A mod five approach to modularity of icosahedral Galois representations

Kevin Buzzard and William A. Stein

July 7, 2000

Abstract

We give eight new examples of icosahedral Galois representations that satisfy Artin's conjecture on holomorphicity of their L-function. We give in detail one example of an icosahedral representation of conductor $\mathbf{1376} = 2^5 \cdot 43$ that satisfies Artin's conjecture. We also briefly explain the computations behind seven additional examples of conductors $\mathbf{2416} = 2^4 \cdot 151$, $\mathbf{3184} = 2^4 \cdot 199$, $\mathbf{3556} = 2^2 \cdot 7 \cdot 127$, $\mathbf{3756} = 2^2 \cdot 3 \cdot 313$, $\mathbf{4108} = 2^2 \cdot 13 \cdot 79$, $\mathbf{4288} = 2^6 \cdot 67$, and $\mathbf{5373} = 3^3 \cdot 199$.

Introduction

Consider a continuous irreducible Galois representation

$$\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_n(\mathbf{C})$$

with $n > 1$. Inspired by his reciprocity law, Artin conjectured in [1] that $L(\rho, s)$ has an analytic continuation to the whole complex plane. Many of the known cases of this conjecture were obtained by proving the apparently stronger assertion that ρ is *automorphic*, in the sense that the L-function of ρ is equal to the L-function of a certain automorphic representation (whose L-function is known to have analytic continuation). In the special case where $n = 2$ and ρ is in addition assumed to be odd, the automorphic representation in question should be the one associated to a classical weight 1 modular eigenform, and in fact there is conjectured to be a bijection between such ρ and the set of all weight 1 cuspidal newforms, which should preserve L-functions. It is this bijection that we are concerned with in this paper, so assume for the rest of the paper that $n = 2$ and ρ is odd.

In this special case, the construction of [7] shows how to construct a continuous irreducible odd 2-dimensional representation from a weight 1 newform, and the problem is to go the other way. Say that a representation is *modular* if it arises in this way.

If the image of ρ is solvable, then ρ is known to be modular [11, 18]; if the image is not solvable, then $\mathrm{Im}(\rho)$ in $\mathrm{PGL}_2(\mathbf{C})$ is isomorphic to the alternating group A_5, and the modularity of ρ is, in general, unknown. We call such a 2-dimensional representation an "icosahedral representation". The published literature contains only eight examples (up to twist) of odd icosahedral Galois representations that are known to satisfy Artin's conjecture: one of conductor $800 = 2^5 \cdot 5^2$ (see [2]), and seven of conductors: 2083, $2^2 \cdot 487$, $2^2 \cdot 751$, $2^2 \cdot 887$, $2^2 \cdot 919$, $2^5 \cdot 73$, and $2^5 \cdot 193$ (see [8]).

After the first draft of this paper was written, the preprint [3] appeared, which contains a general theorem that yields infinitely many (up to twist) modular icosahedral representations. However, we feel that our work, although much less powerful, is still of some worth, because it gives an effective computational approach to proving that certain mod 5 representations are modular, without computing any spaces of weight 1 forms or using effective versions of the Chebotarëv density theorem. We also note that the main theorem of [3] does not apply to any of the examples considered in the present paper. Very recently, the preprint [17] appeared, which gives local conditions under which an icosahedral representation is modular. In particular, [17] also proves that the first three examples in the present paper, of conductors 1376, 2416, 3184, are modular; these correspond to the first, third, and fourth equations at the end of [17]. However, [17] does not apply to our remaining five examples.

In this paper we give eight new examples of modular icosahedral representations that were computed by applying the main theorem of [4] to the mod 5 reduction of ρ. We verify modularity mod 5 on a case-by-case basis. Later we shall explain our approach more carefully, but let us briefly summarise it here. By [4], the problem is to show that the mod 5 reduction of ρ is modular. We do this by finding a candidate mod 5 modular form at weight 5 and then, using the table of icosahedral extensions of $\mathbf{Q}$ in [8] and what we know about the 5-adic representation attached to our candidate form, we deduce that the mod 5 representation attached to our candidate form must be the reduction of ρ. In particular, this paper gives a computational methods for checking the modularity of certain mod 5 representations whose conductors are not too large. We now give more details.

In each of our examples it is easy to compute a few Hecke operators and be morally convinced that a mod 5 representation should be modular; it is far more difficult to prove this. Effective variants of the Chebotarev density theorem require that we check vastly more traces of Frobenius than is practical. Instead we use the Local Langlands theorem for GL_2, the theory of companion forms, and Table 2 of [8], to provide proofs of modularity in certain cases.

More precisely, let K be an icosahedral extension of $\mathbf{Q}$ that is not totally real, and consider a minimal lift $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{C})$ of

$$G_{\mathbf{Q}} \to \mathrm{Gal}(K/\mathbf{Q}) \approx A_5 \subset \mathrm{PGL}_2(\mathbf{C});$$

the lift is minimal in the sense that its conductor is minimal. Assume that 5 does not ramify in K, and that a Frobenius element at 5 in $\mathrm{Gal}(K/\mathbf{Q})$ does not have order 1 or 5. Inspired by the possibility that ρ is modular, we search for a mod 5 modular form of weight 5 whose existence would be forced by modularity of ρ. Indeed, we find a candidate mod 5 form f, and then prove that the fixed field of the kernel of the projective mod 5 representation associated to a certain twist of f must be K. This proves that the mod 5 reduction of a twist of ρ is modular, and the main theorem of [4] then implies that ρ is modular. We carried out this program for icosahedral representations of the following conductors: $\mathbf{1376} = 2^5 \cdot 43$, $\mathbf{2416} = 2^4 \cdot 151$, $\mathbf{3184} = 2^4 \cdot 199$, $\mathbf{3556} = 2^2 \cdot 7 \cdot 127$, $\mathbf{3756} = 2^2 \cdot 3 \cdot 313$, $\mathbf{4108} = 2^2 \cdot 13 \cdot 79$, $\mathbf{4288} = 2^6 \cdot 67$, and $\mathbf{5373} = 3^3 \cdot 199$.

We choose an icosahedral field K and representation ρ, then proceed as follows:

1. Search for a form $f \in S_5(N, \varepsilon; \overline{\mathbf{F}}_5)$ whose associated mod 5 Galois representation looks like it is the mod 5 reduction of ρ.
2. Twist f to obtain an eigenform g with coefficients in $\mathbf{F}_5$.
3. Prove that ρ_g is unramified at 5 by finding a companion form.
4. Prove that the image of $\operatorname{proj}\rho_g$ is A_5 by ruling out all other possibilities.
5. Prove that the fixed field L of $\operatorname{proj}\rho_g$ has root field of discriminant at most 2083^2, so L is in Table 2 of [8]; deduce that $L = K$.
6. Apply the main theorem of [4] to a lift of $\overline{\rho} = \rho_g$ to conclude that ρ is modular.

1 Modularity of an icosahedral representation of conductor $1376 = 2^5 \cdot 43$

In this section we prove the following theorem.

