On ℓ-adic representations attached to non-congruence subgroups II

A. J. Scholl[1]

0. Introduction

In this paper we extend the results of **[9]** to two other subgroups of $SL_2(\mathbb{Z})$. Let $\Gamma \subset SL_2(\mathbb{Z})$ be a subgroup of finite index. In **[8]** and **[9]** it is shown how to attach to the space of cusp forms of weight w on Γ (whose dimension we denote by d) a strictly compatible family $\{\rho_\ell\}$ of $2d$-dimensional ℓ-adic representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$, for a certain number field, mildly generalising the representations constructed many years ago by Deligne **[4]** for congruence subgroups.

If it happens that $d = 1$ and $K = \mathbb{Q}$, then the representations ρ_ℓ are 2-dimensional representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. By the Langlands philosophy, ρ_ℓ should then be the ℓ-adic representation associated to a cusp form of weight w on a congruence subgroup, which is a newform of some level. In **[9]** we verified this for a certain subgroup $\Gamma_{7,1,1}$ and $w = 4$, using Serre's effective version of Faltings' trick (see **[10]** and **[6]**).

In this paper we consider two further subgroups, $\Gamma_{4,3}$ and $\Gamma_{5,2}$ (see §§4–5 below) and prove analogous results for weight 4 (here also $d = 1$ and $K = \mathbb{Q}$). In theory the verification is no different from that of **[9]**. However the case of $\Gamma_{4,3}$ is complicated by the possibilidty of ramification at the prime 3.

The machine computations in §§2, 4–5 were done over a long period of time, using a variety of computer systems. They were completed using the invaluable package PARI-GP by C. Batut, D. Bernardi, H. Cohen and M. Olivier.

The author is pleased to thank the Institute for Advanced Study, Princeton, whose hospitality he enjoyed in the year 1989–90, when a large part of the work for this paper was done. This paper was completed while the author was a visiting fellow at the Isaac Newton Institute for Mathematical Sciences, Cambridge.

[1] Research partially funded by NSF grant #DMS–8610730

1. The ℓ-adic representations

1.1. Let $\Gamma \subset SL_2(\mathbb{Z})$ be a subgroup of finite index. Let $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$ be the extended upper half-plane, on which Γ acts by linear fractional transformations. We assume that Γ is defined over $\mathbb{Q}$ in the following sense: there is a projective curve X_Γ over $\mathbb{Q}$, together with a finite morphism $\phi\colon X_\Gamma \to \mathbb{P}^1_{\mathbb{Q}}$ and an isomorphism $\Xi\colon \Gamma\backslash\mathcal{H}^* \xrightarrow{\sim} X_\Gamma(\mathbb{C})$ such that the following diagram commutes (j being the usual modular function):

$$\begin{array}{ccc} \Gamma\backslash\mathcal{H}^* & \xrightarrow{\Xi} & X_\Gamma(\mathbb{C}) \\ \downarrow & & \downarrow{\scriptstyle \phi_{\mathbb{C}}} \\ SL_2(\mathbb{Z})\backslash\mathcal{H}^* & \xrightarrow{j} & \mathbb{P}^1(\mathbb{C}) \end{array}$$

By abuse of notation we will use j to denote the rational function on X_Γ determined by ϕ.

1.2. Let $U_\Gamma \subset X_\Gamma$ be the complement of the points $j = 0,\ 1728,\ \infty$. Write $g\colon U_\Gamma \hookrightarrow X_\Gamma$ for the inclusion. Let

$$\pi\colon \mathcal{E} \to U_\Gamma$$

be the elliptic curve with affine equation

$$y^2 + xy = x^3 - (36x + 1)/(j - 1728)$$

and let $\mathcal{F}$ be the $\mathbb{Q}_\ell$-sheaf $R^1\pi_*\mathbb{Q}_\ell$ on U_Γ. The parabolic cohomology groups attached to Γ are the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules

$${}_\Gamma\mathcal{W}^k_\ell \overset{\mathrm{def}}{=} H^1(X_\Gamma \otimes \overline{\mathbb{Q}}, g_* \operatorname{Sym}^k \mathcal{F})$$

for $k \geq 0$. The Poincaré duality pairing $\mathcal{F} \otimes \mathcal{F} \to \mathbb{Q}_\ell(-1)$ induces a nondegenerate pairing

$${}_\Gamma\mathcal{W}^k_\ell \otimes {}_\Gamma\mathcal{W}^k_\ell \to \mathbb{Q}_\ell(-k-1)$$

which is alternating (resp. symmetric) if k is even (odd).

