

On icosahedral Artin representations

Kevin Buzzard,
Department of Mathematics,
Imperial College,
London,
U.K.

Mark Dickinson,
Department of Mathematics,
Harvard University,
Cambridge,
MA 02138,
U.S.A.

Nick Shepherd-Barron,
D.P.M.M.S.,
Cambridge University,
Cambridge,
U.K.

Richard Taylor,¹
Department of Mathematics,
Harvard University,
Cambridge,
MA 02138,
U.S.A.

September 20, 1999

¹Partially supported by NSF Grant DMS-9702885 and by the Miller Institute at the University of California at Berkeley

Introduction

Artin [A] conjectured that the L -series $L(r, s)$ of any continuous representation $r : \text{Gal}(\mathbb{Q}^{ac}/\mathbb{Q}) \rightarrow GL_n(\mathbb{C})$ is entire except possibly for a pole at $s = 1$ when r contains the trivial representation. The case $n = 1$ is simply a restatement of the Kronecker-Weber theorem and standard results on the analytic continuation of Dirichlet L -series. Artin proved his conjecture when r is induced from a 1-dimensional representation of an open subgroup of $\text{Gal}(\mathbb{Q}^{ac}/\mathbb{Q})$. Moreover, Brauer [Br] was able to show in general that $L(r, s)$ is meromorphic on the whole complex plane. Since then the only real progress has been for $n = 2$.

When $n = 2$ such representations can be classified according to the image of the projectivised representation $\text{proj } r : \text{Gal}(\mathbb{Q}^{ac}/\mathbb{Q}) \rightarrow PGL_2(\mathbb{C})$. This image is either cyclic, dihedral, the alternating group A_4 (the tetrahedral case), the symmetric group S_4 (the octahedral case) or the alternating group A_5 (the icosahedral case). When the image of $\text{proj } r$ is cyclic then r is reducible and Artin's conjecture follows from the $n = 1$ case. When the image of $\text{proj } r$ is dihedral then r is induced from a character of an open subgroup of index 2, and so Artin himself proved the conjecture in this case. (Note however that the result is implicit in earlier work of Hecke (see [He]).) Langlands [Langl] proved Artin's conjecture for tetrahedral and some octahedral representations. Tunnell [Tu] extended this to all octahedral representations. These results are based on Langlands' theory of cyclic base change for automorphic representations of GL_2 , and so the method seems to be restricted (at best) to cases where the image of r is soluble. A number of people, including Buhler [Buh] and Frey et al. [F], used computer calculations to check Artin's conjecture for a few icosahedral examples.

The contribution here to the problem is to treat some (infinite families of) icosahedral cases. More precisely we prove the following theorem.

Theorem A. *Suppose that $r : \text{Gal}(\mathbb{Q}^{ac}/\mathbb{Q}) \rightarrow GL_2(\mathbb{C})$ is a continuous irreducible representation and that r is odd, i.e., the determinant of complex conjugation is -1 . If r is icosahedral suppose that*

- *$\text{proj } r$ is unramified at 2 and that the image of a Frobenius element at 2 under $\text{proj } r$ has order 3,*
- *and $\text{proj } r$ is unramified at 5.*

Then there is a weight one newform f such that for all prime numbers p the p^{th} Fourier coefficient of f equals the trace of Frobenius at p on the inertia at p coinvariants of r . In particular the Artin L -series for r is the Mellin transform of a weight one newform and is an entire function.

The proof follows a strategy outlined by one of us (R.T.) to Wiles in 1992 (see [Ta2]), which has now been carried out by the four of us in three main steps (see [ST], [Di] and [BT]). The purpose of this article is simply to pull these results together and document some technical results which we require, but do not seem to be available in the literature. The result is that this paper is rather technical. The reader who simply desires to get an overview of the main ideas of the proof should consult [Ta2], perhaps followed by [ST], [BT] and [Di], rather than this paper.

One might hope that extensions of our method may treat all odd two-dimensional icosahedral representations of $\text{Gal}(\mathbb{Q}^{ac}/\mathbb{Q})$, although considerable work remains to be done. On the other hand our method seems to offer no prospect of treating the general Artin conjecture.

1 Mod 2 icosahedral representations.

In this section we will give a slight extension of results in [ST]. This could be avoided by appealing to the results of [G]. However his results depend on certain “unchecked compatibilities”, and so we prefer to make our result unconditional by using this more ad hoc argument. We remark that the hypotheses in our main theorem could be weakened if one could make Gross’ theorem unconditional.

We start with a strengthening of theorem 3.4 of [ST].

Theorem 1.1. *Fix a continuous homomorphism*

$$\bar{\rho} : \text{Gal}(\mathbb{Q}^{ac}/\mathbb{Q}) \longrightarrow SL_2(\mathbb{F}_4).$$

Suppose that $\bar{\rho}$ is unramified at 2 and that $\bar{\rho}(\text{Frob}_2)$ has distinct eigenvalues $\alpha, \beta \in \mathbb{F}_4^\times$. Then there is an abelian surface A/\mathbb{Q} together with a principal polarisation $\lambda : A \longrightarrow A^\vee$ and an embedding $i : \mathbb{Z}[(1 + \sqrt{5})/2] \hookrightarrow \text{End}(A)$ (both defined over \mathbb{Q}) such that

1. $\lambda \circ i(a) = i(a)^\vee \circ \lambda$ for all $a \in \mathbb{Z}[(1 + \sqrt{5})/2]$;
2. *the action of $\text{Gal}(\mathbb{Q}^{ac}/\mathbb{Q})$ on $A[2] \cong \mathbb{F}_4^2$ is equivalent to $\bar{\rho}$;*
3. *A has good ordinary reduction at 2 and $\text{Frob}_2 = \alpha$ on $A[2]^{\text{et}}$ (the generic fibre of the maximal etale quotient of the two torsion on the Néron model of A over \mathbb{Z});*
4. *and the action of $\text{Gal}(\mathbb{Q}^{ac}/\mathbb{Q})$ on the $\sqrt{5}$ -division points, $A[\sqrt{5}]$ is via a surjection $\text{Gal}(\mathbb{Q}^{ac}/\mathbb{Q}) \twoheadrightarrow GL_2(\mathbb{F}_5)$.*

Proof. With the third condition removed this is the main result of [ST]. The proof of this strengthening is a slight variant of the argument of that paper. We start by recalling some of the constructions there.

We fix an identification of \mathbb{F}_4 with $\mathbb{Z}[(1 + \sqrt{5})/2]/(2)$ and of $SL_2(\mathbb{F}_4)$ with A_5 . We let Y/\mathbb{Q} denote the smooth cubic surface given in \mathbb{P}^4 by

$$\sum_{i=1}^5 y_i = \sum_{i=1}^5 y_i^3 = 0.$$

The group A_5 acts on Y by permuting the variables. We let $Y^0 \subset Y$ (resp. $Y^1 \subset Y$) denote the complement of the 15 lines conjugate to $(s : -s : t : -t : 0)$ (resp. the complement of the 10 points conjugate to $(1 : -1 : 0 : 0 : 0)$). We let $Y_{\bar{\rho}}$ (resp. $Y_{\bar{\rho}}^0$, resp. $Y_{\bar{\rho}}^1$) denote the twist of Y (resp. Y^0 , resp. Y^1) by $\bar{\rho} : \text{Gal}(\mathbb{Q}^{ac}/\mathbb{Q}) \rightarrow A_5$. There is an étale \mathbb{P}^1 -bundle $C_{\bar{\rho}} \rightarrow Y_{\bar{\rho}}^1$ together with 6 distinguished sections $s_1, \dots, s_6 : Y_{\bar{\rho}}^1 \times \mathbb{Q}^{ac} \rightarrow C_{\bar{\rho}} \times \mathbb{Q}^{ac}$ such that the set $\{s_1, \dots, s_6\}$ is $\text{Gal}(\mathbb{Q}^{ac}/\mathbb{Q})$ -invariant. Over $Y_{\bar{\rho}}^0$ the sections are distinct. (This is not explicitly proved in [ST], but one may argue as follows. We will use without comment some notation from section 2 of [ST]. By the formulae on pages 15-17 of [DO] the locus in P_1^6 where s_1, \dots, s_6 are distinct is identified with the complement, Z^0 , in $\sum_{i=1}^6 z_i = \sum_{i=1}^6 z_i^3 = 0$ of the 15 S_6 -conjugates of the plane $(s : -s : t : -t : u : -u)$. Then using lemma 2.4 of [ST] it is easy to see that $j^{-1}Z^0 = Y^0$, and the claim follows.)

We let $W_{\bar{\rho}}/\mathbb{Q}$ denote the \mathbb{F}_4 -vector space scheme corresponding to $\bar{\rho} : \text{Gal}(\mathbb{Q}^{ac}/\mathbb{Q}) \rightarrow GL_2(\mathbb{F}_4)$. It comes with a standard pairing

$$W_{\bar{\rho}} \times W_{\bar{\rho}} \longrightarrow \mu_2$$

which on \mathbb{Q}^{ac} -points sends

$$(a, b) \times (c, d) \longmapsto (-1)^{\text{tr}_{\mathbb{F}_4/\mathbb{F}_2}(ad-bc)}.$$

Then there is a coarse moduli space $\mathcal{H}_{\bar{\rho}}/\mathbb{Q}$ parametrising quadruples (A, λ, i, α) where (A, λ) is a principally polarised abelian surface, $i : \mathbb{Z}[(1 + \sqrt{5})/2] \hookrightarrow \text{End}(A)$ has image fixed by the λ -Rosati involution and where $\alpha : W_{\bar{\rho}} \xrightarrow{\sim} A[2]$ is an isomorphism of \mathbb{F}_4 -vector space schemes taking the standard pairing to the λ -Weil pairing. There is a Zariski open subset $\mathcal{H}_{\bar{\rho}}^0 \subset \mathcal{H}_{\bar{\rho}}$ consisting of those geometric points for which the corresponding (A, λ) is a Jacobian. Then there is an isomorphism $Y_{\bar{\rho}}^0 \cong \mathcal{H}_{\bar{\rho}}^0$ so that a geometric point y of $Y_{\bar{\rho}}^0$ maps to the point parametrising a quadruple (A, λ, i, α) such that (A, λ) is the Jacobian of the curve which maps 2 : 1 to $C_{\bar{\rho}, y}$ ramified exactly at $s_1(y), \dots, s_6(y)$. (Again

this is not explicitly stated in [ST]. To prove it one may assume that $\bar{\rho} = 1$. Recall from [ST] we have maps

$$Y - \rightarrow \mathcal{H}_2^* \longrightarrow \mathcal{A}_2^* - \rightarrow P_1^6.$$

(We keep the notation of [ST], so in particular \mathcal{H}_2^* is a compactification of what we are now calling \mathcal{H}_1 .) The locus of Jacobians in \mathcal{A}_2^* is the locus of points where $\mathcal{A}_2^* - \rightarrow P_1^6$ is regular and map to $Z^0 \subset P_1^6$. Thus Y^0 maps to $\mathcal{H}_1^0 \subset \mathcal{H}_2^*$. On the other hand \mathcal{H}_2^* is the disjoint union of the image of Y^0 and some \mathbb{P}^1 's which get contracted to the points of $P_1^6 - (P_1^6)^s$ (see section 2 of [ST]). Thus, if y is a point of \mathcal{H}_2^* not in the image of Y^0 then either $\mathcal{H}_2^* - \rightarrow P_1^6$ is not regular at y or y gets mapped outside Z^0 . In either case y does not lie in \mathcal{H}_1^0 .)

