5329d$	$8t^3-9t$	$\mathfrak{pq}$	1
2977	$4t^3+2t^2-9t+2$	$\mathfrak{pq}$	1	5473	$-9t-8$	$\mathfrak{pq}$	1
3328	$4t^3+8t^2-4t-4$	$\mathfrak{p}^4\mathfrak{q}$	1	5476	$-5t^2-t-5$	$\mathfrak{pqr}$	5
3481	$5t^3-5t^2-6t-1$	$\mathfrak{p}$	2				

https://doi.org/10.1112/S1461157016000048 Published online by Cambridge University Press

a base change of π', and $\mathfrak{p}$ is a prime of F lying above a prime $\mathfrak{q}$ of F', then

$$a_{\mathfrak{p}}(\pi) = \begin{cases} a_{\mathfrak{q}}(\pi') & \text{if } \mathfrak{q} \text{ splits in } F, \\ a_{\mathfrak{q}}(\pi')^2 - 2\,\mathrm{Norm}_{F'/\mathbb{Q}}(\mathfrak{q}) & \text{if } \mathfrak{q} \text{ is inert in } F. \end{cases}$$

TABLE 2. *Rational Hecke eigenclasses over F.*

Class	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_{13,1}$	$\mathfrak{p}_{13,2}$	$\mathfrak{p}_{13,3}$	$\mathfrak{p}_{13,4}$	$\mathfrak{p}_{5,1}$	$\mathfrak{p}_{5,2}$
441	0	$*$	-6	4	4	-6	-4	-4
1156	$*$	0	4	4	-6	-6	6	6
2041	2	-2	2	2	$*$	-4	-4	-10
2257	-3	-4	-1	1	-6	-3	1	-8
2452	$*$	1	-4	-4	-4	5	-1	8
2500*a*	$*$	0	4	4	-1	-1	1	$*$
2977	2	4	2	-4	$*$	-4	2	-10
3328	$*$	2	-2	-2	6	$*$	2	-6
3721*b*	2	-2	-4	-4	2	2	8	8
4033*a*	-1	4	2	-4	2	2	2	-4
4033*b*	2	-2	-4	2	2	2	-4	2
4057	-3	-2	-4	-1	-4	1	-5	-2
4069	-3	-4	-3	1	$*$	-5	7	1
4225*b*	-2	-2	-4	$*$	-2	-6	$*$	4
4516	$*$	5	4	-1	-6	4	-4	6
4672	$*$	2	-2	-2	-2	6	-6	2
4852	$*$	-3	-1	-7	-2	-4	3	-8
5317	-3	2	-2	6	-2	$*$	2	2
5473	-1	-2	2	2	-4	$*$	2	8

TABLE 3. *Generators for prime ideals of F of small norm.*

$\mathfrak{p}$	Generator	$\mathfrak{p}$	Generator
$\mathfrak{p}_2$	$-t^2+t+1$	$\mathfrak{p}_{13,3}$	$-t^3-t+1$
$\mathfrak{p}_3$	t^2+1	$\mathfrak{p}_{13,4}$	t^3+t^2+1
$\mathfrak{p}_{13,1}$	$-t^3+t^2+1$	$\mathfrak{p}_{5,1}$	$2t^2-t-2$
$\mathfrak{p}_{13,2}$	t^3+t+1	$\mathfrak{p}_{5,2}$	t^3-2t^2-t