If k is even then $\dim_{\mathbb{Q}_\ell} {}_\Gamma\mathcal{W}^k_\ell$ is twice the dimension of $S_{k+2}(\Gamma)$, the complex space of cusp forms on Γ of weight $(k+2)$.

1.3. Assume that $X_\Gamma \simeq \mathbb{P}^1_{\mathbb{Q}}$. Choose a generator t of the function field of X_Γ, in such a way that $P(t) + jQ(t) = 0$ for polynomials P, $Q \in \mathbb{Z}[t]$ where P is monic and $\deg P > \deg Q$.

Proposition 1.4. *Let p be prime, and assume the following conditions are satisfied:*

(i) $P(t)$, $Q(t)$ are p-integral, and their reductions $\tilde{P}(t)$, $\tilde{Q}(t)$ modulo p are relatively prime.

(ii) At least one of $\tilde{P}'(t)$, $\tilde{Q}'(t)$ is non-zero.

Then ${}_\Gamma\mathcal{W}^k_\ell$ is unramified at p for every $k \geq 0$ and every $\ell \neq p$.

This is Proposition 2.7 of [**9**].

2. The examples

2.1. Let $\Gamma \subset SL_2(\mathbb{Z})$ be one of the following subgroups:

(i) The subgroup $\Gamma_{4,3}$ of index 7, generated by

$$\begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix}.$$

(ii) The subgroup $\Gamma_{5,2}$, also of index 7, generated by

$$\begin{pmatrix} 1 & 5 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}.$$

2.2. In both cases X_Γ has genus zero, and can therefore be uniformised by an algebraic function t of the modular function j. Methods going back to Klein and Fricke, and systemised by Atkin and Swinnerton-Dyer **[1]**, give a procedure to determine a defining relation of the form

$$j = \frac{E_3(t)F_3(t)^3}{Q(t)} = 1728 + \frac{E_2(t)F_2(t)^2}{Q(t)}$$

for polynomials $E_\alpha(t)$, $F_\alpha(t)$, $Q(t)$ with algebraic coefficients, which may (in theory) be computed by the method of undetermined coefficients.

2.3. Here these polynomials have rational coefficients, and are given as follows:

(i) For $\Gamma_{4,3}$:

$$\begin{aligned} j &= -7^{-7}\frac{(t+432)(t^2+80t-3888)^3}{t^3} \\ &= -7^{-7}\frac{(t-16)(t^3+344t^2+1944t+108^3)^2}{t^3} + 1728. \end{aligned}$$

(ii) For $\Gamma_{5,2}$:

$$\begin{aligned} j &= 7^{-7}\frac{(t+125)(t^2+5t-1280)^3}{t^2} \\ &= 7^{-7}\frac{(t-64)(t^3+102t^2+381t+64000)^2}{t^2} + 1728. \end{aligned}$$

Appying 1.4 to the above equations gives:

Corollary 2.4. *(i) The representations* ${}_{\Gamma_{5,2}}\mathcal{W}_\ell^k$ *are unramified away from* $\{2,\ 5,\ 7,\ \ell\}$.

(ii) The representations ${}_{\Gamma_{4,3}}\mathcal{W}_\ell^k$ *are unramified away from* $\{2,\ 3,\ 7,\ \ell\}$.