Theorem 1.1. *The icosahedral representations whose corresponding icosahedral extension is the splitting field of $x^5 + 2x^4 + 6x^3 + 8x^2 + 10x + 8$ are modular.*

Let K be the splitting field of $h = x^5 + 2x^4 + 6x^3 + 8x^2 + 10x + 8$. The Galois group of K is A_5, so we obtain a homomorphism $G_{\mathbf{Q}} \to A_5 \subset \mathrm{PGL}_2(\mathbf{C})$; let $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{C})$ be a minimal lift, minimal in the sense that the Artin conductor of ρ is minimal. By Table A_5 of [2], the conductor of ρ is $N = 1376 = 2^5 \cdot 43$. Since $h \equiv (x-1)(x^2-x+1)(x^2-x+2) \pmod 5$, and $\operatorname{disc}(h)$ is coprime to 5, any Frobenius element at 5 in $\mathrm{Gal}(K/\mathbf{Q})$ has order 2.

We use the notation of Tables 3.1 and 3.2 of [2, pg. 46]; from Table 3.2 we see that the type of ρ at 2 is 17 and the type at 43 is 2. The mod N Dirichlet character $\varepsilon = \det(\rho)$ factors as $\varepsilon = \varepsilon_2 \cdot \varepsilon_{43}$ where ε_2 is a character mod 2^5 and ε_{43} is a character mod 43. Corresponding to each type in Buhler's table, there is a character, and fortunately Buhler's level 800 example also was of type 17 at 2 (see the first line of [2, Table 3.2]). By [2, pg. 80] ε_2 is the unique character of conductor 4 and order 2. A local computation shows that the image of ε_{43} has order 3.

If ρ is modular, then there is a weight 1 newform $f_? \in S_1(N, \varepsilon; \overline{\mathbf{Q}})$ that gives rise to ρ. Suppose for the moment that ρ is modular, so that $f_?$ exists. Choose a prime of $\overline{\mathbf{Z}}$ lying over 5, and denote by $\overline{f}_?$ the reduction of $f_?$ modulo this prime. The Eisenstein series $E_4 \in M_4(1;\mathbf{F}_5)$ is congruent to 1 modulo 5, so $E_4 \cdot \overline{f}_? \in S_5(N,\varepsilon;\overline{\mathbf{F}}_5)$ has the same q-expansion as $\overline{f}_?$. Using a computer, we can search for a form $f \in S_5(N,\varepsilon,\overline{\mathbf{F}}_5)$ that has the same q-expansion as the conjectural form $E_4 \cdot \overline{f}_?$.

Instead of multiplying $\overline{f}_?$ by E_4, we could have multiplied it by an Eisenstein series of weight 1, level 5, and character ε'. We used E_4 because the dimension of $S_5(N,\varepsilon;\overline{\mathbf{F}}_5)$ is 696 whereas the dimension of the relevant space $S_2(5\cdot 1376,\varepsilon_{43})$ of weight 2 cusp forms is 1040.

1.1 Searching for the newform f

Using modular symbols (see Section 3.1) we compute (at least up to semi-simplification) the space $S_5(1376,\varepsilon;\mathbf{F}_{25})$. Note that there is injective map from the image of ε into $\mathbf{F}_{25}^*$. By computing the kernels of various Hecke operators on this space, we find f. In the following computations, we represent nonzero elements of $\mathbf{F}_{25}$ as powers of a generator α of $\mathbf{F}_{25}^*$, which satisfies

$$\alpha^2 + 4\alpha + 2 = 0.$$

Our character ε_{43} was represented as the map sending $(1,3) \in (\mathbf{Z}/2^5\mathbf{Z})^* \times (\mathbf{Z}/43\mathbf{Z})^*$ to $2\alpha+1$. Note that 3 is a primitive root mod 43, and that $2\alpha+1$ has order 3.

If the least common multiple of the degrees of the factors of the polynomial h modulo an unramified prime p is 2, then $\mathrm{Frob}_p \in \mathrm{Gal}(K/\mathbf{Q})$ has order 2. The minimal polynomial of $\rho(\mathrm{Frob}_p) \in \mathrm{GL}_2(\mathbf{C})$ is then x^2-1, so $\rho(\mathrm{Frob}_p)$ has trace 0. The first three primes $p \nmid 5\cdot 1376$ such that $\rho(\mathrm{Frob}_p)$ has order 2 are $p = 19, 31, 97$. We computed the mod 5 reduction $\boldsymbol{\mathcal{S}}_5(1376,\varepsilon;\mathbf{F}_{25})^+$ of the $\mathbf{Z}_5[\zeta_3]$-lattice of modular symbols of level 1376 and character $\tilde{\varepsilon}$ where complex conjugation acts as $+1$. Here $\tilde{\varepsilon}$ denotes the Teichmüller lift of ε.

Let V be the intersection of the kernels of T_{19}, T_{31}, and T_{97} inside of the space $\boldsymbol{\mathcal{S}}_5(1376,\varepsilon;\mathbf{F}_{25})^+$ of mod 5 modular symbols. The space V is 8-dimensional, and no doubt all the eigenforms in this space give rise to ρ or one of its twists. One of the eigenvalues of T_3 on this space is α^{16}, and the kernel V_1 of $T_3 - \alpha^{16}$ is 2-dimensional over $\mathbf{F}_{25}$. The Hecke operator T_5 acted as a diagonalisable matrix on V_1, with eigenvalues α^{10} and α^{22}, so the corresponding two systems of eigenvalues must correspond to mod 5 modular eigenforms, and furthermore we must have found all mod 5 modular eigenforms of this level, weight and character, such that $a_{19} = a_{31} = 0$ and $a_3 = \alpha^{16}$.

Remark 1.2. The careful reader might wonder how we know that the systems of mod 5 eigenvalues really do correspond to mod 5 modular forms, and not to perhaps some strange mod 5 torsion in the space of modular symbols. However, we eliminated this possibility by computing the dimension of the full space of mod 5 modular symbols where complex conjugation acts as $+1$, and checking that it equals 696, the dimension of $S_5(1376,\tilde{\varepsilon},\mathbf{C})$, which we computed using the formula in [5].