TABLE 4. *'Old' cohomology classes.*

Class	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_{13,1}$	$\mathfrak{p}_{13,2}$	$\mathfrak{p}_{13,3}$	$\mathfrak{p}_{13,4}$	$\mathfrak{p}_{5,1}$	$\mathfrak{p}_{5,2}$	Original class
676 (**i–ii**)	$*$	-4	0	$*$	0	$*$	-2	-2	169
1521 (**i–ii**)	-2	$*$	0	$*$	0	$*$	-2	-2	169
1764 (**i–ii**)	$*$	$*$	-6	4	4	-6	-4	-4	441
1936 (**i–ii**)	$*$	-5	-1	-1	-1	-1	-4	-4	484
2197*a* (**i–ii**)	-2	-4	0	$*$	$*$	$*$	-2	-2	169
2197*b* (**i–ii**)	-2	-4	0	$*$	0	$*$	-2	-2	169
2304 (**i–ii**)	$*$	$*$	-2	-2	-2	-2	-6	-6	576
2704 (**ii–iv**)	$*$	-4	0	$*$	0	$*$	-2	-2	169
3969 (**i–ii**)	0	$*$	-6	4	4	-6	-4	-4	441
4225*a* (**i–ii**)	-2	-4	0	$*$	0	$*$	-2	$*$	169
4356 (**i–ii**)	$*$	$*$	-2	6	-2	6	-6	-6	1089 (**i**)
4356 (**iii–iv**)	$*$	$*$	4	-6	4	-6	6	6	1089 (**ii**)
4356 (**v–vi**)	$*$	$*$	-1	-1	-1	-1	-4	-4	484
4624 (**i–ii**)	$*$	0	4	4	-6	-6	6	6	1156
5184 (**i–ii**)	$*$	$*$	-2	-2	-2	-2	-6	-6	576

https://doi.org/10.1112/S1461157016000048 Published online by Cambridge University Press

For each of these classes, we were able to find an elliptic curve defined over the corresponding subfield whose local data matched these eigenvalues (listed in Table 11).

In Table 6 we list the remaining eigenclasses which correspond to the base change of an automorphic representation π' defined over a subfield of F. In each case, the Hecke eigenvalues $a_{\mathfrak{p}}(\pi')$ lie in a quadratic extension of $\mathbb{Q}$, and so there is no elliptic curve defined over the corresponding subfield of F whose local data matches these eigenvalues. However, for each class, we were able to find an elliptic curve defined over F whose local data matched the eigenvalues $a_{\mathfrak{p}}(\pi)$ (listed in Table 12).

In Table 7 we list the remaining two eigenclasses with rational Hecke eigenvalues, which match those of the Eisenstein cohomology, up to sign. We observe that the ray class group $Cl(\mathcal{O}_F, \mathfrak{n})$ of the corresponding level admits a single non-trivial quadratic character χ, and that the Hecke eigenvalues are given by

$$a_{\mathfrak{p}}(\pi) = \chi(\mathfrak{p})(\mathrm{Norm}_{F/\mathbb{Q}}(\mathfrak{p}) + 1).$$

These appear to correspond to classes denoted by H^*_{res} in [**18**, § 3.2.5].

In Tables 8 and 9 we list the remaining eigenclasses, whose eigenvalues lie in a proper extension of $\mathbb{Q}$. For the classes appearing in Table 8, the field $\mathbb{Q}(a_{\mathfrak{p}}(\pi))$ generated by these