2.5. In §3 of **[9]** we gave a closed formula for $\operatorname{tr}\rho_\ell(\mathrm{Fr}_p)$ for an unramified prime $p > 3$, using the Lefschetz fixed point formula in ℓ-adic cohomology. Table 1 gives the values of $\operatorname{tr}\rho_\ell(\mathrm{Fr}_p)$ for $k = 2$ in the two cases under consideration.

p	5	11	13	17	19	23	29	31	37	41	43	47	53	59
$\Gamma_{5,2}$	–	12	−78	−94	40	32	−50	−248	−434	402	−68	536	22	−560
$\Gamma_{4,3}$	6	−12	−82	−30	68	216	246	−112	110	−246	−172	192	558	540

p	61	67	71	73	79	83	89	97	101	103	107	109	113
$\Gamma_{5,2}$	−278	−164	672	82	−1000	−448	−870	1026	482	272	−444	−1170	−798
$\Gamma_{4,3}$	110	140	−840	−550	−208	516	−1398	1586	−1242	680	996	1382	−750

Table 1

3. The method of Faltings and Serre

3.1. The following theorem is due to Serre (see [**6**], Theorem 4.3 and [**10**]). It is an effective version of Faltings' trick ([**5**], proof of Satz 5).

Theorem 3.2. *Let N be a positive integer, and let ρ, $\rho'\colon G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Q}_2)$ be continuous homomorphisms, unramified at all primes not dividing N. Let $\Sigma_N \subset G$ be a subset with the property that if $\chi_1, \dots \chi_r$ form a basis for the set of quadratic Dirichlet characters of conductor dividing $8N$, than*

$$(\chi_1, \dots \chi_r)\colon \Sigma_N \longrightarrow \{\pm 1\}^r$$

is surjective.

Assume the following two conditions are satisfied.

(i) $\mathrm{Im}\,\rho$ *and* $\mathrm{Im}\,\rho'$ *are pro-2-groups.*

(ii) The characteristic polynomials of $\rho(\sigma)$, $\rho'(\sigma)$ are equal for all $\sigma \in \Sigma_N$.

Then ρ and ρ' are isomorphic.

3.3. To apply the theorem we need a method to check that $\mathrm{Im}\,\rho$ is a pro-2-group. Let $\tilde{\rho}\colon G \to GL_2(\mathbb{F}_2)$ be any reduction of ρ modulo 2. Recall:

(i) If $x \in GL_2(\mathbb{F}_2)$ then x has order 3 if and only if $\mathrm{tr}\, x = 1$;

(ii) if $x \in GL_2(\mathbb{Z}_2)$ is congruent to the identity mod 2 then $\mathrm{tr}\, x \equiv 1 + \det x \pmod 4$.

So if there exists $\sigma \in G$ with $\mathrm{tr}\,\rho(\sigma)$ odd, then $\mathrm{Im}\,\tilde{\rho} \simeq A_3$ or S_3. If there exists $\sigma \in G$ with $\mathrm{tr}\,\rho(\sigma) \equiv -1 + \det\rho(\sigma) \pmod 4$ then $\mathrm{Im}\,\tilde{\rho} \simeq \mathbb{Z}/2$ or S_3. Conversely, by the Tchebotarev density theorem, if $\mathrm{Im}\,\tilde{\rho} \simeq A_3$ or S_3 there exist infinitely many primes p such that $\mathrm{tr}\,\rho(\mathrm{Fr}_p)$ is odd.

3.4. We now assume given a 2-adic representation ρ, unramified away from primes dividing N. We suppose that the characteristic polynomial of $\rho(\mathrm{Fr}_p)$ is explicitly given for a large finite set of primes p, and that for each such p, $\mathrm{tr}\,\rho(\mathrm{Fr}_p)$ is even. We wish to deduce that $\mathrm{Im}\,\tilde{\rho}$ is of even order. The example in [**9**] was sufficiently straightforward for the calculations in class field theory to be left as a pleasant exercise. In the present cases the calculations are considerably longer and a more detailed treatment is appropriate.

