MODULAR FORMS ON NONCONGRUENCE SUBGROUPS AND ATKIN-SWINNERTON-DYER RELATIONS

LIQUN FANG, J. WILLIAM HOFFMAN, BENJAMIN LINOWITZ, ANDREW RUPINSKI, HELENA VERRILL

Abstract. We give an example of a noncongruence subgroup $\Gamma \subset \mathrm{SL}(2, \mathbf{Z})$ whose space of weight 3 cusp forms $S_3(\Gamma)$ admits a basis satisfying the Atkin-Swinnerton-Dyer congruence relations with respect to a weight 3 newform for a certain congruence subgroup. 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

Let $\Gamma \subset \mathrm{SL}(2, \mathbf{Z})$ be a subgroup of finite index. We distinguish two cases:

1. Γ is a congruence subgroup. This means that Γ contains
$$\Gamma(N) \;=\; \{\gamma \in \mathrm{SL}(2, \mathbf{Z}) \mid \gamma \equiv I \bmod N\}$$
for some integer $N \geq 1$.
2. Γ is a noncongruence subgroup, which means that it is not a congruence subgroup.

Recall that $\mathrm{SL}(2, \mathbf{R})$ acts on the upper half-plane of complex numbers $\mathbf{H}$ by linear fractional transformations. For any Γ as above the quotient $\Gamma\backslash\mathbf{H}$ is a Riemann surface, which on adding a finite number of points (cusps) becomes compact. It is known that this Riemann surface is the set of $\mathbf{C}$-points of an algebraic curve defined over a finite extension K of $\mathbf{Q}$. If Γ is a congruence subgroup the explicit K-model of this Riemann surface is a moduli space for a family of elliptic curves with additional structures. We let $M_k(\Gamma)$, resp. $S_k(\Gamma)$, denote the finite-dimensional vector space of modular forms, resp. cusp forms, for Γ. Also $S_k(\Gamma_0(N), \chi)$ is the space of cusp forms with character $\chi : (\mathbf{Z}/N)^* \to \mathbf{C}^*$.

There is a vast theory of modular forms when Γ is a congruence subgroup. Key points are the action of the Hecke algebra $\mathbf{T}$ on the spaces of modular forms, the theory of newforms, and the L-functions associated to the Hecke eigenfunctions. General reference: [Shi71]. Recall:

Date: September 17, 2004.

This research was carried out as part of an REU summer program at LSU, supported by the National Science Foundation grant DMS-0353722 and a Louisiana Board of Regents Enhancement grant, LEQSF (2002-2004)-ENH-TR-17.

Theorem 1.1. *Let $0 \neq f \in M_k(\Gamma_0(N), \chi)$. Suppose that $k \geq 2$ and that f is an eigenfunction of $T_p \in \mathbf{T}$, all $p \nmid N$, with eigenvalue a_p. Let K be the necessarily finite extension of $\mathbf{Q}$ generated by the a_p and the $\chi(p)$. Let λ be a finite place of K, of residual characteristic l, and let K_λ be the completion of K in λ. There exists a semisimple continuous representation*

$$\rho_\lambda : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}(2,\, K_\lambda)$$

which is unramified outside Nl and such that

$$\mathrm{Tr}(\rho_\lambda(\mathrm{Frob}_p)) = a_p, \quad \det(\rho_\lambda(\mathrm{Frob}_p)) = \chi(p)p^{k-1}, \text{ if } p \nmid Nl.$$

The above statement is taken from [DS74], and the result is commonly attributed to Deligne, although a complete proof seems not to have been published by him. See the remark 6.2 in [DS74] for more precisions on this.

For $N \geq 1$ a positive integer let $X(N)$ be the coarse moduli scheme associated to the functor $F_N : (\mathrm{Schemes}/\mathbf{Z}[1/N]) \to (\mathrm{Sets})$:

$$F_N(S) = \left\{ \begin{matrix} (E, \alpha), \text{ where } E/S \text{ is a generalized elliptic curve} \\ \alpha : E[N] \xrightarrow{\sim} \mu_N \times \mathbf{Z}/N \text{ is an isomorphism of determinant one} \end{matrix} \right\}$$

and let $j : Y(N) \hookrightarrow X(N)$ be the inclusion of the open subset corresponding to smooth E/S (a summary of properties of these can be found in [Sch85ii], with details in [DR73],[KM85] and [Con]). When $N = 1$ this is the j-line. One has

$$X(N)^{\mathrm{an}} = X(N)(\mathbf{C}) = \Gamma(N)\backslash\mathbf{H}^*.$$

$X(N)$ is proper and smooth over $\mathbf{Z}[1/N]$ and its geometric fibers are irreducible curves. $X(N) \otimes \mathbf{Q}$ is the curve denoted Γ_N in [Shi58, p. 11] and the function field $\mathbf{Q}(X(N))$ is the field of all modular functions of level N whose Fourier expansion relative to $q^{1/N} = e^{2\pi iz/N}$ have coefficients in $\mathbf{Q}$. When $N \geq 3$ this scheme represents the corresponding functor. In that case we let $f : E \to Y(N)$ be the universal elliptic curve. Recall the parabolic cohomology groups

$$\begin{aligned} {}^k_N V_B &= H^1(X(N)^{\mathrm{an}},\, j_*\mathrm{Sym}^k R^1 f_* \mathbf{Q}) \\ {}^k_N V_l &= H^1_{et}(X(N) \otimes \overline{\mathbf{Q}},\, j_*\mathrm{Sym}^k R^1 f_* \mathbf{Q}_l) \\ &\cong {}^k_N V_B \otimes_{\mathbf{Q}} \mathbf{Q}_l. \end{aligned}$$

Then

$${}^k_N V_{DR} = {}^k_N V_B \otimes \mathbf{C} = S_{k+2}(\Gamma(N)) \oplus \overline{S_{k+2}(\Gamma(N))}$$

which is a Hodge decomposition of type $(k+1, 0) + (0, k+1)$.

Theorem 1.2. *The canonical representation*

$$\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}({}^k_N V_l)$$

is unramified outside Nl, is pure of weight $k+1$, and

$$\det(1-\rho(\mathrm{Frob}_p)U) = \det(1 - T_pU + pS_pU^2 \mid S_{k+2}(\Gamma(N)))$$

for all $p \nmid Nl$. Here T_p and S_p are the standard Hecke operators.

This theorem is due to Deligne [Del73] and it extends earlier results of Eichler, Shimura, Kuga and Ihara, [Eic54], [Shi58], [KS65], [I67]. As a consequence, Deligne proved the Ramanujan-Petersson conjecture on the growth of the q-expansion coefficients of cusp forms. Scholl [Sch90] has constructed motives ${}^k_N\mathcal{V}_l$ whose realizations, Betti, deRham, l-adic, are the spaces ${}^k_NV_B$, ${}^k_NV_{DR}$, ${}^k_NV_l$.

Remark. In fact Scholl constructs motives ${}^k_N\mathcal{W}_l$ based not on $X(N)$, but on the the modular curve M_N which parametrizes *all* level N structures (this is also utilized in [Del73]). M_N is not absolutely irreducible over $\mathbf{Q}$: its analytic space is a disjoint union of $\varphi(N)$ copies of the Riemann surface for $\Gamma(N)$. The function field $\mathbf{Q}(M_N)$ is the field of all modular functions of level N whose $q^{1/N}$-expansion coefficients are in $\mathbf{Q}(\zeta_N)$, $\zeta_N = e^{2\pi i/N}$, the field denoted $\mathfrak{F}_N$ in [Shi71, p. 137]. We can recover the ${}^k_NV_l$, etc. from the ${}^k_NW_l$, etc., by taking invariants under

$$H = \left\{ \begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix} \right\} \subset \mathrm{GL}(2,\, \mathbf{Z}/N)$$

which acts on M_N preserving all relevant structures. Note that $M_N/H \cong X(N)$.

Theorem 1.1 follows from theorem 1.2 and from the action of the Hecke algebra: for each newform f of level N one obtains after tensoring with the eigenvalue field K of f, a projector Ψ_f on the l-adic representation. Similar results hold for $N = 1, 2$ by taking appropriate invariants.