TABLE 5. *Base change from rational Hecke eigenclasses.*

Class	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_{13,1}$	$\mathfrak{p}_{13,2}$	$\mathfrak{p}_{13,3}$	$\mathfrak{p}_{13,4}$	$\mathfrak{p}_{5,1}$	$\mathfrak{p}_{5,2}$	Base field
484	$*$	-5	-1	-1	-1	-1	-4	-4	$\mathbb{Q}(\sqrt{3})$
576	$*$	$*$	-2	-2	-2	-2	-6	-6	$\mathbb{Q}(\sqrt{3})$
1089 (**i**)	-3	$*$	-2	6	-2	6	-6	-6	$\mathbb{Q}(\sqrt{3})$
1089 (**ii**)	0	$*$	4	-6	4	-6	6	6	$\mathbb{Q}(\sqrt{3})$
2209	-3	-2	-6	0	-6	0	-6	-6	$\mathbb{Q}(\sqrt{3})$
2704 (**i**)	$*$	-2	2	$*$	2	$*$	2	2	$\mathbb{Q}(\sqrt{3})$
2916 (**i**)	$*$	$*$	5	-4	5	-4	-1	-1	$\mathbb{Q}(\sqrt{3})$
2916 (**ii**)	$*$	$*$	-4	5	-4	5	-1	-1	$\mathbb{Q}(\sqrt{3})$
3844	$*$	-5	-1	-6	-6	-1	1	1	$\mathbb{Q}(\sqrt{-3})$
4225*c*	-4	-2	$*$	$*$	-4	-4	$*$	-10	$\mathbb{Q}(\sqrt{-1})$
5041 (**i**)	0	5	-6	-1	-6	-1	1	1	$\mathbb{Q}(\sqrt{3})$
5041 (**ii**)	-4	5	2	-1	2	-1	-7	-7	$\mathbb{Q}(\sqrt{3})$
5329*d*	-1	-2	2	2	2	2	2	2	$\mathbb{Q}(\sqrt{-3})$
5476 (**i**)	$*$	-5	-4	-7	-4	-7	2	2	$\mathbb{Q}(\sqrt{3})$

TABLE 6. *Base change from non-rational Hecke eigenclasses.*

Class	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_{13,1}$	$\mathfrak{p}_{13,2}$	$\mathfrak{p}_{13,3}$	$\mathfrak{p}_{13,4}$	$\mathfrak{p}_{5,1}$	$\mathfrak{p}_{5,2}$	Base field
169	-2	-4	0	$*$	0	$*$	-2	-2	$\mathbb{Q}(\sqrt{3})$
4096	$*$	2	-2	-2	-2	-2	2	2	$\mathbb{Q}(\sqrt{3})$

TABLE 7. *Remaining rational eigenclasses.*

Class	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_{13,1}$	$\mathfrak{p}_{13,2}$	$\mathfrak{p}_{13,3}$	$\mathfrak{p}_{13,4}$	$\mathfrak{p}_{5,1}$	$\mathfrak{p}_{5,2}$
5329*a* (**i**)	-5	-10	14	-14	-14	-14	26	-26
5329*a* (**ii**)	-5	-10	14	-14	-14	-14	26	-26

https://doi.org/10.1112/S1461157016000048 Published online by Cambridge University Press

eigenvalues is a quadratic extension of $\mathbb{Q}$, and we list the pair of Galois conjugate eigenvalues for each prime. For the classes appearing in Table 9, the field $\mathbb{Q}(a_{\mathfrak{p}}(\pi))$ is either a cubic or a quartic extension of $\mathbb{Q}$, and for each prime we list the polynomial whose roots are the corresponding eigenvalues.

We provide three tables of data regarding elliptic curves (Tables 10–12). In each case, we list the coefficients a_i of a Weierstrass polynomial

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

defining a representative of an isomorphism class of curves. Each curve was found using a combination of the MAGMA routine ELLIPTICCURVESEARCH [**10**] and the ideas found in [**11**].

In Table 10 we present a list of elliptic curves defined over F whose local data match the Hecke eigenvalues of the classes appearing in Table 2, and whose conductors match the levels at which these eigenclasses appear:

In Table 11 we present a list of elliptic curves defined over a subfield of F whose local data (after base change to the field F) match the Hecke eigenvalues of the classes appearing in Table 5. After base change, the conductors of these curves match the levels of the corresponding eigenclasses.

Finally, in Table 12 we present a list of elliptic curves defined over F whose local data match the Hecke eigenvalues of the classes appearing in Table 6. As before, the conductors of these curves match the levels of the corresponding eigenclasses.

Of the 19 elliptic curves listed in Table 10, 12 had trivial residual image, while the remaining 7 had residual image isomorphic to S_3 (as mentioned previously, we found no curves with residual image isomorphic to C_3). We list these images in Table 13.