3.5. If there exists $\sigma \in G$ with $\operatorname{tr}\rho(\sigma) \equiv -1 + \det\rho(\sigma) \pmod 4$, $\operatorname{Im}\tilde{\rho}$ cannot be A_3 by the remarks above. Otherwise, we can eliminate the possibility that $\operatorname{Im}\tilde{\rho} \simeq A_3$ in the following way: such a $\tilde{\rho}$ cuts out a cyclic cubic extension $F/\mathbb{Q}$, unramified outside primes dividing N. It suffices for each possible F to find an inert prime p for which $\operatorname{tr}\rho(\mathrm{Fr}_p)$ is even. (The Tchebotarev density theorem assures that infinitely many such p must exist.) As it is easy to write down all possibilities for F for any given N, the exclusion of A_3 is straightforward.

3.6. It is somewhat harder to eliminate the possibility that $\operatorname{Im}\tilde{\rho}$ is isomorphic to S_3. Assume that this is the case; then the kernel of $\tilde{\rho}$ cuts out an S_3-extension $M/\mathbb{Q}$, which is unramified away from N. Let E be its quadratic subfield. Since $E/\mathbb{Q}$ is unramified at all $p \nmid N$, there is only a finite, and easily computable, set of possibilities for E. The extension M/E determines a cubic idèle class character

$$\psi\colon J_E/E^* \longrightarrow \boldsymbol{\mu}_3$$

satisfying the two conditions:

(i) $\psi^\tau = \psi^{-1}$ for the non-trivial automorphism τ of E;

(ii) $\psi_\mathfrak{p} = 1$ for $\mathfrak{p}|p$ whenever $\operatorname{tr}\rho(\mathrm{Fr}_p)$ is even.

If ψ is not everywhere unramified, then its restriction to the unit idèles is non-trivial, and therefore gives a homomorphism

$$\theta = \Pi\theta_\mathfrak{p} : \prod_{\mathfrak{p}|N} \mathfrak{o}^*_{E_\mathfrak{p}} \longrightarrow \boldsymbol{\mu}_3$$

satisfying $\theta^\tau = \theta^{-1}$.

3.7. If $3 \nmid N$ then θ is tamely ramified and each $\theta_\mathfrak{p}$ factors through $\mathfrak{o}^*_E/(1+\mathfrak{p})$. Therefore:

(a) If $(p) = \mathfrak{p}^2$ is ramified then τ acts trivially on $\mathfrak{o}/\mathfrak{p}$, so $\theta_\mathfrak{p} = 1$.

(b) If $(p) = \mathfrak{p}\mathfrak{p}^\tau$ is split and $p \not\equiv 1 \pmod 3$ then as $3 \nmid \#(\mathfrak{o}_E/\mathfrak{p})^*$ we have $\theta_\mathfrak{p} = 1$.

(c) If $(p) = \mathfrak{p}$ is inert and $p \not\equiv -1 \pmod 3$ then θ_p must factor through the norm from $\mathfrak{o}/\mathfrak{p}$ to $\mathbb{Z}/p$, so $\theta^\tau_\mathfrak{p} = \theta_\mathfrak{p}$. So in this case $\theta_p = 1$.

If 3 divides N we have to consider separately $\theta_3 = \prod_{\mathfrak{p}|3} \theta_\mathfrak{p}$ and determine in each case the maximal quotient of $\mathfrak{o}^*_{E_\mathfrak{p}}$ of exponent 3.

(a′) If $(3) = \mathfrak{p}\mathfrak{p}'$ is split in E, then $\mathfrak{o}^*_{E_\mathfrak{p}} = \mathbb{Z}^*_3$, so that θ_3 factors through $(\mathfrak{o}_E/9\mathfrak{o}_E)^*$ (which is isomorphic to $(\mathbb{Z}/3)^2 \times (\mathbb{Z}/2)^2$).

(b′) If $(3) = \mathfrak{p}$ is inert in E, then $\mathfrak{o}_{E_\mathfrak{p}} \simeq W(\mathbb{F}_9)$ and again θ_3 factors through $(\mathfrak{o}_E/9\mathfrak{o}_E)^*$ (which is isomorphic to $(\mathbb{Z}/3)^2 \times (\mathbb{Z}/8)$).