The study of modular forms on noncongruence subgroups was initiated by Atkin and Swinnerton-Dyer who performed many computer experiments in the 1960's and discovered emprirically congruences that now bear their names, [ASD71]. A. J. Scholl began a theoretical investigation starting in the 1980's (see [Sch85i], [Sch85ii], [Sch87], [Sch88], [Sch93], [Sch96], [Sch97]). In particular, he constructed l-adic representaions ${}^k_\Gamma V_l$ for any Γ, but there is no simple relation to the Hecke algebra, nor any analog of theorem 1.1, if Γ is noncongruence, for the reason that the Hecke algebra does not act by correspondances on the associated curve $X(\Gamma)$. General philosophy suggests that these l-adic representations should be governed by automorphic representations associated to symplectic groups when k is even, and orthogonal groups when k is odd, but one does not expect classical cusp forms, associated to $\mathrm{GL}(2,\, \mathbf{Q})$, to appear in general when Γ is noncongruence. When $k = 0$, these l-adic representations include the H^1's of essentally all smooth projective curves over $\overline{\mathbf{Q}}$ since by Belyi's theorem, every smooth and projective curve over $\overline{\mathbf{Q}}$ has a nonempty Zariski open subset with a uniformization by a subgroup Γ, generally noncongruence. Moreover, Scholl has given explicit examples of Γ, k where the image of the Galois group is an open subgroup of $\mathrm{GSp}(2d, \mathbf{Q}_l)$, so these cannot be associated to classical cusp forms, [Sch04].

Nonetheless, there are situations where classical cusp forms arise in the l-adic representations of noncongruence subgroups. Let $d = \dim S_{k+2}(\Gamma)$, hence $2d = \dim {}^k_\Gamma V_l$. When $d = 1$ we have a 2-dimensional representation, and one can expect modular forms on congruence subgroups. Scholl examined several examples of these, [Sch88], [Sch93]. For instance if $\Gamma = \Gamma_{711}$, a subgroup of index 9 with three cusps of width 7, 1, 1, he found that

$$\mathrm{Tr}(\mathrm{Frob}_p \mid {}^2_\Gamma V_l) = c_p(g) \text{ for all } p \neq 2, 7, l$$

where $c_p(g)$ is the pth q-expansion coefficient of the unique newform $g \in S_4(\Gamma_0(14), \chi)$ for a certain character χ. Also, by studying the crystalline realization ${}^2_\Gamma V_p$ he was able to prove the ASwD congruences for the expansion coefficients of the unique element $f \in S_4(\Gamma)$, relative to the $\{c_p(g)\}$. Let us recall the definitions.

The Riemann surface $\Gamma\backslash\mathbf{H}^*$ is the set of $\mathbf{C}$-points of an algebraic curve $X(\Gamma)$ defined over a number field K. There exists a subfield L of K, an element $\kappa \in K$ with $\kappa^\mu \in L$, where μ is 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 $f \in S_k(\Gamma)$ is called M-integral if in its Fourier expansion at the cusp ∞

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

the Fourier coefficients $a_n(f)$ can be written as $\kappa^n b_n(f)$ with $b_n(f)$ lying in the ring $O_L[1/M]$, where O_L denotes the ring of integers of L. Note that the expansion coefficients of a modular form on a noncongruence subgroup can have unbounded denominators, contrary to what happens for congruence subgroups.

Let $f = \sum_{n \geq 1} a_n(f) q^{n/\mu}$ be an M-integral cusp form in $S_k(\Gamma)$, and let $g = \sum_{n \geq 1} c_n(g) q^n$ be a normalized newform of weight k level N and character χ. The following definition is taken from [LLY03].

Definition 1.3. *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 $n \geq 1$,*

$$(a_{np}(f) - c_p(g) a_n(f) + \chi(p) p^{k-1} a_{n/p}(f))/(np)^{k-1} \tag{2}$$

is integral at all places dividing p.

Scholl proved the following in [Sch85ii]

Theorem 1.4. *Suppose that $X(\Gamma)$ has a model over $\mathbf{Q}$ as before. Attached to $S_k(\Gamma)$ is a compatible family of $2d$-dimensional l-adic representations ρ_l of the Galois group $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ unramified outside lM such that for primes $p > k+1$ not dividing Ml, the following hold.*

(i) The characteristic polynomial

$$H_p(T) = \sum_{0 \le r \le 2d} B_r(p) T^{2d-r} \tag{3}$$

of $\rho_l(\mathrm{Frob}_p)$ *lies in* $\mathbf{Z}[T]$ *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*

(4)

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

for $n \ge 1$*.*

Thus, if $d = 1$, and $f \in S_k(\Gamma)$ is M-integral, it will satisfy ASwD congruences relative to a newform g on a congruence subgroup if one can prove that the l-adic representation above is *modular*, that is, isomorphic with the representation attached by Deligne to the newform g.

In a recent paper, Li, Long and Yang [LLY03] have given the first example with $d = 2$ and $k \ge 3$ where one can establish ASwD relations for a noncongruence subgroup. Their Γ is of index three inside $\Gamma_1(5)$, and they show the existence of a basis f_+, f_- of $S_3(\Gamma)$ which satisfies ASwD relations relative to a basis g_+, g_- of $S_3(\Gamma_0(27), \chi)$, where χ is the unique character of order 2 and conductor 3. Since $\Gamma_1(5)$ is a normal subgroup of index 4 in $\Gamma_0(5)$ there is $A \in \Gamma_0(5)$ of order 4 that acts on the curve $X_1(5) \sim \mathbf{P}^1$ permuting the four cusps in pairs. Γ corresponds to the cyclic covering of degree 3: $X(\Gamma) \to X_1(5)$ that ramifies the two cusps of width 5, and A extends to an operator on $X(\Gamma)$ and also on the elliptic surface $E \to X(\Gamma)$ gotten by pulling back the universal elliptic curve over $X_1(5)$. Thus $S_k(\Gamma)$ is an A-module. When $k = 3$ this is two-dimensional, and $f_\pm$ are the A-eigenvectors with eigenvalues $\pm i$. The operator A also commutes with the action of the Galois group on the 4-dimensional ${}^1_\Gamma V_l$.

Heuristically, the success of their method can be understood as follows. There is a nondegenerate bilinear pairing

$$b : {}^1_\Gamma V_l \otimes {}^1_\Gamma V_l \longrightarrow \mathbf{Q}_l(-2)$$

which is symmetric since $k = 1$ is odd. Thus the Galois representation ρ takes values in the group of orthogonal similitudes $\mathrm{GO}(b)$. It is well-known that $\mathrm{SO}(4, \mathbf{C}) = \mathrm{SL}(2, \mathbf{C}) \times \mathrm{SL}(2, \mathbf{C})$ up to covering. We may regard ${}^1_\Gamma V_l$ as a rank 2 module over $\mathbf{Q}(A) \otimes \mathbf{Q}_l = \mathbf{Q}(i) \otimes \mathbf{Q}_l$, and the Galois representation takes values in $\mathrm{GO}(b) \subset G(\mathbf{Q}_l)$ where

$$G = \mathrm{Res}_{\mathbf{Q}}^{\mathbf{Q}(i)}(\mathrm{GL}(2)),$$

which is a form of $\mathrm{GL}(2) \times \mathrm{GL}(2)$. One then expects that ρ should be automorphic for this G, which means that we expect to find a pair of newforms

$g_\pm$ with coefficients in $\mathbf{Q}(i)$ and conjugate under $i \to -i$, such that

$$\mathrm{Tr}(\mathrm{Frob}_p \mid {}^1_\Gamma V_l) = c_p(g_+) + c_p(g_-)$$

for almost all p, which is exactly what LLY found. Similar results should be true for k odd and $d = 2$, or for any k in which there are sufficient symmetries to decompose the l-adic representation into pieces with $d \le 2$, this being what happens for congruence subgroups, the symmetries coming from the Hecke algebra.

2. The method

We give another example of a noncongruence subgroup Γ, with $\dim S_3(\Gamma) = 2$ for which we can establish modularity and ASwD congruences. The example in [LLY03] is of index three in $\Gamma_1(5)$, which is one of the 6 torsion free genus 0 subgroups of index 12 in $\mathbf{PSL}(2,\mathbf{Z})$ identified by Sebbar [Seb01]. We use the same construction, but applied to another subgroup on this list. Namely, we define a subgroup Γ of index 3 inside $\Gamma' = \Gamma_0(8) \cap \Gamma_1(4)$, whose image in PSL(2, $\mathbf{Z}$) is of index 12, by constructing an explicit covering $X(\Gamma) \to X(\Gamma')$ of degree 3 with certain ramification properties. We identify an operator A that normalizes Γ' and extends to an automorphism of $X(\Gamma)$ and also to the elliptic surface $E \to X(\Gamma)$. That done, we find explicit q-expansions for the cusp forms in $S_3(\Gamma)$, which is a 2-dimensional space. Next, we compute a table of traces of Frob_p and Frob_{p^2} acting on $H^1(X(\Gamma),\mathcal{F})$, where $\mathcal{F} = j_* R^1 f_* \mathbf{Q}_l$. This is an application of the Grothendieck-Lefschetz formula which asserts here that

$$\mathrm{Tr}(\mathrm{Frob}_q | H^1(X(\Gamma),\mathcal{F})) = -\sum_{x \in X(\mathbf{F}_q)} \mathrm{Tr}(\mathrm{Frob}_x | \mathcal{F}_x).$$