Table 1: Eigenvalues of f

2	0	59	4	137	0	227	α^{10}	313	0	419	3	509	α^{8}
3	α^{16}	61	α^{14}	139	α^{22}	229	0	317	0	421	α^{20}	521	α^{10}
5	α^{22}	67	α^{4}	149	α^{4}	233	α^{14}	331	α^{14}	431	4	523	α^{14}
7	α^{14}	71	α^{20}	151	1	239	0	337	0	433	α^{4}	541	α^{20}
11	4	73	α^{2}	157	α^{14}	241	α^{2}	347	α^{16}	439	α^{20}	547	α^{22}
13	α^{14}	79	α^{20}	163	0	251	α^{2}	349	α^{4}	443	0	557	3
17	α^{14}	83	α^{4}	167	α^{22}	257	3	353	0	449	0	563	1
19	0	89	α^{10}	173	4	263	α^{16}	359	0	457	0	569	α^{16}
23	α^{16}	97	0	179	α^{2}	269	2	367	α^{22}	461	0	571	α^{22}
29	α^{8}	101	α^{8}	181	α^{14}	271	α^{8}	373	0	463	α^{10}	577	α^{14}
31	0	103	α^{14}	191	α^{10}	277	0	379	3	467	0	587	α^{20}
37	α^{10}	107	0	193	4	281	α^{16}	383	3	479	0	593	0
41	1	109	α^{10}	197	0	283	0	389	1	487	α^{8}	599	α^{22}
43	α^{10}	113	2	199	3	293	3	397	α^{16}	491	α^{2}	601	0
47	1	127	0	211	0	307	α^{4}	401	0	499	α^{20}	607	α^{16}
53	α^{22}	131	2	223	0	311	α^{22}	409	2	503	α^{2}	613	2

Let f be the eigenform in V_1 that satisfies $a_5 = \alpha^{22}$; the q-expansion of f begins

$$f = q + \alpha^{16}q^3 + \alpha^{22}q^5 + \alpha^{14}q^7 + \alpha^{14}q^9 + 4q^{11} + \cdots .$$

Further eigenvalues are given in Table 1. The primes p in the table such that $a_p = 0$ are exactly those predicted by considering the splitting behavior of h. This is strong evidence that ρ is modular, and also that our modular symbols algorithm have been correctly implemented.

1.2 Twisting into $\mathrm{GL}(2, \mathbf{F}_5)$

Although there is a representation $\rho_f : G_{\mathbf{Q}} \to \mathrm{GL}(2, \mathbf{F}_{25})$ attached to f, it is difficult to say anything about its image without further work. We use a trick to show that the image of ρ_f is small. Firstly, for a character $\chi : G_{\mathbf{Q}} \to \overline{\mathbf{F}}_5$, let $\tilde{\chi}$ denote its Teichmüller lift to $\overline{\mathbf{Q}}_5$. By a result of Carayol, there is a characteristic 0 eigenform $\tilde{f} \in S_5(N, \tilde{\varepsilon}; \overline{\mathbf{Q}}_5)$ lifting f. The twist $\tilde{g} = \tilde{f} \otimes \tilde{\varepsilon}_{43}$ is, by [14, Prop. 3.64], an eigenform in $S_5(43N, \tilde{\varepsilon}_2; \overline{\mathbf{Q}}_5)$, and its reduction is a form $g \in S_5(43N, \varepsilon_2, \mathbf{F}_{25})$. The eigenvalues $a_p(g) = a_p(f)\varepsilon_{43}(p)$, for the first few $p \nmid 5N$, are given in Table 2.

Proposition 1.3. *Let $g = f \otimes \varepsilon_{43}$. Then $a_p(g) \in \mathbf{F}_5$ for all $p \nmid \ell N$.*

Proof. Consider an eigenform $\tilde{f} \in S_5(N, \tilde{\varepsilon}; \overline{\mathbf{Q}}_5)$ lifting f as above. Associated to $\tilde{f}$ there is an automorphic representation $\pi = \otimes'_v \pi_v$ of $\mathrm{GL}(2, \mathbf{A})$, where $\mathbf{A}$

Table 2: Eigenvalues of $g = f \otimes \varepsilon_{43}$

2	*	59	4	137	0	227	3	313	0	419	3	509	1	617	0
3	1	61	2	139	2	229	0	317	0	421	4	521	3	619	4
5	*	67	4	149	4	233	2	331	2	431	4	523	2	631	4
7	2	71	4	151	1	239	0	337	0	433	4	541	4	641	4
11	4	73	3	157	2	241	3	347	1	439	4	547	2	643	1
13	2	79	4	163	0	251	3	349	4	443	0	557	3	647	4
17	2	83	4	167	2	257	3	353	0	449	0	563	1	653	1
19	0	89	3	173	4	263	1	359	0	457	0	569	1	659	2
23	1	97	0	179	3	269	2	367	2	461	0	571	2	661	2
29	1	101	1	181	2	271	1	373	0	463	3	577	2	673	1
31	0	103	2	191	3	277	0	379	3	467	0	587	4	677	4
37	3	107	0	193	4	281	1	383	3	479	0	593	0	683	0
41	1	109	3	197	0	283	0	389	1	487	1	599	2	691	1
43	*	113	2	199	3	293	3	397	1	491	3	601	0	701	2
47	1	127	0	211	0	307	4	401	0	499	4	607	1	709	4
53	2	131	2	223	0	311	2	409	2	503	3	613	2	719	4

is the adèle ring of $\mathbf{Q}$. Because $43 \,||\, N$, and 43 divides the conductor of ε, we see that the local component π_{43} of π at 43 must be ramified principal series. By Carayol's theorem, $\rho_{\tilde{f}}|_{D_{43}} \sim \left(\begin{smallmatrix}\Psi_1 & 0\\ 0 & \Psi_2\end{smallmatrix}\right)$ with, without loss of generality, Ψ_2 unramified. We have $(\Psi_1 \cdot \Psi_2)|_{I_{43}} = \tilde{\varepsilon}|_{I_{43}} = \tilde{\varepsilon}_{43}$, therefore, $\rho_{\tilde{f}}|_{I_{43}} \sim \left(\begin{smallmatrix}\tilde{\varepsilon}_{43} & 0\\ 0 & 1\end{smallmatrix}\right)$.

Now twist $\tilde{f}$ by $\tilde{\varepsilon}_{43}^{-1}$; we find that $\rho_{\tilde{f}\otimes\tilde{\varepsilon}_{43}^{-1}}|_{I_{43}} \sim \left(\begin{smallmatrix}1 & 0\\ 0 & \tilde{\varepsilon}_{43}^{-1}\end{smallmatrix}\right)$. In particular, there is an eigenform $\tilde{f}' \in S_5(N, \tilde{\varepsilon}_2\tilde{\varepsilon}_{43}^{-1}, \overline{\mathbf{Q}}_5)$ whose associated Galois representation is the twist by $\tilde{\varepsilon}_{43}^{-1}$ of that of $\tilde{f}$ (recall that $N = 1376$ and so 43 divides N exactly once). Let f' denote the mod 5 reduction of $\tilde{f}'$. Then one checks easily that $f' \in S_5(N, \varepsilon_2\varepsilon_{43}^{-1}, \mathbf{F}_{25}) = S_5(N, \varepsilon^5, \mathbf{F}_{25})$.

