2-1-2008

On Atkin and Swinnerton-Dyer congruence relations (2)

A. O.L. Atkin
University of Illinois at Chicago

Wen Ching Winnie Li
Pennsylvania State University

Ling Long
Iowa State University

ON ATKIN-SWINNERTON-DYER CONGRUENCE RELATIONS

WEN-CHING WINNIE LI, LING LONG, AND ZIFENG YANG

Abstract. In this paper we exhibit a noncongruence subgroup Γ whose space of weight 3 cusp forms $S_3(\Gamma)$ admits a basis satisfying the Atkin-Swinnerton-Dyer congruence relations with two weight 3 newforms for certain congruence subgroups. This gives a modularity interpretation of the motive attached to $S_3(\Gamma)$ by A. Scholl and also verifies the Atkin-Swinnerton-Dyer congruence conjecture for this space.

1. Introduction

The theory of modular forms for congruence subgroups is well developed. Given a cuspidal normalized newform $g = \sum_{n\geq 1} a_n(g)q^n$, where $q = e^{2\pi i\tau}$, of weight $k \geq 2$ level N and character χ, the Fourier coefficients of g satisfy the recursive relation

$$a_{np}(g) - a_p(g)a_n(g) + \chi(p)p^{k-1}a_{n/p}(g) = 0 \tag{1}$$

for all primes p not dividing N and for all $n \geq 1$. Thanks to the work of Eichler [5], Shimura [20], and Deligne [4], there exists a compatible family of λ-adic representations $\rho_{\lambda,g}$ of the Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, unramified outside lN, where λ divides l, such that

$$\begin{aligned}\mathrm{Tr}(\rho_{\lambda,g}(\mathrm{Frob}_p)) &= a_p(g),\\ \det(\rho_{\lambda,g}(\mathrm{Frob}_p)) &= \chi(p)p^{k-1},\end{aligned}$$

for all primes p not dividing lN. Combining both, we see that the characteristic polynomial $H_p(T) = T^2 - A_1(p)T + A_2(p)$ of $\rho_{\lambda,g}(\mathrm{Frob}_p)$ is independent of the λ's not dividing p, and the Fourier coefficients of g satisfy the relation

$$a_{np}(g) - A_1(p)a_n(g) + A_2(p)a_{n/p}(g) = 0 \tag{2}$$

for all $n \geq 1$ and all primes p not dividing N.

The knowledge on modular forms for noncongruence subgroups, however, is far from satisfactory. For example, the paper [16] by Scholl and Serre's letter to Thompson in [24] indicate that the obvious definitions of Hecke operators for non-congruence subgroups would not work well. On the positive side, Atkin and Swinnerton-Dyer [1] initiated the study of

1991 *Mathematics Subject Classification.* 11F33,14J27.

The research of the first author was supported in part by a NSF grant DMS 99-70651 and a NSA grant MDA904-03-1-0069. The second author was supported in part by a NSF grant No. DMS 97-29992 and a Liftoff grant from the Clay Mathematical Institute.

the arithmetic properties of modular forms for noncongruence subgroups, and they have observed very interesting congruence relations for such forms, which we now explain.

Let Γ be a non-congruence subgroup of $SL_2(\mathbb{Z})$ with finite index. For an integer $k \geq 2$, denote by $S_k(\Gamma)$ the space of cusp forms of weight k for Γ and by d its dimension. The modular curve X_Γ, the compactification by adding cusps of the quotient of the Poincaré upper half plane by Γ, has a model defined over a number field K in the sense of Scholl [12] §5.

As explained in [1], [12], [13], there exists a subfield L of K, an element $\kappa \in K$ with $\kappa^\mu \in L$ with μ being the width of the cusp ∞, and a positive integer M such that κ^μ is integral outside M and $S_k(\Gamma)$ has a basis consisting of M-integral forms. Here a form f of Γ is called M-integral if in its Fourier expansion at the cusp ∞

$$f(\tau) = \sum_{n \geq 1} a_n(f) q^{n/\mu}, \tag{3}$$

the Fourier coefficients $a_n(f)$ can be written as $\kappa^n c_n(f)$ with $c_n(f)$ lying in the ring $\mathcal{O}_L[1/M]$, where $\mathcal{O}_L$ denotes the ring of integers of L.

Based on their numerical data, Atkin and Swinnerton-Dyer [1] made an amazing discovery of congruence relations for certain cusp forms for noncongruence subgroups. It is tempting to extrapolate from their observations and from our own numerical data to formulate the following congruence conjecture.

Conjecture 1.1 (Atkin-Swinnerton-Dyer congruences)**.** Suppose that the modular curve X_Γ has a model over $\mathbb{Q}$ in the sense of [12] §5. There exist a positive integer M and a basis of $S_k(\Gamma)$ consisting of M-integral forms f_j, $1 \leq j \leq d$, such that for each prime p not dividing M, there exist a nonsingular $d \times d$ matrix $\{\lambda_{i,j}\}_{i,j=1,\ldots,d}$ whose entries are in a finite extension of $\mathbb{Q}_p$, algebraic integers $A_p(j)$, $1 \leq j \leq d$, with $|\sigma(A_p(j))| \leq 2p^{(k-1)/2}$ for all embeddings σ, and characters χ_j unramified outside M so that for each j the Fourier coefficients of $h_j := \sum_i \lambda_{i,j} f_i$ satisfy the congruence relation

$$\operatorname{ord}_p(a_{np}(h_j) - A_p(j)a_n(h_j) + \chi_j(p)p^{k-1}a_{n/p}(h_j)) \geq (k-1)(1 + \operatorname{ord}_p n) \tag{4}$$

for all $n \geq 1$; or equivalently, for all $n \geq 1$,

$$(a_{np}(h_j) - A_p(j)a_n(h_j) + \chi_j(p)p^{k-1}a_{n/p}(h_j))/(np)^{k-1}$$

is integral at all places dividing p.

In other words, the recursive relation (1) on Fourier coefficients of modular forms for congruence subgroups is replaced by the congruence relation (4) for forms of noncongruence subgroups. The meaning of $A_p(j)$'s is mysterious; the examples in [1] suggest that they satisfy the Sato-Tate conjecture.

In [12] Scholl proved a "collective version" of this conjecture.

Theorem 1.1 (Scholl). *Suppose that X_Γ has a model over $\mathbb{Q}$ as before. Attached to $S_k(\Gamma)$ is a compatible family of $2d$-dimensional l-adic representations ρ_l of the Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ unramified outside lM such that for primes $p > k+1$ not dividing Ml, the following hold.*

(i) The characteristic polynomial

$$H_p(T) = \sum_{0 \le r \le 2d} B_r(p) T^{2d-r} \tag{5}$$

of $\rho_l(\mathrm{Frob}_p)$ lies in $\mathbb{Z}[T]$ and is independent of l, and its roots are algebraic integers with absolute value $p^{(k-1)/2}$;

(ii) For any M-integral form f in $S_k(\Gamma)$, its Fourier coefficients $a_n(f)$, $n \ge 1$, satisfy the congruence relation

$$\begin{aligned} &\mathrm{ord}_p(a_{np^d}(f) + B_1(p) a_{np^{d-1}}(f) + \cdots + B_{2d-1}(p) a_{n/p^{d-1}}(f) + B_{2d}(p) a_{n/p^d}(f)) \\ &\ge (k-1)(1 + \mathrm{ord}_p n) \end{aligned} \tag{6}$$

for $n \ge 1$.

Scholl's theorem establishes the Atkin-Swinnerton-Dyer congruences if $S_k(\Gamma)$ has dimension 1. If the Atkin-Swinnerton-Dyer congruences were established in general, then

$$H_p(T) = \prod_{1 \le j \le d} (T^2 - A_p(j) T + \chi_j(p) p^{k-1}).$$

Scholl's congruence relation (6) may be regarded as a collective replacement for forms of non-congruence subgroup of the equality (2) for newforms.

Let $f = \sum_{n \ge 1} a_n(f) q^{n/\mu}$ be a M-integral cusp form in $S_k(\Gamma)$, and let $g = \sum_{n \ge 1} b_n(g) q^n$ be a normalized newform of weight k level N and character χ.

Definition 1.1. The two forms f and g above are said to satisfy the Atkin-Swinnerton-Dyer congruence relation if, for all primes p not dividing MN and for all $n \ge 1$,

$$(a_{np}(f) - b_p(g) a_n(f) + \chi(p) p^{k-1} a_{n/p}(f))/(np)^{k-1} \tag{7}$$

is integral at all places dividing p.

In particular, if $S_3(\Gamma)$ has a basis of M-integral forms f_j, $1 \le j \le d$, such that each f_j satisfies the Atkin-Swinnerton-Dyer congruence relation with some cuspidal newform g_j of weight 3 for certain congruence subgroup, then this not only establishes the Atkin-Swinnerton-Dyer congruences conjecture for the space $S_3(\Gamma)$, but also provides an interpretation of the $A_p(j)$'s in the conjecture. Geometrically, this means that the motive attached to $S_3(\Gamma)$ by Scholl comes from modular forms for congruence subgroups. Furthermore, if $-I \notin \Gamma$ and $\mathcal{E}_\Gamma$ is the elliptic modular surface associated to Γ in the sense of [19], then $\mathcal{E}_\Gamma$ is an elliptic surface with base curve X_Γ. The product of the L-functions $\prod_{1\le j\le d} L(s,g_j)$ occurs in the Hasse-Weil L-function $L(s,\mathcal{E}_\Gamma)$ attached to the surface $\mathcal{E}_\Gamma$, and it is the part arising from the transcendental lattice of the surface. In this case, $L(s,\mathcal{E}_\Gamma)$ has both its numerator and denominator product of automorphic L-functions. In other words, the Hasse-Weil L-function of $\mathcal{E}_\Gamma$ is "modular". To-date, only a few such examples are known. In a recent preprint of Livné and Yui [7], the L-functions of some rank 4 motives associated to non-rigid Calabi-Yau threefolds are proven to be the L-functions of some automorphic forms.

For the non-congruence subgroup $\Gamma_{7,1,1}$ studied in [1], the space $S_4(\Gamma_{7,1,1})$ is one-dimensional. Let f be a nonzero 14-integral form in $S_4(\Gamma_{7,1,1})$. Scholl proved in [14] that there is a normalized newform g of weight 4 level 14 and trivial character such that f and g satisfy the Atkin-Swinnerton-Dyer congruence relation. In the unpublished paper [15], Scholl obtained a similar result for $S_4(\Gamma_{4,3})$ and $S_4(\Gamma_{5,2})$; both spaces are also 1-dimensional.