(Note that $H^i(X(\Gamma),\mathcal{F}) = 0$ for $i = 0, 2$.) The local traces are of two types:

1. The fiber E_x is smooth. Then

$$\mathrm{Tr}(\mathrm{Frob}_x|\mathcal{F}_x) = \mathrm{Tr}(\mathrm{Frob}_x|H^1(E_x,\mathbf{Q}_l)) = q + 1 - \#E_x(\mathbf{F}_q).$$

2. The fiber E_x is singular. Tate's algorithm ([Tate72]) is then used to determine the fiber in the minimal model of the reduction mod x. Then

$$\mathrm{Tr}(\mathrm{Frob}_x|\mathcal{F}_x) = \begin{cases} 1 \text{ if the fiber is split multiplicative.} \\ -1 \text{ if the fiber is nonsplit multiplicative.} \\ 0 \text{ if the fiber is additive.} \end{cases}$$

Code was written in Magma to accomplish this. Next, William Stein's tables ([Stein]) were searched to find spaces of cusp forms on congruence subgroups that matched the traces we computed. The modular forms having been found, the method of Faltings/Serre/Livné ([Fal83], [Ser84], [Liv87])is applied to establish rigorously that the Galois representation

$${}^1_\Gamma V_l = H^1(X(\Gamma),\mathcal{F})$$

is isomorphic to the one coming from this space of cusp forms. The ASwD congruences then follow from the general theory developed in [Sch85i], [Sch85ii]. Our main result is

Theorem 2.1. *1.) Let*

$$\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathbf{GL}({}_\Gamma^1 V_l)$$

be the 4-dimensional Galois representation constructed by Scholl associated to the cusp forms of weight 3 on the noncongruence subgroup $\Gamma \subset \Gamma_0(8) \cap \Gamma_1(4)$ *defined by a cyclic covering of degree three* $X(\Gamma) \to X_0(8)$*. The unique normalized newform*

$$f \in S_3(\Gamma_0(12), \chi), \quad \text{with } \chi \text{ of order 2 and conductor 3}$$

satisfies the relation

$$\mathrm{Tr}(\rho(\mathrm{Frob}_p)) = 2c_p(f), \quad p \neq 2, 3, l,$$

where $c_p(f)$ *is the* p^{th} *coefficient in the* q*-expansion of* f*. In other words,*

$${}_\Gamma^1 V_l \cong V_{f,l}^2$$

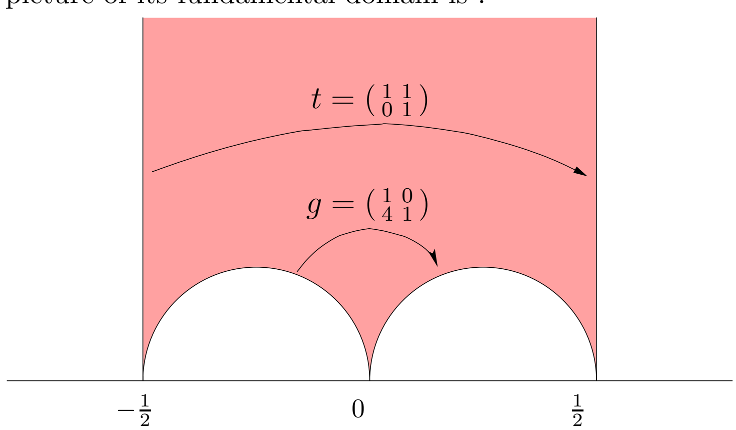
where $V_{f,l}$ *is the representation attached to the cusp form f.*

2.) There is a basis h_1, h_2 *of* $S_3(\Gamma)$ *each member of which satisfies ASwD congruences relative to f.*

3. Results

We start with $\Gamma' = \Gamma_0(8) \cap \Gamma_1(4)$, which has the same image in $\mathbf{PSL}(2, \mathbf{Z})$ as $\Gamma_0(8)$. The modular curve $X_0(8)$ has genus zero, and we can choose a convenient Hauptmodul t for it as follows.

Consider $\Gamma_1(4)$. This has 3 cusps: $0, 1/2, \infty$ of widths $4, 1, 1$ respectively. A picture of its fundamental domain is :



By definition, a Hauptmodul of a genus 0 curve X is a generator for the function field of X relative to its constant field. For a modular curve of genus 0 such as $\Gamma_1(4)$, this is a meromorphic automorphic form of weight 0, in particular, $s(\gamma.z) = s(z)$, for all $\gamma \in \Gamma_1(4)$ and the function field of $X_1(4)$ is $\mathbf{Q}(s)$. We can choose a Hauptmodul for $X_1(4)$ by letting $s(0) =$

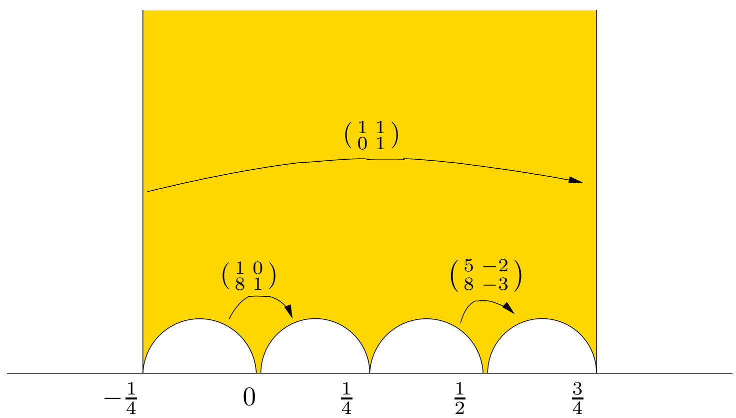
1, $s(1/2) = \infty$, $s(\infty) = 0$, which fixes it uniquely. From Kubert's paper [Ku76] we find an equation for the universal elliptic curve over $X_1(4)$ to be, after a change of variables $s = 16b + 1$,

$$y^2 + 4xy + 4(1-s)y = x^3 + (1-s)x^2.$$

The j-invariant is

$$j = \frac{16(s^2 + 14s + 1)^3}{s(s-1)^4}$$

which shows cusp widths of $4, 1, 1$ at $s = 1, \infty, 0$ as it should be. The double covering $X_0(8) \to X_1(4)$ ramifies the cusp of width 4 and one of the cusps of width 1. We can accomplish this by setting $t^2 = 1 - s$. Note that $t \to -t$ generates the Galois group of this covering. The four cusps of $\Gamma_0(8)$ occur at $t = 0, \infty, 1, -1$ of widths $8, 2, 1, 1$ respectively. Note that $\Gamma_0(8)\backslash\mathbf{H}$ is isomorphic with the t-line $\mathbf{C} - \{0, 1, -1\}$. We compactify this by adding cusps to get $\mathbb{P}^1$. The universal family of elliptic curves is obtained by this substitution. A picture of the fundamental domain is:



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

$$y^2 + 4xy + 4t^2y = x^3 + t^2x^2$$

where the parameter t runs through the points in the projective line $\mathbb{P}^1$. Viewed as an elliptic curve defined over $\mathbf{Q}(t)$, its discriminant is

$$\Delta = -256t^{10} + 256t^8.$$

We easily get the j-invariant using MAGMA:

$$j = \frac{16(t^4 - 16t^2 + 16)^3}{t^8(1+t)(1-t)}. \tag{5}$$

This shows cusp widths of $8, 2, 1, 1$ at $t = 0, \infty, 1, -1$.

Here is a table of cusps and the generators of stabilizers for each cusp. This was computed using MAGMA.

Let g be the unique element of $S_6(\Gamma_1(4))$. We know that

$$\dim S_6(\Gamma_1(4)) = 1.$$

Cusps of $\Gamma_0(8)$	Widths	Generators of stabilizers
∞	1	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$
0	8	$\begin{pmatrix} 1 & 0 \\ -8 & 1 \end{pmatrix}$
1/4	1	$\begin{pmatrix} -3 & 1 \\ -16 & 5 \end{pmatrix}$
1/2	2	$\begin{pmatrix} -3 & 2 \\ -8 & 5 \end{pmatrix}$

TABLE 1. Table of cusps of $\Gamma_0(8)$

In fact it is easy to see that

$$g(z) = \sqrt{\Delta(2z)} = \eta(2z)^{12} = q \prod_{n=1}^{\infty} (1 - q^{2n})^{12}, \; q = e^{2\pi i z}.$$

The general theory of Eisenstein series guarantees the existence of $E_1, E_2 \in M_3(\Gamma_0(8))$ which are 0 at all cusps except $t = \infty, 0$ respectively. Since the number of zeros on $X_0(8)$ of any modular form of weight k is

$$\frac{\mu \cdot k}{12} = k$$

where μ is the index of the subgroup, here 12, we see that Table 2 displays all the zeros and poles of the indicated modular forms.