(c′) If $(3) = \mathfrak{p}^2$ is ramified in E, then $E_\mathfrak{p} \simeq \mathbb{Q}_3(\omega)$ for $\omega = \sqrt{\pm 3}$, and we distinguish two cases:

(c′+) $\omega^2 = 3$. Then $\mathfrak{o}^*_{E_\mathfrak{p}} \simeq \mathbb{Z}^2_3$, generated by $1+\omega$ and 4. In other words, if $E = \mathbb{Q}(\sqrt{3d})$ with $d \equiv 1 \pmod 3$ then $\theta_\mathfrak{p}$ factors through $(\mathfrak{o}_E/3\mathfrak{p})^*$.

(c′−) $\omega^2 = -3$. Then $\boldsymbol{\mu}_3 \subset E_{\mathfrak{p}}$ and so $\mathfrak{o}_{E_{\mathfrak{p}}}^* \simeq \mathbb{Z}_3^2 \times \boldsymbol{\mu}_3$, generated by $1+3\omega$, 4 and $(-1+\omega)/2$. Therefore if $E = \mathbb{Q}(\sqrt{3d})$ with $d \equiv -1 \pmod 3$ then $\theta_{\mathfrak{p}}$ factors through $(\mathfrak{o}_E/9\mathfrak{o}_E)^*$.

3.8. We conclude that we can write θ in the form

$$\theta = \Pi\theta_p\colon \prod_{p|N} (\mathfrak{o}_E/\mathfrak{f}_p)^* \longrightarrow \boldsymbol{\mu}_3$$

where:

- if $p \neq 3$ then

  p ramified in $E \quad \Rightarrow \quad \mathfrak{f}_p = (1)$;

  p split in $E \quad \Rightarrow \quad \mathfrak{f}_p = (p)$ if $p \equiv 1 \pmod 3$, $\mathfrak{f}_p = (1)$ otherwise;

  p inert in $E \quad \Rightarrow \quad \mathfrak{f}_p = (p)$ if $p \equiv 2 \pmod 3$, $\mathfrak{f}_p = (1)$ otherwise;

- if $p = 3$ then

  $(p) = \mathfrak{p}^2$ ramified in E and $E_{\mathfrak{p}} = \mathbb{Q}_3(\sqrt{3}) \quad \Rightarrow \quad \mathfrak{f}_p = \mathfrak{p}^3$;

  in other cases $\mathfrak{f}_p = (9)$.

Moreover $\theta^\tau = \theta^{-1}$, θ is trivial on the images of global units, and if (π) is a principal ideal of E such that $N((\pi)) = p^r$ for which $\operatorname{tr}\rho(\mathrm{Fr}_p)$ is even, then $\theta(\pi) = 1$.

Write $\mathfrak{f} = \Pi\mathfrak{f}_p$, and let $G_{\mathfrak{f}}$ be the maximal quotient of $(\mathfrak{o}_E/\mathfrak{f})^*$ of exponent 3 on which τ acts as -1. The character θ then factors through $G_{\mathfrak{f}}$. To show that $\theta = 1$ it is enough to find a set of elements $\pi \in \mathfrak{o}_E$ prime to $\mathfrak{f}$ whose residue classes generate $G_{\mathfrak{f}}$, and which are either global units, or elements with prime power norm p^r for which $\operatorname{tr}\rho(\mathrm{Fr}_p)$ is even.

3.9. To show that the case of S_3 does not occur a possible algorithm is therefore to consider in turn each candidate field E, and show that $\theta = 1$ by the above procedure. This shows that M/E must be everywhere unramified, so given by a cubic character χ of the ideal class group H_E of E with $\chi^\tau = \chi^{-1}$. To exclude this possibility, let H' be the maximal quotient of H_E of exponent 3 on which τ acts by -1. It is enough to find a set of primes $p = \mathfrak{p}\mathfrak{p}'$ which split in E for which $\operatorname{tr}(\mathrm{Fr}_p)$ is even, such that the ideal classes of such $\mathfrak{p}$ generate H'. Moreover Tchebotarev's density theorem ensures that if the image of $\tilde{\rho}$ is not S_3, then this algorithm is guaranteed to eventually succeed.