If $X_{\bar{\rho}}^l$ denotes the blow up of $Y_{\bar{\rho}} \times Y_{\bar{\rho}}$ along the diagonal, then $X_{\bar{\rho}}^l$ has an involution t which exchanges the two factors. We let $X_{\bar{\rho}}$ denote the twist of $X_{\bar{\rho}}^l$ by

$$\text{Gal}(\mathbb{Q}^{ac}/\mathbb{Q}) \twoheadrightarrow \text{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q}) \xrightarrow{\sim} \{1, t\},$$

and $X_{\bar{\rho}}^2$ the complement in $X_{\bar{\rho}}^l$ of the strict transforms of $L \times L$ as L runs over lines on $Y_{\bar{\rho}}$. Then there is a morphism

$$\theta : X_{\bar{\rho}}^2 \longrightarrow Y_{\bar{\rho}}$$

which (loosely speaking) sends (P, Q) to the third point of intersection of the line through P and Q with $Y_{\bar{\rho}}$ (see [ST] for details). We will let $X_{\bar{\rho}}^0$ (resp. $X_{\bar{\rho}}^1$, resp. $D_{\bar{\rho}}/X_{\bar{\rho}}^1$) denote the preimage of $Y_{\bar{\rho}}^0$ (resp. the preimage of $Y_{\bar{\rho}}^1$, resp. the pull back of $C_{\bar{\rho}}$) under θ . Then it is proved in [ST] (lemma 3.1 and proposition 3.2) that $X_{\bar{\rho}}/\mathbb{Q}$ is rational and that $D_{\bar{\rho}}/X_{\bar{\rho}}^1$ is a Zariski \mathbb{P}^1 -bundle.

The argument preceding lemma 2.7 of [ST] shows that given $x \in X_{\bar{\rho}}^0$ we can find a Zariski open subset $U \subset X_{\bar{\rho}}^0$ containing x and a principally polarised abelian surface $(A_U, \lambda_U)/U$ such that

1. for all $x_1 \in U$ the fibre $(A_U, \lambda_U)_{x_1}$ is the Jacobian of a curve which maps $2 : 1$ to $D_{\bar{\rho}, x_1}$ ramified exactly at $s_1(x_1), \dots, s_6(x_1)$;
2. there is an isomorphism $\alpha_U : W_{\bar{\rho}} \xrightarrow{\sim} A_U[2]$ of finite flat group schemes over U with alternating pairings;
3. and there exists $i_U : \mathbb{Z}[(1 + \sqrt{5})/2] \hookrightarrow \text{End}(A_U)$ which is compatible with α_U and the action of \mathbb{F}_4 on $W_{\bar{\rho}}$.

(In [ST] the existence of i_U is only explained over a non-empty open subset of U . That it extends to the whole of U follows from remark 1.10 (a) of chapter I of [CF].) We remind the reader that A_U is not canonical. Suppose that \bar{x} is a geometric point of U . If f is an automorphism of $(A_U, \lambda_U, i_U, \alpha_U)_{\bar{x}}$ then $T_2(f) \equiv 1 \pmod{2}$ and so $T_2(f^2) \equiv 1 \pmod{4}$. As f has finite order this implies that $f^2 = 1$. If $f \neq \pm 1$ then $A_{U, \bar{x}} \cong (1+f)/2A_{U, \bar{x}} \oplus (1-f)/2A_{U, \bar{x}}$ and λ_U correspondingly decomposes as the direct sum of two polarisations. This contradicts the fact that $\theta(\bar{x}) \in Y_{\bar{\rho}}^0 \cong \mathcal{H}_{\bar{\rho}}^0$. Thus we must have $\text{Aut}((A_U, \lambda_U, i_U, \alpha_U)_{\bar{x}}) = \{\pm 1\}$. In particular if we set

$$\tilde{U} = \{(a, b) \in (A_U \times A_U)[\sqrt{5}] \mid \langle a, b \rangle \neq 1\} / \sim,$$

where $(a, b) \sim (a', b')$ if and only if $(a, b) = \pm(\mu a', b')$ for some $\mu \in \mathbb{F}_5^\times$, then the construction of \tilde{U} is canonical and so we can glue the \tilde{U}/U to give an étale cover $\tilde{X}_{\bar{\rho}}^0/X_{\bar{\rho}}^0$ of degree 60. The argument of lemma 2.7 of [ST] shows that $\tilde{X}_{\bar{\rho}}^0$ is geometrically irreducible.

Suppose for the moment that we can find a point $x_2 \in X_{\bar{\rho}}^0(\mathbb{Q}_2)$, a Zariski open $U_2 \subset X_{\bar{\rho}}^0 \times \mathbb{Q}_2$ as above and a continuous character $\chi_2 : \text{Gal}(\mathbb{Q}_2^{ac}/\mathbb{Q}_2) \rightarrow \{\pm 1\}$ such that

- the twist $A_{U_2, x_2}(\chi_2)$ of A_{U_2, x_2} by χ_2 has good reduction
- and, if $\overline{A}_{U_2, x_2}(\chi_2)$ denotes the mod 2 reduction of the Néron model of $A_{U_2, x_2}(\chi_2)$ over \mathbb{Z}_2 , then $\overline{A}_{U_2, x_2}(\chi_2)[2]^{\text{ét}} \neq (0)$ and Frob_2 acts on $\overline{A}_{U_2, x_2}(\chi_2)[2]^{\text{ét}}$ by α .

Then we can find a neighbourhood (for the 2-adic topology) $\mathcal{U} \subset X_{\bar{\rho}}^0(\mathbb{Q}_2)$ of x_2 such that if $x \in \mathcal{U}$ then

- $x \in U_2$,
- $A_{U_2, x}(\chi_2)$ has good reduction at 2
- and $\overline{A}_{U_2, x}(\chi_2)[2] \cong \overline{A}_{U_2, x_2}(\chi_2)[2]$.

Because $X_{\bar{\rho}}$ is rational, it follows from Ekedahl's version of the Hilbert irreducibility theorem (see theorem 1.3 of [E]) that we can find a point $x \in X_{\bar{\rho}}^0(\mathbb{Q})$ such that

- $x \in \mathcal{U}$
- and if \tilde{x} is a point of $\tilde{X}_{\bar{\rho}}^0$ above x then $[\mathbb{Q}(\tilde{x}) : \mathbb{Q}] = 60$.

Suppose that U is a Zariski neighbourhood of x in $X_{\bar{p}}^0$ as above. Then $(A_U, \lambda_U, i_U, \alpha_U)_x \times \mathbb{Q}_2$ is a twist by some character $\chi'_2 : \text{Gal}(\mathbb{Q}_2^{ac}/\mathbb{Q}_2) \rightarrow \{\pm 1\}$ of $(A_{U_2}, \lambda_{U_2}, i_{U_2}, \alpha_{U_2})_x$. Choose a character $\chi : \text{Gal}(\mathbb{Q}^{ac}/\mathbb{Q}) \rightarrow \{\pm 1\}$ which restricts to $\chi_2 \chi'_2$ on $\text{Gal}(\mathbb{Q}_2^{ac}/\mathbb{Q}_2)$. Then $A_{U,x}(\chi)$ has the following properties.

- $(A_{U,x}(\chi), \lambda_{U,x})/\mathbb{Q}$ is a principally polarised abelian surface.
- $i_{U,x} : \mathbb{Z}[(1 + \sqrt{5})/2] \hookrightarrow \text{End}(A_{U,x}(\chi))$ and the image is fixed by the $\lambda_{U,x}$ -Rosati involution.
- As an $\mathbb{F}_4[\text{Gal}(\mathbb{Q}^{ac}/\mathbb{Q})]$ -module, $A_{U,x}(\chi)[2](\mathbb{Q}^{ac})$ is equivalent to ρ .
- $A_{U,x}(\chi) \times \mathbb{Q}_2 \cong A_{U_2,x}(\chi_2)$ and so $A_{U,x}(\chi)$ has good reduction at 2.
- $\overline{A}_{U,x}(\chi)[2] \cong \overline{A}_{U_2,x_2}(\chi_2)[2]$ and so $\overline{A}_{U,x}(\chi)[2]^{\text{et}} \neq (0)$ and Frob_2 acts on $\overline{A}_{U,x}(\chi)[2]^{\text{et}}$ by α .
- If G denote the image $\text{Gal}(\mathbb{Q}^{ac}/\mathbb{Q})$ in $\text{Aut}_{\mathbb{F}_4}(A_{U,x}(\chi)[\sqrt{5}]) \cong GL_2(\mathbb{F}_5)$ then $\det G = \mathbb{F}_5^\times$ (because of the λ -Weil pairing) and

$$\#G/G \cap \left\{ \begin{pmatrix} \mu & 0 \\ 0 & \nu \end{pmatrix} \middle| \nu = \pm 1, \mu \in \mathbb{F}_5^\times \right\} = 60.$$

Then it is elementary to check that $G = GL_2(\mathbb{F}_5)$.

It remains to explain the construction of x_2 . This we will do in two steps. More precisely we will show the following two results.

1. There is a quadruple (A, λ, i, α) (as above) defined over K such that A has good reduction and, if \overline{A} denotes the reduction of its Néron model, then $\overline{A}[2]^{\text{et}} \neq (0)$ and Frob_2 acts on $\overline{A}[2]^{\text{et}}$ by α .
2. If $y \in Y_{\bar{p}}^0(\mathbb{Q}_2)$ then there is a point of $X_{\bar{p}}^0(\mathbb{Q}_2)$ mapping to y under θ .

The first assertion gives a point $y_2 \in \mathcal{H}_{\bar{p}}^0(\mathbb{Q}_2) = Y_{\bar{p}}^0(\mathbb{Q}_2)$ and the second a point $x_2 \in X_{\bar{p}}^0(\mathbb{Q}_2)$ mapping to y_2 under θ . This point x_2 will suffice.

We turn first to the second assertion. Suppose $y \in Y_{\bar{p}}^0(\mathbb{Q}_2)$ and let $Y_{\bar{p}}(y)'$ denote the complement in $Y_{\bar{p}}$ of the intersection of $Y_{\bar{p}}$ with the tangent plane to $Y_{\bar{p}}$ at y . Thus $Y_{\bar{p}}(y)'$ is a smooth affine cubic surface. There is an involution ι_y of $Y_{\bar{p}}(y)$ which sends any point z to the third point of intersection of the line through y and z with the cubic surface $Y_{\bar{p}}$. We will let $Y_{\bar{p}}(y)$ denote the twist of $Y_{\bar{p}}(y)'$ by ι_y over $\text{Gal}(\mathbb{Q}_2(\sqrt{5})/\mathbb{Q}_2)$. We may identify $Y_{\bar{p}}(y)$ as a Zariski open subset of the fibre of $\theta : X_{\bar{p}}^0 \rightarrow Y_{\bar{p}}^0$ above y , and so it suffices to show that $Y_{\bar{p}}(y)(\mathbb{Q}_2) \neq \emptyset$.

Note that the equations defining Y also define a smooth projective surface over \mathbb{Z}_2 , which we will also denote by Y . The construction of $Y_{\bar{\rho}}$, $Y_{\bar{\rho}}(y)'$ and $Y_{\bar{\rho}}(y)$ from Y all make sense over \mathbb{Z}_2 and give rise to smooth relative surfaces over \mathbb{Z}_2 , which we will denote by the same symbols. (We are using the fact that $\bar{\rho}$ is unramified. We are not asserting that these integral models have any moduli theoretic meaning.) By Hensel's lemma it will suffice to show that $Y_{\bar{\rho}}(y)(\mathbb{F}_2)$ is non-empty.

Without loss of generality the surface $Y_{\bar{\rho}} \times \mathbb{F}_2$ is given in \mathbb{P}^3 by the equation

$$X_1^3 + X_1X_2^2 + X_2^3 + X_3^2X_4 + X_3X_4^2 = 0.$$

(If γ is a root of $T^3 + T + 1 = 0$, then $(X_1 : X_2 : X_3 : X_4)$ corresponds to the point

$$\begin{aligned} ((X_3 + X_4) + X_1\gamma + X_2\gamma^2 : (X_3 + X_4) + X_1\gamma^2 + X_2\gamma^4 : \\ (X_3 + X_4) + X_1\gamma^4 + X_2\gamma : X_3 : X_4) \end{aligned}$$

of $Y \times \mathbb{F}_2$.) Thus $Y_{\bar{\rho}}(\mathbb{F}_2)$ has three points $P = (0 : 0 : 1 : 0)$, $Q = (0 : 0 : 0 : 1)$ and $R = (0 : 0 : 1 : 1)$.