Widths	2	8	1	1
z	1/2	0	∞	1/4
s	∞^2	1	0	0
t	∞	0	1	-1
g	0^2	0^2	0	0
E_1	1	0	0	0
E_2	0	1	0	0
E_1^2/g	∞^2	*	0	0

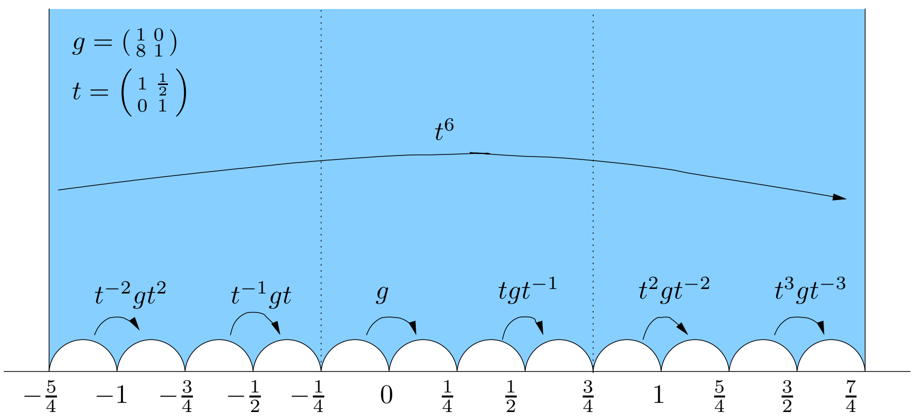
TABLE 2. Data for modular forms on $\Gamma_0(8)$

Recalling that a meromorphic modular form of weight 0 for $\Gamma_0(8)$ is a rational function of t, and that a rational function is determined up to constant multiple by its zeros and poles, we see that $t = E_1/E_2$, up to a scaling of the E_i. From the above table, E_1^2/g has weight 0 and hence is in the function field, and looking at zeros and poles we see $E_1^2 = g \cdot (t^2 - 1)$ and hence $E_1 = \sqrt{g \cdot (t^2 - 1)}$.

We let $\Gamma \subset \Gamma_0(8) \cap \Gamma_1(4)$ be the subgoup of index 3 defined by the covering $X \to X_0(8)$ with equation $t = u^3$. In other words, we let $X = \mathbf{P}^1$ with coordinate u and define a map $X \to X_0(8)$ by this rule. This covering ramifies only the cusps $t = 0, \infty$ with ramification index 3, so that Γ has 8 cusps, at $u = 0, \infty, u = \zeta^i,\ i = 0, ...5$ with widths $24, 6, 1$ respectively. Here ζ is a primitive sixth root of unity. Looking at Sebbar's table [Seb01] we see that Γ is not a congruence subgroup. Using standard formulas, we compute

$$\dim S_3(\Gamma) = 2.$$

Here is a picture of its fundamental domain:



We found explicit expansions for 2 cusp forms in a basis of this. We chose as expansion point for the modular forms, the point $u = 1$ of width 1. Since this lies over the point where $z = i\infty$, the expansion parameter will be $q = \exp(2\pi i z)$, which is the standard local parameter for the cusp $z = i\infty$. We define $h_1, h_2 \in S_3(\Gamma)$ as in the paper LLY as

$$h_1 = \sqrt[3]{E_1^2 E_2}, \quad h_2 = \sqrt[3]{E_1 E_2^2}. \tag{6}$$

Since these have zeros of order 3 at the cusps $t = \pm 1$, which are unramified in the covering by X these become single valued holomorphic on X, whereas their order at the ramified cusps $t = 0, \infty$ only become integral on X. We find the r-expansion of h_1, h_2 by first finding the q-expansion of E_1, E_2. Note that q is a local coordinate at $t = 1$ on $X(\Gamma_0(8) \cap \Gamma_1(4))$. Unlike the LLY paper, we do not use the explicit formulas from the theory of Eisenstein series. Instead, we use a computer to recursively solve the j-equation (5) in unknowns:

$$t - 1 = aq + bq^2 + cq^3 + \dots$$

It is clear that $t-1$ has a simple zero in q since j has a simple pole in q. Thus, we can find that

$$\begin{aligned} t &= 1-8q+32q^2-96q^3+256q^4-624q^5+1408q^6-3008q^7 \\ &\quad +6144q^8-12072q^9+22976q^{10}-42528q^{11}+76800q^{12} \\ &\quad -135728q^{13}+235264q^{14}-400704q^{15}+671744q^{16}-1109904q^{17} \\ &\quad +1809568q^{18}-2914272q^{19}+4640256q^{20}-7310592q^{21} \\ &\quad +11404416q^{22}-17626944q^{23}+o(q^{24}) \end{aligned}$$

Since we also know the expansion of g at this point, we get that of E_1, E_2 as below.

$$\begin{aligned} E_1 &= q-4q^2+8q^3-16q^4+26q^5-32q^6+48q^7-64q^8+73q^9 \\ &\quad -104q^{10}+120q^{11}-128q^{12}+170q^{13}-192q^{14}+208q^{15} \\ &\quad -256q^{16}+290q^{17}-292q^{18}+360q^{19}-416q^{20}+384q^{21} \\ &\quad -480q^{22}+528q^{23}+O(q^{24}) \end{aligned}$$

and

$$\begin{aligned} E_2 &= q+4q^2+8q^3+16q^4+26q^5+32q^6+48q^7+64q^8+73q^9 \\ &\quad +104q^{10}+120q^{11}+128q^{12}+170q^{13}+192q^{14}+208q^{15} \\ &\quad +256q^{16}+290q^{17}+292q^{18}+360q^{19}+416q^{20}+384q^{21} \\ &\quad +480q^{22}+528q^{23}+O(q^{24}) \end{aligned}$$

Using the relations (6), therefore, we immediately get h_1 and h_2. However, these two expressions disagree with the signs of corresponding coefficients we expected. One effective way to solve this is to rewrite them by taking $r = iq$ and then divide the whole expression by i in each. Therefore, the cusp forms for Γ are

$$\begin{aligned} h_1 &= r-\frac{4i}{3}r^2-\frac{8}{9}r^3+\frac{176i}{81}r^4-\frac{850}{243}r^5+\frac{3488i}{729}r^6+\frac{5988}{6561}r^7 \\ &\quad -\frac{152512i}{19683}r^8+\frac{56881}{59049}r^9-\frac{2497000i}{1594323}r^{10}+\frac{35104520}{4782969}r^{11} \\ &\quad +\frac{152464464i}{14348907}r^{12}+\frac{952141694}{129140163}r^{13}+O(r^{14}) \end{aligned}$$

and

$$\begin{aligned} h_2 &= r+\frac{4i}{3}r^2-\frac{8}{9}r^3-\frac{176i}{81}r^4-\frac{850}{243}r^5-\frac{3488i}{729}r^6+\frac{5988}{6561}r^7 \\ &\quad +\frac{152512i}{19683}r^8+\frac{56881}{59049}r^9+\frac{2497000i}{1594323}r^{10}+\frac{35104520}{4782969}r^{11} \\ &\quad -\frac{152464464i}{14348907}r^{12}+\frac{952141694}{129140163}r^{13}+O(r^{14}) \end{aligned}$$

We observe that the coefficients in prime (starting from 5) degrees of h_1 and h_2 turn out to be the same as Table 3 shows.

c_5	c_7	c_{11}	c_{13}	c_{17}	$\cdots$
$-\frac{850}{243}$	$\frac{5968}{6561}$	$\frac{35104520}{478269}$	$\frac{952141694}{129140163}$	$-\frac{206256733102}{31381059609}$	$\cdots$

TABLE 3. Coefficients in prime degrees of h_1 and h_2

p	5	7	11	13	17	19	23
Tr_p	0	4	0	-44	0	52	0
Tr_{p^2}	100	-188	484	292	1156	-92	2116
p	29	31	37	41	43	47	53
Tr_p	0	-92	52	0	-44	0	0
Tr_{p^2}	3364	388	-4124	6724	-6428	8836	11236

TABLE 4. Table of $\mathrm{Tr}\,\rho^*(\mathrm{Frob}_q)$

On the other hand, we have the following the expansion of the unique element of $S_3(\Gamma_0(12),\chi)$, where $\chi : (\mathbf{Z}/12)^* \to \mathbf{C}^*$ is the unique character of order 2 and conductor 3:

$$\begin{aligned} f \quad = \quad & q - 3q^3 + 2q^7 + 9q^9 - 22q^{13} + 26q^{19} - 6q^{21} + 25q^{25} - 27q^{27} \\ & -46q^{31} + 26q^{37} + 66q^{39} - 22q^{43} - 45q^{49} - 78q^{57} + 74q^{61} + 18q^{63} \\ & +122q^{67} - 46q^{73} - 75q^{75} - 142q^{79} + 81q^{81} - 44q^{91} + 138q^{93} \\ & +2q^{97} + O(q^{102}) \end{aligned}$$

This was found using MAGMA and corresponds to $12k3A[0,1]1$ in William Stein's database, [Stein]. A computer program written in MAGMA yields the results in Table 4 on Tr_p, the traces of Frob_p.