The purpose of this paper is to present an example of 2-dimensional space of cusp forms of weight 3 and the existence of a M-integral basis, independent of

p, such that each satisfies the Atkin-Swinnerton-Dyer congruence relation with a cusp form of a congruence subgroup. More precisely, we shall prove

Theorem 1.2. *Let Γ be the index 3 non-congruence subgroup of $\Gamma^1(5)$ such that two of its cusps, including ∞, are of width 15. Then X_Γ has a model over $\mathbb{Q}$, $\kappa = 1$, and the space $S_3(\Gamma)$ is 2-dimensional with a basis consisting of 3-integral forms*

$$\begin{aligned} f_+(\tau) &= q^{1/15} + iq^{2/15} - \frac{11}{3}q^{4/15} - i\frac{16}{3}q^{5/15} - \frac{4}{9}q^{7/15} + i\frac{71}{9}q^{8/15} + \frac{932}{81}q^{10/15} + O(q^{11/15}),\\ f_-(\tau) &= q^{1/15} - iq^{2/15} - \frac{11}{3}q^{4/15} + i\frac{16}{3}q^{5/15} - \frac{4}{9}q^{7/15} - i\frac{71}{9}q^{8/15} + \frac{932}{81}q^{10/15} + O(q^{11/15}). \end{aligned}$$

Further, there are two cuspidal newforms of weight 3 level 27 and character χ_{-3} given by

$$\begin{aligned} g_+(\tau) &= q - 3iq^2 - 5q^4 + 3iq^5 + 5q^7 + 3iq^8 + 9q^{10} + 15iq^{11} - 10q^{13} - 15iq^{14} - 11q^{16}\\ &\quad -18iq^{17} - 16q^{19} - 15iq^{20} + 45q^{22} + 12iq^{23} + O(q^{24})\\ g_-(\tau) &= q + 3iq^2 - 5q^4 - 3iq^5 + 5q^7 - 3iq^8 + 9q^{10} - 15iq^{11} - 10q^{13} + 15iq^{14} - 11q^{16}\\ &\quad +18iq^{17} - 16q^{19} + 15iq^{20} + 45q^{22} - 12iq^{23} + O(q^{24}), \end{aligned}$$

such that f_+ and g_+ (resp. f_- and g_-) satisfy the Atkin-Swinnerton-Dyer congruence relation.

Here χ_{-3} is the quadratic character attached to the field $\mathbb{Q}(\sqrt{-3})$. The precise definition of Γ in terms of generators and relations is given at the end of §3.

The proof of this theorem occupies §2 - §7. Here we give a sketch. The modular curve X_Γ of Γ is a three fold cover of the congruence modular curve $X_{\Gamma^1(5)}$ ramified only at two cusps of $\Gamma^1(5)$. By explicitly computing the Eisenstein series of weight 3 for $\Gamma^1(5)$, we obtain in §4 an explicit basis f_+ and f_- of $S_3(\Gamma)$ which are 3-integral, as stated above.

To establish the congruence relations, we take advantage of the existence of an elliptic surface $\mathcal{E}$ over X_Γ with an explicit algebraic model. There exists a $\mathbb{Q}$-rational involution A on X_Γ which induces an action on $\mathcal{E}$ of order 4, which commutes with the action of the Galois group over $\mathbb{Q}$. In fact, f_+ and f_- are eigenfunctions of A with eigenvalues $-i$ and i, respectively. The explicit defining equation of $\mathcal{E}$ gives rise to a 4-dimensional l-adic representation ρ_l^* of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ which is isomorphic to the l-adic representation ρ_l Scholl constructed in [12] at most up to a quadratic twist ϕ. Take $l = 2$. The dyadic representations are unramified outside 2 and 3. Making use of the action of A, we may regard ρ_2^* as a two-dimensional representation over $\mathbb{Q}_2(i)$, which is isomorphic to the completion of $\mathbb{Q}(i)$ at the place with $1 + i$ as a uniformizer, denoted by $\mathbb{Q}(i)_{1+i}$ for convenience. The explicit defining equation allows us to determine the characteristic polynomial of the Frob_p under ρ_2^* over $\mathbb{Q}_2$ for small primes, and that over $\mathbb{Q}(i)_{1+i}$ except for primes congruent to 2 mod 3, in which case the trace is determined up to sign (cf. Table (1)).

On the other hand, the two cuspidal newforms g_+ and g_- combined come from a 4-dimensional 2-adic representation $\tilde{\rho}_2$ of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, on whose space the Atkin-Lehner operator W_{27} acts. It has order 4. So we may also regard $\tilde{\rho}_2$ as a 2-dimensional representation over $\mathbb{Q}(i)_{1+i}$. The characteristic polynomials of the Frobenius elements under $\tilde{\rho}_2$ are easily read off from the Fourier coefficients of $g_\pm$, which we obtained from W. Stein's website. Since the residue field of $\mathbb{Q}(i)_{1+i}$ is $\mathbb{F}_2$, we use Serre's method [18] to show that ρ_2^* and $\tilde{\rho}_2$ are isomorphic from the incomplete information of the characteristic polynomials of the Frobenius elements at primes $5 \leq p \leq 19$.

This also implies that ρ_2^* is isomorphic to its twist by the quadratic character χ_{-3}.

To prove that ρ_2^* and ρ_2 are isomorphic, we show that ρ_2^* satisfies the congruence relation (6) for $n = 1$, $p = 7$ and $p = 13$. This in turn forces ϕ to be either χ_{-3} or trivial. In either case, we have the desired isomorphism. The conclusion that $f_\pm$ and $g_\pm$ satisfy the Atkin-Swinnerton-Dyer congruence relation follows from Remark 5.8 of [12].

We end the paper by observing that if the space of cusp forms of weight 3 for a non-congruence subgroup Γ' is 1-dimensional with a nonzero M-integral form f and there is an elliptic $K3$ surface over the modular curve $X_{\Gamma'}$, then there is a cuspidal newform g such that f and g satisfy the Atkin-Swinnerton-Dyer congruence relation.

The authors would like to thank Prof. J.-P. Serre for many stimulating and helpful communications. We are particularly grateful to him for explaining how to apply his method to our situation.

2. An elliptic surface

Let $\mathcal{E}$ denote the minimal smooth model of the elliptic surface given by

$$y^2 + (1-t^3)xy - t^3y = x^3 - t^3x^2\,, \tag{8}$$

where the parameter t runs through the points in the complex projective line $\mathbb{C}P^1$. Viewed as an elliptic curve defined over $\mathbb{C}(t)$, its j-invariant is

$$j = \frac{(t^{12} - 12t^9 + 14t^6 + 12t^3 + 1)^3}{t^{15}(t^6 - 11t^3 - 1)}\,. \tag{9}$$

Its Mordell-Weil group is isomorphic to $\mathbb{Z}/5\mathbb{Z}$. Indeed, it is a subgroup of $\mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$ and it contains $\mathbb{Z}/5\mathbb{Z}$ as a subgroup. By examining the restriction of the determinant of its transcendental lattice, we find that this group has order a power of 5. We conclude that the group is $\mathbb{Z}/5\mathbb{Z}$ from a result of Cox and Parry [3].

It is clear that at a generic $t \in \mathbb{C}$, the fiber of the natural projection

$$\pi: \; E \;\to\; \mathbb{C}P^1 \tag{10}$$

$$(x,y,t) \;\mapsto\; t \tag{11}$$

is an elliptic curve, namely, a smooth compact curve of genus one. This is the case except for 8 values of t: 0, ∞, and the six roots of $t^6 - 11t^3 - 1 = 0$. At these 8 exceptional values of t, there are 8 special fibers. They are identified, using Tate algorithm, to be of respective type I_{15}, I_{15}, I_1, I_1, I_1, I_1, I_1, I_1 in Kodaira's notation. The surface $\mathcal{E}$ is an elliptic modular surface by [19], [10]. Denote by Γ an associated modular group, which is a subgroup of $SL_2(\mathbb{Z})$ of finite index. Let $\bar{\Gamma} = \pm\Gamma/\pm I$ be its projection in $PSL_2(\mathbb{Z})$. We know from the information of the special fibers that the group Γ has no elliptic points. In another words, it is a torsion free subgroup of $SL_2(\mathbb{Z})$.

Now we consider some topological and geometrical invariants of $\mathcal{E}$. By Kodaira's formula [6], the Euler characteristic of $\mathcal{E}$ is 36. Its irregularity, which equals the genus of the base curve, is 0. Its geometric genus is 2 by Noether's formula. Denote by $h^{i,j} = \dim H^j(\mathcal{E}, \Omega^i_{\mathcal{E}})$ the (i,j)'s Hodge number of $\mathcal{E}$. Then the Hodge numbers of $\mathcal{E}$ can be arranged into the following Hodge diamond

$$\begin{array}{ccccc} & & 1 & & \\ & 0 & & 0 & \\ 2 & & 30 & & 2 \\ & 0 & & 0 & \\ & & 1 & & \end{array}$$

where on the $(i+1)$th row, the $(j+1)$th number is $h^{i-j,j}$, with $j = 0, ..., i$ for $0 \le i \le 2$, and $j = 0, 4-i$ for $3 \le i \le 4$.

As the group $\bar{\Gamma}$ is not among the genus-zero torsion free congruence subgroups of $PSL_2(\mathbb{Z})$ listed by A. Sebbar [17], we conclude that Γ is a non-congruence subgroup of $SL_2(\mathbb{Z})$.

Let L be the free part of the cohomology group $H^2(\mathcal{E}, \mathbb{Z})$. It is an even unimodular lattice with the bilinear form given by the cup-product. The signature of this lattice is $(5, 29)$ by the Hodge index theory. It follows from the classification of even unimodular lattices that L is isometric to $U^5 \oplus E_8(-1)^3$, where U denotes the hyperbolic matrix and $E_8(-1)$ denotes the unique negative definite even unimodular lattice of rank 8.

By the Shioda-Tate formula [19], the Picard number is $2 + 2(15 - 1) = 30$. The Néron-Severi group $NS(\mathcal{E})$, which is the group of divisors on $\mathcal{E}$ modulo algebraic equivalence, is a torsion-free $\mathbb{Z}$-module of rank 30. This group can be imbedded into L by a cohomology sequence. The determinant of this sublattice, by a formula in [19], is equal to

$$|\det(NS(\mathcal{E}))| = \frac{15^2}{5^2} = 9.$$

The orthogonal complement $T_{\mathcal{E}}$ of $NS(\mathcal{E})$ in L, called the transcendental lattice of L, has rank 4 and $|\det(T_{\mathcal{E}})| = |\det(NS(\mathcal{E}))| = 9$ since L is unimodular,

As we are interested in the arithmetic properties of $\mathcal{E}$, we shall consider the reductions of $\mathcal{E}$. It turns out that for this particular elliptic surface $\mathcal{E}$ the only bad prime is 3. (The prime 5 is good because the 5 torsion points have killed the contribution of 5 from the special fibres.) Hence we may regard $\mathcal{E}$ as a normal connected smooth scheme over $\mathbb{Z}[1/3]$; it is tamely ramified along the closed subscheme formed by the cusps.