4. $\Gamma_{5,2}$

4.1. Write as usual

$$P(\tau) = 1 - 24\sum_{n=1}^{\infty} \sigma_1(n)q^n, \quad \eta(\tau) = q^{1/24}\prod_{n=1}^{\infty}(1-q^n)$$

where $q = \exp 2\pi i\tau$.

Proposition 4.2. *Let*

$$h_1(\tau) = \eta(\tau)^2\eta(35\tau)^2, \quad h_2(\tau) = \eta(5\tau)^2\eta(7\tau)^2, \quad h_3(\tau) = \eta(\tau)\eta(5\tau)\eta(7\tau)\eta(35\tau);$$
$$g(\tau) = \frac{1}{24}\big(35P(35\tau) - 7P(7\tau) - 5P(5\tau) + P(\tau)\big).$$

Then the function

$$f_{35}(\tau) = g(\tau)\big(-h_1(\tau) + h_2(\tau) + 2h_3(\tau)\big) = \sum_{n=1}^{\infty} a_n q^n$$

is a newform of weight 4 *on* $\Gamma_0(35)$.

Proof. From classical formulae it is simple to check that f_{35} is a cusp form of weight 4 on $\Gamma_0(35)$. It suffices to check it is a newform. First observe that $f_{35}|W_{35} = -f_{35}$ from the explicit description of f_{35} and the transformation formulae for $\eta(\tau)$ and $P(\tau)$. Therefore f_{35} vanishes at the 8 fixed points of W_{35}. The weight 2 modular form $g(\tau)$ also vanishes at the fixed points of W_{35} since $g|W_{35} = g$. As $X_0(35)$ has genus 3 and 4 cusps, g has no other zeroes, hence f_{35}/g is a cusp form of weight 2 which transforms by -1 under W_{35}. One can then identify f_{35}/g from the tables in [**2**].

4.3. We write ρ_ℓ for the representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on ${}_{\Gamma_{5,2}}\mathcal{W}_\ell^2$ as in §1. By Deligne's original construction [**4**] there is a strictly compatible system $\{\rho'_\ell\}$ of 2-dimensional ℓ-adic representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, unramified away from 5, 7 and ℓ such that that $\det\rho'_\ell = \chi_{\mathrm{cycl}}^3$ and $\mathrm{tr}\,\rho'_\ell(\mathrm{Fr}_p) = a_p$ for all primes $p \notin \{5, 7, \ell\}$.

Theorem 4.4. ρ_ℓ *and* ρ'_ℓ *are isomorphic for every* ℓ.

Proof. Since it is easy to show that ρ_ℓ and ρ'_ℓ are irreducible (cf. [**7**] Theorem 2.3) and both of the systems $\{\rho_\ell\}$, $\{\rho'_\ell\}$ are compatible, it is enough to prove the theorem for $\ell = 2$. We apply the algorithm described in §3. Firstly, by calculation and comparing with Table 1 we find that $\mathrm{tr}\,\rho_\ell(\mathrm{Fr}_p) = \mathrm{tr}\,\rho'_\ell(\mathrm{Fr}_p)$ for $11 \le p \le 113$.

4.5. Since from the values of $\mathrm{tr}\,\rho_2(\mathrm{Fr}_p)$ there is no evidence of σ with $\mathrm{tr}\,\rho(\sigma) \equiv -1+\det\rho(\sigma) \pmod 4$, we consider the possible cyclic cubic fields $F/\mathbb{Q}$ occurring in 3.5. The only possible extension is $\mathbb{Q}(\zeta_7)^+$. But $p = 11$ is inert in $\mathbb{Q}(\zeta_7)^+$, and $a_{11} = 12$. So $\tilde{\rho}_2$ cannot have image A_3.