First suppose that y reduces to P . Then $Y_{\bar{\rho}}(y) \times \mathbb{F}_2$ is the surface given in affine 3-space by the equation

$$x_1^3 + x_1x_2^2 + x_2^3 + x_3 + x_3^2 = 0$$

and ι_y maps (x_1, x_2, x_3) to

$$(x_1, x_2, x_3 + 1).$$

(Here we set $x_i = X_i/X_4$.) Thus $Y_{\bar{\rho}}(y) \times \mathbb{F}_2$ is given in affine 3-space by the equation

$$y_1^3 + y_1y_2^2 + y_2^3 + 1 + y_3 + y_3^2 = 0.$$

(Here we let (y_1, y_2, y_3) correspond to the point $(x_1, x_2, x_3) = (y_1, y_2, y_3 + (1 + \sqrt{5})/2)$.) Thus $Y_{\bar{\rho}}(y)(\mathbb{F}_2)$ consists of 6 points.

The case that y reduces to Q is exactly analogous, and again we see that $Y_{\bar{\rho}}(y)(\mathbb{F}_2)$ consists of 6 points.

Thirdly suppose that y reduces to R . Introducing a new variable $X'_4 = X_3 + X_4$ we see that $Y_{\bar{\rho}} \times \mathbb{F}_2$ can also be described in \mathbb{P}^3 by the equation

$$X_1^3 + X_1X_2^2 + X_2^3 + X_3^2X'_4 + X_3(X'_4)^2 = 0,$$

and that in these new coordinates R becomes the point $(0 : 0 : 1 : 0)$. Thus the analysis is the same again and we see that $Y_{\bar{\rho}}(y)(\mathbb{F}_2)$ again consists of 6 points.

Finally we turn to our first assertion. Let K denote the field $\mathbb{Q}(a)$, where a is a root of

$$T^4 + 13T^2 + 41 = 0.$$

Then $13 + 2a^2$ is a square root of 5, which we will denote $\sqrt{5}$. Moreover K is a CM field with totally real subfield $\mathbb{Q}(\sqrt{5})$. The inverse different $\mathfrak{d}_{K/\mathbb{Q}}^{-1}$ is principal with generator $\xi = (13a + 2a^3)^{-1}$. We have the prime factorisation

$$2\mathcal{O}_K = (((1 + \sqrt{5})/2 + a)/2)((1 + \sqrt{5})/2 - a)/2).$$

As ± 1 are the only roots of unity in K , the only elements of K^\times with norm down to $\mathbb{Q}(\sqrt{5})$ equal to 2 are $(\pm(1 + \sqrt{5})/2 \pm a)/2$.

The normal closure of K/\mathbb{Q} is $K(\sqrt{41})/\mathbb{Q}$ and $\text{Gal}(K(\sqrt{41})/\mathbb{Q})$ is generated by two elements σ and τ , where

$$\begin{aligned} \sigma(a) &= \sqrt{41}/a & \tau(a) &= a \\ \sigma(\sqrt{41}) &= -\sqrt{41} & \tau(\sqrt{41}) &= -\sqrt{41}. \end{aligned}$$

Thus $\sigma^4 = \tau^2 = 1$, $\tau\sigma\tau = \sigma^3$ and $\sigma^2 = c$. By the Chebotarev density theorem we may choose a prime \wp of \mathcal{O}_K which is split completely and lies above a rational prime $p \equiv 3 \pmod{4}$. Let α_0 denote the character

$$\mathcal{O}_{K,p}^\times \twoheadrightarrow \mathcal{O}_{K,\wp}^\times \twoheadrightarrow \{\pm 1\}.$$

Fix an embedding $K(\sqrt{41}) \hookrightarrow \mathbb{C}$ such that a has negative imaginary part, $13 + 2a^2 > 0$ and $\sqrt{41} > 0$. Then $\Phi = \{1, \sigma\}$ is a CM-type with reflex (L, Φ') , where $L = K(\sqrt{41})^{\{1, \sigma\}}$ and $\Phi' = \{1, \sigma^3\}$. The field L is also a CM field and has totally real subfield $\mathbb{Q}(\sqrt{41})$. It is isomorphic to the field obtained by adjoining a root of $T^4 + 26T^2 + 5$ to \mathbb{Q} . Then L has class number 1 and \mathcal{O}_L^\times is generated by -1 and $32 + 5\sqrt{41}$. We have a prime factorisation $2\mathcal{O}_L = II^cJ$ with $\#\mathcal{O}_L/I = 2$ and $\#\mathcal{O}_L/J = 4$. We have a homomorphism

$$\begin{aligned} N_{\Phi'} : L^\times &\longrightarrow K^\times \\ x &\longmapsto x\sigma^3(x). \end{aligned}$$

Then $N_{\Phi'}$ extends to a map $\mathbb{A}_L^\times \rightarrow \mathbb{A}_K^\times$. Define a continuous homomorphism

$$\alpha : \mathbb{A}_L^\times \longrightarrow K^\times$$

by setting

- $\alpha|_{L^\times} = N_{\Phi'}$,
- $\alpha|_{\mathcal{O}_{L,p}^\times} = \alpha_0 \circ N_{\Phi'}$,
- $\alpha|_{\mathcal{O}_{L,p'}^\times} = 1$ for any rational prime $p' \neq p$,
- and $\alpha|_{L_v^\times} = 1$ for any infinite place v of L .

(This makes sense because the class number of L is one and because $(\alpha_0 \circ N_{\Phi'})|_{\mathcal{O}_L^\times} = N_{\Phi'}|_{\mathcal{O}_L^\times}$.)

Then there is a triple $(A, \lambda, i)/L$ (a principally polarised simple abelian surface with an action i of \mathcal{O}_K) which has type $(K, \Phi, \mathcal{O}_K, \xi)$ and character α . (See [Lang], especially theorems 3.6 and 4.5 of chapter 1 and corollary 5.3 of chapter 5.) Because α is trivial on $\mathcal{O}_{L,I}^\times$, we see from the fundamental theorem of complex multiplication (see theorem 1.1 of chapter 4 of [Lang]) that, for a rational prime $l > 2$, inertia at I acts trivially on $T_l A$, the l -adic Tate module of A . Thus A has good reduction at I . Let \overline{A} denote the reduction mod I of the Néron model of A . Moreover, if $I = (a)$ then Frob_2 acts on $T_l A$ via $\pm N_{\Phi'} a$. As $N_{K/\mathbb{Q}(\sqrt{5})} N_{\Phi'} a = 2$ we see that $\pm N_{\Phi'} a = (\pm(1 + \sqrt{5})/2 \pm a)/2$ and so

$$\pm N_{\Phi'} a \equiv (1 + \sqrt{5})/2 \pmod{(N_{\Phi'} I)^c}.$$

Thus $\overline{A}[N_{\Phi'} I^c]$ is étale and Frob_2 acts on it as $(1 + \sqrt{5})/2$.

If $\alpha = (1 + \sqrt{5})/2$ then $(A, \lambda, i|_{\mathbb{Z}[(1+\sqrt{5})/2]})/L_I$ will suffice to give the desired example. If on the other hand $\alpha = (1 - \sqrt{5})/5$ then $(A, \lambda, i|_{\mathbb{Z}[(1+\sqrt{5})/2]} \circ \sigma)/L_I$ will suffice to give the desired example. \square

We would now like to apply this theorem to deduce the modularity of certain mod 2 representations. If N , M and k are positive integers we will denote by $h_k(N; M)$ the \mathbb{Z} -algebra generated by the Hecke operators T_p and $\langle p \rangle$ for any prime $p \nmid NM$, and by the Hecke operators U_p for any prime $p|NM$ acting on the space of weight k cusp forms for $\Gamma_1(N) \cap \Gamma_0(M)$. If $M|N$ we will drop it from the notation and write simply $h_k(N)$. If $p \nmid NM$ set $S(p) = p^{k-2} \langle p \rangle$. Also for every positive integer n define $T(n)$ by the relations

- $T(n_1 n_2) = T(n_1) T(n_2)$ if n_1 and n_2 are coprime,
- $(1 - T_p X + p S(p) X^2) \sum_{r=1}^{\infty} T(p^r) X^r = 1$ for any prime $p \nmid NM$,
- and $T(p^r) = U_p^r$ for every prime $p|NM$.

Corollary 1.2. *Fix a continuous homomorphism*

$$\bar{\rho} : \text{Gal}(\mathbb{Q}^{ac}/\mathbb{Q}) \longrightarrow SL_2(\mathbb{F}_4).$$

Suppose that $\bar{\rho}$ is unramified at 2 and 5 and that $\bar{\rho}(\text{Frob}_2)$ has distinct eigenvalues $\alpha, \beta \in \mathbb{F}_4^\times$. Then there is an odd positive integer N divisible by all primes at which $\bar{\rho}$ ramifies and a homomorphism

$$\bar{f}_\alpha : h_2(N) \longrightarrow \mathbb{F}_4$$

which takes

1. T_p to $\text{tr} \bar{\rho}(\text{Frob}_p)$ for all primes $p \nmid 2N$;
2. T_2 to α ;
3. and U_p to 0 for all $p \mid N$.

Proof. First note that in [BCDT] theorem 4.1 of [ST] is improved to suppress the condition on $\bar{\rho}(I_3)$. Thus theorem 4.2 of [ST] can be improved to suppress the condition that A has semi-stable reduction at 3. The proof of this corollary is then the same as the proof of theorem 4.3 in [ST] except that we replace references to theorem 4.2 by this improvement and references to theorem 3.6 by references to theorem 1.1 of this paper. \square

2 2-adic modular forms.

In this section we will recall some facts about 2-adic modular forms. (The most important for us is the assertion that a 2-adic limit of ordinary classical modular forms is overconvergent - see lemma 2.9.) Many of these assertions appear in the literature, but we have not been able to locate proofs for them. For primes $l > 3$ such results are due to Katz [K], but we will follow Coleman's approach via rigid geometry. In this section we will work with an arbitrary rational prime l as it makes no difference to the arguments.

Fix an integer $N \geq 5$ which is not divisible by l . Let $X_1(N)/\mathbb{Z}_l$ denote the usual compactification of the moduli scheme for pairs (E, i) where E is an elliptic curve and i is an embedding $\mu_N \hookrightarrow E[N]$. Also let $X_1(N; l)/\mathbb{Z}_l$ denote the usual compactification of the moduli scheme for pairs $(E, i, E \xrightarrow{\alpha} E')$ where E is an elliptic curve, i is an embedding $\mu_N \hookrightarrow E[N]$ and $\alpha : E \rightarrow E'$ is an isogeny of degree l . There are two natural projections π_1 and $\pi_2 : X_1(N; l) \rightarrow X_1(N)$, which take $(E, i, E \xrightarrow{\alpha} E')$ to (E, i) and $(E', \alpha \circ i)$ respectively.

We will let $\omega_{X_1(N)}$ (resp. $\omega_{X_1(N;l)}$) denote the canonical extension to the cusps of the pullback by the identity section of the sheaf of relative differentials of the universal elliptic curve over the non-cuspidal locus of $X_1(N)$ (resp. $X_1(N;l)$). Then $\pi_1^*\omega_{X_1(N)} = \omega_{X_1(N;l)}$ and there is a natural map $j = (\alpha^\vee)^* : \omega_{X_1(N;l)} \rightarrow \pi_2^*\omega_{X_1(N)}$. After one inverts l , j becomes an isomorphism.