3. Determining the non-congruence subgroup Γ

For any positive integer N let

$$\Gamma^0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : N|b \right\},$$
$$\Gamma^1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma^0(N) : a \equiv d \equiv 1 \mod N \right\}.$$

With t^3 in (8) replaced by t, the new equation defines an elliptic modular surface $\mathcal{E}'$ over the modular curve for the group $\Gamma^1(5)$. The surface $\mathcal{E}$ is a three fold cover of $\mathcal{E}'$, and thus the group Γ is a subgroup of $\Gamma^1(5)$ of index three. We proceed to determine Γ in terms of generators and relations.

First we decompose the full modular group $SL_2(\mathbb{Z})$ as

$$SL_2(\mathbb{Z}) = \bigcup_{1 \le i \le 6} \Gamma^0(5)\gamma_i,$$

where $\gamma_i = \begin{pmatrix} 1 & i-1 \\ 0 & 1 \end{pmatrix}$ for $1 \le i \le 5$ and $\gamma_6 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Further,

$$\Gamma^0(5) = \bigcup_{1 \le j \le 4} \Gamma^1(5) A^j = \pm\Gamma^1(5) \bigcup \pm\Gamma^1(5)A,$$

where $A = \begin{pmatrix} -2 & -5 \\ 1 & 2 \end{pmatrix}$, $A^2 = -I$. Hence the coset representatives of $\pm\Gamma^1(5)$ in $SL_2(\mathbb{Z})$ may be taken as γ_i and $A\gamma_i$ for $1 \le i \le 6$.

Listed below are the cusps of $\pm\Gamma^1(5)$ and a choice of generator of their stabilizers in $SL_2(\mathbb{Z})$:

cusps of $\pm\Gamma^1(5)$	generators of stabilizers
∞	$\gamma = \begin{pmatrix} 1 & 5 \\ 0 & 1 \end{pmatrix}$
0	$\delta = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$
-2	$A\gamma A^{-1} = \begin{pmatrix} 11 & 20 \\ -5 & -9 \end{pmatrix}$
$-\frac{5}{2}$	$A\delta A^{-1} = \begin{pmatrix} 11 & 25 \\ -4 & -9 \end{pmatrix}$

Therefore the group $\Gamma^1(5)$ is generated by γ, δ, $A\gamma A^{-1}$, $A\delta A^{-1}$ with the relation

$$(A\delta A^{-1})(A\gamma A^{-1})\delta\gamma = I.$$

In particular, $\Gamma^1(5)$ is actually generated by $A\delta A^{-1}$, δ, γ.

For Γ, we may assume that its cusp at ∞ has width 15 so that

$$\Gamma^1(5) = \bigcup_{0 \le j \le 2} \Gamma\gamma^j.$$

The information on types of special fibers of $\mathcal{E}$ and the above table give rise to the following information on cusps of Γ and a choice of generator of stabilizers of each cusp:

cusps of Γ	width	generators of stabilizers
∞	15	γ^3
-2	15	$A\gamma^3A^{-1}$
0	1	δ
5	1	$\gamma\delta\gamma^{-1}$
10	1	$\gamma^2\delta\gamma^{-2}$
$-\frac{5}{2}$	1	$A\delta A^{-1}$
$\frac{5}{2}$	1	$\gamma A\delta A^{-1}\gamma^{-1}$
$\frac{15}{2}$	1	$\gamma^2 A\delta A^{-1}\gamma^{-2}$

This shows that Γ is generated by γ^3, δ, $A\gamma^3A^{-1}$, $A\delta A^{-1}$, $\gamma\delta\gamma^{-1}$, $\gamma A\delta A^{-1}\gamma^{-1}$, $\gamma^2\delta\gamma^{-2}$, $\gamma^2 A\delta A^{-1}\gamma^{-2}$ with the relation

$$(A\delta A^{-1})(A\gamma^3A^{-1})\delta(\gamma A\delta A^{-1}\gamma^{-1})(\gamma\delta\gamma^{-1})(\gamma^2A\delta A^{-1}\gamma^{-2})(\gamma^2\delta\gamma^{-2})\gamma^3 = I.$$

Remark 3.1. Similar to the above, if we take elements γ^2, δ, $A\delta A^{-1}$, $A\gamma^2A^{-1}$, $\gamma\delta\gamma^{-1}$, $\gamma A\delta A^{-1}\gamma^{-1}$ as generators with the relation

$$(A\delta A^{-1})(A\gamma^2A^{-1})(\delta)(\gamma A\delta A^{-1})(\gamma\delta\gamma^{-1})(\gamma^2) = I,$$

then we get the non-congruence subgroup Γ_2 of $\Gamma^1(5)$ of index 2 associated to the elliptic modular surface defined by

$$y^2 + (1-t^2)xy - t^2y = x^3 - t^2x^2\,. \tag{12}$$

4. The space of weight 3 cusp forms for Γ

It follows readily from the dimension formula in Shimura [21] that the space $S_3(\Gamma)$ of cusp forms of weight 3 for Γ has dimension 2. We shall give a basis of this space in terms of the weight 3 Eisenstein series of $\Gamma^1(5)$ by using Hecke's construction as described in Ogg [11]. The space of weight 3 Eisenstein series of $\Gamma^1(5)$ has dimension 4, equal to the number of cusps of $\Gamma^1(5)$. We are only interested in the two Eisenstein series that vanish at all but only one of the two cusps ∞ and -2.

Let $k \geq 3$, and $c, d \in \mathbb{Z}$. The Eisenstein series

$$G_k(\tau;(c,d);N) = \sum{}'_{\substack{m\equiv c \pmod N\\ n\equiv d \pmod N}} (m\tau+n)^{-k}$$

is a weight k modular form for the principal congruence subgroup $\Gamma(N)$. Moreover, for any $L \in SL_2(\mathbb{Z})$, we have

$$G_k(\tau;(c,d);N)|L = G_k(\tau;(c,d)L;N).$$

This Eisenstein series has the following Fourier expansion:

$$G_k(\tau;(c,d);N) = \sum_{\lambda=0}^{\infty} a_\lambda z^\lambda, \qquad z = e^{2\pi i\tau/N} \tag{13}$$

where

$$a_0 = \begin{cases} 0 & \text{if } c \not\equiv 0 \pmod N, \\ \sum_{n\equiv d \pmod N} n^{-k} & \text{if } c \equiv 0 \pmod N, \end{cases}$$

and for $\lambda \geq 1$,

$$a_\lambda = \frac{(-2\pi i)^k}{N^k\Gamma(k)} \sum_{\substack{m\nu=\lambda\\ m\equiv c \pmod N}} (\mathrm{sgn}\nu)\nu^{\mathrm{k}-1}\mathrm{e}^{2\pi\mathrm{i}\nu\mathrm{d}/\mathrm{N}}. \tag{14}$$

The restricted Eisenstein series is defined by

$$G_k^*(\tau;(c,d);N) = \sum_{\substack{m\equiv c \pmod N\\ n\equiv d \pmod N\\ (m,n)=1}} (m\tau+n)^{-k},$$

which is a weight k modular form for $\Gamma(N)$, satisfying

$$G_k^*(\tau;(c,d);N)|L = G_k^*(\tau;(c,d)L;N)$$

for all $L \in SL_2(\mathbb{Z})$. Let $\mu(n)$ denote the Möbius function. Then $G_k^*(\tau;(c,d);N)$ can be expressed in terms of the series $G_k(\tau;(c,d);N)$:

$$\begin{aligned} G_k^*(\tau;(c,d);N) &= \sum_{a=1}^{\infty} \mu(a)a^{-k} G_k(\tau;(a'c,a'd);N) \\ &= \sum_{\substack{(t,N)=1\\ t \mod N}} c_t \cdot G_k(\tau;(ct,dt);N), \end{aligned} \tag{15}$$

where a' is chosen such that $aa' \equiv 1 \pmod N$, and $c_t = \sum_{at\equiv 1 \pmod N, a>0} \mu(a)a^{-k}$. The Eisenstein series $G_k^*(\tau;(c,d);N)$ has value 1 at the cusp $-\frac{d}{c}$ and 0 at all other cups.

In the special case $k=3$, $N=5$, for any character χ of $(\mathbb{Z}/5\mathbb{Z})^*$ we have

$$\sum_{(t,N)=1} \bar{\chi}(t)c_t = \sum_t \sum_{a\equiv t^{-1}, a>0} \mu(a)a^{-k} = L^{-1}(k,\chi).$$

Denote by $\chi_3 : (\mathbb{Z}/5\mathbb{Z})^* \to \mathbb{C}$ the character given by $\chi_3(2) = i$, $\chi_2 = \chi_3^2$, $\chi_4 = \chi_3^3$, and χ_1 the trivial character of $(\mathbb{Z}/5\mathbb{Z})^*$. Then the constants c_t can be expressed via the values of L-series:

$$\begin{aligned} c_1 &= \frac{1}{4}\left(L^{-1}(3,\chi_1) + L^{-1}(3,\chi_2) + L^{-1}(3,\chi_3) + L^{-1}(3,\chi_4)\right), \\ c_2 &= \frac{1}{4}\left(L^{-1}(3,\chi_1) - L^{-1}(3,\chi_2) + iL^{-1}(3,\chi_3) - iL^{-1}(3,\chi_4)\right), \\ c_3 &= \frac{1}{4}\left(L^{-1}(3,\chi_1) - L^{-1}(3,\chi_2) - iL^{-1}(3,\chi_3) + iL^{-1}(3,\chi_4)\right), \\ c_4 &= \frac{1}{4}\left(L^{-1}(3,\chi_1) + L^{-1}(3,\chi_2) - L^{-1}(3,\chi_3) - L^{-1}(3,\chi_4)\right). \end{aligned}$$

Using the functional equation of the L-function $L(s,\chi)$ and the Bernoulli polynomials, we obtain two explicit L-values

$$\begin{aligned} L(3,\chi_3) &= \frac{\tau(\chi_3)}{2i}\left(-\frac{1}{2}\right)\left(\frac{2\pi}{5}\right)^3\left(-\frac{1}{3}\right)\frac{6}{5}(2-i), \\ L(3,\chi_4) &= \frac{\tau(\chi_4)}{2i}\left(-\frac{1}{2}\right)\left(\frac{2\pi}{5}\right)^3\left(-\frac{1}{3}\right)\frac{6}{5}(2+i), \end{aligned}$$

where $\tau(\chi)$ denotes the Gauss sum of the character χ.