For each example, we were able to compute the eigenvalues of the Hecke operators $T_{\mathfrak{p}}$ at sufficiently many primes $\mathfrak{p}$ to prove that the curve was indeed modular. A list of these primes, and the corresponding eigenvalues (which necessarily are equal to the traces $\mathrm{Tr}(\widetilde{\rho_E}(\mathrm{Frob}_{\mathfrak{p}}))$), can be found for each curve in the supplementary file (available online from the publisher's website).

TABLE 8. *Eigenclasses with eigenvalues lying in a quadratic extension of* $\mathbb{Q}$.

Class	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_{13,1}$	$\mathfrak{p}_{13,2}$	$\mathfrak{p}_{13,3}$	$\mathfrak{p}_{13,4}$	$\mathbb{Q}(a_{\mathfrak{p}}(\pi))$
625 (**i–ii**)	$\frac{1\pm\sqrt{17}}{2}$	$-1\pm\sqrt{17}$	$-1\pm\sqrt{17}$	$-1\pm\sqrt{17}$	$-1\pm\sqrt{17}$	$-1\pm\sqrt{17}$	$\mathbb{Q}(\sqrt{17})$
1369 (**i–ii**)	$\frac{-3\pm\sqrt{17}}{2}$	$\frac{-5\pm\sqrt{17}}{2}$	$\frac{3\pm\sqrt{17}}{2}$	$1\pm\sqrt{17}$	$\frac{3\pm\sqrt{17}}{2}$	$1\pm\sqrt{17}$	$\mathbb{Q}(\sqrt{17})$
2116 (**i–ii**)	$*$	$-2\pm2\sqrt{3}$	$-1\pm3\sqrt{3}$	$2\pm2\sqrt{3}$	$-1\pm3\sqrt{3}$	$2\pm2\sqrt{3}$	$\mathbb{Q}(\sqrt{3})$
2500*b* (**i–iv**)	$*$	$-1\pm\sqrt{17}$	$-1\pm\sqrt{17}$	$-1\pm\sqrt{17}$	$-1\pm\sqrt{17}$	$-1\pm\sqrt{17}$	$\mathbb{Q}(\sqrt{17})$
3481 (**i–ii**)	$\frac{-5\pm\sqrt{5}}{2}$	$\frac{-5\pm3\sqrt{5}}{2}$	$-1\pm2\sqrt{5}$	$\frac{-7\pm3\sqrt{5}}{2}$	$-1\pm2\sqrt{5}$	$\frac{-7\pm3\sqrt{5}}{2}$	$\mathbb{Q}(\sqrt{5})$
5329*b* (**i–ii**)	$\pm\sqrt{7}$	$\pm2\sqrt{7}$	-4	-4	$1\pm\sqrt{7}$	$1\pm\sqrt{7}$	$\mathbb{Q}(\sqrt{7})$
5476 (**ii–v**)	$*$	$\frac{-5\pm\sqrt{17}}{2}$	$1\pm\sqrt{17}$	$\frac{3\pm\sqrt{17}}{2}$	$1\pm\sqrt{17}$	$\frac{3\pm\sqrt{17}}{2}$	$\mathbb{Q}(\sqrt{17})$

TABLE 9. *Eigenclasses with eigenvalues lying in a cubic or quartic extension of* $\mathbb{Q}$.

Class	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathbb{Q}(a_{\mathfrak{p}}(\pi))$
2401 (**i–iii**)	$x^3+2x^2-11x-20$	$x^3+2x^2-32x-80$	$\mathbb{Q}[x]/(x^3+x^2-8x-10)$
3721*a* (**i–iii**)	x^3+2x^2-9x-6	x^3+5x^2-x-2	$\mathbb{Q}[x]/(x^3-x^2-9x+12)$
4761 (**i–iii**)	x^3+3x^2-4x-4	$*$	$\mathbb{Q}[x]/(x^3-x^2-4x+2)$
5329*c* (**i–iv**)	$x^4+4x^3-3x^2-16x-8$	$x^4+8x^3+6x^2-48x-64$	$\mathbb{Q}[x]/(x^4-9x^2-2x+2)$

https://doi.org/10.1112/S1461157016000048 Published online by Cambridge University Press