4.6. Now we eliminate the possibility that $\tilde{\rho}_2$ is surjective. There are 15 possible candidate fields E, namely $\mathbb{Q}(\sqrt{d})$ where $d \in \{-1, \pm 2, \pm 5, \pm 7, \pm 10, \pm 14, \pm 35, \pm 70\}$. None of these have class number divisible by 3, so it suffices to show that the character θ is trivial. For every p with $7 < p < 100$ we have $\operatorname{tr} \tilde{\rho}_2(\mathrm{Fr}_p) = 0$. From the discussion in 3.8 one obtains Table 2. Here f is the positive integer such that $\mathfrak{f} = f\mathfrak{o}_E$ is the maximal conductor of θ, and $\omega = \sqrt{d}$ or $(1+\sqrt{d})/2$ as usual. The fourth column gives a list of elements which are either global units or elements of prime power norm, whose classes generate $G_\mathfrak{f}$. We can therefore conclude that the image of ρ_2 is a pro-2-group, and the same argument applies to ρ_2'.

Bad primes: 2, 5, 7			
d	f	$\#G_\mathfrak{f}$	generators for $G_\mathfrak{f}$
-1	1	1	—
2	35	9	$1+\omega$; $5+2\omega$
-2	5	3	$3+\omega$
5	2	3	ω
-5	7	3	$22+3\omega$
10	1	1	—
-10	7	3	$1+\omega$
7	5	3	$8+3\omega$
-7	5	3	$1+2\omega$
14	1	1	—
-14	1	1	—
35	1	1	—
-35	2	3	$1+\omega$
70	1	1	—
-70	1	1	—

Table 2

4.7. The proof of the theorem is then finished once we exhibit a suitable set Σ_N; here $N = 70$. There are four quadratic characters of conductor dividing $8 \cdot 5 \cdot 7$, from which it is easily checked that the Frobenius classes of the primes p with $11 \leq p \leq 113$, together with the identity element, suffice, by examining Table 3.

p	11	13	17	19	23	29	31	41	43	47	53	61	71	83	113
$\left(\frac{-1}{p}\right)$	−	+	+	−	−	+	−	+	−	−	+	+	−	−	+
$\left(\frac{2}{p}\right)$	−	−	+	−	+	−	+	+	−	+	−	−	+	−	+
$\left(\frac{5}{p}\right)$	+	−	−	+	−	+	+	+	−	−	−	+	+	−	−
$\left(\frac{7}{p}\right)$	−	−	−	+	−	+	+	−	−	+	+	−	−	+	+

Table 3

5. $\Gamma_{4,3}$

Proposition 5.1. *Let*

$$g(\tau) = 14P(14\tau) - 7P(7\tau) + 2P(\tau) - P(\tau), \quad h(\tau) = \eta(\tau)\eta(2\tau)\eta(7\tau)\eta(14\tau).$$

Then the function

$$f_{28}(\tau) = \frac{1}{8}\big(g(2\tau)h(\tau) + g(\tau)h(2\tau)\big) = \sum_{n=1}^{\infty} a_n q^n$$

is a newform of weight 4 *on* $\Gamma_0(28)$.

Proof. The usual transformation formulae show that it is a cusp form of weight 4 on $\Gamma_0(28)$. There seems to be no way of checking that it is a newform without some brutal calculation. The quickest way is to evaluate the first few Fourier coefficients and compare with the tables of [**3**].

5.2. Let σ_ℓ be the ℓ-adic representation ${}_{\Gamma_{4,3}}\mathcal{W}_\ell^2$, and let $\{\sigma'_\ell\}$ be the compatible system of 2-dimensional ℓ-adic representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ attached to f_{28}.

Theorem 5.3. σ_ℓ *and* σ'_ℓ *are isomorphic.*

Proof. We proceed as in §3, and only indicate the changes that have to be made to the argument given there. Table 1 and the explicit formula for f_{28} shows that $\operatorname{tr}\sigma_2(\mathrm{Fr}_p) = \operatorname{tr}\sigma'_2(\mathrm{Fr}_p)$ for $p = 5$, $11 \le p \le 113$. Again the only candidate for a cyclic cubic extension cut out by $\tilde{\sigma}_2$ is $\mathbb{Q}(\zeta_7)^+$, which is eliminated at once by considering $p = 11$ as before.