As $\Gamma^1(5) = \bigcup_{a=0}^4 \Gamma(5) \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$, we let

$$\begin{aligned} E_1(\tau) &= \sum_{0\le a\le 4} G_k^*(\tau;(0,1);5) | \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} = \sum_a G_k^*(\tau;(a,1);5) \\ &= c_1 \sum_a G_k(\tau;(a,1);5) + c_2 \sum_a G_k(\tau;(2a,2);5) + c_3 \sum_a G_k(\tau;(3a,3);5) \qquad (16) \\ &+ c_4 \sum_a G_k(\tau;(4a,4);5). \end{aligned}$$

Applying the Fourier expansion of the Eisenstein series $G_k(\tau;(c,d);5)$ and the equations for $c_i's$, we have the Fourier expansion of $E_1(\tau)$:

$$E_1(\tau) = 1 - \frac{1}{2}\sum_{\lambda=1}^{\infty}\left(2\sum_{\nu|\lambda,\,\nu>0}\nu^2\left(\chi_3(\nu)+\chi_4(\nu)\right) + i\sum_{\nu|\lambda,\,\nu>0}\nu^2\left(\chi_4(\nu)-\chi_3(\nu)\right)\right)q^{\lambda/5}. \qquad (17)$$

In particular, the Fourier coefficients of $E_1(\tau)$ are rational integers. And from the definition of $E_1(\tau)$, it has value 1 at the cusp ∞, and 0 at the other cusps 0, -2, $-\frac{5}{2}$.

Let

$$\begin{aligned} E_2(\tau) &= E_1(\tau)|A^{-1} \\ &= c_1 \sum_a G_k(\tau;(-2a+1,-5a+2);5) + c_2 \sum_a G_k(\tau;(-4a+2,-10a+4);5) \\ &+ c_3 \sum_a G_k(\tau;(-6a+3,-15a+6);5) + c_4 \sum_a G_k(\tau;(-8a+4,-20a+8);5). \end{aligned}$$

Then $E_2(\tau)$ has value -1 at the cusp -2, and 0 at other cusps. In the same way we calculate the Fourier expansion of this Eisenstein series to get

$$E_2(\tau) = \frac{1}{2}\sum_{\lambda=1}^{\infty}\left(\sum_{\nu|\lambda,\,\nu>0}\nu^2\left(\chi_3(\nu)+\chi_4(\nu)\right) + 2i\sum_{\nu|\lambda,\,\nu>0}\nu^2\left(\chi_3(\nu)-\chi_4(\nu)\right)\right)q^{\lambda/5}. \qquad (18)$$

Since $E_1(\tau)$ has values 1, 0, 0, 0 at the cusps ∞, -2, 0, $-\frac{5}{2}$, respectively, and $E_2(\tau)$ has values 0, -1, 0, 0 at these cusps, both modular forms have no other zero points. Consider the natural covering map

$$\Gamma\backslash\mathcal{H} \to \Gamma^1(5)\backslash\mathcal{H},$$

where $\mathcal{H}$ denotes the Poincaré upper half plane. It ramifies only at the two cusps ∞ and -2, with index 3. Therefore the two functions

$$f_1 = \sqrt[3]{E_1^2(\tau)E_2(\tau)} \qquad \text{and} \qquad f_2 = \sqrt[3]{E_1(\tau)E_2^2(\tau)} \qquad (19)$$

are well-defined entire modular forms of weight 3 for Γ. Further, they vanish at every cusp, hence they are cusp forms. It is clear that f_1 and f_2 are linearly independent, and thus form a basis of the space $S_3(\Gamma)$. Choosing a proper cubic root of one, we may assume that the

Fourier coefficients of both f_1 and f_2 are rational numbers with denominators involving only powers of 3.

Since the action of the matrix A interchanges the cusp ∞ with the cusp -2, it defines an operator on the space $S_3(\Gamma)$. More precisely, its actions on f_1 and f_2 are

$$(f_1)|A = f_2 \qquad \text{and} \qquad (f_2)|A = -f_1.$$

Thus the operator A on $S_3(\Gamma)$ has eigenforms $f_+ = f_1 + if_2$ and $f_- = f_1 - if_2$ with eigenvalues $-i$ and i, respectively. The Fourier expansions of these two eigenforms are as follows:

$$\begin{aligned} f_+(\tau) &= q^{1/15} + iq^{2/15} - \frac{11}{3}q^{4/15} - i\frac{16}{3}q^{5/15} - \frac{4}{9}q^{7/15} + i\frac{71}{9}q^{8/15} + \frac{932}{81}q^{10/15} \\ &\quad + i\frac{247}{81}q^{11/15} + \frac{443}{243}q^{13} - i\frac{3832}{243}q^{14/15} - \frac{13151}{729}q^{16/15} + i\frac{9131}{729}q^{17/15} + O(q^{18/15}), \\ f_-(\tau) &= q^{1/15} - iq^{2/15} - \frac{11}{3}q^{4/15} + i\frac{16}{3}q^{5/15} - \frac{4}{9}q^{7/15} - i\frac{71}{9}q^{8/15} + \frac{932}{81}q^{10/15} \\ &\quad - i\frac{247}{81}q^{11/15} + \frac{443}{243}q^{13} + i\frac{3832}{243}q^{14/15} - \frac{13151}{729}q^{16/15} - i\frac{9131}{729}q^{17/15} + O(q^{18/15}). \end{aligned}$$

This proves the first assertion of Theorem 1.2.

Let X be the modular curve of the non-congruence subgroup Γ, that is, $X(\mathbb{C}) = \overline{\Gamma\backslash\mathcal{H}}$. As seen in §2, it is a projective line over $\mathbb{C}$. The two cusp forms constructed in section 4 give rise to a Hauptmodul of X:

$$t = \frac{f_1}{f_2} = \sqrt[3]{\frac{E_1}{E_2}}.$$

Since the Fourier coefficients of t are in $\mathbb{Q}$, the curve X is defined over $\mathbb{Q}$. It is easy to check from the generators and relation exhibited in §3 that the matrix A lies in the normalizer of the non-congruence subgroup Γ in $SL_2(\mathbb{Z})$. Therefore A induces a $\mathbb{Q}$-rational involution on the modular curve X, given by

$$A(t) = -\frac{1}{t}. \tag{20}$$

Further, A induces an order 4 $\mathbb{Q}$-rational action on the elliptic surface $\mathcal{E}$. To see this, make the following change of variables:

$$\begin{aligned} x &= t^3X - 1/12t^6 + 1/2t^3 - 1/12 \\ y &= t^4Y + 1/2t^6X - 1/2t^3X - 1/24t^9 + 7/24t^6 + 5/24t^3 + 1/24 \end{aligned}$$

so that the original defining equation (8) becomes

$$Y^2 = t(X^3 - \frac{1 + 12t^3 + 14t^6 - 12t^9 + t^{12}}{48t^6}X + \frac{1 + 18t^3 + 75t^6 + 75t^{12} - 18t^{15} + t^{18}}{864t^9}). \tag{21}$$

The action of A sends t to $-1/t$, Y to Y/t, and X to $-X$. Hence it is defined over $\mathbb{Q}$ and has order 4.

5. The l-adic representation attached to $S_3(\Gamma)$

As explained in §1, given a non-congruence subgroup Γ' of $SL_2(\mathbb{Z})$ of finite index with the modular curve $X_{\Gamma'}$ defined over $\mathbb{Q}$, Scholl in [12] defined a compatible family of l-adic representations ρ_l of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ associated to $S_k(\Gamma')$, $k \geq 3$, from which he derived the congruence relation Theorem 1.2. When $k = 3$, the representation ρ_l is defined as follows. Choose an integer $N \geq 3$ such that $\pm\Gamma'\Gamma(N) = SL_2(\mathbb{Z})$. Denote by $X(N)$ the compactified modular curve for the principal congruence subgroup $\Gamma(N)$, and by $X(N)^o$ the part of $X(N)$ with cusps removed. Let $G(N) = SL(\mu_N \times \mathbb{Z}/N)$, let $f^{\mathrm{univ}} : E^{\mathrm{univ}} \to X(N)^o$ be the restriction to $X(N)^o$ of the universal elliptic curve of $X(N)$, and let $V(N)$ (resp. $V(N)^o$) be the normalization of the fiber product $X_{\Gamma'} \times_{X(1)} X(N)$ (resp. $X_{\Gamma'} \times_{X(1)} X(N)^o$). The finite group scheme $G(N)$ acts on the second factor of $V(N)$, E^{univ}, and the sheaf $\mathcal{F}_l^{\mathrm{univ}} = R^1 f_*^{\mathrm{univ}} \mathbb{Q}_l$, respectively. We have the projection map $\pi_0' : V(N)^o \to X(N)^o$ and the inclusion map $i_N : V(N)^o \to V(N)$. The representation ρ_l of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is the action of the Galois group on the $\mathbb{Q}_l$-space

$$H^1(V(N) \otimes \overline{\mathbb{Q}}, (i_N)_* \pi_0'^* \mathcal{F}_l^{\mathrm{univ}})^{G(N)}.$$

The reason that an auxiliary modular curve $X(N)$ is involved is that the curve $X_{\Gamma'}$ does not have a universal elliptic curve, while $X(N)$ for $N \geq 3$ does. As shown above, the l-adic sheaf comes from this universal elliptic curve. At the end, $G(N)$ invariants are taken to rid the dependence of $X(N)$.