We will let SS denote the finite set of points in $X_1(N)(\mathbb{F}_l^{ac})$ corresponding to supersingular elliptic curves. For $s \in SS$ choose $T_s \in \mathcal{O}_{X_1(N) \times W(\mathbb{F}_l^{ac}), s}$ so that

$$(X_1(N) \times W(\mathbb{F}_l^{ac}))_s^\wedge \cong \mathrm{Spf} W(\mathbb{F}_l^{ac})[[T_s]],$$

and so that if $\sigma \in \mathrm{Gal}(\mathbb{F}_l^{ac}/\mathbb{F}_l)$ and $s \in SS$ then

$$(1 \times \sigma^*)^*(T_{(1 \times \sigma^*)(s)}) = T_s.$$

(Here $W(k)$ denotes the Witt vectors of k .) We will let $X_1(N)^{\mathrm{an}}$ denote the rigid analytic space over \mathbb{C}_l (the completion of \mathbb{Q}_l^{ac}) associated to $X_1(N)$. It is connected. If $r \in l^\mathbb{Q}$ and $1 \geq r \geq 1/l$ we will let $X_1(N)_{\geq r}$ (if $r \neq 1/l$) (resp. $X_1(N)_{> r}$ (if $r \neq 1$)) denote the rigid analytic subspace of $X_1(N)^{\mathrm{an}}$ where for each $s \in SS$ we remove all points x in the residue disc of s with $|T_s(x)|_l < r$ (resp. $\leq r$). (Here $|\cdot|_l$ is the l -adic absolute value normalised by $|l|_l = 1/l$.) We note that $X_1(N)_{\geq r}$ is connected. (Suppose that $X_1(N)_{\geq r}$ had an admissible open cover $\{U, V\}$, with U and V non-empty and disjoint. For each $s \in SS$ the preimage of s in $X_1(N)_{\geq r}$ is an annulus and hence connected and contained in either U or V . Let \tilde{U} (resp. \tilde{V}) denote the union of U (resp. V) with the residue disc of each $s \in SS$ for which the preimage of s in $X_1(N)_{\geq r}$ is contained in U (resp. V). Then $\{\tilde{U}, \tilde{V}\}$ is an admissible open cover of $X_1(N)^{\mathrm{an}}$ by disjoint non-empty sets, a contradiction.)

We will let $\mathcal{M}_k^{\geq r}(N)$ (resp. $\mathcal{M}_k^{> r}(N)$) denote the space of sections of $(\omega_{X_1(N)}^{\mathrm{an}})^{\otimes k}$ over $X_1(N)_{\geq r}$ (resp. $X_1(N)_{> r}$). The spaces $\mathcal{M}_k^{\geq r}(N)$ have natural norms making them Banach spaces. More precisely we set

$$|f|_r = \sup_{x \in X_1(N)_{\geq r}(\mathbb{C}_l)} |f|_x,$$

where we define $|f|_x$ as follows. Let $\bar{x} \in X_1(N)(\mathbb{F}_l^{ac})$ denote the reduction of x and let f_0 denote a local generator for $\omega_{X_1(N)}^{\otimes k}$ near \bar{x} . Then we set

$$|f|_x = |(f/f_0)(x)|_l,$$

which is easily checked to be independent of the choice of f_0 . Note that if $r_1 \geq r_2$ and if $f \in \mathcal{M}_k^{\geq r_2}(N)$ then

$$|f|_{r_1} \leq |f|_{r_2}.$$

We will let $X_1(N)^0$ denote the formal completion of $X_1(N)$ along its locally closed subscheme $X_1(N) \times \mathbb{F}_l - SS$. It is a formal scheme over \mathbb{Z}_l . The base change to \mathbb{C}_l of the rigid analytic space associated to $X_1(N)^0$ is just $X_1(N)_{\geq 1}$. Thus we get an identification

$$\Gamma(X_1(N)^0, \omega_{X_1(N)}^{\otimes k}) \widehat{\otimes}_{\mathbb{Z}_l} \mathbb{C}_l \xrightarrow{\sim} \mathcal{M}_k^{\geq 1}(N),$$

under which $\Gamma(X_1(N)^0, \omega_{X_1(N)}^{\otimes k}) \widehat{\otimes}_{\mathbb{Z}_l} \mathcal{O}_{\mathbb{C}_l}$ is identified to the unit ball in $\mathcal{M}_k^{\geq 1}(N)$.

There is a map

$$\mathrm{Spec} \mathbb{Z}_l((q)) \longrightarrow X_1(N)$$

corresponding to the pair $(\mathbb{G}_m/q^{\mathbb{Z}}, i^{can})$, where $\mathbb{G}_m/q^{\mathbb{Z}}$ denotes the Tate curve (Tate(q) in the notation of section 8.8 of [KM]) and where i^{can} comes from the tautological embedding $\mu_N \hookrightarrow \mathbb{G}_m$ (see proposition 8.11.7 of [KM]). This map extends to a map

$$\mathrm{Spec} \mathbb{Z}_l[[q]] \longrightarrow X_1(N),$$

(use theorem 8.11.10 of [KM]) and this gives rise to a map

$$\mathrm{Spf} \mathbb{Z}_l[[q]] \longrightarrow X_1(N)^0.$$

If $f \in \Gamma(X_1(N)^0, \omega_{X_1(N)}^{\otimes k})$ then its pullback to $\mathrm{Spf} \mathbb{Z}_l[[q]]$ has the form

$$\left(\sum_{n=0}^{\infty} c_n(f) q^n \right) (dt/t)^{\otimes k},$$

where t is the usual parameter on \mathbb{G}_m and where we refer to $\sum_{n=0}^{\infty} c_n(f) q^n$ as the q -expansion at infinity of f . This extends to a map

$$\mathcal{M}_k^{\geq 1}(N) \longrightarrow \mathbb{C}_l[[q]]$$

$$f \longmapsto \sum_{n=0}^{\infty} c_n(f) q^n.$$

From the q -expansion principle (see section 1.6 of [K] and note that $X_1(N) \times \mathbb{F}_l^{qc}$ is irreducible) we deduce that for $f \in \mathcal{M}_k^{\geq 1}(N)$ we have

$$|f|_1 = \sup_n |c_n(f)|_l.$$

If $l \geq 5$ we will let E denote the section of $\omega_{X_1(N)}^{\otimes(l-1)}$ over $X_1(N)$ with q -expansion at infinity

$$1 - (2(l-1)/B_{l-1}) \sum_{n=1}^{\infty} \sigma_{l-2}(n) q^n$$

where B_k denotes the Bernoulli number, and $\sigma_t(n) = \sum_{0 < d|n} d^t$. Then the q -expansion at infinity of E is congruent to 1 modulo l . For $l = 3$ we may choose a section E of $\omega_{X_1(N)}^{\otimes 2}$ over $X_1(N)$ with the same property (because $N \geq 5$ and $3 \nmid N$, see section 2.1 of [K]). If $l = 2$ and if $5|N$ we can again choose a section E of $\omega_{X_1(N)}$ over $X_1(N)$ with the same property (again see section 2.1 of [K]). In all these cases the section E , when pulled back to $X_1(N) \times \mathbb{F}_l^{qc}$, has a simple zero at each element of SS and no other zeroes (see for instance theorem 12.4.3 of [KM]). In particular if for each $s \in SS$ we make a choice of local generator f_s of $\omega_{X_1(N)}^{\otimes (l-1)}$ near s such that for all $\sigma \in \text{Gal}(\mathbb{F}_l^{qc}/\mathbb{F}_l)$ we have

$$(1 \times \sigma^*)^* f_{(1 \times \sigma^*)(s)} = f_s,$$

then the E/f_s for $s \in SS$ form one possible choice for a collection of local parameters T_s at $s \in SS$ satisfying

$$(1 \times \sigma^*)^* T_{(1 \times \sigma^*)(s)} = T_s$$

for all $\sigma \in \text{Gal}(\mathbb{F}_l^{qc}/\mathbb{F}_l)$ and $s \in SS$. Hence E has no zero on $X_1(N)_{>1/l}$.

If $l \geq 3$ we will set $E' = E$. If $l = 2$ we will take E' to be the section of $\omega_{X_1(N)}^{\otimes 4}$ over $X_1(N)$ with q -expansion at infinity

$$1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n.$$

In either case the q -expansion at infinity of E' is congruent to 1 modulo l and E' has no zeroes in $X_1(N)_{>l^{-1/4}}$.

We recall some elementary results about rigid analytic functions on annuli. The set of analytic functions on the annulus $\beta \leq |z|_l \leq \alpha$ is the set of functions

$$f(z) = \sum_{n=-\infty}^{\infty} a_n z^n$$

for which $|a_n|_l \beta^n \rightarrow 0$ as $n \rightarrow -\infty$ and $|a_n|_l \alpha^n \rightarrow 0$ as $n \rightarrow \infty$. If $r \in l^{\mathbb{Q}}$ and $\beta \leq r \leq \alpha$ then the supremum of $|f(z)|_l$ on $|z|_l = r$ equals

$$\sup_n |a_n|_l r^n.$$

(To see this set $A = \sup_n |a_n|_l r^n$. Then

$$\sup_{|z|_l=r} |f(z)|_l = A \sup_{|w|_l=1} \left| \sum_{|a_n|_l r^n = A} c_n w^n \right|_l$$

for some c_n with $|c_n|_l = 1$. However for $|w|_l = 1$ we see that

$$\left| \sum_{|a_n|_l r^n = A} c_n w^n \right|_l \leq 1,$$

with equality for some such choice of w .) In particular we see that $|f(z)|_l$ will always achieve its maximum on either $|z|_l = \alpha$ or $|z|_l = \beta$ (or possibly on both). In the former case this maximum equals

$$\sup_n |a_n|_l \alpha^n = \sup_{n \geq 0} |a_n|_l \alpha^n$$

and in the latter case it equals

$$\sup_n |a_n|_l \beta^n = \sup_{n \leq 0} |a_n|_l \beta^n.$$

Suppose now that f is an analytic function on the annulus $\beta \leq |z|_l < \alpha$ such that $|f(z)|_l$ is bounded by A . Then we have

$$f(z) = \sum_{n=-\infty}^{\infty} a_n z^n,$$

where $|a_n|_l \beta^n \rightarrow 0$ as $n \rightarrow -\infty$ and where for all n we have

$$|a_n|_l \leq A \alpha^{-n}$$

and

$$|a_n|_l \leq A \beta^{-n}.$$

If $|f(z)|_l$ achieves its supremum it does so on $|z|_l = \beta$ and the supremum equals

$$\sup_n |a_n|_l \beta^n = \sup_{n \leq 0} |a_n|_l \beta^n.$$

Lemma 2.1. *Suppose that $1 > r > 1/l$, that $r \in l^{\mathbb{Q}}$ and that f is a rigid analytic function on $X_1(N)_{\geq r}$. Then $|f(x)|_l$ achieves its supremum and does so at some point y which reduces to an element $s \in SS$ and satisfies $|T_s(y)|_l = r$.*

Proof. Because $X_1(N)_{\geq r}$ is a finite union of affinoids the maximum modulus principle tells us that $|f(x)|_l$ does achieve its supremum. Thus we may assume that this supremum equals 1. If $|f(x)|_l$ does not achieve its supremum in $X_1(N)_{\geq 1}$ then it does so in the inverse image under reduction of some $s \in SS$ and the lemma follows from the facts about rigid analytic functions on annuli which we recalled above. Thus suppose that f achieves its maximum in $X_1(N)_{\geq 1}$.