5.4. To eliminate the possibility that $\tilde{\sigma}_2$ has image S_3 we consider again candidate quadratic fields $E = \mathbb{Q}(\sqrt{d})$, where now $d \in \{-1, \pm 2, \pm 3, \pm 6, \pm 7, \pm 14, \pm 21, \pm 42\}$. Applying

Bad primes: 2, 3, 7			
d	f	$\#G_{\mathfrak{f}}$	generators for $G_{\mathfrak{f}}$
-1	9	3	$2+\omega$
2	63	9	$1+\omega$; $5+\omega$
-2	9	3	$3+\omega$
3	9	3	$2+\omega$
-3	126	81	$3+\omega$; $3+2\omega$; $5+\omega$; $4+3\omega$
6	9	9	$5+2\omega$; $1+\omega$
-6	63	9	$1+2\omega$; $5+4\omega$
7	9	3	$8+3\omega$
-7	9	3	$1+2\omega$
14	9	3	$15+4\omega$
-14	9	3	$11+6\omega$
21	18	9	$2+\omega$; ω
-21	9	9	$2+\omega$; $10+\omega$
42	9	9	$13+2\omega$; $17+2\omega$
-42	9	3	$1+2\omega$

Table 4

the algorithm of §3 we arrive at Table 4, in which the entries have the same meaning as in Table 2. This shows that the images of σ_2 and σ_2' are pro-2-groups.

5.5. The final step is to exhibit a set Σ_N; here $N = 42$, and from Table 5 we see that it is enough to take the Frobenius elements for primes p with $p = 5$ or $11 \le p \le 113$. This concludes the proof of the theorem.

p	5	11	13	19	23	29	31	37	43	47	59	73	79	101	113
$\left(\frac{-1}{p}\right)$	+	−	+	−	−	+	−	+	−	−	−	+	−	+	+
$\left(\frac{2}{p}\right)$	+	−	−	−	+	−	+	−	−	+	−	+	+	−	+
$\left(\frac{3}{p}\right)$	−	+	+	−	+	−	−	+	−	+	+	+	−	−	−
$\left(\frac{7}{p}\right)$	−	−	−	+	−	+	+	+	−	+	+	−	−	−	+

Table 5

References

1 A. O. L. Atkin, H. P. F. Swinnerton-Dyer; *Modular forms on noncongruence subgroups.* AMS Proc. Symp. Pure Math. XIX (1971), 1–25

2 B. J. Birch, W. Kuyk; *Modular functions of one variable IV.* Lect. notes in mathematics 476 (Springer 1973)

3 H. Cohen, Skoruppa, D. Zagier; Tables of Hecke eigenvalues . Unpublished

4 P. Deligne; *Formes modulaires et représentations ℓ-adiques.* Sém. Bourbaki, éxposé 355. Lect. notes in mathematics **179,** 139–172 (Springer, 1969)

5 G. Faltings; *Endlichkeitsättze für abelsche Varietäten über Zahlkörpern.* Inventiones math. **73** (1983), 349–366

6 R. Livné; *Cubic exponential sums and Galois representations.* Contemp. Math. **67** (1987), 247–261

7 K. Ribet; *Galois representations attached to eigenforms with Nebentypus.* Modular functions of one variable V. Lect. notes in mathematics **601,** 17–52 (Springer, 1977)

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

9 A. J. Scholl; *The ℓ-adic representations associated to a certain noncongruence subgroup.* J. fur die reine und ang. Math. **392** (1988), 1–15

10 J.-P. Serre; *Résumé de cours 1984–5, Collège de France.*

Department of Mathematical Sciences
Science Laboratories
University of Durham
Durham DH1 3LE
England

e-mail: a.j.scholl@durham.ac.uk