When there is an elliptic surface $\mathcal{E}'$ over the modular curve $X_{\Gamma'}$ with $h' : \mathcal{E}' \to X_{\Gamma'}$ tamely ramified along the cusps and elliptic points, inspired by [14], we introduce another l-adic representation ρ_l^* of the Galois group of $\mathbb{Q}$ using $\mathcal{E}'$ as follows. Let $X_{\Gamma'}^0$ be the part of $X_{\Gamma'}$ with the cusps and elliptic points removed. Denote by i the inclusion from $X_{\Gamma'}^0$ into $X_{\Gamma'}$, and by

$$h : \mathcal{E}' \to X_{\Gamma'}^0$$

the restriction map, which is étale. For almost all prime l, we obtain a sheaf

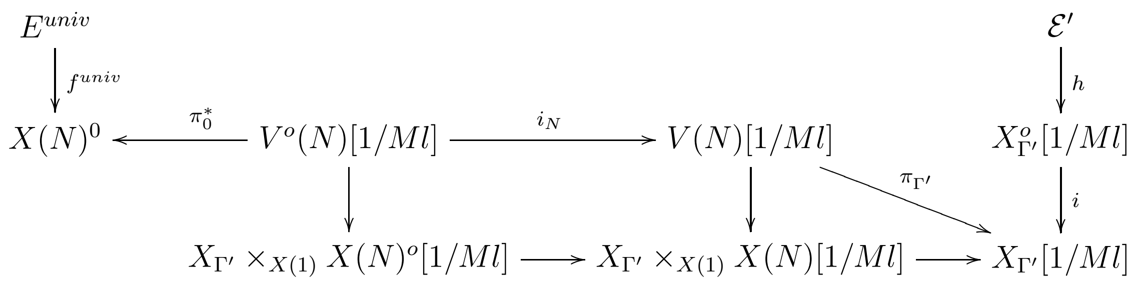
$$\mathcal{F}_l = R^1 h_* \mathbb{Q}_l$$

on $X_{\Gamma'}^0$. The i_* map then transports it to a sheaf $i_* \mathcal{F}_l$ on $X_{\Gamma'}$. The action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the $\mathbb{Q}_l$-space

$$W_l = H^1(X_{\Gamma'} \otimes \overline{\mathbb{Q}}, i_* \mathcal{F}_l) \tag{22}$$

defines an l-adic representation, denoted by ρ_l^*, of the Galois group of $\mathbb{Q}$.

The following diagram depicts the relationship of the curves and surfaces involved. For a scheme X and a non-zero integer M, we use $X[1/M]$ to denote $X \times_{\mathrm{Spec}\mathbb{Z}} \mathrm{Spec}\mathbb{Z}[1/M]$. The integer M below is chosen so that both modular curves $X(N)$ and $X_{\Gamma'}$ are smooth and proper over the ring $\mathbb{Z}[1/M]$. The maps π_0' and $\pi_{\Gamma'}$ are the natural projections.



Proposition 5.1. *The two representations ρ_l^* and ρ_l are isomorphic up to twist by a character ϕ_l of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *of order at most 2.*

Proof. Using the projection $\pi_{\Gamma'}$ from the fiber product $V(N)[1/Ml]$ to the factor $X_{\Gamma'}[1/Ml]$, we pull back the sheaf $i_*\mathcal{F}_l$ on $X_{\Gamma'}[1/Ml]$ to the sheaf $\pi_{\Gamma'}^* i_*\mathcal{F}_l$ on $V(N)[1/Ml]$. It follows from an argument similar to §1.3 of [14] that the sheaf $(i_N)_*\pi_0'^*\mathcal{F}_l^{\mathrm{univ}}$ is isomorphic to the sheaf $\pi_{\Gamma'}^* i_*\mathcal{F}_l \otimes \mathcal{L}$, where $\mathcal{L}$ is a rank one sheaf on $V(N)[1/Ml]$ with $\mathcal{L}^{\otimes 2}$ isomorphic to the constant sheaf $\mathbb{Q}_l$. Consequently, $H^1(V(N)\otimes\overline{\mathbb{Q}}, \pi_{\Gamma'}^* i_*\mathcal{F}_l)$ and $H^1(V(N)\otimes\overline{\mathbb{Q}}, (i_N)_*\pi_0'^*\mathcal{F}_l^{\mathrm{univ}})$ are isomorphic

$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ modules up to twist by a character ϕ_l of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of order at most 2. Since $G(N)$ acts only on $X(N)$, the $G(N)$-invariant part of $H^1(V(N)\otimes\overline{\mathbb{Q}}, \pi_{\Gamma'}^* i_*\mathcal{F}_l)$ is isomorphic to W_l. Therefore the representation ρ_l^* on W_l is isomorphic to ρ_l on $H^1(V(N)\otimes\overline{\mathbb{Q}}, (i_N)_*\pi_0'^*\mathcal{F}_l^{\mathrm{univ}})^{G(N)}$ up to twist by ϕ_l.

□

Apply the above discussion to the case where $\Gamma' = \Gamma$. We shall show later in §6 that our ρ_l^* is in fact isomorphic to Scholl's representation ρ_l. The simpler description of ρ_l^* allows us to get more information about the representation, and eventually leading to a finer congruence result than the one provided by Theorem 1.1.

By Scholl's result in [12], $\dim_{\mathbb{Q}_l} W_l = h^{2,0}(\mathcal{E}) + h^{0,2}(\mathcal{E}) = 4$. As remarked at the end of the previous section, the action of A on X and on $\mathcal{E}$ are both $\mathbb{Q}$-rational, thus A commutes with the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the space W_l. Moreover, the action of A on the sheaf $\mathcal{F}_l$ or the representing space W_l has order 4. This makes W_l a 2-dimensional module over the algebra $K = \mathbb{Q}_l(A)$.

Now fix the prime $l = 2$. Then $K = \mathbb{Q}_2(A)$ is a degree two field extension of $\mathbb{Q}_2$ and ρ_2^* is a degree two representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ over the 2-dimensional vector space W_2 over K. We may choose $N = 4$, $M = 6$ in the Proposition above so that all Galois representations involved are unramified outside 2 and 3. We calculate the characteristic polynomial $H_p(T)$ (resp. $H_p'(T)$) of $\rho_2^*(\mathrm{Frob}_p)$ over $\mathbb{Q}_2$ (resp. $\mathbb{Q}_2(A) = K = \mathbb{Q}(A)_{1+A}$) for varying primes $p \neq 2, 3$. By Scholl's work [12], the characteristic polynomial $H_p(T)$ of $\rho_2^*(\mathrm{Frob}_p)$ can be factored as

$$\begin{aligned} H_p(T) &= (T-\alpha_p)(T-\beta_p)(T-p^2/\alpha_p)(T-p^2/\beta_p) \\ &= T^4 - C_1(p)\,T^3 + C_2(p)\,T^2 - p^2 C_1(p)\,T + p^4 \in \mathbb{Z}[T], \end{aligned} \tag{23}$$

where

$$C_1(p) = \alpha_p + \beta_p + p^2/\alpha_p + p^2/\beta_p = \mathrm{Tr}(\rho_2^*(\mathrm{Frob}_p)),$$
$$C_2(p) = \frac{1}{2}\left(C_1^2 - \mathrm{Tr}(\rho_2{*}(\mathrm{Frob}_p^2))\right) = \frac{1}{2}\left((\mathrm{Tr}(\rho_2^*(\mathrm{Frob}_p)))^2 - \mathrm{Tr}(\rho_2^*(\mathrm{Frob}_{p^2}))\right).$$

Since there are no elliptic points for Γ, we can easily get the following trace formula of $\mathrm{Tr}(\rho_2^*(\mathrm{Frob}_q))$, for $q = p^r$, as in [14]:

$$\mathrm{Tr}_q(\rho_2^*(\mathrm{Frob}_q)) = -\sum_{x \in X(\mathbb{F}_q)} \mathrm{Tr}(x), \tag{24}$$

where

$$\mathrm{Tr}(x) = \mathrm{Tr}\left((\mathrm{Frob}_p)_x : (i_*\mathcal{F}_2)_x\right),$$

the trace of Frob_p restricted to the stalk at x of the sheaf $i_*\mathcal{F}_2$.

There are only two different cases in the computation of $\mathrm{Tr}(x)$. The first case is when $j(x) = \infty$. In this case, $\mathrm{Tr}(x) = 1$. The second case is when $j(x) \neq \infty$. Then letting E_x be the fibre of the elliptic curve $f : E \to Y$ at the point x, we get

$$\mathrm{Tr}(x) = 1 + q - \#E_x(\mathbb{F}_q).$$

A computer program yields the following table on Tr_q, the traces of Frob_q:

p	5	7	11	13	17	19	23	29	31
Tr_p	0	10	0	-20	0	-32	0	0	-2
Tr_{p^2}	82	-146	34	-476	508	-932	1828	1564	-3842

Therefore we obtain the characteristic polynomials $H_p(T)$ of $\rho_2^*(\mathrm{Frob}_p)$, with p the primes between 5 and 31. For such a prime p, the characteristic polynomial $H_p'(T)$ of $\rho_2^*(\mathrm{Frob}_p)$ over K has degree 2, and it has the property that $H_p'(T)H_p''(T) = H_p(T)$, where $H_p''(T)$ are the conjugate of $H_p'(T)$ under the automorphism of K over $\mathbb{Q}_2$ sending A to $-A$. Since Scholl [12] proved that all roots of H_p are algebraic integers, the first step towards determining H_p' is to figure out how to separate the four roots of H_p into two conjugate pairs to form the roots of H_p' and H_p''. It turns out that for the primes from 5 to 31 such separation is unique except for $p = 13$ and 19. For these primes, while we cannot choose between H_p' and H_p'' without further work, we do know the determinant of the two-dimensional representation ρ_2^* over K at these primes since the constant term of $H_p'(T)$ is $\pm p^2$.

Next we prove that the information so far determines the determinant of ρ_2^*, which in turn will allow us determine H_{13}' and H_{19}'.

Lemma 5.1. *If two integral 1-dimensional representations σ_1 and σ_2 of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *over the field* $\mathbb{Q}_2(A)$*, which are unramified away from 2 and 3, agree on the elements* Frob_p *for* $p = 5, 7, 11, 17$*, then they are equal.*

Proof. The images of the 1-dimensional representations are in $(\mathbb{Z}_2[A])^* = (\mathbb{Z}(A)_\mathfrak{p})^*$, where $\mathfrak{p} = (1+A)$ is the maximal ideal of the local ring $\mathbb{Z}_2(A)$. Note that $(\mathbb{Z}(A)_\mathfrak{p})^* = \langle A\rangle \times (1+\mathfrak{p}^3)$. Let log denote the $(1+A)$-adic logarithm on $(\mathbb{Z}_2[A])^*$. More precisely, it has kernel the group $\langle A\rangle$ of roots of unity in $\mathbb{Q}_2(A)$, and it maps $1+x \in 1+\mathfrak{p}^3$ to $\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} x^n \in \mathbb{Z}_2[A]$. As such, log gives an isomorphism between the multiplicative group $1+\mathfrak{p}^3$ and the additive group $\mathfrak{p}^3$. Consider

$$\psi = \log \circ \sigma_1 - \log \circ \sigma_2,$$

which is a homomorphism from $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to $\mathfrak{p}^3$.