As $|f(x)|_l \leq 1$ on $X_1(N)_{\geq 1}$, f is a global section of the structure sheaf of the formal completion of $X_1(N) \times \mathcal{O}_{\mathbb{C}_l}$ along $X_1(N) \times \mathbb{F}_l^{qc} - SS$ and thus reduces to give a regular function \bar{f} on $X_1(N) \times \mathbb{F}_l^{qc} - SS$. Thus we may choose $s \in SS$ such that either \bar{f} has a pole at s or \bar{f} is constant. Choose also an affine neighbourhood U of s in $X_1(N) \times \mathbb{F}_l^{qc}$ which contains no other element of SS and which admits a regular function \bar{g} which has a simple zero at s and no other zero on U . Let the formal completion of $X_1(N) \times W(\mathbb{F}_l^{qc})$ along U equal $\text{Spf } A$ and let $g \in A$ be a lift of \bar{g} . Note that the formal completion of $X_1(N) \times W(\mathbb{F}_l^{qc})$ at s is isomorphic to $\text{Spf } W(\mathbb{F}_l^{qc})[[g]]$. The formal completion of $X_1(N) \times \mathcal{O}_{\mathbb{C}_l}$ along $U - \{s\}$ is $\text{Spf } (A \widehat{\otimes} \mathcal{O}_{\mathbb{C}_l}) \langle\langle S \rangle\rangle / (gS - 1)$. Thus we may expand f as

$$\sum_{i=0}^{\infty} f_i S^i$$

with $f_i \in (A \widehat{\otimes} \mathcal{O}_{\mathbb{C}_l})$ and $f_i \rightarrow 0$ as $i \rightarrow \infty$. The same expansion holds on the rigid analytic subspace of $X_1(N)_{\geq r}$ consisting of points which reduce to U (as this space is connected, being the inverse image under reduction of a Zariski connected space). Moreover on U we see that

$$\bar{f} = \sum_{i=0}^{\infty} \bar{f}_i g^{-i},$$

where \bar{f}_i denotes the reduction of f_i and where now the sum is finite.

In the formal completion of $X_1(N) \times \mathcal{O}_{\mathbb{C}_l}$ at s we may expand

$$f_i = \sum_{j=0}^{\infty} a_{ij} g^j$$

with $a_{ij} \in \mathcal{O}_{\mathbb{C}_l}$. Thus, on the rigid analytic subspace of $X_1(N)_{\geq r}$ consisting of points which reduce to s , we see that

$$f = \sum_{k=-\infty}^{\infty} \left(\sum_i a_{i,i+k} \right) g^k.$$

(The second sum is over $i \in \mathbb{Z}$ such that $i \geq 0$ and $i + k \geq 0$.) Similarly we see that in the formal completion of $X_1(N) \times \mathbb{F}_l^{ac}$ at s we have

$$\bar{f} = \sum_{k=-\infty}^{\infty} \left(\sum_i a_{i,i+k} \right) \bar{g}^k.$$

Write b_k for $\sum_i a_{i,i+k}$. Then $b_k \in \mathcal{O}_{\mathbb{C}}$ and either

- for some $k < 0$, b_k is a unit;
- or b_0 is a unit and b_k reduces to zero for all $k \neq 0$.

In the either case we see that the supremum of $|f(x)|_l$ on $|g(x)|_l = r$ (i.e. on $|T_s(x)|_l = r$) is ≥ 1 , as desired. \square

Lemma 2.2. *If $1 > r > 1/l$ then there is a constant C (depending on k , N and r) such that for all $f \in \mathcal{M}_k^{\geq r}(N)$ we have*

$$|f|_r \leq C \sup_{s,x} |f|_x,$$

where s runs over SS and where x runs over elements of the residue disc of s with $|T_s(x)|_l = r$.

Proof. If $l = 2$ reduce to the case $5|N$ by passing to a cover. By lemma 2.1 we see that $|f^{l-1}/E^k|_l$ on $X_1(N)_{\geq r}$ achieves its supremum at some point x which reduces to some $s \in SS$ and which satisfies $|T_s(x)|_l = r$. Thus for all $y \in X_1(N)_{\geq r}$ we have

$$|f|_y^{l-1}/|E|_y^k \leq \sup_{s,x} |f|_x^{l-1}/|E|_x^k$$

where s and x run over the sets described in the statement of the lemma. Hence

$$|f|_r^{l-1} \leq |E|_r^k \sup_{s,x} (|f|_x^{l-1}/r^k),$$

where again s and x run over the sets described in the statement of the lemma. The lemma follows with $C = (|E|_r/r)^{k/(l-1)}$. \square

For each $s \in SS$, choose a local generator f_s of $\omega_{X_1(N)}^{\otimes k}$ near s . If $f \in \mathcal{M}_k^{\geq r}(N)$ and $s \in SS$ then restricting f to the annulus $1 > |T_s(x)|_l \geq r$ in the residue disc of s we see that f/f_s can be expanded

$$f/f_s = \sum_{n=-\infty}^{\infty} a_n(s, f) T_s^n,$$

where the $a_n(s, f)$ are bounded for $n > 0$ and where

$$|a_n(s, f)|_l r^n \longrightarrow 0$$

as $n \rightarrow -\infty$. Choose a non-negative integer M such that $r^{-M} > C$ (the constant from the lemma), and choose $\pi_r \in \mathbb{C}_l$ with $|\pi_r|_l = r$. Now consider the map Θ from $\mathcal{M}_k^{\geq r}(N)$ to the direct sum of $\#SS$ Tate algebras $\mathbb{C}_l\langle T \rangle^{SS}$ which sends f to

$$\left(\sum_{n=0}^{\infty} a_{M-n}(s, f) \pi_r^{M-n} T^n \right)_{s \in SS}.$$

One clearly has $|\Theta(f)| \leq |f|_r$. (Here, as usual, we set $|(\sum_n b_n(s) T^n)_{s \in SS}| = \sup_{s,n} |b_n(s)|_l$.) On the other hand for all $n \in \mathbb{Z}$ and $s \in SS$ we have $|a_n(s, f) \pi_r^n|_l \leq |\Theta(f)|$. (Suppose not. Choose s and n so that $|a_n(s, f) \pi_r^n|_l$ is maximal. Then we must have $n > M$ and we see that

$$|f|_r \geq |a_n(s, f)|_l = r^{-n} \sup_{s,x} |f|_x > C \sup_{s,x} |f|_x \geq |f|_r,$$

a contradiction.) Thus

$$C|\Theta(f)| \geq C \sup_{s,x} |f|_x \geq |f|_r.$$

We deduce that Θ is a homeomorphism onto a closed subspace of $\mathbb{C}_l\langle T \rangle^{SS}$.

Lemma 2.3. *Suppose that $1 > r_1 > r_2 > 1/l$. Then the natural inclusion*

$$\mathcal{M}_k^{\geq r_2}(N) \hookrightarrow \mathcal{M}_k^{\geq r_1}(N)$$

is completely continuous.

Proof. We have a commutative diagram

$$\begin{array}{ccc} \mathcal{M}_k^{\geq r_2}(N) & \hookrightarrow & \mathcal{M}_k^{\geq r_1}(N) \\ \downarrow & & \downarrow \\ \mathbb{C}_l\langle T \rangle^{SS} & \longrightarrow & \mathbb{C}_l\langle T \rangle^{SS} \end{array}$$

$$\left(\sum_{n=0}^{\infty} b_n(s) T^n \right)_{s \in SS} \longmapsto \left(\sum_{n=0}^{\infty} b_n(s) (\pi_{r_2}/\pi_{r_1})^n T^n \right)_{s \in SS},$$

where the vertical arrows are homeomorphisms onto closed subspaces (and where we have made the same choice of M to define both vertical arrows). The lower horizontal arrow is a limit of continuous operators with finite range and hence completely continuous. It follows that the upper horizontal arrow is completely continuous. \square

The reduction $X_1(N; l) \times \mathbb{F}_l^{ac}$ of $X_1(N; ; l)$ has two irreducible components which we will denote $\overline{X}_1(N; l)_\infty$ and $\overline{X}_1(N; l)_0$. We choose the labelling so that

- $\pi_1 : \overline{X}_1(N; l)_\infty \xrightarrow{\sim} X_1(N) \times \mathbb{F}_l^{ac}$,
- $\pi_2 : \overline{X}_1(N; l)_\infty \rightarrow X_1(N) \times \mathbb{F}_l^{ac}$ has degree l ,
- $\pi_1 : \overline{X}_1(N; l)_0 \rightarrow X_1(N) \times \mathbb{F}_l^{ac}$ has degree l ,
- and $\pi_2 : \overline{X}_1(N; l)_0 \xrightarrow{\sim} X_1(N) \times \mathbb{F}_l^{ac}$.

The two curves $\overline{X}_1(N; l)_\infty$ and $\overline{X}_1(N; l)_0$ intersect in a finite number of points which we shall denote SS_l . Then $\pi_1 : SS_l \xrightarrow{\sim} SS$ and $\pi_2 : SS_l \xrightarrow{\sim} SS$ are both bijections. (See for instance lemma 5.3.1 of [KM] for these assertions.) If $s \in SS_l$ we will write $T_{s,i}$ for $\pi_i^* T_{\pi_i s}$.

Lemma 2.4. *If $s \in SS_l$ then $(X_1(N; l) \times W(\mathbb{F}_l^{ac}))_s^\wedge$ is isomorphic to*

$$\mathrm{Spf} W(\mathbb{F}_l^{ac})[[T_{s,1}, T_{s,2}]] / ((T_{s,1} - T_{s,2}^l)(T_{s,2} - T_{s,1}^l) - lu_s),$$

for some $u_s \in W(\mathbb{F}_l^{ac})[[T_{s,1}, T_{s,2}]]^\times$.

Proof. Theorem 6.6.2 of [KM] tells us that $(X_1(N; l) \times W(\mathbb{F}_l^{ac}))_s^\wedge \cong \mathrm{Spf} R$, for some 2-dimensional, regular complete local ring R , which is flat over $W(\mathbb{F}_l^{ac})$. Theorem 13.4.7 of [KM] tells us that

$$R/lR \cong \mathbb{F}_l^{ac}[[T_{s,1}, T_{s,2}]] / ((T_{s,1} - T_{s,2}^l)(T_{s,2} - T_{s,1}^l)).$$

Thus we have a surjection $W(\mathbb{F}_l^{ac})[[T_{s,1}, T_{s,2}]] \twoheadrightarrow R$ and the kernel must be generated by one element f with

- $f \equiv (T_{s,1} - T_{s,2}^l)(T_{s,2} - T_{s,1}^l) \pmod{l}$,
- and $f \notin (l, T_{s,1}, T_{s,2})^2$.

The lemma follows. □

Corollary 2.5. *If $s \in SS_l$ then*

$$(X_1(N; l) \times W(\mathbb{F}_l^{ac}))_s^\wedge \cong \mathrm{Spf} W(\mathbb{F}_l^{ac})[[X_1, X_2]] / (X_1 X_2 - l).$$

Proof. Take for instance $X_1 = (T_{s,1} - T_{s,2}^l)$ and $X_2 = (T_{s,2} - T_{s,1}^l)u_s^{-1}$. □

For $r \in l^\mathbb{Q}$ and $1 \geq r > 1/l$ we will define $X_1(N; l)_{\geq r}^\infty$ (resp. $X_1(N; l)_{\geq r}^0$) to be the admissible open subset of $X_1(N; l)^{\mathrm{an}}$ consisting of

- all points of $X_1(N; l)^{\text{an}}$ which reduce to a point of $\overline{X}_1(N; l)_\infty - SS_l$ (resp. $\overline{X}_1(N; l)_0 - SS_l$)
- and all points $x \in X_1(N; l)^{\text{an}}$ which reduce to some $s \in SS_l$ and for which

$$|T_{s,1}(x) - T_{s,2}(x)|_l \geq r$$

(resp.

$$|T_{s,2}(x) - T_{s,1}(x)|_l \geq r).$$

If in fact $1 > r^2 > 1/l$ and $s \in SS_l$ then we will let $U_s(r)$ denote the admissible open subset of $X_1(N; l)^{\text{an}}$ consisting of points which reduce to s and which satisfy

$$|T_{s,1}(x) - T_{s,2}(x)|_l \leq r$$

and

$$|T_{s,2}(x) - T_{s,1}(x)|_l \leq r.$$

It is easy to check that these sets do not depend on the choice of $\{T_s\}$ as long as they satisfy

$$(1 \times \sigma^*)^*(T_{(1 \times \sigma^*)(s)}) = T_s.$$

for $\sigma \in \text{Gal}(\mathbb{F}_l^{\text{ac}}/\mathbb{F}_l)$. If $r_1, r_2, r_3 \in l^{\mathbb{Q}}$, $1 > r_1^2 > 1/l$, $r_1 > r_2 > 1/l$ and $r_1 > r_3 > 1/l$ then the sets

- $X_1(N; l)_{\geq r_2}^\infty$,
- $X_1(N; l)_{\geq r_3}^0$,
- and for each $s \in SS_l$ the set $U_s(r_1)$

form an admissible cover of $X_1(N; l)^{\text{an}}$ by connected admissible open subsets.