Comparing the coefficients of the cusp forms and the modular forms in this example, we can find that

$$c_5 = -\frac{850}{243} \equiv 0 \bmod 5^2,$$

$$c_7 = \frac{5968}{6561} \equiv 2 \bmod 7^2,$$

$$c_{11} = \frac{35104520}{478269} \equiv 0 \bmod 11^2,$$

$$c_{13} = \frac{952141694}{129140163} \equiv -22 \bmod 13^2,$$

$$\cdots\cdots$$

Since 2 and 3 are primes of bad reduction, the congruences do not hold for these two primes.

4. Modularity

We prove the modularity assertion, part 1 of theorem 2.1, via Serre's method. Let ρ denote the 2-adic Scholl's representation attached to $S_3(\Gamma)$, and let ρ^* denote the representation attached to $H^1(X(\Gamma), \mathcal{F})$ where $\mathcal{F} = j_* R^1 f_* \mathbf{Q}_2$, with $f : E \to X(\Gamma)$ the elliptic surface considered in section 3. Unless stated otherwise, representation means continuous representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.

Recall that ρ is known to differ from ρ^* at most by a twist by a character of order two. We will establish the modularity of ρ^*, which implies the modularity of ρ. The fibration $f : E \to X(\Gamma)$ is invariant under $A : u \to -u$. Hence, A induces an operator, also called A on the 4-dimensional vector space underlying ρ^* and commuting with the action of the Galois group. Thus we have a decomposition $\rho^* = \rho_1^* \oplus \rho_{-1}^*$, where ρ_1^*, resp., ρ_{-1}^* is the restriction of ρ^* to $\mathrm{Ker}(A-1)$, resp. $\mathrm{Ker}(A+1)$. It will be seen that both ρ_1^* and ρ_{-1}^* are isomorphic with $\rho_f = \rho_{f,2}$ the 2-adic representation attached by Deligne (see theorem 1.1) to the cusp form $f \in S_3(\Gamma_0(12), \chi)$ in section 3. Both ρ_1^* and ρ_{-1}^* are 2-dimensional. This can be seen as follows. The operator A decomposes the motive associated to $S_3(\Gamma)$, and in particular the deRham realizations of both $\mathrm{Ker}(A \pm 1)$ carry Hodge structures of type $(2,0) + (0,2)$, which implies that both spaces are even-dimensional, so the same goes for the 2-adic realizations ρ_1^* and ρ_{-1}^*. If one of them were 4-dimensional, the operator A would have to act as either 1 or -1 on all of $S_3(\Gamma)$ which is the $(2,0)$-part of the deRham realization of the motive attached to $S_3(\Gamma)$. Thus, A would act trivially on h_1/h_2. But this rational function is, up to constant multiple, the Hauptmodul u of the curve $X(\Gamma)$, as we have already seen, and A acts on this nontrivially: $u \to -u$. Note that all these representations are unramified outside $S = \{\infty, 2, 3\}$.

Now

$$\mathrm{Ker}(A-1) = H^1(X(\Gamma)/A, \mathcal{F}/A)$$

where $X(\Gamma)/A$ denotes the quotient by the group of order 2 generated by A. The sheaf $\mathcal{F}/A$ is $j_* R^1 \tilde{f}_* \mathbf{Q}_2$, where $\tilde{f} : E/A \to X(\Gamma)/A$ is the quotient elliptic surface. These are easily seen to be $\tilde{X}, \tilde{E}$ where $\tilde{X}$ is the projective line with coordinate $v = u^2$, and $\tilde{E}$ is the elliptic surface with equation $y^2 + 4xy + 4v^3 y = x^3 + v^3 x^2$. We compute the $\mathrm{Tr}\rho_1^*(\mathrm{Frob}_p)$ in the representation ρ_1^* by the same method as in section 3, as outlined in section 2. This is done with the same Magma program, but applied to the elliptic surface whose equation we just gave. The result is the same as table 4, but with every entry divided by 2. Thus

$$\frac{1}{2}\mathrm{Tr}\rho^*(\mathrm{Frob}_p) = \mathrm{Tr}\rho_1^*(\mathrm{Frob}_p) = \mathrm{Tr}\rho_{-1}^*(\mathrm{Frob}_p) = c_p(f)$$

where $c_p(f)$ is the pth q-expansion coefficient of the newform f, for all primes $5 \le p \le 201$.

The following is proved in [Liv87, Theorem 4.3]:

Theorem 4.1. *Let K be a global field, S a finite set of places of K, E a finite extension of $\mathbf{Q}_2$, with ring of integers O_E and maximal ideal $\mathfrak{m}$. Then there exists a finite set T of primes of K, disjoint from S, with the following property: Let*

$$\rho_1,\ \rho_2 : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{GL}(2,\, E)$$

be two continuous representations that are unramified outside S and such that

1. $\mathrm{Tr}\rho_1 \equiv \mathrm{Tr}\rho_2 \equiv 0$ *mod* $\mathfrak{m}$, *and* $\det\rho_1 \equiv \det\rho_2$ *mod* $\mathfrak{m}$.
2. $\mathrm{Tr}\rho_1(\mathrm{Frob}_t) = \mathrm{Tr}\rho_2(\mathrm{Frob}_t)$, *and* $\det\rho_1(\mathrm{Frob}_t) = \det\rho_2(\mathrm{Frob}_t)$ *for all* $t \in T$.

Then ρ_1 and ρ_2 have isomorphic semi-simplifications. Such a set of primes T is called sufficient for S.

Our application will be to the case $K = \mathbf{Q}$, $S = \{\infty, 2, 3\}$ and the representations $\rho_1 = \rho_f$ and $\rho_2 = \rho_1^*$ where f is the newform in the statement of theorem 2.1 (the case $\rho_2 = \rho_{-1}^*$ is exactly the same).

Lemma 4.2. $T = \{5, 7, 11, 13, 19, 23, 73\}$ *is sufficient for* $S = \{\infty, 2, 3\}$.

Proof. This exactly as in [Liv87, Prop. 4.11]. The image of the map called F there is a noncubic subset of $(\mathbf{Z}/2)^3$, indeed, it is all of $(\mathbf{Z}/2)^3 - 0$. ☐

First we verify that condition 1. of the above theorem is true here:

Lemma 4.3. *Let $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}(2,\, \mathbf{Q}_2)$ be a continuous representation unramified outside $S = \{\infty, 2, 3\}$, and suppose that* $\mathrm{Tr}\,\rho(\mathrm{Frob}_p) \equiv 0$ *mod* 2, *for* $p = 5, 7, 11, 13$. *Then* $\mathrm{Tr}\,\rho \equiv 0$ *mod* 2 *identically.*

Proof. (see [Liv87, Prop. 4. 10]). Let $\overline{\rho} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}(2,\, \mathbf{Z}/2)$ be the reduction mod 2 of this representation. This is well-defined: ρ preserves a $\mathbf{Z}_2$-lattice and so defines a representation in $\mathrm{GL}(2,\, \mathbf{Z}_2)$ which is independent up to isomorphism of the choice of the lattice, and has thus a unique reduction modulo 2. Let $L/\mathbf{Q}$ be the extension defined by $\mathrm{Ker}(\overline{\rho})$, and so $\mathrm{Gal}(L/\mathbf{Q}) = \mathrm{Im}(\overline{\rho})$, which is a subgroup of $\mathrm{GL}(2,\, \mathbf{Z}/2) \cong S_3$. The elements of order ≤ 2 in this last group have trace 0, whereas the elements of order 3 have trace 1. Suppose that $\mathrm{Tr}\,\rho \not\equiv 0$ mod 2. Then $\mathrm{Gal}(L/\mathbf{Q})$ contains an element of order 3, and so this Galois group must be either cyclic C_3 or S_3. Also $\mathrm{Tr}\,\rho(g) \equiv 1$ mod 2 on any such element of order 3.

If it were C_3 then L would have to be $\mathbf{Q}(\zeta_9 + \zeta_9^{-1})$, the real subfield of the field of ninth roots of unity. This can be seen by classfield theory: By the Kronecker-Weber theorem, L would be a subfield of a cyclotomic field $\mathbf{Q}(\zeta_N)$ and L being unramified outside S by the properties of ρ, we can take N of the form 2^a3^b. Its Galois group, namely $(\mathbf{Z}/2^a3^b)^*$, must have C_3 as a quotient, so we must have $b \geq 2$, and in fact the only such quotient would factor through the projection $(\mathbf{Z}/2^a3^b)^* \to (\mathbf{Z}/3^2)^* \to C_3$, which shows that we L is a subfield of the ninth cyclotomic field. That being the case, we see that Frob_5 acts as a 3-cycle on $\mathbf{Q}(\zeta_9 + \zeta_9^{-1})$. In other words, we have

$\mathrm{Tr}\,\overline{\rho}(\mathrm{Frob}_5) = 1$, which is contrary to our assumption, and so C_3 cannot occur.