If $\psi \neq 0$, then

$$n_0 = \min\left\{\mathrm{ord}_\mathfrak{p}\left(\psi(\tau)\right) : \tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\right\}$$

is finite. Then

$$\bar{\psi} := \frac{1}{(1+A)^{n_0+1}}\psi \pmod{\mathfrak{p}}$$

is a continuous surjective homomorphism from $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to $\mathbb{F}_2$ which is trivial at the Frobenius elements at primes $p = 5, 7, 11, 17$ by assumption. This representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ factors through a quadratic extension of $\mathbb{Q}$ unramified outside 2 and 3. Such fields are extensions of $\mathbb{Q}$ by adjoining square roots of $2, 3, 6, -1, -2, -3, -6$, respectively. It is easy to check that the prime $p = 5, 5, 11, 7, 5, 5, 17$ is inert in the respective field, and thus $\bar{\psi}$ at such Frob_p would be nontrivial, a contradiction. Therefore $\psi = 0$, in other words, the image of the representation $\sigma := \sigma_1(\sigma_2)^{-1}$ is a subgroup of $\langle A\rangle$, a cyclic group of order 4. Hence we consider all Galois extensions of $\mathbb{Q}$ with group equal to a subgroup of a cyclic group of order 4, unramified away from 2 and 3, and in which $p = 5, 7, 11, 17$ split completely. If a nontrivial such extension exists, then it contains a quadratic subextension unramified outside 2 and 3, and in which $p = 5, 7, 11, 17$ split completely. As shown above, this is impossible. Therefore the image of σ can only be $\{1\}$, in other words, σ_1 and σ_2 are equal. □

Denote by χ_{-3} the quadratic character attached to the field $\mathbb{Q}(\sqrt{-3})$, that is, $\chi_{-3}(x)$ is equal to the Legendre symbol $\left(\frac{-3}{x}\right)$. The 1-dimensional representation σ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ over K given by $\tilde{\chi}_{-3}(\mathrm{Frob}_p) = \chi_{-3}(p)p^2$ for primes $p \neq 2, 3$ agrees with $\det(\rho_2^*)$ at Frob_p for $p = 5, 7, 11, 17$ by checking the constant term of $H_p'(T)$, and hence we conclude from Lemma 5.1 that the two degree one representations agree.

Corollary 5.1. *Let $\tilde{\chi}_{-3}$ be as above. We have* $\det(\rho_2^*) = \tilde{\chi}_{-3}$.

In particular, we know that the constant term of H_{13}' (resp. H_{19}') is $(13)^2$ (resp. $(19)^2$). This information enables us to determine $H_{13}'(T)$ and $H_{19}'(T)$. We record the result so far in the following proposition.

Proposition 5.2. *The character polynomials $H_p(T)$ and $H'_p(T)$ of $\rho_2^*(\mathrm{Frob}_p)$ over $\mathbb{Q}_2$ and $K = \mathbb{Q}_2(A) = \mathbb{Q}(A)_{1+A}$, respectively, for primes $5 \le p \le 31$ are as follows.*

p	$H_p(T)$	$H'_p(T)$
5	$T^4 - 41\,T^2 + 625$	$T^2 \pm 3A\,T - 25$
7	$T^4 - 10\,T^3 + 123\,T^2 - 490\,T + 7^4$	$T^2 - 5\,T + 7^2$
11	$T^4 - 17\,T^2 + 11^4$	$T^2 \pm 15A\,T - 11^2$
13	$T^4 + 20\,T^3 + 438\,T^2 + 20 \cdot 13^2\,T + 13^4$	$T^2 + 10\,T + 13^2$
17	$T^4 - 254\,T^2 + 17^4$	$T^2 \pm 18A\,T - 17^2$
19	$T^4 + 32\,T^3 + 978\,T^2 + 32 \cdot 19^2\,T + 19^4$	$T^2 + 16\,T + 19^2$
23	$T^4 - 914\,T^2 + 23^4$	$T^2 \pm 12A\,T - 23^2$
29	$T^4 - 782\,T^2 + 29^4$	$T^2 \pm 30A\,T - 29^2$
31	$T^4 + 2\,T^3 + 1923\,T^2 + 2 \cdot 31^2\,T + 31^4$	$T^2 + T + 31^2$

(Table 1)

In case $p \equiv 2 \pmod 3$, the coefficient of T in $H'_p(T)$ is determined up to sign.

6. Comparison with the representation $\tilde{\rho}_2$ attached to certain cusp forms in $S_3(\Gamma_1(27))$

In the space of weight 3 level 27 cusp forms $S_3(\Gamma_1(27))$, we find from William A. Stein's website two Hecke eigenforms g_a whose q expansion ($q = e^{2\pi i z}$) to order 31 are as follows:

$$\begin{aligned} g_a &= q + aq^2 - 5q^4 - aq^5 + 5q^7 - aq^8 + 9q^{10} - 5aq^{11} - 10q^{13} + 5aq^{14} - 11q^{16} + 6aq^{17} \\ &\quad -16q^{19} + 5aq^{20} + 45q^{22} - 4aq^{23} + 16q^{25} - 10aq^{26} - 25q^{28} + 10aq^{29} - q^{31} + O(q^{32}), \end{aligned}$$

where a is a root of $x^2 + 9$. The character of this modular form is χ_{-3}. Denote by $\tilde{\rho}_2$ the 4-dimensional 2-adic representation of the Galois group of $\mathbb{Q}$ attached to $g_a + g_{-a}$, established by Deligne [4]. The Atkin-Lehner operator W_{27} acts on the curve $X_1(27)$ as an involution, and it is $\mathbb{Q}$-rational. Further, it induces an action of order 4 on the representation space of $\tilde{\rho}_2$ so that $\tilde{\rho}_2$ may be regarded as a 2-dimensional representation over $\mathbb{Q}_2(i) = \mathbb{Q}(i)_{1+i}$. In view of Corollary 5.1, we have

Corollary 6.1. $\det(\rho_2^*) = \det(\tilde{\rho}_2)$.

Fix an isomorphism from K to $\mathbb{Q}_2(i) = \mathbb{Q}(i)_{1+i}$ such that the characteristic polynomial of $\rho_2^*(\mathrm{Frob}_5)$ agrees with that of $\tilde{\rho}_2(\mathrm{Frob}_5)$.

Denote by ρ'_2 the representation ρ_2* viewed over $\mathbb{Q}(i)_{1+i}$. Our goal in this section is to show that ρ'_2 and $\tilde{\rho}_2$ are isomorphic.

To compare two representations from $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to $\mathbf{GL}_2(\mathbb{Z}[i]_{1+i})$, we will apply Serre's method [18] below.

Theorem 6.1 (Serre). *Let ρ_1 and ρ_2 be representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *to* $\mathbf{GL}_2(\mathbb{Z}[i]_{1+i})$. *Assume they satisfy the following two conditions:*

(1) $\det(\rho_1) = \det(\rho_2)$;
(2) *the two homomorphisms from* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *to* $\mathbf{GL}_2(\mathbb{F}_2)$, *obtained from the reductions of ρ_1 and ρ_2 modulo $1+i$, are surjective and equal.*

If ρ_1 and ρ_2 are not isomorphic, then there exists a pair $(\widetilde{G}, t)$, where $\widetilde{G}$ is a group isomorphic to either $S_4 \times \{\pm 1\}$, or S_4, or $S_3 \times \{\pm 1\}$, and the map $t : \widetilde{G} \to \mathbb{F}_2$ has value 0 on the elements of $\widetilde{G}$ of order ≤ 3, and 1 on the other elements.

In Serre's theorem above, $\widetilde{G}$ is a "deviation" group constructed from the two representations, which measures the difference between the two nonisomorphic representations ρ_1 and ρ_2 satisfying the conditions (1)-(2), and the map t, arising from comparing traces, tells where the "deviation" between the two representations occurs. In particular, at elements s in $\widetilde{G}$ of order at least 4, $\rho_1(s)$ and $\rho_2(s)$ have different trace. Therefore, to show that ρ_1 and ρ_2 are isomorphic (and necessarily they ramify at the same places), we search for Galois extensions of $\mathbb{Q}$ with Galois groups isomorphic to those listed in the theorem above, and unramified where the representations are unramified. In each of such extensions, if we can find a Frobenius element of order ≥ 4 in the Galois group at which ρ_1 and ρ_2 have the same trace, then they must be isomorphic. See the explanation in [18] for more detail.

Corollary 6.1 shows that condition (1) holds. We now proceed to prove that both representations satisfy condition (2) as well. Note that the residue field of $\mathbb{Q}(i)$ at $1+i$ is $\mathbb{F}_2$, hence the reductions of ρ_2' and $\tilde{\rho}_2$ mod $1+i$ yield two representations of the Galois group of $\mathbb{Q}$ to $GL_2(\mathbb{F}_2)$. While we do not know the characteristic polynomial of the Frobenius at almost all primes $p \geq 5$ for the representation ρ_2', we do know them modulo $1+i$ for $5 \leq p \leq 31$ from Table 1, and it is easy to check that they agree with those from representation $\tilde{\rho}_2$ mod $1+i$. Thus condition (2) for our two representations will follows from

Lemma 6.1. *There is only one representation ρ from* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *to* $\mathbf{GL}_2(\mathbb{F}_2)$, *unramified outside 2 and 3, such that the characteristic polynomial of $\rho(\mathrm{Frob}_p)$ is equal to H_p' mod $(1+A)$ from Table 1 for primes $p = 5, 7, 13$. Further ρ is surjective.*

Proof. The existence is obvious. We prove the uniqueness. Note that $\mathbf{GL}_2(\mathbb{F}_2)$ is isomorphic to the symmetric group on three letters S_3, which is generated by an element of order 2 and an element of order 3. Denote by σ the sign homomorphism from S_3 to $\{\pm 1\}$, and by ε the composition $\sigma \circ \rho$. Then ε is a character of the Galois group of $\mathbb{Q}$ of order at most two and it is unramified outside 2 and 3.

We see from Table 1 that the characteristic polynomials of $\rho(\mathrm{Frob}_5)$ and $\rho(\mathrm{Frob}_7)$ are $T^2 + T + 1$, hence $\rho(\mathrm{Frob}_5)$ and $\rho(\mathrm{Frob}_7)$ both have order 3. The characteristic polynomial of $\rho(\mathrm{Frob}_{13})$ is $T^2 + 1$, hence $\rho(\mathrm{Frob}_{13})$ has order 1 or 2. In particular, $\varepsilon(\mathrm{Frob}_p) = 1$ for $p = 5, 7$.

If ε is nontrivial, then it arises from a quadratic extension of $\mathbb{Q}$ unramified outside 2 and 3. Such extensions are $\mathbb{Q}(\sqrt{d})$ with $d = 2, 3, 6, -1, -2, -3, -6$. Since 5 is inert in $\mathbb{Q}(\sqrt{d})$ with $d = 2, 3, -2, -3$ and 7 is inert in $\mathbb{Q}(\sqrt{d})$ with $d = 6, -1$, this leaves $\varepsilon = \left(\frac{-6}{\cdot}\right)$ or $\varepsilon = 1$ as the only possibilities.