TABLE 10. *Elliptic curves corresponding to the classes in Table 2.*

Class	a_1	a_2	a_3	a_4	a_6
441	t^2+t+1	$-t^3-1$	t^2+t	t^3	$-t^2-2t-1$
1156	t^3+t^2+1	t^3+t^2+t-1	t^3	$-5t^3-5t^2+3t-2$	t^3+5t^2-4t+3
2041	t^3+1	t^3-t	t^2	$-2t^2-2t-2$	$-t^3-2t^2-t$
2257	t^2+1	t^3+t^2-t-1	t^3+t+1	$-2t^3-t^2-t-1$	$-t^3-t^2+1$
2452	1	t^3-t^2+t	1	$-t^3+t^2+t-1$	0
2500a	$t+1$	$-t^3+t^2+1$	t^2+t	t^2-t	$2t^2-t-1$
2977	t^3+1	$-t^3$	t	$-t^3+t-1$	t^3-2t^2+t
3328	t^3+t^2+t	$-t^3+t+1$	t^3+1	$21t^3-37t-26$	$51t^3+t^2-113t-94$
3721b	t^3+1	$-t^3-t^2+t$	$t+1$	$-t^3+t^2-2t$	$2t^3-2t^2-t+1$
4033a	t	$-t+1$	t	$-t$	0
4033b	t^2+t+1	t^2	t^3+t^2+1	$-t^2-1$	$-t^2$
4057	t^3+t	$-t^3+t^2+t+1$	t^2+1	$-2t^3+t^2+2t$	$-t^2$
4069	t^3+t^2	t^3-t^2	t	$-t^3+t$	0
4225b	t^3+1	$-t-1$	t^3+t^2	$-t^3+t+1$	0
4516	t^3+t	$-t^2+t+1$	t^2	1	0
4672	t^3+1	1	t^3+t^2+t	$-11t^3+15t^2+10t-10$	$-21t^3+30t^2-5t-22$
4852	1	$-t^3-t^2-t+1$	t^2	$-t-1$	0
5317	t^2+t	-1	t^2+t	$-2t^3-2t^2+1$	0
5473	$t+1$	$-t^3+t^2-t+1$	0	$-16t^3+31t^2-25t$	$21t^3+12t^2-56t+44$

TABLE 11. *Elliptic curves corresponding to the classes in Table 5.*

Class	a_1	a_2	a_3	a_4	a_6
484	$\sqrt{3}$	$\sqrt{3}+1$	$\sqrt{3}$	$2\sqrt{3}+2$	$\sqrt{3}+1$
576	$\sqrt{3}+1$	$-\sqrt{3}+1$	0	$-5\sqrt{3}-6$	$3\sqrt{3}+6$
1089 (**i**)	1	$-\sqrt{3}$	0	1	0
1089 (**ii**)	$\sqrt{3}+1$	$-\sqrt{3}$	1	$5\sqrt{3}-9$	$-6\sqrt{3}+10$
2209	1	$-\sqrt{3}$	1	$-\sqrt{3}-1$	0
2704 (**i**)	0	$\sqrt{3}-1$	0	2	$2\sqrt{3}+3$
2916 (**i**)	1	-1	$\sqrt{3}+1$	$-23\sqrt{3}-41$	$217\sqrt{3}+377$
2916 (**ii**)	1	-1	$\sqrt{3}+1$	$22\sqrt{3}-41$	$-218\sqrt{3}+377$
3844	1	1	$\frac{1}{2}(\sqrt{-3}+3)$	$\frac{1}{2}(9\sqrt{-3}-21)$	$\sqrt{-3}+7$
4225c	$\sqrt{-1}+1$	$-\sqrt{-1}$	$\sqrt{-1}$	1	0
5041 (**i**)	0	-1	$\sqrt{3}$	$-2\sqrt{3}-4$	$3\sqrt{3}+5$
5041 (**ii**)	0	1	$\sqrt{3}$	$\sqrt{3}+2$	$\sqrt{3}+1$
5329d	$3\sqrt{-3}$	$\sqrt{-3}+7$	$\frac{1}{2}(\sqrt{-3}-5)$	$4\sqrt{-3}+1$	$\frac{1}{2}(\sqrt{-3}-3)$
5476 (**i**)	1	$-\sqrt{3}+1$	$\sqrt{3}$	$-\sqrt{3}+1$	$-\sqrt{3}+1$