For all primes $p \nmid 5N$ we have $a_p(f') = \varepsilon_{43}(p)^{-1}a_p(f)$. In particular, we have $a_p(f') = 0$ for $p = 19, 31$. Also, $\varepsilon_{43}(3) = \alpha^8$ and $\varepsilon_{43}(5) = \alpha^8$, so

$$a_3(f') = \alpha^{16}/\alpha^8 = \alpha^8 = (\alpha^{16})^5$$

$$a_5(f') = \alpha^{22}/\alpha^8 = \alpha^{14} = (\alpha^{22})^5.$$

Now if σ is the non-trivial automorphism of $\mathbf{F}_{25}$, then $\sigma(f')$ and f both lie in $S_5(1376, \varepsilon; \mathbf{F}_{25})$ and have same a_p for $p = 3, 5, 19, 31$, so they are equal because we found f by computing the unique eigenform with given a_p for $p = 3, 5, 19, 31$. So $g = f \otimes \varepsilon_{43} = \sigma(f) \otimes \varepsilon_{43}^2$. Thus for all $p \nmid 5N$, we see that $a_p(g) = a_p(f)^5\varepsilon_{43}^2$ has fifth power $a_p(g)^5 = a_p(f)^{25}\varepsilon_{43}^{10} = a_p(f)\varepsilon_{43} = a_p(g)$. $\square$

1.3 Proof that ρ_g is unramified at 5

We begin with a generalisation of [16]. Let $M > 4$ be an integer, and let $h = \sum_{n\geq 1} c_n q^n$ be a normalised cuspidal eigenform of some weight $k \geq 1$, level M and character χ, defined over some field of characteristic not dividing M. Even though the base field might not have characteristic zero, we may still define the conductor of χ to the the largest divisor f of M such that χ factors through $(\mathbf{Z}/f\mathbf{Z})^\times$. Let I be a set of primes, with the property that for all p in I, one of the following conditions hold:

(i) p divides M but p does not divide $M/\operatorname{cond}(\chi)$, or

(ii) p divides M exactly once, and h is p-new, in the sense that there is no eigenform h' of level M/p such that the T_n-eigenvalues of h and h' agree for all n prime to p.

Let C denote the orbit of the cusp ∞ in $X_1(M)$ under the action of the group generated by w_p for $p \in I$, and the Diamond operators $\langle d\rangle_M$. The orbit of ∞ under the Diamond operators has size $\phi(M)/2$, and each w_p increases the size of the orbit by a factor of 2. In this situation, we have

Lemma 1.4. *The first t terms of the q-expansion of h at any cusp in C are determined by M, k, χ, c_p for p in I, and c_n for $1 \leq n \leq t$.*

Remark 1.5. Our proof is just a translation of Corollary 4.6.18 of [13] into the language of moduli problems (Miyake's argument technically is only valid over the complex numbers).

Proof. If $J \subseteq I$ is any subset, and w_J denotes the product of w_p for $p \in J$, then $h|w_J$ is an eigenform for all the Diamond operators, and this observation reduces the proof of the lemma to showing that for $p \in I$, if $h|w_p = \sum_n d_n q^n$, then d_j for $1 \leq j \leq n$ and d_q for all $q \in I$ are determined by M, k, χ, p, c_j for $1 \leq j \leq n$ and c_q for all $q \in I$.

We first deal with primes p of the form (i). Say $M = p^m R$, where R is prime to p. Thinking of h as a rule for attaching k-fold differentials to elliptic curves equipped with points of order p^m and R, we have by definition that

$$h(\mathbf{G}_m/q^{\mathbf{Z}}, \zeta, \zeta_R) = \left(\sum c_n q^n\right)(dt/t)^k,$$

where $\zeta = \zeta_{p^m}$ and ζ_R are fixed p^mth and Rth roots of unity in $\mathbf{G}_m$ which correspond to the cusp ∞, and dt/t is the canonical differential on the Tate curve $\mathbf{G}_m/q^{\mathbf{Z}}$. We normalise things such that

$$h(\mathbf{G}_m/q^{p^m\mathbf{Z}}, q, \zeta_R) = \left(\sum d_n q^n\right)(dt/t)^k,$$

and remark that because h is an action for the diamond operators, we do not have to worry too much about whether this corresponds to the standard normalisation of the w_p-operator.

We recall that the operator pU_p in this setting can be thought of as being defined by the rule:

$$(pU_ph)(E,P,Q)=\sum_C \pi^*h(E/C,\overline{P},\overline{Q}),$$

where C runs through the subgroups of E of order p which have trivial intersection with $\langle P\rangle$, and π denotes the canonical projection $E\to E/C$. We see that

$$\begin{aligned}(pc_p)^m\big(\sum d_nq^n\big)(dt/t)^k &= (p^mU_{p^m}h)(\mathbf{G}_m/q^{p^m\mathbf{Z}},q,\zeta_R)\\ &=\sum_{c=0}^{p^m-1}\pi^c*h(\mathbf{G}_m/\langle q^{p^m},\zeta q^c\rangle,q,\zeta_R),\end{aligned}$$

where π denotes the canonical projection from $\mathbf{G}_m/\langle q^{p^m}\rangle$ to the appropriate quotient. This last sum can be written as a double sum

$$\begin{aligned}&\sum_{c\in(\mathbf{Z}/p^m\mathbf{Z})^\times}\pi^*h(\mathbf{G}_m/\langle q^{p^m},\zeta q^c\rangle,q,\zeta_R)+\sum_{a=0}^{p^{m-1}-1}\pi^*h(\mathbf{G}_m/\langle q^{p^m},\zeta q^{pa}\rangle,q,\zeta_R)\\ =&\sum_{b\in(\mathbf{Z}/p^m\mathbf{Z})^\times}\pi^*h(\mathbf{G}_m/\langle q^{p^m},\zeta^{-b}q\rangle,q,\zeta_R)+p^{m-1}\pi^*U_{p^{m-1}}h(\mathbf{G}_m/\langle q^{p^m},\zeta^{p^{m-1}}\rangle,q,\zeta_R)\\ =&\sum_{b\in(\mathbf{Z}/p^m\mathbf{Z})^\times}\pi^*h(\mathbf{G}_m/\langle\zeta^{-b}q\rangle,\zeta^b,\zeta_R)+(pc_p)^{m-1}\pi^*h(\mathbf{G}_m/\langle q^{p^m},\zeta^{p^{m-1}}\rangle,q,\zeta_R)\\ =&\sum_b\chi_p(b)\sum_{n\geq1}c_n(\zeta^{-b}q)^n(dt/t)^k+p^k(pc_p)^{m-1}\pi^*h(\mathbf{G}_m/\langle q^{p^{m+1}}\rangle,q^p,\zeta_R^p),\end{aligned}$$

where we have written $\chi=\chi_R\chi_p$, for χ_R a character of level R and χ_p a character of level p^m. We deduce that

$$\begin{aligned}&(pc_p)^m\big(\sum d_nq^n\big)(dt/t)^k-p^k(pc_p)^{m-1}\chi_R(p)\pi^*h(\mathbf{G}_m/\langle q^{p^{m+1}}\rangle,q^p,\zeta_R)\\ =&\Big(\sum_n\big(\sum_b\chi_p(b)\zeta^{-bn}\big)c_nq^n\Big)(dt/t)^k\\ =&W(\chi_p)\big(\sum_{p\nmid n}\chi_p(-n)^{-1}c_nq^n\big)(dt/t)^k\end{aligned}$$

where $W(\chi_p)=\sum_{b\in(\mathbf{Z}/p^m\mathbf{Z})^\times}\chi_p(b)\zeta^b$ can be checked to be nonzero because the conductor of χ_p is p^m. Hence

$$(pc_p)^m\sum_n d_nq^n-p^k(pc_p)^{m-1}\chi_R(p)\sum_n d_nq^{np}=W(\chi_p)\chi_p(-1)\sum_{p\nmid n}\chi_p(n)^{-1}c_nq^n.$$

Equating coefficients of q we deduce that $W(\chi_p)\chi_p(-1)=(pc_p)^md_1$, and because $h|w_p$ is an eigenform for T_n for all n prime to p, with eigenvalues determined by χ and c_n, we deduce that we can determine d_n for n prime to

p from c_n. It remains to establish what d_p is, and equating coefficients of q^p in the above equation gives us that $(pc_p)^m d_p = p^k (pc_p)^{m-1} \chi_R(p) d_1$ and hence that d_p is determined by χ and c_p. Note that as a consequence we see that $d_p/d_1 = p^{k-1}\chi_R(p)/c_p$, a classical formula if the base field is the complexes.