Assume $\varepsilon = 1$. Then ρ factors through $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow C_3 \subset \mathbf{GL}_2(\mathbb{F}_2)$. But the unique C_3 extension of $\mathbb{Q}$ unramified outside of $\{2, 3\}$ is $\mathbb{Q}(\zeta_9 + \zeta_9^{-1})$, in which primes $p \equiv \pm 1 \mod 9$ split completely. Hence

$$\mathrm{ord}\,(\rho(\mathrm{Frob}_p)) = \begin{cases} 1 & \text{if} \quad p \equiv \pm 1 \mod 9, \\ 3 & \text{if} \quad p \not\equiv \pm 1 \mod 9. \end{cases}$$

This contradicts the fact that $\rho(\mathrm{Frob}_{13})$ has order at most 2.

Therefore $\varepsilon = \left(\frac{-6}{\cdot}\right)$ and ρ is surjective.

Finally, we know that $\mathrm{Ker}(\rho) = \mathrm{Gal}(\overline{\mathbb{Q}}/K_6)$ for some S_3-Galois extension K_6 of $\mathbb{Q}$ containing the quadratic field $\mathbb{Q}(\sqrt{-6})$ and with discriminant of type $\pm 2^\alpha 3^\beta$. Such a field K_6 is unique by applying the class field theory to the extension K_6 over $\mathbb{Q}(\sqrt{-6})$. And it is given as the splitting field of a cubic polynomial over $\mathbb{Q}$:

$$K_6 = \mathrm{Split}(x^3 + 3x - 2)$$

from the table by H. Cohen in [2]. The uniqueness of ρ then follows from the uniqueness of K_6 and the uniqueness of degree 2 irreducible representation over $\mathbb{F}_2$ of S_3. $\square$

Now we are ready to apply Serre's theorem to our representations ρ_2' and $\tilde{\rho}_2$. It follows from the above proof that the fixed field of the possible deviation group $\widetilde{G}$ contains the field K_6. We start by finding all quartic fields M with $\mathrm{Gal}(M/\mathbb{Q}) = S_4$, which contain K_6 and are unramified outside 2 and 3. There are three such fields. Listed below are their defining equations, discriminants, and certain primes p such that Frob_p is of order 4 in the group $\mathrm{Gal}(L/\mathbb{Q})$.

defining equation	discriminant	p with order 4 Frobenius
$x^4 - 4x - 3 = 0$	$(-216) \cdot 8^2 = -2^9 \cdot 3^3$	13, 17, 19, 23
$x^4 - 8x + 6 = 0$	$(-216) \cdot 16^2 = -2^13 \cdot 3^3$	13, 17
$x^4 - 12x^2 - 16x + 12 = 0$	$(-216) \cdot 16^2 = -2^13 \cdot 3^3$	19, 23

As $H_p'(T)$ agrees with the characteristic polynomial of $\tilde{\rho}_2(\mathrm{Frob}_p)$ for primes $p = 13, 19$, the value of t at such Frob_p is zero. Hence we may rule out two possible deviation groups $\widetilde{G} = S_4 \times \{\pm 1\}$ and $\widetilde{G} = S_4$. For the case $\widetilde{G} = S_3 \times \{\pm 1\}$, elements of interest are those primes $p \neq 2, 3$ such that

(6.i) Frob_p has order 3 in S_3, which is equivalent to the trace of Frob_p being odd under both representations;

and

(6.ii) There is a quadratic extension $\mathbb{Q}(\sqrt{d})$ of $\mathbb{Q}$, unramified outside 2 and 3, in which p is inert.

(Consequently, Frob_p in $\widetilde{G}$ has order 6.) For the second statement, we consider $\mathbb{Q}(\sqrt{d})$ with $d = 2, 3, 6, -1, -2 - 3$ since $\mathbb{Q}(\sqrt{-6})$ is contained in K_6 and $\mathrm{Gal}(K_6/\mathbb{Q})$ is S_3. As 5 is inert in $\mathbb{Q}(\sqrt{d})$ with $d = 2, 3, -2, -3$ and 7 is inert in $\mathbb{Q}(\sqrt{d})$ with $d = -1, 6$, and the trace of Frob_p is odd at $p = 5, 7$ under both representations, we may take p to be 5 or 7. On the other hand, Frob_p has the same trace under ρ_2' and $\tilde{\rho}_2$ for $p = 5, 7$. Hence the last case of $\widetilde{G}$ is also eliminated, and ρ_2' and $\tilde{\rho}_2$ are isomorphic. We record this in

Theorem 6.2. *The two representations ρ_2^* and $\tilde{\rho}_2$ are isomorphic.*

It is worth pointing out that this theorem uses the information of H_p for primes $5 \le p \le 19$ only. Further, the $H_p'(T)$'s for $p \equiv 1 \pmod 3$ in Table 1 are uniquely determined, given by the characteristic polynomial of $\tilde{\rho}_2(\mathrm{Frob}_p)$ as in the list below.

Corollary 6.2. *The characteristic polynomials $H_p(T)$ and $H_p'(T)$ of $\rho_2^*(\mathrm{Frob}_p)$ over $\mathbb{Q}_2$ and $K = \mathbb{Q}_2(A) = \mathbb{Q}(A)_{1+A}$, respectively, for primes $5 \le p \le 31$ are as follows.*

p	$H_p(T)$	$H_p'(T)$
5	$T^4 - 41\,T^2 + 625$	$T^2 - 3A\,T - 25$
7	$T^4 - 10\,T^3 + 123\,T^2 - 490\,T + 7^4$	$T^2 - 5\,T + 7^2$
11	$T^4 - 17\,T^2 + 11^4$	$T^2 - 15A\,T - 11^2$
13	$T^4 + 20\,T^3 + 438\,T^2 + 20 \cdot 13^2\,T + 13^4$	$T^2 + 10\,T + 13^2$
17	$T^4 - 254\,T^2 + 17^4$	$T^2 + 18A\,T - 17^2$
19	$T^4 + 32\,T^3 + 978\,T^2 + 32 \cdot 19^2\,T + 19^4$	$T^2 + 16\,T + 19^2$
23	$T^4 - 914\,T^2 + 23^4$	$T^2 - 12A\,T - 23^2$
29	$T^4 - 782\,T^2 + 29^4$	$T^2 + 30A\,T - 29^2$
31	$T^4 + 2\,T^3 + 1923\,T^2 + 2 \cdot 31^2\,T + 31^4$	$T^2 + T + 31^2$

(Table 2)

Finally we prove

Theorem 6.3. *The representations ρ_2, ρ_2^*, and $\tilde{\rho}_2$ are isomorphic to each other.*

Proof. We know from Theorem 6.2 that ρ_2^* and $\tilde{\rho}_2$ are isomorphic. Further, by Proposition 5.1, ρ_2 is isomorphic to $\rho_2^* \otimes \phi_2$ for some character ϕ_2 of order at most 2. Therefore it remains to determine ϕ_2. Since ρ_2 and ρ_2^* are unramified outside 2 and 3, the character ϕ_2, if nontrivial, is associated to a quadratic field $\mathbb{Q}(\sqrt{d})$ with $d = 2, 3, 6, -1, -2, -3, -6$. Write $\phi(p)$ for $\phi_2(\mathrm{Frob}_p)$ for brevity. For odd primes $p \ge 5$, the characteristic polynomial of $\rho_2(\mathrm{Frob}_p)$ is

$$\tilde{H}_p(T) := T^4 - C_1(p)\phi(p)T^3 + C_2T^2 - p^2C_1(p)\phi(p)T + p^4,$$

where

$$H_p(T) = T^4 - C_1(p)T^3 + C_2T^2 - p^2C_1(p)T + p^4$$

is the characteristic polynomial of $\rho_2^*(\mathrm{Frob}_p)$. By Theorem 1.1, the cusp form

$$f_+(\tau) = \sum_{n\geq 1} a(n)q^{n/15} = q^{1/15} + iq^{2/15} - \frac{11}{3}q^{4/15} - i\frac{16}{3}q^{5/15} - \frac{4}{9}q^{7/15} + i\frac{71}{9}q^{8/15} + \frac{932}{81}q^{10/15} + \cdots,$$

in $S_3(\Gamma)$ satisfies the congruence relation

$$\mathrm{ord}_p((a(np^2) - C_1(p)\phi(p)a(np) + C_2(p)a(n) - p^2C_1(p)\phi(p)a(n/p) + p^4a(n/p^2)) \geq 2(\mathrm{ord}_p n + 1)$$

for all $n \geq 1$ and $p \geq 5$. Applying this congruence relation to $n = 1$, $p = 7, 13$ and using the explicit values of $C_1(p), C_2(p)$ from Proposition 5.2 as well as the known Fourier coefficients of f_+ from §4, we find that $\phi(7) = \phi(13) = 1$. Therefore either ϕ_2 is trivial or ϕ_2 is χ_{-3}, the quadratic character attached to the field $\mathbb{Q}(\sqrt{-3})$. On the other hand, the two newforms g_{3i} and g_{-3i} are twist of each other by χ_{-3}, which in turn implies that the representation $\tilde{\rho}_2$ is invariant under twisting by χ_{-3}, and hence so is ρ_2^*. Therefore in both cases of ϕ_2 we have ρ_2 isomorphic to ρ_2^*. □

7. The Atkin-Swinnerton-Dyer congruence relations

As discussed in §4, the operator A is defined over $\mathbb{Q}$ and it commutes with the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Further, A diagonalizes the space $S_3(\Gamma)$ with eigenvectors $f_\pm$. Following the notation in Scholl's proof of Theorem 1.1 presented in section 5 of [12], we may choose f_1 and f_2 as a basis of $S_3(\Gamma, \mathbb{Z}_p)$ of forms in $S_3(\Gamma)$ with Fourier coefficients in $\mathbb{Z}_p$ for any prime $p \neq 2, 3$. Then the matrix $\mathbf{C}$ such that $p^2\mathbf{C}$ represents the action of the Frobenius F on $S_3(\Gamma, \mathbb{Z}_p)$ identified as a quotient space is diagonalizable. The same is true for the matrix $\mathbf{A} = \mathbf{C^{-1}} + p^2\mathbf{C}$. Consequently, by Remark 5.8 of [12], f_+ (resp. f_-) satisfies the congruence relation (7) with respect to $H_p'(T)$ (resp. $H_p''(T)$). Recall that the characteristic polynomial of $\rho_2(\mathrm{Frob}_p)$ is $H_p(T)$, which is the product $H_p'(T)H_p''(T)$ as discussed in §5. Finally we note that $H_p'(T)$ (resp. $H_p''(T)$) is nothing but the characteristic polynomial of the $(1+i)$-adic representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ attached to $g_+ = g_{-3i}$ (resp. $g_- = g_{3i}$). Hence f_+ and g_+ (resp. f_- and g_-) satisfy the Atkin-Swinnerton-dyer congruence relations. This completes the proof of Theorem 1.2.