For the case where the Galois group is S_3, we need a list of the S_3 extensions of $\mathbf{Q}$ that are unramified outside $\{\infty, 2, 3\}$. Such lists can be found at the web page of John Jones [JJ]. We find that there are 8 such fields, given as the Galois closures of the cubic fields whose defining polynomials are $x^3 - 3x - 2$, $x^3 - 3x - 4$, $x^3 - 9x - 6$, $x^3 - 2$, $x^3 - 3$, $x^3 - 12$,$x^3 - 3x - 10$,$x^3 - 6$. Each of these polynomials is irreducible mod p for at least one of $p = 5, 7, 11, 13$, so that in each of these fields Frob_p acts as a 3-cycle, and we get a nonzero trace on this Frobenius element, contrary to our assumptions, so the case S_3 cannot happen either. □

Corollary 4.4. $\mathrm{Tr}\,\rho_1^* \equiv \mathrm{Tr}\,\rho_{-1}^* \equiv \mathrm{Tr}\,\rho_f^* \equiv 0$ *mod 2.*

The following is a variant of [LLY03, Lemma 5.1]:

Lemma 4.5. *Let*

$$\sigma_1, \sigma_2 : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathbf{Z}_2^*$$

be two continuous representations which are unramified away from 2 and 3, and agree on the elements Frob_p *for* $p = 5, 7, 11, 17$. *Then they are equal.*

Proof. Recall that $\mathbf{Z}_2^* = \{\pm 1,\ \pm 5\} \times (1 + \mathfrak{p}^3)$, where $\mathfrak{p} = 2\mathbf{Z}_2$ is the maximal ideal. Let log denote the $\mathfrak{p}$-adic logarithm on $\mathbf{Z}_2^*$. More precisely, it has kernel $\{\pm 1,\ \pm 5\}$ and it maps $1 + x \in 1 + \mathfrak{p}^3$ to $\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} x^n \in \mathbf{Z}_2$. This 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 $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ to $\mathfrak{p}^3$.

If $\psi \neq 0$, then

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

is finite. Then

$$\bar{\psi} := \frac{1}{2^{n_0}} \psi \bmod \mathfrak{p}$$

is a continuous surjective homomorphism from $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ to $\mathbf{F}_2$ which is trivial at the Frobenius elements at primes $p = 5, 7, 11, 17$ by assumption. This representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ factors through a quadratic extension of $\mathbf{Q}$ unramified outside 2 and 3. Such fields are extensions of $\mathbf{Q}$ 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 $\{\pm 1,\ \pm 5\}$. Hence we consider all Galois extensions of $\mathbf{Q}$ with group equal to a subgroup of a cyclic group of $\mathbf{Z}/2 \times \mathbf{Z}/2$, 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. □

Corollary 4.6. $\det \rho_1^* = \det \rho_{-1}^* = \det \rho_f^* = \tilde{\chi}$*, where* $\tilde{\chi}$ *is the Galois character defined by* $\tilde{\chi}(\mathrm{Frob}_p) = \chi(p)p^2$*, where* χ *is the Dirichlet nebentypus character of the newform* f*.*

Proof. Let $H_{1,p}(T)$ and $H_{-1,p}(T)$ be the characteristic polynomials of Frob_p in ρ_1^* and ρ_{-1}^*. These have the form $T^2 - \mathrm{Tr}_p T + \det_p$, and the traces are determined for primes in a range $5 \le p \le 201$. Also, $H_{1,p}(T)H_{-1,p}(T) = H_p(T)$ where

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

is the characteristic polynomial of the Frobenius at p in the representation ρ^*. These polynomials are determined from table 4 by the formulas

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

Everything is computed explicitly for the primes $5 \le p \le 53$, except for the determinants in the representations $\rho_{\pm 1}^*$, which are the constant terms of the $H_{\pm 1,p}(T)$. But one checks that there is only one possible factorization $H_{1,p}(T)H_{-1,p}(T) = H_p(T)$ for these values, which gives the determinants as claimed, especially for the primes $5, 7, 11, 17$. □

Theorem 4.7. *The* l*-adic representation* ρ_l *attached to* $S_3(\Gamma)$ *is modular. More precisely,* ρ_l^**, the* l*-adic representation on* $H^1(X(\Gamma), j_* R^1 f_* \mathbf{Q}_l)$*, which differs from* ρ_l *by at most a twist by a character of order two, is isomorphic with* $\rho_{f,l}^2$*, where* $\rho_{f,l}$ *is the representation attached by Deligne to the newform* $f \in S_3(\Gamma_0(12), \chi)$*.*

Proof. Each of these representations forms a strictly compatible system as l varies, so it is enough to verify the claim for one prime, say $l = 2$. We can apply Serre's theorem 4.1 as we have verified that all the conditions of that theorem hold for the pair ρ_1^* and ρ_f (or ρ_{-1}^* and ρ_f). The traces of Frobenius under all three of these representaions agree for the primes $5, 7, 11.13.19, 23, 73$ so the semisimplifications of ρ_1^*, ρ_{-1}^* and ρ_f are isomorphic. By a theorem of Ribet [Ri75] the representation ρ_f is irreducible, so these threee representaions are isomorphic. Finally $\rho^* = \rho_1^* \oplus \rho_{-1}^*$.

□

5. Congruences

We now prove the ASwD congruences for our cusp forms $h_1,\ h_2 \in S_3(\Gamma)$. Before doing so, we prove the following proposition, which is necessary to justify the use of the results of [Sch85ii] in the case of odd weights (see p. 76 of loc.cit.)

Proposition 5.1. *Let* $\Gamma \subset \mathrm{SL}(2, \mathbf{Z})$ *be a torsion-free subgroup of finite index (in particular* $-1 \notin \Gamma$*). Assume that there is a model* $X(\Gamma)$ *for* Γ *over* $\mathbf{Q}$ *in the sense of* [Sch85ii, sect. 5.1]*, and that there is an elliptic surface* $f : E_\Gamma \to X(\Gamma)$ *defined over* $\mathbf{Q}$*, such that the analytic space underlying the smooth locus* $f : E_\Gamma^\circ \to Y(\Gamma)$ *is the usual fibration of elliptic curves associated to* Γ *(see proof). Then for every integer* $N \geq 3$ *such that* $\Gamma \cdot \Gamma(N) = \mathrm{SL}(2, \mathbf{Z})$*, there is a model* $V/\mathbf{Q}$ *for the Riemann surface* $\pm(\Gamma \cap \Gamma(N))\backslash \mathbf{H}^*$*, such that the* j*-morphism* $\pi : V \to \mathbf{P}^1_{\mathbf{Q}}$ *factors through* $X(N)_{\mathbf{Q}}$ *and such that there is an action of* $G_N = \mathrm{SL}(\mu_N \times \mathbf{Z}/N)$ *on* V*, which is compatible with its action on* $X(N)_{\mathbf{Q}}$ *and with the action of*

$$G_N(\mathbf{C}) = \Gamma/\Gamma \cap \Gamma(N)$$

on $V(\mathbf{C})$.

Proof. As Scholl points out, the fiber product $S = X(\Gamma) \times_{\mathbf{P}^1_{\mathbf{Q}}} X(N)$ will not work for this since its underlying analytic space is the Riemann surface

$$(\pm\Gamma \cap \pm\Gamma(N))\backslash \mathbf{H}^*$$

whereas the Riemann surface we want is a double cover of this. We define

$$V = \underline{\mathrm{Isom}}(p_1^* E_\Gamma, p_2^* E(N))$$

where p_1 and p_2 are the projections of S to $X(\Gamma)$ and $X(N)$ respectively, and $E_N \to X(N)$ is the universal generalized elliptic curve. First, we note that V is a double cover of S. This is because of the following

Proposition 5.2. *(*[Del75, Prop. 5.3, 5.4]*) Let* E *and* F *be two curves of genus one over* S *without additive fiber. Then* $\underline{\mathrm{Isom}}(E, F)$ *is representable finite and nonramified over* S*. If* $j_E = j_F$*, the projection of* $\underline{\mathrm{Isom}}(E, F)$ *to* S *is surjective and is an étale covering of degree 2 over the subset of* S *where* $j_E = j_F$ *does not take the values* 0 *or* 1728*.*

I claim that the Riemann surface $V(\mathbf{C})$ is $\pm(\Gamma \cap \Gamma(N))\backslash \mathbf{H}^*$. The reason is that, because $\Gamma \cap \Gamma(N)$ is a subgroup of both Γ and $\Gamma(N)$, the pull-back of both $E_\Gamma^\circ \to Y(\Gamma)$ and $E_N^\circ \to Y(N)$ to $\pm(\Gamma \cap \Gamma(N))\backslash \mathbf{H}$ are complex-analytically isomorphic. This clear in view of the constructions of these families, to be recalled in a moment. It follows that these pulled-back families are algebraically isomorphic. By the universal mapping property of V, there is a morphism $X(\Gamma \cap \Gamma(N)) \to V$ over S. Note that, a priori, $X(\Gamma \cap \Gamma(N))$ has a model defined over some finite extension of $\mathbf{Q}$. But both of these are double covers of S. Also, V is a nontrivial covering of S, that is, it does not break into two components. If it did, there would be a section over S, and hence a global isomorphism from $p_1^* E_\Gamma$ to $p_2^* E(N)$, which is impossible, by lemma 5.3, applied to $\Delta_1 = \Gamma \cap (\pm\Gamma(N))$ and $\Delta_2 = (\pm\Gamma) \cap \Gamma(N)$ Therefore, $X(\Gamma \cap \Gamma(N)) \to V$ is an isomorphism over S.