TABLE 12. *Elliptic curves corresponding to the classes in Table 6.*

Class	a_1	a_2	a_3	a_4	a_6
169	$3t^3-3t^2-3t$	$-t^3+2t^2-3t-2$	$-2t^3+2t^2-t+2$	$-6t^3+t^2+9t-3$	$5t^3-3t^2-t+2$
4096	$2t+2$	$-t^2+t-1$	$2t^3+2$	$-2t^3+2t^2-2t$	0

https://doi.org/10.1112/S1461157016000048 Published online by Cambridge University Press

TABLE 13. *Images of the residual representations attached to the elliptic curves in Table 10.*

Class	$\mathrm{Im}(\widetilde{\rho_E})$	Class	$\mathrm{Im}(\widetilde{\rho_E})$	Class	$\mathrm{Im}(\widetilde{\rho_E})$
441	Id	3328	Id	4225b	Id
1156	Id	3721b	Id	4516	S_3
2041	Id	4033a	Id	4672	Id
2257	S_3	4033b	Id	4582	S_3
2452	S_3	4057	S_3	5317	Id
2500a	S_3	4069	S_3	5473	Id
2977	Id				

Acknowledgements. I would like to thank Tobias Berger for suggesting this topic, and for his continued support and encouragement throughout, and to extend my gratitude to Paul Gunnells and Dan Yasaki for their helpful advice. Finally, I would like to thank the EPSRC, whose funding made this study possible.

References

1. A. Ash, P. E. Gunnells and M. McConnell, 'Resolutions of the Steinberg module for GL(n)', *J. Algebra* 349 (2012) 380–390.

2. A. Ash, P. E. Gunnells and M. McConnell, 'Mod 2 homology of GL(4) and Galois representations', *J. Number Theory* 146 (2015) 4–22.

3. T. Berger and G. Harcos, 'ℓ-adic representations associated to modular forms over imaginary quadratic fields', *Int. Math. Res. Not. IMRN* 23 (2007) Art. ID rnm113.

4. D. Blasius and J. Rogawski, 'Galois representations for Hilbert modular forms', *Bull. Amer. Math. Soc. (N.S.)* 21 (1989) no. 1, 65–69.

5. A. Borel and J. P. Serre, 'Corners and arithmetic groups', *Comment. Math. Helv.* 48 (1973) 436–491; with an appendix, 'Arrondissement des variétés à coins', by A. Douady and L. Hérault.

6. D. Bump, *Automorphic forms and representations*, Cambridge Studies in Advanced Mathematics 55 (Cambridge University Press, Cambridge, 1998).

7. H. Carayol, 'Sur les représentations ℓ-adiques associées aux formes modulaires de Hilbert', *Ann. Sci. Éc. Norm. Supér.* (4) 19 (1986) 409–468.

8. H. Carayol, 'Modular forms and Galois representations with values in a complete local ring', *Contemp. Math.* 165 (1994) 213–237.

9. G. Chênevert, 'Exponential sums, hypersurfaces with many symmetries and Galois representations', PhD Thesis, McGill University, Montreal, 2008.

10. Computational Algebra Group, University of Sydney, 'MAGMA, Version 2.20-9', 2014, http://magma.maths.usyd.edu.au/magma.

11. S. Donnelly, P. E. Gunnells, A. Klages-Mundt and D. Yasaki, 'A table of elliptic curves over the cubic field of discriminant -23', *Exp. Math.* 24 (2015) no. 4, 375–390.