(This seems to be very well known, but as we are unable to find a reference let us sketch the argument. Take an affine Zariski cover U^0 , U^∞ and U_s for $s \in SS_l$ of $X_1(N; l) \times \mathbb{F}_l^{\text{ac}}$, where for $s \in SS_l$ we have $SS_l \cap U_s = \{s\}$, where $U^0 = X_1(N; l) \times \mathbb{F}_l^{\text{ac}} - \overline{X}_1(N; l)_\infty$ and where $U^\infty = X_1(N; l) \times \mathbb{F}_l^{\text{ac}} - \overline{X}_1(N; l)_0$. Shrinking U_s if necessary, choose a regular function x_s^0 on U_s which is identically zero on $\overline{X}_1(N; l)_\infty \cap U_s$ and non-zero on $(\overline{X}_1(N; l)_0 \cap U_s) - \{s\}$ with a simple zero at s . We can lift x_s^0 to some affine open subset of $X_1(N; l) \times W(\mathbb{F}_l^{\text{ac}})$ which

intersects the special fibre in U_s . Set $x_s^\infty = p/x_s^0$. In $(X_1(N; l) \times W(\mathbb{F}_l^{ac}))_s^\wedge$ we have $x_s^0 = \sum_{i=1}^\infty a_i X_2^i + lf = X_2(\sum_{i=1}^\infty a_i X_2^{i-1} + X_1 f)$, i.e. x_s^0 is X_2 times a unit (the same X_1, X_2 as in corollary 2.5). Thus again shrinking U_s if necessary we may assume that x_s^∞ is regular on U_s , identically zero on $\overline{X}_1(N; l)_0 \cap U_s$ and non-zero on $(\overline{X}_1(N; l)_\infty \cap U_s) - \{s\}$. Moreover in $(X_1(N; l) \times W(\mathbb{F}_l^{ac}))_s^\wedge$, x_s^∞ is a unit times X_1 . We will let \mathcal{U}_∞ (resp. \mathcal{U}_0 , resp. \mathcal{U}_s) denote the preimage in $X_1(N; l)^{\text{an}}$ of U_∞ (resp. U_0 , resp. U_s). They form an admissible affinoid cover of $X_1(N; l)^{\text{an}}$. For $r \in l^\mathbb{Q}$ and $1 \geq r > 1/l$ set $\mathcal{U}_{s, \geq r}^0 \subset \mathcal{U}_s$ (resp. $\mathcal{U}_{s, \geq r}^\infty \subset \mathcal{U}_s$) to be the locus where $|x_s^0|_l \geq r$ (resp. $|x_s^\infty|_l \geq r$). Note also that $U_s(r)$ is the subspace of \mathcal{U}_s where $|x_s^0|_l \leq r$ and $|x_s^\infty|_l \leq r$. Note that $X_1(N; l)_{\geq r}^0$ (resp. $X_1(N; l)_{\geq r}^\infty$) is the union of \mathcal{U}_0 and $\mathcal{U}_{s, \geq r}^0$ for $s \in SS_l$ (resp. \mathcal{U}_∞ and $\mathcal{U}_{s, \geq r}^\infty$ for $s \in SS_l$). If $r_1, r_2, r_3 \in l^\mathbb{Q}$, $1 > r_1^2 > 1/l$, $r_1 > r_2 > 1/l$ and $r_1 > r_3 > 1/l$, then $\mathcal{U}_{s, \geq r_2}^\infty$, $\mathcal{U}_{s, \geq r_3}^0$ and $U_s(r_1)$ form an admissible affinoid cover of \mathcal{U}_s . Thus $X_1(N; l)_{\geq r_2}^\infty$, $X_1(N; l)_{\geq r_3}^0$ and $U_s(r_1)$ for $s \in SS_l$ form an admissible open cover of $X_1(N; l)^{\text{an}}$.

It remains to show that for $r \in l^\mathbb{Q}$ and $1 \geq r > 1/l$ the spaces $X_1(N; l)_{\geq r}^0$ and $X_1(N; l)_{\geq r}^\infty$ are connected. To save on notation we will only explain the case of $X_1(N; l)_{\geq r}^0$. It suffices to check that \mathcal{U}_0 and $\mathcal{U}_{s, \geq r}^0$ for $s \in SS_l$ are all connected. This follows because in each case the reduction map gives a continuous map with connected fibres to a connected (in the Zariski topology) space.)

If $r \in l^\mathbb{Q}$ and $1 \geq r > l^{-l/(1+l)}$ then it is easy to check that

$$\pi_1^{-1} X_1(N)_{\geq r} = X_1(N; l)_{\geq r}^\infty \amalg X_1(N; l)_{\geq r^{1/l}}^0$$

and

$$\pi_2^{-1} X_1(N)_{\geq r} = X_1(N; l)_{\geq r^{1/l}}^\infty \amalg X_1(N; l)_{\geq r}^0.$$

Moreover $X_1(N; l)_{\geq r}^\infty$ and $X_1(N; l)_{\geq r^{1/l}}^0$ (resp. $X_1(N; l)_{\geq r}^0$ and $X_1(N; l)_{\geq r^{1/l}}^\infty$) form an admissible open cover of $\pi_1^{-1} X_1(N)_{\geq r}$ (resp. $\pi_2^{-1} X_1(N)_{\geq r}$). As $X_1(N; l) \rightarrow X_1(N)$ is finite flat of degree $l + 1$, the same is true of the analytifications. Thus

$$\pi_1 : X_1(N; l)_{\geq r}^\infty \amalg X_1(N; l)_{\geq r^{1/l}}^0 \longrightarrow X_1(N)_{\geq r}$$

and

$$\pi_2 : X_1(N; l)_{\geq r^{1/l}}^\infty \amalg X_1(N; l)_{\geq r}^0 \longrightarrow X_1(N)_{\geq r}$$

are both finite and flat of degree $l + 1$. Looking at the cardinality of the preimages of points we deduce the following lemma.

Lemma 2.6. 1. Suppose that $r \in l^{\mathbb{Q}}$ and $1 \geq r > l^{-l/(1+l)}$ then

$$\pi_1 : X_1(N; l)_{\geq r}^{\infty} \xrightarrow{\sim} X_1(N)_{\geq r}$$

and

$$\pi_2 : X_1(N; l)_{\geq r}^0 \xrightarrow{\sim} X_1(N)_{\geq r}.$$

2. Suppose that $r \in l^{\mathbb{Q}}$ and $1 \geq r > l^{-1/(1+l)}$ then

$$\pi_2 : X_1(N; l)_{\geq r}^{\infty} \longrightarrow X_1(N)_{\geq r^l}$$

and

$$\pi_1 : X_1(N; l)_{\geq r}^0 \longrightarrow X_1(N)_{\geq r^l}$$

are both finite flat of degree l .

We define a bounded linear map

$$U = (1/l)\mathrm{tr}_{\pi_2} \circ j \circ \pi_1|_{X_1(N; l)_{\geq r}^{\infty}}^{-1} : \mathcal{M}_k^{\geq r}(N) \longrightarrow \mathcal{M}_k^{\geq r^l}(N).$$

One may check that U is compatible with the map on q -expansions which sends

$$\sum_{n=0}^{\infty} a_n q^n \longmapsto \sum_{n=0}^{\infty} a_{nl} q^n.$$

Note that for $1 \geq r \geq l^{-l/(1+l)}$ using π_1 to identify $X_1(N; l)_{\geq r}^{\infty}$ and $X_1(N)_{\geq r}$ we get a map

$$\mathrm{Hom}(h_k(N; l), \mathbb{C}_l) \hookrightarrow \mathcal{M}_k^{\geq r}(N)$$

which sends f to the form with q -expansion at infinity

$$\sum_{n=1}^{\infty} f(T(n))q^n.$$

Under this map the Hecke operator U_l corresponds to the linear map U .

Suppose that $1 > r > l^{-1/(1+l)}$. Combining $U : \mathcal{M}_k^{\geq r}(N) \rightarrow \mathcal{M}_k^{\geq r^l}(N)$ with the inclusion $\mathcal{M}_k^{\geq r^l}(N) \hookrightarrow \mathcal{M}_k^{\geq r}(N)$ we get a continuous endomorphism of $\mathcal{M}_k^{\geq r}(N)$, which we will also denote U . It follows from lemma 2.3 that U is completely continuous as an endomorphism of $\mathcal{M}_k^{\geq r}(N)$. From the theory

of completely continuous operators on p -adic Banach spaces (see [S1]) we see that we may write

$$\mathcal{M}_k^{\geq r}(N) = \mathcal{M}_k^{\geq r}(N)^0 \oplus \mathcal{M}_k^{\geq r}(N)^1$$

as a direct sum of U -invariant subspaces, where $\mathcal{M}_k^{\geq r}(N)^0$ is finite dimensional, all the eigenvalues of $U|_{\mathcal{M}_k^{\geq r}(N)^0}$ are l -adic units and $U|_{\mathcal{M}_k^{\geq r}(N)^1}$ is topologically nilpotent (i.e. if $f \in \mathcal{M}_k^{\geq r}(N)^1$ then $U^r f \rightarrow 0$ as $r \rightarrow \infty$). We will let e denote projection onto the summand $\mathcal{M}_k^{\geq r}(N)^0$, so that

$$ef = \lim_{r \rightarrow \infty} U^r f.$$

Lemma 2.7. *If $f \in \mathcal{M}_k^{\geq r}(N)^0$ for some $1 > r > l^{-1/(1+l)}$ then*

$$f \in \mathcal{M}_k^{> l^{-1/(1+l)}}(N).$$

Proof. Choose a minimal integer i such that $r^i \leq l^{-1/(1+l)}$ and write $f = U^{i+1} f'$ for some $f' \in \mathcal{M}_k^{\geq r}(N)^0$. Then we see that

$$U^i f' \in \mathcal{M}_k^{\geq r^i}(N) \subset \mathcal{M}_k^{> l^{-1/(1+l)}}(N)$$

and hence that

$$f = U(U^i f') \in \mathcal{M}_k^{> l^{-1/(1+l)}}(N).$$

□

Lemma 2.8. *Suppose that $1 > r \geq l^{-1/(1+l)}$, that $f \in \mathcal{M}_k^{\geq r}(N)$, that $a \in \mathbb{C}_l$ is an l -adic unit and that $\epsilon \in \mathbb{R}_{>0}$. If*

$$|Uf - af|_1 \leq \epsilon,$$

then

$$|f - ef|_1 \leq \epsilon.$$

Proof. For all positive integers t we see that

$$|U^t f - a^t f|_1 \leq \epsilon.$$

Taking the limit as $t \rightarrow \infty$ and noting that $||_1 \leq ||_r$ the lemma follows. (We remark that $a^t \rightarrow 1$ as $t \rightarrow \infty$.) □

Lemma 2.9. *Suppose we are given an integer k and a formal q -expansion*

$$\sum_{n=1}^{\infty} a_n q^n \in \mathbb{C}_l[[q]]$$

such that for all n we have $a_{nl} = a_l a_n$ and such that a_l is an l -adic unit. Suppose we also have two series of positive integers t_i and k_i and a series of abelian group homomorphisms

$$f_i : h_{k_i}(N; l) \rightarrow \mathbb{C}_l$$

such that

1. $t_i \rightarrow \infty$ as $i \rightarrow \infty$,
2. $k_i \equiv k \pmod{(l-1)l^{t_i-1}}$,
3. *and for all positive integers n and for all i we have*

$$f_i(T(n)) \equiv a_n \pmod{l^{t_i}}.$$

Then $\sum a_n q^n$ is the q -expansion at infinity of an element of $\mathcal{M}_k^{>l^{-1}/(1+l)}(N)$.