Since $\Gamma \cap \Gamma(N)$ is a normal subgroup of Γ it is clear that $G_N(\mathbf{C}) = \Gamma/\Gamma \cap \Gamma(N)$ acts on $V(\mathbf{C})$. □

Let $\Delta \subset \mathrm{SL}(2, \mathbf{Z})$ be a subgroup of finite index not containing -1. We associate a family of elliptic curves E_Δ over $\pm\Delta\backslash\mathbf{H}$, as the quotient of $\mathbf{H}\times\mathbf{C}$ by the equivalence

$$(\tau, z) \sim (\delta \cdot \tau, (c\tau + d)^{-1}(z + m\tau + n))$$

$$\text{for all } m, n \in \mathbf{Z} \text{ and all } \delta = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Delta.$$

It is clear that for an inclusion $\Delta' \subset \Delta$, $E_{\Delta'}$ is the pull-back of E_Δ via the map $\pm\Delta'\backslash\mathbf{H} \to \pm\Delta\backslash\mathbf{H}$. Every one of these families of elliptic curves, when pulled back to $\mathbf{H}$ become isomorphic to the tautological family

$$\{\mathbf{C}/\mathbf{Z} + \mathbf{Z}\tau \mid \tau \in \mathbf{H}\}.$$

Lemma 5.3. *Let $\Delta_1, \Delta_2 \subset \mathrm{SL}(2, \mathbf{Z})$ be subgroups of finite index, neither of which contains -1. Suppose that $\pm\Delta_1 = \pm\Delta_2$, but that $\Delta_1 \neq \Delta_2$. Then E_{Δ_1} is not isomorphic with E_{Δ_2} over $\pm\Delta_1\backslash\mathbf{H} = \pm\Delta_2\backslash\mathbf{H}$.*

Proof. Any isomorphism $\varphi : E_{\Delta_1} \to E_{\Delta_2}$ over $\pm\Delta_1\backslash\mathbf{H}$ pulls back to an isomorphism of the tautological family over $\mathbf{H}$. These are well-known to be of the form $(\tau, z) \to (\tau, \pm z)$. But neither of these maps intertwines the equivalence relations given by Δ_1 and Δ_2. Take the minus sign, for instance. One would need that for every $\delta_1 \in \Delta_1$ there exists $\delta_2 \in \Delta_2$ and integers m, n such that

$$(\delta_1 \cdot \tau, -(c_1\tau + d_1)^{-1}z) = (\delta_2 \cdot \tau, (c_2\tau + d_2)^{-1}(-z + m\tau + n))$$

The equation $\delta_1 \cdot \tau = \delta_2 \cdot \tau$ means that $\delta_1 = \pm\delta_2$. But the hypotheses $\pm\Delta_1 = \pm\Delta_2$ and $\Delta_1 \neq \Delta_2$ means that there is a δ_1 for which we must take the negative sign. This implies $z = -z + m\tau + n$, which must hold for any fixed τ all z, which is absurd. □

The main principle of Scholl's proof of these identities is the following. We assume Γ has a model $X = X(\Gamma)$ defined over $\mathbf{Z}[1/M]$ in the sense of [Sch85ii, section 5.1]. He defines A-modules ${}^{(m)}L_k(X, A)$ and ${}^{(m)}L_k^\infty(X, A)$ for any $\mathbf{Z}[1/M]$-algebra A, and shows that there is a canonical exact sequence

$$0 \longrightarrow S_{k+2}(X, A) \longrightarrow {}^{(m)}L_k(X, A) \longrightarrow m^{k+1}S_{k+2}(X, A)^\vee \longrightarrow 0$$

When $A = \mathbf{C}$ and $m = 1$, the term in the middle is the deRham version of parabolic cohomology and the above gives its Hodge decomposition, since $S_{k+2}(X, \mathbf{C}) = S_{k+2}(\Gamma)$. ${}^{(m)}L_k^\infty(X, A)$ is a local version of this defined at a cusp. The choice of an appropriate local parameter t at this cusp defines an expansion map

$$\text{taylor} : {}^{(m)}L_k(X, A) \longrightarrow {}^{(m)}L_k^\infty(X, A)$$

which when restricted to $S_{k+2}(X, A)$ is injective ("t-expansion principle".) Moreover,

$$ {}^{(m)}L_k^\infty(X, A) \xrightarrow{\sim} \mathrm{Coker}((m\partial)^{k+1} : tA[[t]] \to tA[[t]]) $$

for a differential operator ∂. When $A = \mathbf{Z}_p$, these groups have an interpretation in crystalline cohomology, and in particular, carry a canonical endomophisms F, which are respected by the evaluation map taylor. The endomorphism F acts quite simply on the target group:

$$ \text{If } x \in {}^{(p)}L_k(X, \mathbf{Z}_p) \subset L_k(X, \mathbf{Z}_p) \text{ has } \mathrm{taylor}(x) \equiv \sum a_n t^n \mod \mathrm{Im}(p\partial)^{k+1} $$

then

$$ \mathrm{taylor}(Fx) \equiv \sum p^{k+1}\gamma_p^n a_n t^{np} \mod \mathrm{Im}(p\partial)^{k+1} $$

for a certain $\gamma_p \in 1+p\mathbf{Z}_p$ which depends on the choice of the local parameter t.

Let $f \in S_{k+2}(X, \mathbf{Z}[1/M]) \subset S_{k+2}(X, \mathbf{Z}_p) \subset {}^{(p)}L_k(X, \mathbf{Z}_p)$, $p \nmid M$. Let $H(T) \in \mathbf{Z}[T]$ be a polynomial such that $H(F)f = 0$ in ${}^{(p)}L_k(X, \mathbf{Z}_p)$ (note that F preserves ${}^{(p)}L_k(X, \mathbf{Z}_p)$). Then

$$ \mathrm{taylor}(H(F)f) \in \mathrm{Im}(p\partial)^{k+1} $$

Writing this out explicitly, using the simple form of the action of F on ${}^{(p)}L_k(X, \mathbf{Z}_p)$, gives p-adic congruence relations on the expansion coefficients of f.

Theorem 5.4. [Sch85ii, Thm. 5.4] *Let $f \in S_k(X(\Gamma), \mathbf{Z}[1/M])$, and let*

$$ \tilde{f} = \sum_{n \geq 1} a(n) \cdot \exp(2\pi i n\tau/\mu) $$

be its Fourier expansions as in 5.2.1 of loc. cit. Fix a prime $p \nmid M$ and suppose that

$$ H(T) = \sum_{r=0}^{e} A_r \cdot T^{e-r} \in \mathbf{Z}[T] $$

is a polynomial such that $H(F)f = 0$ in ${}^{(p)}L_k(X, \mathbf{Z}_p)$. The the coefficients $a(n)$, $n \geq 1$, satisfy the congruence relation

$$ \mathrm{ord}_p(\sum_{r=0}^{e} A_r a(np^{d-r})) \geq (k-1)(1 + \mathrm{ord}_p n). $$

For instance, let

$$ H(T) = \det(1 - T\,\mathrm{Frob}_p \mid {}^k_\Gamma V_l) $$

be the characteristic polynomial of Frobenius in l-adic cohomology. One knows that $\det(1-T\,\mathrm{Frob}_p \mid {}^k_\Gamma V_l) = \det(1-TF \mid L_k(X, \mathbf{Q}_p))$ so that $H(F) \equiv 0$ on $L_k(X, \mathbf{Q}_p))$, leading to congruences for every $f \in S_{k+2}(X, \mathbf{Z}[1/M])$. This is how Scholl proved part (ii) of 1.4.