Now we deal with primes of the form (ii) (note that we never use this case in the rest of the paper). We think of h as a rule associating k-fold differentials to triples (E, C, Q) where C a cyclic subgroup of order p and Q a point of order $R = M/p$. Because h is p-new, the trace of h down to $X_1(M/p)$ must be zero, and hence we see that for any elliptic curve E equipped with a point Q of order R,

$$\sum_C \pi^* h(E/C, E[p]/C, \overline{Q}) = 0.$$

As before, normalise things so that

$$h(\mathbf{G}_m/q^{\mathbf{Z}}, \mu_p, \zeta_R) = \left(\sum_n c_n q^n\right)(dt/t)^k$$

and

$$h(\mathbf{G}_m/q^{p\mathbf{Z}}, \langle q \rangle, \zeta_R) = \left(\sum_n d_n q^n\right)(dt/t)^k.$$

The fact that the trace of h is zero implies that

$$(pU_p)h(\mathbf{G}_m/q^{p\mathbf{Z}}, \langle q \rangle, \zeta_R) + \pi^* h(\mathbf{G}_m/q^{\mathbf{Z}}, \mu_p, \zeta_R) = 0,$$

and hence that

$$c_p \sum d_n q^n + p^{k-1} \sum c_n q^n = 0$$

from which we deduce that the d_n can be read off from c_p and the c_n. □

Remark 1.6. The size of C is $\phi(M).2^{|I|-1}$, and the usefulness of this lemma is that if h_1 and h_2 are two normalised eigenforms of the same level, weight and character as above, both new at all primes in I, and the coefficients of q^n in the q-expansions of h_1 and h_2 agree for $n \in I$ and $n \leq t$, then $h_1 - h_2$ has a zero of order at least $t+1$ at all cusps in C, and in particular if $\phi(M).2^{|I|-1}(t+1) > k/12[\mathrm{SL}_2(\mathbf{Z}) : \Gamma_1(M)] = \deg(\omega^k)$ on $X_1(M)$ then $h_1 = h_2$. Using the fact that $[\Gamma_0(M) : \Gamma_1(M)] = \phi(M)/2$, we deduce

Corollary 1.7. *Let h_1 and h_2 be two normalised eigenforms as above. If the coefficients of q^n in the q-expansions of h_1 and h_2 agree for all primes in I and for all $n \leq \frac{k}{12}[\mathrm{SL}_2(\mathbf{Z}) : \Gamma_0(M)]/2^{|I|}$ then $h_1 = h_2$.*

Remark 1.8. One can certainly do better than this corollary in many cases. For example, when $n > 1$ and p^n exactly divides both the level of an eigenform and the conductor of its character, then one can compute the q-expansion of the eigenform at many "middle cusps" too, and hence increase the size of C in the result above.

We now go back to the explicit situation we are concerned with. Although g is an eigenform of level $59168 = 2^5 \cdot 43^2$, we can still consider the corresponding representation $\rho_g : G_{\mathbf{Q}} \to \mathrm{GL}(2, \mathbf{F}_5)$, and then directly analyze its ramification.

Proposition 1.9. *The representation ρ_g is unramified at 5.*

Proof. Continuing the modular symbols computations as above, we find that V_1 is spanned by the two eigenforms

$$\begin{aligned} f\ &= q + \alpha^{16}q^3 + \alpha^{22}q^5 + \alpha^{14}q^7 + \alpha^{14}q^9 + 4q^{11} + \cdots \\ f_1 &= q + \alpha^{16}q^3 + \alpha^{10}q^5 + \alpha^{14}q^7 + \alpha^{14}q^9 + 4q^{11} + \cdots . \end{aligned}$$

For $p \neq 5$ and $p \leq 997$, we have $a_p(f_1) = a_p(f)$. To check that $a_p(f) = a_p(f_1)$ for all $p \neq 5$, it suffices to show that the difference $f - f_1$ has q-expansion involving only powers of q^5; for this we use the θ-operator $q\frac{d}{dq}$: $S_5(1376, \varepsilon, \mathbf{F}_{25}) \to S_{11}(1376, \varepsilon; \mathbf{F}_{25})$. Since θ sends normalized eigenforms to normalized eigenforms, it suffices to check that the subspace of $S_{11}(1376, \varepsilon; \mathbf{F}_{25})$ generated by $\theta(f)$ and $\theta(f_1)$ has dimension 1. Corollary 1.7 implies that it suffices to verify that the coefficients $a_p(\theta(f))$ and $a_p(\theta(f_1))$ are equal for all

$$p \leq \frac{11}{12} \cdot [\mathrm{SL}_2(\mathbf{Z}) : \Gamma_0(1376)] \cdot \frac{1}{2} = 968.$$

The eigenform f must be new because we computed it by finding the intersections of the kernels of Hecke operators T_p with $p \nmid 1376$; if f were an oldform then the intersection of the kernels of these Hecke operators would necessarily have dimension greater than 1. Because it takes less than a second to compute each $a_p(\theta(f))$, we were easily able to verify that the space generated by $\theta(f)$ and $\theta(f_1)$ has dimension 1.

Remark 1.10. It is possible to avoid appealing to Corollary 1.7 by using one of the following two alternative methods:

1. Define θ directly on modular symbols and compute it.

2. Compute the intersection

$$\bigcap_{p \geq 2} \ker(T_p - p a_p(f)) \subset S_{11}(1376, \varepsilon; \mathbf{F}_{25}).$$

   Since $\theta(f)$ and $\theta(f_1)$ both lie in the intersection, the moment the dimension of a partial intersection is 1, it follows that $\theta(f - f_1) = 0$.

We successfully carried out both alternatives. For the first, we showed that θ on modular symbols is induced by multiplication by $X^5Y - Y^5X$. For the second, we find that after intersecting kernels for $p \leq 11$, the dimension is already 1. The first of these two methods took much less time than the second.