8. The Atkin-Swinnerton-Dyer congruence relations and elliptic modular K3 surfaces over $\mathbb{Q}$

In this section we derive similar results for the Atkin-Swinnerton-Dyer congruence relations arising from K3 surfaces over $\mathbb{Q}$.

First consider an explicit example. Let Γ_2 denote the group associated to the algebraic equation (12). A similar discussion shows that this is a non-congruence subgroup. The space $S_3(\Gamma_2)$ of weight 3 cusp forms for Γ_2 is 1-dimensional and it is generated by

$$h_2 = \sqrt{E_1E_2} = q^{1/10} - \frac{3^2}{2}q^{3/10} + \frac{3^3}{2^3}q^{5/10} + \frac{3\cdot 7^2}{2^4}q^{7/10} - \frac{3^2\cdot 7\cdot 19}{2^7}q^{9/10} + O(q^{10/10})$$

where E_1 and E_2 are given by (17) and (18) respectively. It is clear that the Fourier expansion of h_2 at the cusp ∞ has coefficients in the ring $\mathbb{Z}[1/2]$. Let g_2 be a level 16 newform with the first few terms of its Fourier expansion (provided by Stein's data base) as

$$g_2 = q - 6q^5 + 9q^9 + 10q^{13} - 30q^{17} + 11q^{25} + 42q^{29} + O(q^{32})$$

Using Serre's method, we can show that the Atkin-Swinnerton-Dyer congruence relation holds for h_2 and g_2. In fact, a more general result regarding this situation can be proved.

Recall that a *K3 surface* S is a simply connected compact complex surface with trivial canonical bundle. Its Hodge diamond, as the one defined in section 2, is

$$\begin{array}{ccccc} & & 1 & & \\ & 0 & & 0 & \\ 1 & & 20 & & 1 \\ & 0 & & 0 & \\ & & 1 & & \end{array}$$

Hence as a compact complex surface, its Picard number $\rho(S) \leq h^{1,1} = 20$. The cohomology group $\Lambda = H^2(S,\mathbb{Z})$ is a rank 22 free $\mathbb{Z}$-module, called a K3 lattice. As a lattice, Λ is unimodular due to the Poincaré duality, even by Wu's formula, with signature (3, 19) by the Hodge index theorem. Its Néron-Severi group $NS(S)$, defined as in section 2, is a sublattice of Λ of signature $(1, \rho(S)-1)$ again by the Hodge index theorem. An *elliptic surface* $\pi : S \to C$ is a two dimensional complex variety over the base curve C such that every fiber $\pi^{-1}(t)$ is a smooth genus one curve except for finitely many points t in C. A compact elliptic surface is called an *elliptic modular surface* if its monodromy group Γ_S is a finite index subgroup of $SL_2(\mathbb{Z})$ and $-I \notin \Gamma_S$ [19].

Theorem 8.1. *Let S be an elliptic modular K3 surface defined over $\mathbb{Q}$ with Γ_S being the associated modular group. Let f_{Γ_S} be a nonzero M-integral form in the 1-dimensional space $S_3(\Gamma_S)$ for some integer M. Then there is a weight 3 cusp form g_{Γ_S} with integral Fourier coefficients for some congruence subgroup such that f_{Γ_S} and g_{Γ_S} satisfy the Atkin-Swinnerton-Dyer congruence relations.*

Proof. Since S is an elliptic modular K3 surfaces, by Shioda's result [19], its Picard number $\rho(S) = 20$. Further, the work of Shioda and Inose [22] on K3 surfaces with Picard number 20 shows that the Hasse-Weil L-function attached to S contains a factor $L(s,\chi^2)$, where χ

is a Grossencharacter of some imaginary quadratic extension of $\mathbb{Q}$ associated to an elliptic curve over $\mathbb{Q}$ with complex multiplications, arising from the K3 lattice of S. Combining the analytic behavior of $L(s,\chi^2)$ proved by Hecke and the converse theorem for GL_2 proved by Weil, we know that $L(s,\chi^2)$ is also the L-function attached to a weight 3 cuspidal newform h_{Γ_S} with integral coefficients for a congruence subgroup.

Let $\rho_l(S)$ be the l-adic representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ associated to h_{Γ_S}, which exists for almost all primes l. In particular, this representation is isomorphic to ρ_l^* defined in section 5 induced by the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on W_l. This isomorphism of representations can be seen explicitly via the characteristic polynomials of Frobenius elements. Due to a trace formula of Monsky [9], for almost all prime p, the Euler p-factor $P_{21,p}(p^{-s})$ of the L-function of h_{Γ_S} appears as one part of the characteristic polynomial of the Frobenius endomorphism F_p acting on the crystalline cohomology $H^2_{cris}(\mathcal{S}_p/\mathbb{Z}_p)$, where $\mathcal{S}_p$ is the Néron minimal model of S over $\mathbb{F}_p$. In particular, $F_{21,p}(p^{-s})$ corresponds to the characteristic polynomial of F_p acting on the orthogonal complement of the Néron-Severi group $NS(\mathcal{S}_p \otimes \bar{\mathbb{F}}_p) \otimes \mathbb{Q}$ in $H^2_{cris}(\mathcal{S}_p/\mathbb{Z}_p) \otimes \mathbb{Q}$, where $\bar{\mathbb{F}}_p$ is the algebraic closure of $\mathbb{F}_p$ (for details see [23] §12). By the Lefschetz fixed point theorem, the coefficients of $F_{21,p}(p^{-s})$ can be calculated by the same trace formula [14] §3 for the Frobenius endomorphism on $Frob_p$ on the l-adic cohomology W_l.

Denote by $\rho_l(\Gamma_S)$ the l-adic representation of the Galois group of $\mathbb{Q}$ associated to the space $S_3(\Gamma_S)$ constructed by Scholl in [12]. By Proposition 5.1, $\rho_l(\Gamma_S)$ and $\rho_l(S)$ are isomorphic up to a quadratic twist. Let ϕ be a character of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of order at most two such that $\rho_l(\Gamma_S)$ is isomorphic to $\rho_l(S) \otimes \phi$. By class field theory, we may regard ϕ as a Dirichlet character of order at most two. Let g_{Γ_S} be the newform having the same eigenvalues as the twist of h_{Γ_S} by ϕ. Then g_{Γ_S} also has integral Fourier coefficients and $\rho_l(\Gamma_S)$ is isomorphic to the l-adic representation attached to g_{Γ_S}. Applying Theorem 1.1 to $\rho_l(\Gamma_S)$ and f_{Γ_S}, we conclude that f_{Γ_S} and g_{Γ_S} satisfy the Atkin-Swinnerton-Dyer relation. □

References

[1] *A. O. L. Atkin and H. P. F. Swinnerton-Dyer*, Modular forms on non-congruence subgroups, Combinatorics (Proc. Sympos. Pure Math., Vol. XIX, Univ. California, Los Angeles, Calif., 1968), Amer. Math. Soc., Providence, R.I., (1971), 1–25.

[2] *H. Cohen,* Introduction to computational number theory, GTM 138

[3] *D. A. Cox and W. R. Parry*, Torsion in elliptic curves over $k(t)$, Compositio Math. **41** (1980), no. 3, 337–354.

[4] *P. Deligne*, Formes modulaires et représentations de gl(2), Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, (1973), 55–105. Lecture Notes in Math., Vol. 349.

[5] *M. Eichler*, Eine Verallgemeinerung der Abelschen Integrale, Math. Z. **67** (1957), 267–298.

[6] *L. Kodaira,* On compact analytic surfaces, II, III, Ann. of Math. **(2) 77** (1963), 563–626; ibid. **78** (1963), 1–40.

[7] *R. Levné and N. Yui*, The modularity of certain non-rigid Calabi-Yau threefolds math.AG/0304497 (2003).

[8] *R. Miranda and U. Persson*, On extremal rational elliptic surfaces, Math. Z. **193** (1986), no. 4, 537–558.

[9] *P. Monsky*, Formal cohomology. III. Fixed point theorems, Ann. of Math. (2) **93** (1971), 315–343.

[10] *M. Nori,* On certain elliptic surfaces with maximal Picard number, Topology **24** (1985), no. 2, 175–186.

[11] *A. Ogg*, Modular forms and Dirichlet series, W. A. Benjamin, Inc., New York-Amsterdam, (1969).

[12] *A. J. Scholl,* Modular forms and de Rham cohomology; Atkin-Swinnerton-Dyer congruences, Invent. Math. **79** (1985), 49–77

[13] —–, Modular forms on noncongruence subgroups. Séminaire de Théorie des Nombres, Paris 1985-86, Progr. Math. 71, Birkhäuser Boston, boston, MA, (1987), 199–206.

[14] —–, The l-adic representations attached to a certain non-congruence subgroup, J. Reine Angew. Math. **392** (1988), 1–15.

[15] —–, The l-adic representations attached to non-congruence subgroups II, preprint, (1993).

[16] —–, On the Hecke algebra of a noncongruence subgroup, Bull. London Math.Soc. **29** (1997), 395–399.

[17] *A. Sebbar,* Classification of torsion-free genus zero congruence groups, Proc. Amer. Math. Soc. **129** (2001), no. 9, 2517–2527 (electronic).

[18] *J. P. Serre,* Résumé de cours, 1984-5, Collège de France

[19] *T. Shioda,* On elliptic modular surfaces, J. Math. Soc. Japan **24** (1972), 20–59.

[20] *G. Shimura*, Sur les intégrales attachées aux formes automorphes, J. Math. Soc. Japan **11** (1959), 291–311.

[21] *G. Shimura*, Introduction to the arithmetic theory of automorphic functions, Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo, (1971), Kanô Memorial Lectures, No. 1.

[22] *T. Shioda and H. Inose*, On singular $K3$ surfaces, Complex analysis and algebraic geometry, Iwanami Shoten, Tokyo, (1977), 119–136.

[23] *J. Stienstra and F. Beukers*, On the Picard-Fuchs equation and the formal Brauer group of certain elliptic $K3$-surfaces, Math. Ann. **271** (1985), no. 2, 269–304.

[24] *J. Thompson,* Hecke operators and non congruence subgroups, Group Theory, de Gruyter, New York, (1989), 219–224.

Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA

E-mail address: `wli@math.psu.edu`

Department of Mathematics, Iowa State University, Ames, IA 50011, USA

E-mail address: `linglong@iastate.edu`

Department of Mathematics, Capital Normal University, Beijing 100037, P.R.China

E-mail address: `yangzf@mail.cnu.edu.cn`