We apply this to our Γ. The involution A also decomposes $L_k(X, \mathbf{Q}_p)$ into ± 1 eigenspaces, on which F acts. This gives characteristic polynomials $H_{\pm 1}(T)$ for these, with

$$H_1(T)H_{-1}(T) = \text{characteristic polynomial of } F \text{ on } L_k(X, \mathbf{Q}_p) = H(T)$$

We know that $H_p(T) = H_{1,p}(T)H_{-1,p}(T)$ and that

$$H_{1,p}(T) = H_{-1,p}(T) = T^2 - c_p(f)T + \chi(p)p^2$$

for our weight 3 newform f. We claim

Proposition 5.5. *$H(T) = H_p(T)$ and $H_1(T) = H_{-1}(T) = T^2 - c_p(f)T + \chi(p)p^2$. In other words, the characteristic polynomials of* Frob_p *acting on the étale comomology spaces* $\mathrm{Ker}(A \pm 1)_l \subset {}^k_\Gamma V_l$ *coincide with the characteristic polynomials of F acting on the crystalline cohomology spaces* $\mathrm{Ker}(A \pm 1)_p \subset L_k(X, \mathbf{Q}_p)$.

Proof. The involution A acts on the fibration $E_\Gamma \to X(\Gamma)$, and hence on the parabolic cohomology groups in various realizations. The subspace $\mathrm{Ker}(A-1)_*$ in these various realizations is just the parabolic cohomology of the quotient situation $E_\Gamma/A \to X(\Gamma)/A$. We have already identified this quotient explicitly in section 4, and it is easy to check that this family of elliptic curves has multiplicative reduction in all its cusps, so in particular, it is semi-stable. This is also true of $E_\Gamma \to X(\Gamma)$. We can apply theorem [**?**] of the next section to the parabolic cohomologies both situations to conclude that $H(T) = H_p(T)$ and $H_1(T) = H_{1,p}(T)$. Since $H_p(T) = H_{1,p}(T)^2$, we get that $H_{-1}(T) = H_{-1,p}(T)$ also. □

Theorem 5.6. *The cusp forms $h_1, h_2 \in S_3(\Gamma)$ satisfy Atkin-Swinnerton-Dyer congruences relative to $f \in S_3(\Gamma_0(12),\ \chi)$.*

Proof. h_1 is in $\mathrm{Ker}(A-1) \subset S_3(\Gamma, \mathbf{Z}_p)$ which is in $\mathrm{Ker}(A-1)_p$, and the previous proposition shows that the characteristic polynomial $H_1(T)$ on this latter space is $T^2 - c_p(f)T + \chi(p)p^2$. By the Cayley-Hamilton theorem $H_1(F)$ annihilates the space, and in particular h_1. The congruences then follow from Scholl's results as discussed above. □

6. Parabolic cohomology

We gather some well-known results on parabolic cohomology that were utilized in this paper. The general situation is of a proper morphism $f : E \to X$ deifined over a field K where X is a smooth projective curve, and the general fiber of f is an elliptic curve. We assume that f is nonconstant. Let $j : Y \subset X$ be the inclusion of the open subset over which f is smooth and let f stand also for the restriction of f to $f^{-1}(Y)$. In l-adic theory, the parabolic cohomology groups are by definition $H^i(X, j_*\mathrm{Sym}^k(R^1 f_* \mathbf{Q}_l))$, $k \geq 0$. It is known that when $k \geq 1$ these vanish when $i \neq 1$.

References

[ASD71] 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, pp. 1–25.

[Beau82] A. Beauville, Les familles stable de courbes elliptiques sur $\mathbf{P}^1$ admettant quatre fibres singulières, C.R. Acad. Sci. **294** (1982), 657-660.

[Con] B. Conrad, Modular forms, Cohomology, and the Ramanujan Conjecture, to appear.

[Del73] P. Deligne, *Formes modulaires et représentations l-adiques*, Sém. Bourbaki 68/69, no. **355**, Lecture Notes in Math., **179**, Springer, Berlin, 1971, pp. 139–172.

[DS74] P. Deligne and J. P. Serre, *Formes modulaires de poids 1*, Ann. Sci. Ec. Norm. Sup, **7**(1974), pp. 507–530 in Jean-Pierre Serre, Œuvres. Collected papers. III. 1972–1984. Springer-Verlag, Berlin, 1986.

[DR73] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, in Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), 143–316. Lecture Notes in Math., Vol. 349,Springer,Berlin,1973.

[Del75] P. Deligne, Courbes elliptiques: Formulaire(d'après Tate), Modular functions of one variable IV, Lect. Notes in Math. **476** (1975), 53-73.

[Eic54] M. Eichler, *Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion*, Arch. Math.**5** (1954), 355–366.

[Fal83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366.

[Fr1922] R. Fricke, Die Elliptischen Funktionen und ihre Anwendungen, Zweiter Teil, Teubner Verlag, Leipzig and Berlin, 1922.

[I67] Y. Ihara, *Hecke polynomials as congruence ζ functions in the elliptic modular case*, Ann. of Math. **85** (1967), 267-295.

[JJ] J. Jones. http://math.la.asu.edu/ jj/numberfields.

[KM85] N. M. Katz and B. Mazur, Arithmetic Moduli of Elliptic Curves, Annals of Mathematics Studies, **108**, Princeton University Press, 1985.

[Ku76] D.Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. **33**, (1976), 193-237.

[KS65] M. Kuga and G.Shimura, *On the zeta function of a fibre variety whose fibres are abelian varieties*, Ann. of Math. **82** (1965), 478-539.

[LLY03] Wen-Ching Winnie Li, Ling Long, Zifeng Yang, *On Atkin-Swinnerton-Dyer congruence relations*, preprint at http://arxiv.org/math.NT/0311287.

[Liv87] R. Livné, *Cubic exponential sums and Galois representations*, Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985), Amer. Math. Soc., Providence, RI, 1987, pp. 247–261.

[Ri75] K. A. Ribet, On l-adic representations attached to modular forms, *Invent. Math.*, **28** (1975), 245-275.

[Sch85i] A. J. Scholl, A trace formula for F-crystals. *Invent. Math.*, **79** (1985), 31-48.

[Sch85ii] ——, Modular forms and deRham cohomology; Atkin-Swinnerton-Dyer congruences. *Invent. Math.*, **79** (1985), 49-77.

[Sch87] ——, Modular forms on noncongruence subgroups. *Séminaire de Théorie des Nombres, Paris 1985-86*, 199-206, Progr. Math. 71, Birkhäuser, Boston, MA, 1987.

[Sch88] ——, The l-adic representations attached to a certain non-congruence subgroup, *J. Reine Angew. Math.* **392** (1988), 1–15.

[Sch90] ——, Motives for modular forms. *Invent. Math.* **100** (1990), 419–430.

[Sch93] ——, The l-adic representations attached to non-congruence subgroups II, preprint, 1993.

[Sch96] ——, Vanishing cycles and non-classical parabolic cohomology. *Invent. Math.* **124** (1996), 503-524.

[Sch97] ——, On the Hecke algebra of a noncongruence subgroup, *Bull. London Math.Soc.* **29** (1997), 395-399.

[Sch04] ——, On some l-adic representations of Gal(Qbar/Q) attached to noncongruence subgroups, preprint at http://arxiv.org/math.NT/0402111.

[Seb01] A. Sebbar, Classification of torsion-free genus zero congruence groups, *Proc. Amer. Math. Soc.* **129** (2001), no. 9, 2517–2527 (electronic).

[Ser84] J. P. Serre, Résumé de cours, 1984-5, Collège de France, in Jean-Pierre Serre, Œuvres. Collected papers. IV. 1985–1998. Springer-Verlag, Berlin, 2000.

[Shi58] G. Shimura, *Correspondances modulaires et les functions ζ de courbes algébriques*, J. Math. Soc. Japan **10** (1958), 1–28.

[Shi71] 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.

[Stein] W. Stein *The Modular Forms database* http://modular.fas.harvard.edu/Tables

[Tate72] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil.*, Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), pp. 33–52. Lecture Notes in Math., Vol. 476, Springer, Berlin, 1975.

(Fang, Hoffman and Verrill) Mathematics Department, Louisiana State University, Baton Rouge 70803, Louisiana

(Linowitz) Mathematics Department, University of Pennsylvania, Philadelphia 19104, Pennsylvania

(Rupinski) Mathematics Department, Notre Dame University, South Bend 46556, Indiana

E-mail address, Fang: `liqun@math.lsu.edu`

E-mail address, Hoffman: `hoffman@math.lsu.edu`

E-mail address, Linowitz: `liqun@math.lsu.edu`

E-mail address, Rupinski: `arupinsk@nd.edu`

E-mail address, Verrill: `verrill@math.lsu.edu`