Next we use that $\theta(f - f_1) = 0$ to show that ρ_g is unramified, thus finishing the proof of the proposition. Since f is ordinary, Deligne's theorem (see [9, §12]) implies that

$$\rho_f|_{D_5} \sim \begin{pmatrix} \alpha & * \\ 0 & \beta \end{pmatrix} \qquad \text{over } \overline{\mathbf{F}}_5$$

with both α, β unramified, $\alpha(\mathrm{Frob}_5) = \varepsilon(5)/a_5 = \alpha^8/\alpha^{22} = \alpha^{10}$, and $\beta(\mathrm{Frob}_5) = \alpha^{22}$. Since $a_p(f_1) = a_p(f)$, for $p \neq 5$, we have

$$\rho_f|_{D_5} \sim \rho_{f_1}|_{D_5} \sim \begin{pmatrix} \alpha' & * \\ 0 & \beta' \end{pmatrix}$$

with $\alpha'(\mathrm{Frob}_5) = \alpha^8/\alpha^{10} = \alpha^{22}$ and $\beta'(\mathrm{Frob}_5) = \alpha^{10}$; in particular, $\alpha' = \beta$. Thus $\rho_f|_{D_5}$ contains $\alpha \oplus \beta$, so $\rho_f|_{D_5} \sim \alpha \oplus \beta$ and hence there is a choice of basis so that $* = 0$.

□

1.4 The image of $\mathrm{proj}\,\rho_g$

Proposition 1.11. *The image of* $\mathrm{proj}\,\rho_g$ *is* A_5.

Proof. The image H of $\mathrm{proj}\,\rho_g$ in $\mathrm{PGL}_2(\mathbf{F}_5)$ is easily checked to lie in $\mathrm{PSL}_2(\mathbf{F}_5) \cong A_5$ because of what we know about the determinant of ρ_g. Hence H is a subgroup of A_5 that contains an element of order 2 (complex conjugation) and an element of order 3 (for example, $\rho_g(\mathrm{Frob}_7)$ has characteristic polynomial $x^2 - 2x - 1$). This proves that H is isomorphic to either S_3, A_4, or A_5. Let L be the number field cut out by H. If L were an S_3-extension, then there would be a quadratic extension contained in it which is unramified outside $2 \cdot 5 \cdot 43$; it is furthermore unramified at 5 by the previous section and unramified at 43 because I_{43} has order 3. Thus it is one of the three quadratic fields unramified outside 2. In particular, the trace of Frob_p would be zero for all primes in a certain congruence class modulo 8. However, there are primes p congruent to 3, 5, and 7 mod 8 such that $a_p(g) \neq 0$, e.g., 3, 7, and 13.

If H were isomorphic to A_4, then let M denote the cyclic extension of degree 3 over $\mathbf{Q}$ contained in L. Now M is unramified at 2 and 5, and hence is the subfield of $\mathbf{Q}(\zeta_{43})$ of degree 3. Choose $p \nmid 1376 \cdot 5$ that is inert in M, i.e., so that p is not a cube mod 43. The order of $\rho_g(\mathrm{Frob}_p)$ in $\mathrm{GL}_2(\mathbf{F}_5)$ must be divisible by 3. However, a quick check using Table 2 shows that this is usually not the case, even for $p = 3$. □

1.5 Bounding the ramification at 2 and 43

Let L be the fixed field of $\ker(\mathrm{proj}(\rho_g))$. We have just shown that $\mathrm{Gal}(L/\mathbf{Q})$ is isomorphic to A_5. By a root field for L, we mean a non-Galois extension of $\mathbf{Q}$ of degree 5 whose Galois closure is L.

Proposition 1.12. *The discriminant of a root field for L divides* $(43 \cdot 8)^2 = 344^2$*, and in particular, L must be mentioned in Table 1 of [8, pg 122].*

Proof. The analysis of the local behavior of ρ_f at 43 given in Proposition 1.3 shows that the inertia group at 43 in $\mathrm{Gal}(L/\mathbf{Q})$ has order 3. Using Table 3.1 of [2], we see that if $\mathrm{Gal}(L/\mathbf{Q}) \cong A_5$ then it must be "type 2" at 43, and hence the discriminant of a root field of L, that is, of a non-Galois extension of $\mathbf{Q}$ of degree 5 whose Galois closure is L, must be 43^2 at 43.

At 2 the behavior of ρ is more subtle and we shall not analyze it fully. But we can say that, because ρ has arisen from a form of level $1376 = 2^5.43$, we must be either of type 5 or one of types 14–17. In particular, the discriminant at 2 of a root field for L will be at most 2^6.

Finally, L is unramified at all other primes, because ρ is. Hence the discriminant of a root field for L, assuming that $\mathrm{Gal}(L/\mathbf{Q}) \cong A_5$, divides $(43.8)^2 = 344^2$. □

We know that L is an icosahedral extension of $\mathbf{Q}$ with discriminant dividing $43^2 \cdot 2^6$. Table 1 of [8, pg 122] contains all icosahedral extensions, such that the discriminant of a root field is bounded by 2083^2. The table must contain L; there is only one icosahedral extension with discriminant dividing $43^2 \cdot 2^6$, so $L = K$.

1.6 Obtaining a classical weight one form

We have shown that a twist of the icosahedral representation $\rho : G_{\mathbf{Q}} \to \mathrm{GL}(2,\mathbf{C})$, nobtained by lifting $G_{\mathbf{Q}} \to \mathrm{Gal}(K/\mathbf{Q}) \approx A_5$, has a mod 5 reduction $\rho_g : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F}_5)$ that is modular. Since ρ ramifies at only finitely many primes, and ρ is unramified at 5 with distinct eigenvalues, [4] implies that ρ arises from a classical weight 1 newform.

2 More examples

The data necessary to deduce modularity of each of our eight icosahedral examples is summarized in Tables 3–6.

The notation in Table 3 is as follows. The first column contains the conductor. The second column contains a 5-tuple $[a_4, a_3, a_2, a_1, a_0]$ such that the A_5-extension is the splitting field of the polynomial $h = x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$. The column labeled $\mathrm{ord}(\mathrm{Frob}_5)$ contains the order of the image of Frob_5 in A_5. The next column, which is labeled "p with $a_p = 0$", contains the first few p such that a_p is easily seen to equal 0 by considering the splitting of h mod p. The ε column contains the character of the representation, where the notation is as follows. Write $(\mathbf{Z}/N\mathbf{Z})^*$ as a product of cyclic groups corresponding to the prime divisors of N in ascending order, and then the tuples give the orders of the images of these cyclic factors; when $8 \mid N$, there are two cyclic factors corresponding to the prime 2. Finally, the last column records the dimension of $S_5(\Gamma_1(N), \varepsilon)$.

The notation in Table 4 is as follows. The first column contains the conductor. The second column contains an eigenform that was found by first intersecting the kernels of the Hecke operators T_p with p as in Table 3, and then locating an eigenform. In each case, a companion form was found, by computing $a_p(f)$ for $p \leq$ bound, where bound is the bound from Corollary 1.7.