Proof. By the last lemma we only need show that $\sum a_n q^n$ is the q -expansion at infinity of an element of $\mathcal{M}_k^{\geq r}(N)$ for some $r < 1$. Choose such an r with $r > l^{-1/4}$ and $r > l^{-1/(1+l)}$. We may suppose that each $t_i \geq 3$. Set $h = 4$ if $l = 2$ and $h = l - 1$ otherwise. Then f_i corresponds to an element of $\mathcal{M}_{k_i}^{\geq r}(N)$ which we will also denote by f_i . Moreover $f_i/(E')^{(k_i-k)/h} \in \mathcal{M}_k^{\geq r}(N)$ and has q expansion at infinity congruent to $\sum_n a_n q^n$ modulo l^{t_i} . (If $l = 2$ note that E' is congruent to 1 modulo 2^4 .) Thus $e(f_i/(E')^{(k_i-k)/h}) \in \mathcal{M}_k^{\geq r}(N)^0$ also has q expansion at infinity congruent to $\sum_n a_n q^n$ modulo l^{t_i} . As $\mathcal{M}_k^{\geq r}(N)^0$ is finite dimensional all l -adic norms are equivalent. The $e(f_i/(E')^{(k_i-k)/h})$ form a Cauchy sequence for $|\cdot|_1$ and hence also for $|\cdot|_r$. Let $f \in \mathcal{M}_k^{\geq r}(N)^0$ denote the limit of the $e(f_i/(E')^{(k_i-k)/h})$ in both of these norms. Then f has q -expansion at infinity $\sum_n a_n q^n$, as desired. \square

Finally we state the generalisation of theorem 4 of [BT] to $l = 2$ and 3. Although in [BT] there is a running hypothesis that $l \geq 5$, the proof given there of this theorem makes no use of that hypothesis.

Theorem 2.10. *Let N and k denote integers with $N \geq 5$. Let $l \nmid N$ be a prime. Suppose α and β are distinct non-zero elements of \mathbb{C}_l and that $f_\alpha, f_\beta \in$*

$\mathcal{M}_k^{>l/(1+l)}(N)$ are eigenvectors for U with eigenvalues α and β . Suppose also f_α (resp. f_β) have q -expansions at infinity $\sum_{n \geq 1} a_n(f_\alpha)q^n$ (resp. $\sum_{n \geq 1} a_n(f_\beta)q^n$) and that for all positive integers n not divisible by l we have

$$a_n(f_\alpha) = a_n(f_\beta).$$

Then $f = (\alpha f_\alpha - \beta f_\beta)/(\alpha - \beta)$ is classical, i.e. there is an abelian group homomorphism $f' : h_k(N) \rightarrow \mathbb{C}_l$ such that for all n

$$f'(T(n)) = (\alpha a_n(f_\alpha) - \beta a_n(f_\beta))/(\alpha - \beta).$$

3 2-adic Hida theory and deformation theory.

In this section we will draw together some results about 2-adic Hida theory which are not well documented in the literature and deduce some slight extensions of the results of [Di].

If $N \geq 5$ is an odd positive integer we will let $h^0(N)$ denote

$$\lim_{\leftarrow r} e(h_2(2^r N) \otimes_{\mathbb{Z}} \mathbb{Z}_2),$$

where e denotes Hida's idempotent

$$e = \lim_{t \rightarrow \infty} U_2^{t!}.$$

Taking the limit of the homomorphisms

$$\langle \rangle : (\mathbb{Z}/2^r N \mathbb{Z})^\times \longrightarrow e(h_2(2^r N) \otimes_{\mathbb{Z}} \mathbb{Z}_2)^\times$$

we get a continuous homomorphism

$$S = S^2 \times S_2 : (\mathbb{Z}/N \mathbb{Z})^\times \times \mathbb{Z}_2^\times \longrightarrow h^0(N)^\times.$$

We will let Λ denote the completed group ring $\mathbb{Z}_2[[1 + 4\mathbb{Z}_2]] \cong \mathbb{Z}_2[[T]]$, where $T = S_2(5) - 1$. Then S_2 induces a continuous homomorphism $\Lambda \rightarrow h^0(N)$.

According to theorems 3.3 and 3.4 of [Hi], $h^0(N)$ is a finitely generated, torsion free Λ -module and for any integer $k \geq 2$ we have a surjection

$$h^0(N)/(S_2(5) - 5^{k-2}) \twoheadrightarrow e(h_k(4N) \otimes_{\mathbb{Z}} \mathbb{Z}_2)$$

which sends $T(n)$ to $T(n)$ for all n and which becomes an isomorphism after tensoring with \mathbb{Q}_2 .

Set $e_{\pm} = (1 \pm S_2(-1))/2$ and $h^0(N)_{\pm} = e_{\pm}h^0(N) \subset h^0(N) \otimes_{\mathbb{Z}_2} \mathbb{Q}_2$. Then

$$h^0(N) \subset h^0(N)_+ \oplus h^0(N)_- \subset (1/2)h^0(N).$$

Thus we see that $h^0(N)_{\pm}$ are finitely generated torsion free Λ -modules, and so from the structure theory of finitely generated Λ -modules we see that we have exact sequences of Λ -modules

$$(0) \longrightarrow h^0(N)_{\pm} \longrightarrow \Lambda^{r_{\pm}} \longrightarrow X_{\pm} \longrightarrow (0),$$

where r_{\pm} are non-negative integers and where X_{\pm} have finite cardinality $2^{a_{\pm}}$. If $k \geq 2$ is an integer with the same parity as $(1 \mp 1)/2$ then we see that there is a surjection

$$h^0(N)_{\pm}/(S_2(5) - 5^{k-2}) \twoheadrightarrow e(h_k(2N) \otimes_{\mathbb{Z}} \mathbb{Z}_2)$$

which sends $T(n)$ to $T(n)$ for all n and which becomes an isomorphism after tensoring with \mathbb{Q}_2 . In fact the kernel of this surjection has order divisible by $2^{a_{\pm}}$. (The key point is that for $k \equiv (1 \mp 1)/2 \pmod{2}$ we have an equality

$$ee_{\pm}(h_k(4N) \otimes \mathbb{Q}_2) = e(h_k(2N) \otimes \mathbb{Q}_2).$$

This results from the fact that U_2 maps the space of modular forms of weight k and level $\Gamma_1(2N) \cap \Gamma_0(4)$ to the space of modular forms of weight k and level $\Gamma_1(2N)$ (compare for instance proposition 8.3 of [Hi].)

Similarly set $h_2(4N)_- = e_-h_2(4N) \subset h_2(4N) \otimes \mathbb{Q}$.

Lemma 3.1. *Suppose that $f : h^0(N)_- \rightarrow \mathbb{Q}_2^{ac}$ is a continuous \mathbb{Z}_2 -algebra homomorphism such that $f(S_2(5)) = 1/5$. Then*

$$\sum_{n=1}^{\infty} f(T(n))q^n$$

is the q -expansion at infinity of an element of $\mathcal{M}_1^{\geq 2-2/3}(N)$.

Proof. For each integer $r \geq 1$ set $k(r) = 1 + 2^{a-r}$. Then we can find a continuous homomorphism of \mathbb{Z}_2 -modules

$$f_r : e(h_{k(r)}(2N) \otimes_{\mathbb{Z}} \mathbb{Z}_2) \longrightarrow \mathbb{Q}_2^{ac}$$

such that $f_r(T(n)) \equiv f(T(n)) \pmod{2^{r+2}}$ for all n . The lemma follows from lemma 2.9. \square

Suppose that $k \geq 2$ is an integer. If \wp is a minimal prime ideal of $h^0(N)_\pm$ containing $S_2(5) - 5^{k-2}$ then $h^0(N)_\pm/\wp$ is a 1-dimensional integral domain. Thus \wp contains

$$\ker(h^0(N)_\pm \twoheadrightarrow ee_\pm(h_k(4N) \otimes_{\mathbb{Z}} \mathbb{Z}_2)).$$

Thus contraction gives a bijection between prime ideals of $ee_\pm(h_k(4N) \otimes_{\mathbb{Z}} \mathbb{Z}_2)$ and prime ideals of $h^0(N)_\pm$ containing $S_2(5) - 5^{k-2}$, hence also a bijection between maximal ideals of $ee_\pm(h_k(4N) \otimes_{\mathbb{Z}} \mathbb{Z}_2)$ and maximal ideals of $h^0(N)_\pm$. Hence to any maximal ideal \mathfrak{m} of $h^0(N)_\pm$ we can associate a continuous semi-simple representation

$$\bar{\rho}_{\mathfrak{m}} : \text{Gal}(\mathbb{Q}^{ac}/\mathbb{Q}) \longrightarrow GL_2(h^0(N)_\pm/\mathfrak{m})$$

such that for all but finitely many primes p we have

- $\text{tr } \bar{\rho}_{\mathfrak{m}}(\text{Frob}_p) = T_p$
- and $\det \bar{\rho}_{\mathfrak{m}}(\text{Frob}_p) = pS(p)$.

(To see that $\bar{\rho}_{\mathfrak{m}}$ can be defined over $h^0(N)_\pm/\mathfrak{m}$ use the facts that its trace is valued in $h^0(N)_\pm/\mathfrak{m}$ (which follows from the Chebotarev density theorem) and that the Brauer group of any finite field extension of $h^0(N)_\pm/\mathfrak{m}$ is trivial.) We will call \mathfrak{m} Eisenstein if $\bar{\rho}_{\mathfrak{m}}$ is not absolutely irreducible.

Note that the intersection over all integers $k \geq 2$ with $k \equiv (1 \mp 1)/2$ of

$$\ker(h^0(N)_\pm \twoheadrightarrow e(h_2(2N) \otimes \mathbb{Q}_2))$$

equals

$$h^0(N)_\pm \cap \bigcap_k (S_2(5) - 5^{k-2})\Lambda^{r^\pm} = (0).$$

Thus

$$h^0(N)_\pm = \varprojlim_{\leftarrow} (h^0(N)_\pm / \bigcap_{k \in K} \ker(h^0(N)_\pm \twoheadrightarrow e(h_k(2N) \otimes \mathbb{Z}_2))),$$

where the inverse limit is over finite sets K of integers $k \geq 2$ with $k \equiv (1 \mp 1)/2 \pmod{2}$.

For each $k \geq 2$ there is a continuous 2-dimensional pseudo-representation (see [Ta1] for the definition of pseudo-representation)

$$T : \text{Gal}(\mathbb{Q}^{ac}/\mathbb{Q}) \longrightarrow e(h_k(2N) \otimes \mathbb{Z}_2)$$

such that for all primes $p \nmid 2N$ the pseudo-representation T is trivial on I_p (the inertia group at p) (i.e. $T(\sigma\tau) = T(\tau)$ for all $\sigma \in I_p$ and $\tau \in \text{Gal}(\mathbb{Q}^{ac}/\mathbb{Q})$) and $T(\text{Frob}_p) = T_p$ and $T(\text{Frob}_p^2) = T_p^2 - 2pS(p)$. By the Chebotarev density theorem we see that there is at most one such pseudo-representation T . Thus for any finite set K as in the last paragraph we get a continuous pseudo-representation

$$\begin{aligned} T : \text{Gal}(\mathbb{Q}^{ac}/\mathbb{Q}) &\longrightarrow h^0(N)_\pm / \bigcap_{k \in K} \ker(h^0(N)_\pm \twoheadrightarrow e(h_k(2N) \otimes \mathbb{Z}_2)) \\ &\subset \bigoplus_{k \in K} e(h_k(2N) \otimes_{\mathbb{Z}} \mathbb{Z}_2), \end{aligned}$$

such that for all primes $p \nmid 2N$ the pseudo-representation T is trivial on I_p , $T(\text{Frob}_p) = T_p$ and $T(\text{Frob}_p^2) = T_p^2 - 2pS(p)$. Taking the limit over K we find a continuous pseudo-representation

$$T : \text{Gal}(\mathbb{Q}^{ac}/\mathbb{Q}) \longrightarrow h^0(N)_\pm$$

such that for all primes $p \nmid 2N$ the pseudo-representation T is trivial on I_p , $T(\text{Frob}_p) = T_p$ and $T(\text{Frob}_p^2) = T_p^2 - 2pS(p)$. By the main theorem of [N] (see also [R]) we see that if \mathfrak{m} is a non-Eisenstein maximal ideal of $h^0(N)_\pm$ then there is a continuous representation

$$\rho_{\mathfrak{m}}^{\text{ord}} : \text{Gal}(\mathbb{Q}^{ac}/\mathbb{Q}) \longrightarrow GL_2(h^0(N)_{\pm, \mathfrak{m}})$$

such that $\rho_{\mathfrak{m}}^{\text{ord}}$ is unramified at all primes $p \nmid 2N$ and satisfies

- $\text{tr } \rho_{\mathfrak{m}}^{\text{ord}}(\text{Frob}_p) = T_p$
- and $\det \rho_{\mathfrak{m}}^{\text{ord}}(\text{Frob}_p) = pS(p)$.