12. L. V. Dieulefait, L. Guerberoff and A. Pacetti, 'Proving modularity for a given elliptic curve over an imaginary quadratic field', *Math. Comp.* 79 (2010) 1145–1170.

13. N. Freitas, B. Le Hung and S. Siksek, 'Elliptic curves over real quadratic fields are modular', *Invent. Math.* 201 (2015) 159–206.

14. P. E. Gunnells, F. Hajir and D. Yasaki, 'Modular forms and elliptic curves over the field of fifth roots of unity', *Exp Math.* 22 (2013) no. 2, 203–216.

15. P. E. Gunnells, 'Computing Hecke eigenvalues below the cohomological dimension', *Exp. Math.* 9 (2000) no. 3, 351–367.

16. P. E. Gunnells, 'Lectures on computing cohomology of arithmetic groups', *Computations with modular forms*, Contributions in Mathematical and Computational Sciences 6 (Springer, Cham, 2014) 3–45.

17. P. E. Gunnells and D. Yasaki, 'Modular forms and elliptic curves over the cubic field of discriminant 23', *Int. J. Number Theory* 9 (2013) no. 1, 53–76.

18. G. Harder, 'Eisenstein cohomology of arithmetic groups. The case GL_2', *Invent. Math.* 89 (1987) 37–118.

19. G. Harder, 'Cohomology of arithmetic groups', 2006, http://www.math.uni-bonn.de/people/harder/Manuscripts/.

20. H. Hida, *Elementary theory of L-functions and Eisenstein series*, London Mathematical Society Student Texts 26 (Cambridge University Press, Cambridge, 1993).

21. M. Harris, K. W. Lan, R. Taylor and J. Thorne, 'On the rigid cohomology of certain Shimura varieties', Preprint, 2013, http://www.math.ias.edu/∼rtaylor/rigcoh.pdf.

https://doi.org/10.1112/S1461157016000048 Published online by Cambridge University Press

22. M. Harris, D. Soudry and R. Taylor, 'ℓ-adic representations associated to modular forms over imaginary quadratic fields. I. Lifting to $\mathrm{GSp}_4(\mathbb{Q})$', *Invent. Math.* 112 (1993) no. 2, 377–411.
23. F. Jarvis and J. Manoharmayum, 'On the modularity of supersingular elliptic curves over certain totally real number fields', *J. Number Theory* 128 (2008) no. 3, 589–618.
24. A. Jones, 'Modular elliptic curves over quartic CM fields', PhD Thesis, University of Sheffield, 2015, http://tberger.staff.shef.ac.uk/Jones_thesis.pdf.
25. M. Koecher, 'Beiträge zu einer Reduktionstheorie in Positivitätsbereichen. I', *Math. Ann.* 141 (1960) 384–432.
26. C. P. Mok, 'Galois representations attached to automorphic forms on GL_2 over CM fields', *Compos. Math.* 150 (2014) no. 4, 523–567.
27. P. Scholze, 'On torsion in the cohomology of locally symmetric varieties', *Ann. of Math. (2)* 182 (2015) no. 3, 945–1066.
28. J. Schwermer, 'The cohomological approach to cuspidal automorphic representations', *Cont. Math.* 488 (2006) 257–285.
29. W. Stein, *Modular forms, a computational approach*, Graduate Studies in Mathematics 79 (American Mathematical Society, Providence, RI, 2007), with an appendix by Paul E. Gunnells.
30. R. Taylor, 'On Galois representations associated to Hilbert modular forms', *Invent. Math.* 98 (1989) 265–280.
31. R. Taylor, 'ℓ-adic representations associated to modular forms over imaginary quadratic fields. II', *Invent. Math.* 116 (1994) 619–643.

Andrew Jones
School of Mathematics and Statistics
University of Sheffield
Hounsfield Road
Sheffield S3 7RH
United Kingdom

andrew.j.jones@cantab.net

https://doi.org/10.1112/S1461157016000048 Published online by Cambridge University Press