Table 5 shows that the fixed field of the image of each $\mathrm{proj}(\rho_g)$ is icosahedral. The first column contains the conductor N. The second column contains a twist g of f such that $a_p(g) \in \mathbf{F}_5$ for all $p \nmid 5N$. The third column contains a Frob_p such that $\mathrm{proj}(\rho_g(\mathrm{Frob}_p))$ has order 3, along with the characteristic polynomial of $\rho_g(\mathrm{Frob}_p)$. As in the proof of Proposition 1.11, the other two boxes give data that allows us to deduce that the fixed field of the image of $\mathrm{proj}(\rho_g)$ is icosahedral. The case 5373 must be treated separately, because there are three possibilities M_1, M_2, and M_3 for the cubic field M of the analogue of Proposition 1.11. For M_1 we find a prime p such that

$$(p^2 \mod 9,\ \ p^{66} \mod 199) \not\in \{(1,1),(4,1),(7,1)\}$$

with $\rho_g(\mathrm{Frob}_p)$ of order not divisible by 3; for this, $p = 2$ suffices, since the characteristic polynomial of $\rho_g(\mathrm{Frob}_2)$ is $(x+2)^2$ and $(p^2 \bmod 9,\ p^{66} \bmod 199) = (4,106)$. For M_2 we find a prime p such that

$$(p^2 \mod 9,\ \ p^{66} \mod 199) \not\in \{(1,1),(4,92),(7,106)\}$$

with $\rho_g(\mathrm{Frob}_p)$ of order not divisible by 3; again, $p = 2$ suffices. For M_3 we find a prime p such that

$$(p^2 \mod 9,\ \ p^{66} \mod 199) \not\in \{(1,1),(4,106),(7,92)\}$$

with $\rho_g(\mathrm{Frob}_p)$ of order not divisible by 3; here, $p = 13$ suffices, as the characteristic polynomial of $\rho_g(\mathrm{Frob}_p)$ is $(x+4)^2$ and $(p^2 \bmod 9,\ p^{66} \bmod 199) = (7,106)$.

Table 6 gives upper bounds on the ramification of the fixed field of the image of $\mathrm{proj}(\rho_g)$. These bounds were deduced using Table 3.1 of [2] by restricting the possible "types" using information about the character ε. Note that though the bounds are not sharp, e.g., the discriminant of the representation of conductor 2416 is $2^4 \cdot 151^2$, they are all less than 2083^2, so the corresponding field must appear in Table 2 of [8].

3 Computing mod p modular forms

3.1 Higher weight modular symbols

The second author developed software that computes the space of weight k modular symbols $\boldsymbol{\mathcal{S}}_k(N,\varepsilon)$, for $k \geq 2$ and arbitrary ε. See [12] for the standard facts about higher weight modular symbols, and [15] for a description of how to compute with them.

Let $K = \mathbf{Q}(\varepsilon)$ be the field generated by the values of ε. The cuspidal modular symbols $\boldsymbol{\mathcal{S}}_k(N,\varepsilon)$ are a finite dimensional vector space over K, which is generated by all linear combinations of higher weight modular symbols

$$X^iY^{k-2-i}\{\alpha,\beta\}$$

Table 3: Data on icosahedral representations mod 5

N	h	ord(Frob$_5$)	p with $a_p = 0$	ε	$\dim S_5(N,\varepsilon)$
1376	$[2, 6, 8, 10, 8]$	2	$19, 31, 97$	$[2, 1, 3]$	696
2416	$[0, -2, 2, 5, 6]$	2	$53, 97, 127$	$[2, 1, 3]$	1210
3184	$[5, 8, -20, -21, -5]$	2	$31, 89, 97$	$[2, 1, 3]$	1594
3556	$[3, 9, -6, -4, -40]$	3	$19, 29, 89$	$[1, 2, 3]$	2042
3756	$[0, -3, 10, 30, -18]$	3	$17, 61, 67$	$[1, 2, 3]$	2506
4108	$[4, 3, 9, 4, 5]$	3	$17, 23, 31, 89$	$[1, 3, 2]$	2234
4288	$[4, 5, 8, 3, 2]$	3	$19, 23, 47$	$[1, 2, 3]$	2164
5373	$[2, 1, 7, 23, -11]$	2	$7, 23, 37, 79, 89$	$[2, 3]$	2394

Table 4: The newform f and the companion form bound

N	f	bound
1376	$q + \alpha^{16}q^3 + \alpha^{22}q^5 + \alpha^{14}q^7 + \alpha^{14}q^9 + 4q^{11} + \alpha^{14}q^{13} + \cdots$	968
2416	$q + 3q^3 + \alpha^{22}q^5 + \alpha^{16}q^7 + \alpha^4q^{11} + \alpha^2q^{13} + \alpha^{16}q^{15} + \cdots$	1672
3184	$q + \alpha^{16}q^3 + 3q^5 + \alpha^{22}q^7 + \alpha^{14}q^9 + 3q^{11} + \alpha^{22}q^{13} + \cdots$	2200
3556	$q + \alpha^{16}q^3 + \alpha^{14}q^5 + \alpha^{10}q^7 + \alpha^{14}q^9 + \alpha^2q^{11} + \alpha^{22}q^{13} + \cdots$	1408
3756	$q + \alpha^{14}q^3 + \alpha^{14}q^5 + 3q^7 + \alpha^4q^9 + \alpha^{16}q^{11} + \alpha^{10}q^{13} + \cdots$	1727
4108	$q + \alpha^{16}q^3 + \alpha^{11}q^5 + \alpha^{20}q^7 + \alpha^{14}q^9 + \alpha^{10}q^{11} + 4q^{13} + \cdots$	1540
4288	$q + 3q^3 + \alpha^{14}q^5 + \alpha^{20}q^7 + 3q^9 + \alpha^{20}q^{11} + \alpha^{16}q^{13} + \cdots$	2992
5373	$q + \alpha^{16}q^2 + \alpha^{14}q^4 + 4q^5 + 3q^8 + \alpha^4q^{10} + 2q^{11} + \cdots$	3300

Table 5: Verification that the image of $\mathrm{proj}(\rho_g)$ is A_5

Find a Frobenius element with projective order 3.

N	g	proj. order 3	charpoly
1376	$f \otimes \varepsilon_{43}$	Frob_7	$x^2 - 2x - 1$
2416	$f \otimes \varepsilon_{151}$	Frob_{19}	$x^2 + 2x - 1$
3184	$f \otimes \varepsilon_{199}$	Frob_7	$x^2 + 3x + 4$
3556	$f \otimes \varepsilon_{127}$	Frob_{13}	$x^2 + 3x + 4$
3756	$f \otimes \varepsilon_{313}$	Frob_{23}	$x^2 + 2x + 4$
4108	$f \otimes \varepsilon_{13}$	Frob_{29}	$x^2 + 3x + 4$
4288	$f \otimes \varepsilon_{67}$	Frob_{11}	$x^2 + x + 1$
5373	$f \otimes \varepsilon_{199}$	Frob_{11}	$x^2 + 3x + 4$

Not S_3: For all $t \in T$, find unramified p s.t. $t \not\equiv \square \mod p$ and $a_p(g) \neq 0$.

N	T	p
1376	$\{-1, -2\}$	3, 7
2416	$\{-1, -2\}$	3, 7
3184	$\{-1, -2\}$	3, 7
3556	$\{-1, -2, -7, -14\}$	3, 13, 3, 11
3756	$\{-1, -2, -3, -6\}$	7, 7, 11, 13
4108	$\{-1, -2, -79, -158\}$	3, 7, 3, 7
4288	$\{-1, -2\}$	3, 7
5373	$\{-3\}$	11

Not A_4: Unramified p, not cube mod ℓ, order of $\rho_g(\mathrm{Frob}_p)$ not divisible by 3.

N	ℓ	p	$\mathrm{charpoly}(\rho_g(\mathrm{Frob}_p))$
1376	43	3	$(x+2)^2$
2416	151	7	$(x+2)^2$
3184	199	3	$(x+2)^2$
3556	127	3	$(x+2)^2$
3756	313	11	$(x+2)^2$
4108	13	3	$(x+2)^2$
4288	67	7	$(x+3)^2$
5373	—	(see text)	

Table 6: Bounding the discrimant of the fixed field of $\mathrm{proj}(\rho_g)$

N	Bound on discriminant
1376	$2^6 \cdot 43^2$
2416	$2^6 \cdot 151^2$
3184	$2^6 \cdot 199^2$
3556	$2^2 \cdot 7^2 \cdot 127^2$
3756	$2^2 \cdot 3^2 \cdot 313^2$
4108	$2^2 \cdot 13^2 \cdot 79^2$
4288	$2^6 \cdot 67^2$
5373	$3^4 \cdot 199^2$

that lie in the kernel of an appropriate boundary map. There is an involution $*$ that acts on $\boldsymbol{\mathcal{S}}_k(N,\varepsilon)$, and $\boldsymbol{\mathcal{S}}_k(N,\varepsilon)^+ \otimes_K \mathbf{C}$ is isomorphic, as a module over the Hecke algebra, to the space $S_k(N,\varepsilon;\mathbf{C})$ of cusp forms.

Fix $k=5$. In each case considered in this paper, there is a prime ideal λ of the ring of integers $\mathcal{O}$ of K such that $\mathcal{O}/\lambda \cong \mathbf{F}_{25}$. Let $\mathcal{L}$ be the $\mathcal{O}$-module generated by all modular symbols of the form $X^iY^{3-i}\{\alpha,\beta\}$, and let

$$\boldsymbol{\mathcal{S}}_5(N,\varepsilon;\mathbf{F}_{25}) = (\mathcal{L}\otimes_{\mathcal{O}}\mathbf{F}_{25}) \cap \boldsymbol{\mathcal{S}}_5(N,\varepsilon).$$

This is the space that we computed. The Hecke algebra acts on $\boldsymbol{\mathcal{S}}_5(N,\varepsilon;\mathbf{F}_{25})$, so when we find an eigenform we find a maximal ideal of the Hecke algebra.

As an extra check on our computation of $\boldsymbol{\mathcal{S}}_5(N,\varepsilon;\mathbf{F}_{25})$, we computed the dimension of $S_5(N,\varepsilon;\mathbf{C})$ using both the formula of [5] and the Hijikata trace formula (see [10]) applied to the identity Hecke operator.

3.2 Complexity

We implemented the modular symbols algorithms mentioned above in MAGMA (see [6]) because of its robust support for linear algebra over small finite fields.

The following table gives a flavor of the complexity of the machine computations appearing in this paper. The table indicates how much CPU time on a Sun Ultra E450 was required to compute all data for the given level, including the matrices T_p on the 2-dimensional spaces, for $p<2000$. For example, the total time for level $N=1376$ was 6 minutes and 58 seconds.

N	time (minutes)
1376	6:58
2416	10:42
3184	14:16
3556	19:55
3756	27:47
4108	23:11
4288	15:18
5376	24:49

3.3 Acknowledgment

Some of the computing equipment was purchased by the second author using a UC Berkeley Vice Chancellor Research Grant. Additional computer runs were made on the Sun Ultra E450 of the Computational Algebra Group at the University of Sydney. Allan Steel was very helpful in optimizing our code.

References

[1] E. Artin, *Über eine neue Art von L-reihen*, Abh. Math. Sem. in Univ. Hamburg **3** (1923/1924), no. 1, 89–108.

[2] J.P. Buhler, *Icosahedral Galois representations*, Springer-Verlag, Berlin, 1978, Lecture Notes in Mathematics, Vol. 654.

[3] K. Buzzard, M. Dickinson, N. Shepherd-Barron, and R. Taylor, *On icosahedral Artin representations*, in preparation.

[4] K. Buzzard and R. Taylor, *Companion forms and weight one forms*, Ann. of Math. (2) **149** (1999), no. 3, 905–919.

[5] H. Cohen and J. Oesterlé, *Dimensions des espaces de formes modulaires*, (1977), 69–78. Lecture Notes in Math., Vol. 627.

[6] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system I: The user language*, J. Symb. Comp. **24** (1997), no. 3-4, 235–265, http://www.maths.usyd.edu.au:8000/u/magma/.

[7] P. Deligne and J-P. Serre, *Formes modulaires de poids* 1, Ann. Sci. École Norm. Sup. (4) **7** (1974), 507–530 (1975).

[8] G. Frey (ed.), *On Artin's conjecture for odd* 2*-dimensional representations*, Springer-Verlag, Berlin, 1994.

[9] B.H. Gross, *A tameness criterion for Galois representations associated to modular forms (mod p)*, Duke Math. J. **61** (1990), no. 2, 445–517.

[10] H. Hijikata, *Explicit formula of the traces of Hecke operators for* $\Gamma_0(N)$, J. Math. Soc. Japan **26** (1974), no. 1, 56–82.

[11] R. P. Langlands, *Base change for* GL(2), Princeton University Press, Princeton, N.J., 1980.

[12] L. Merel, *Universal Fourier expansions of modular forms*, On Artin's conjecture for odd 2-dimensional representations (Berlin), Springer, 1994, pp. 59–94. Lecture Notes in Math., Vol. 1585.

[13] T. Miyake, *Modular forms*, Springer-Verlag, Berlin, 1989, Translated from the Japanese by Yoshitaka Maeda.

[14] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, Princeton, NJ, 1994, Reprint of the 1971 original, Kan Memorial Lectures, 1.

[15] W. A. Stein, *Explicit approaches to modular abelian varieties*, U. C. Berkeley Ph.D. thesis (2000).

[16] J. Sturm, *On the congruence of modular forms*, Number theory (New York, 1984–1985), Springer, Berlin, 1987, pp. 275–280. Lecture Notes in Math., Vol. 1240.

[17] R. Taylor, *On icosahedral Artin representations II*, in preparation.

[18] J. Tunnell, *Artin's conjecture for representations of octahedral type*, Bull. Amer. Math. Soc. (N.S.) **5** (1981), no. 2, 173–175.