It is known (by [De] or [W], theorem 2.1.4) that $\bar{\rho}_{\mathfrak{m}}|_{\text{Gal}(\mathbb{Q}_2^{ac}/\mathbb{Q}_2)}^{ss}$ is unramified. We will suppose that $\bar{\rho}_{\mathfrak{m}}|_{\text{Gal}(\mathbb{Q}_2^{ac}/\mathbb{Q}_2)}^{ss}(\text{Frob}_2)$ has two distinct eigenvalues α and β . Then it is also known that $\alpha, \beta \in h^0(N)_\pm/\mathfrak{m}$ and that either $U_p - \alpha \in \mathfrak{m}$ or $U_p - \beta \in \mathfrak{m}$ ([De] or [W], theorem 2.1.4). We will suppose it is the former. Choose an element $\sigma_0 \in \text{Gal}(\mathbb{Q}_2^{ac}/\mathbb{Q}_2)$ above Frob_2 . It follows from Hensel's lemma that $\rho_{\mathfrak{m}}^{\text{ord}}(\sigma_0)$ has distinct eigenvalues A and B in $h^0(N)_{\pm, \mathfrak{m}}$ with $A \equiv \alpha \pmod{\mathfrak{m}}$ and $B \equiv \beta \pmod{\mathfrak{m}}$. Choose a basis (e_B, e_A) of $h^0(N)_{\pm, \mathfrak{m}}^2$ consisting of eigenvectors of $\rho_{\mathfrak{m}}^{\text{ord}}(\sigma_0)$ with eigenvalues B and A respectively. With respect to this basis write

$$\rho_{\mathfrak{m}}^{\text{ord}}(\sigma) = \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix}.$$

Also write

- ψ_a for the unramified character of $\text{Gal}(\mathbb{Q}_2^{ac}/\mathbb{Q}_2)$ which takes Frob_2 to a ,
- χ_2 for the 2-adic cyclotomic character,
- and S for the composite

$$\text{Gal}(\mathbb{Q}^{ac}/\mathbb{Q}) \longrightarrow \text{Gal}(\mathbb{Q}(\mu_{2^\infty N})/\mathbb{Q}) \xrightarrow{\sim} \mathbb{Z}_2^\times \times (\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{S} h^0(N)^\times.$$

Then by theorem 2.1.4 of [W] we see that for any integer $k \geq 2$ with $k \equiv (1 \mp 1)/2 \pmod{2}$ and for any $\sigma \in \text{Gal}(\mathbb{Q}_2^{ac}/\mathbb{Q}_2)$ we have

- $a(\sigma) \equiv (\chi_2 S \psi_{U_2}^{-1})(\sigma)$,
- $c(\sigma) \equiv 0$,
- and $d(\sigma) \equiv \psi_{U_2}(\sigma)$,

all modulo

$$\ker(h^0(N)_{\pm, \mathfrak{m}} \rightarrow e(h_k(2N) \otimes_{\mathbb{Z}} \mathbb{Z}_2)_{\mathfrak{m}}).$$

We conclude that

$$\rho_{\mathfrak{m}}^{\text{ord}}|_{\text{Gal}(\mathbb{Q}_2^{ac}/\mathbb{Q}_2)} \sim \begin{pmatrix} \chi_2 S \psi_{U_2}^{-1} & * \\ 0 & \psi_{U_2} \end{pmatrix}$$

and that $A = U_2$.

Now suppose that

$$\bar{\rho} : \text{Gal}(\mathbb{Q}^{ac}/\mathbb{Q}) \longrightarrow GL_2(\mathbb{F}_2^{ac})$$

is a continuous representation such that

- $\bar{\rho}(c) \neq 1$,
- $\bar{\rho}|_{\text{Gal}(\mathbb{Q}_2^{ac}/\mathbb{Q}_2)}^{ss}$ is unramified and $\bar{\rho}|_{\text{Gal}(\mathbb{Q}_2^{ac}/\mathbb{Q}_2)}^{ss}(\text{Frob}_2)$ has distinct eigenvalues α and β ,
- $\bar{\rho}|_{\text{Gal}(\mathbb{Q}(\sqrt{-1})^{ac}/\mathbb{Q}(\sqrt{-1}))}$ is irreducible,
- and such that there exists an odd integer $N \geq 5$ and a homomorphism $\bar{f} : h_2(N) \rightarrow \mathbb{F}_2^{ac}$ satisfying
 - $\bar{f}(T_2) = \alpha$,
 - $\bar{f}(T_p) = \text{tr } \bar{\rho}(\text{Frob}_p)$ for all primes $p \nmid 2N$,

– and $\overline{f}(pS(p)) = \det \overline{\rho}(\text{Frob}_p)$ for all primes $p \nmid 2N$.

We will let $N(\overline{\rho})$ denote the conductor of $\overline{\rho}$.

Suppose also that S is a finite set of odd primes containing all where $\overline{\rho}$ ramifies and some prime $p \geq 5$. Then set

$$N_S(\overline{\rho}) = N(\overline{\rho}) \prod_{p \in S} p^{\dim \overline{\rho}_{I_p}}.$$

It follows from theorem 3.1 of [Buz] that we can find a ring homomorphism

$$h_2(2N_S(\overline{\rho})) \longrightarrow \mathbb{F}_2^{\text{ac}}$$

such that

- U_2 maps to α ,
- U_p maps to 0 if $p \in S$,
- T_p maps to $\text{tr } \overline{\rho}(\text{Frob}_p)$ if $p \nmid 2N_S(\overline{\rho})$,
- and $pS(p)$ maps to $\det \overline{\rho}(\text{Frob}_p)$ if $p \nmid 2N_S(\overline{\rho})$.

(It is here we use that $\overline{\rho}|_{\text{Gal}(\mathbb{Q}(\sqrt{-1})^{\text{ac}}/\mathbb{Q}(\sqrt{-1}))}$ is irreducible, rather than the weaker assumption that $\overline{\rho}$ is irreducible.) We will let $\mathfrak{m}_S(\overline{\rho}, \alpha)_+$ denote the kernel of this homomorphism.

Lemma 3.2. *Keep the above notation and assumptions.*

1. *There is a ring homomorphism $h_2(4N_S(\overline{\rho}))_- \rightarrow \mathbb{F}_2^{\text{ac}}$ such that*

- U_2 maps to α ,
- U_p maps to 0 if $p \in S$,
- T_p maps to $\text{tr } \overline{\rho}(\text{Frob}_p)$ if $p \nmid 2N_S(\overline{\rho})$,
- and $pS(p)$ maps to $\det \overline{\rho}(\text{Frob}_p)$ if $p \nmid 2N_S(\overline{\rho})$.

We will denote its kernel $\mathfrak{m}_S(\overline{\rho}, \alpha)_-$.

2. *There is a surjection*

$$h_2(4N_S(\overline{\rho}))_{-\mathfrak{m}_S(\overline{\rho}, \alpha)_-} / (2) \twoheadrightarrow h_2(2N_S(\overline{\rho}))_{\mathfrak{m}_S(\overline{\rho}, \alpha)_+} / (2)$$

which takes $T(n)$ to $T(n)$ for all n .

Proof. Let \mathbb{T} denote the polynomial algebra over \mathbb{Z}_2 generated by variables t_p and s_p for $p \nmid 2N_S(\bar{\rho})$ and u_p for $p \mid 2N_S(\bar{\rho})$. Then there is a natural map $\mathbb{T} \rightarrow h_2(2N_S(\bar{\rho}))_{\mathfrak{m}_S(\bar{\rho}, \alpha)_+}/(2)$ which sends t_p to T_p etc. Let \mathfrak{m} denote the pullback of $\mathfrak{m}_S(\bar{\rho}, \alpha)_+$. It is a maximal ideal of \mathbb{T} . Let Y denote the open (i.e. with the cusps removed) modular curve of level $\Gamma_1(2N_S(\bar{\rho})) \cap \Gamma_0(4)$. Let ϵ denote the order two character of $\Gamma_1(4N_S(\bar{\rho})) / (\Gamma_1(2N_S(\bar{\rho})) \cap \Gamma_0(4))$ thought of as a character of the fundamental group of Y . It is known that

$$H^1(Y, \mathbb{Z}_2)_{\mathfrak{m}} \cong h_2(2N_S(\bar{\rho}))_{\mathfrak{m}_S(\bar{\rho}, \alpha)_+}^2,$$

where \mathbb{T} acts on the cohomology by sending t_p to T_p etc. (See proposition 12.10 of [G].) Because $H^2(Y, \mathbb{Z}_2) = (0)$ (as Y is affine) we conclude that

$$H^1(Y, \mathbb{F}_2)_{\mathfrak{m}} \cong (h_2(2N_S(\bar{\rho}))_{\mathfrak{m}_S(\bar{\rho}, \alpha)_+}/(2))^2.$$

Thus to prove the lemma it suffices to see that the action of \mathbb{T} on $H^1(Y, \mathbb{F}_2)_{\mathfrak{m}}$ factors through $h_2(4N_S(\bar{\rho}))_{-\mathfrak{m}_S(\bar{\rho}, \alpha)_-}$. However

$$H^1(Y, \mathbb{F}_2)_{\mathfrak{m}} = H^1(Y, \mathbb{F}_2(\epsilon))_{\mathfrak{m}} \cong H^1(Y, \mathbb{Z}_2(\epsilon))_{\mathfrak{m}} \otimes \mathbb{F}_2,$$

because $H^2(Y, \mathbb{Z}_2(\epsilon)) = (0)$ (as Y is affine). Finally the action of \mathbb{T} on $H^1(Y, \mathbb{Z}_2(\epsilon))_{\mathfrak{m}}$ factors through $h_2(4N_S(\bar{\rho}))_{-\mathfrak{m}_S(\bar{\rho}, \alpha)_-}$, because $H^1(Y, \mathbb{Z}_2(\epsilon))_{\mathfrak{m}}$ is torsion free (because in turn $H^0(Y, \mathbb{F}_2(\epsilon))_{\mathfrak{m}} = H^0(Y, \mathbb{F}_2)_{\mathfrak{m}} = (0)$, as \mathfrak{m} is non-Eisenstein). \square

We remark that by our choice of $N_S(\bar{\rho})$, for $p \in S$ we have $U_p = 0$ in each of $h_2(2N_S(\bar{\rho}))_{\mathfrak{m}_S(\bar{\rho}, \alpha)_+}$, $h_2(4N_S(\bar{\rho}))_{-\mathfrak{m}_S(\bar{\rho}, \alpha)_-}$ and $h^0(N_S(\bar{\rho}))_{\pm, \mathfrak{m}_S(\bar{\rho}, \alpha)_{\pm}}$. (In fact it suffices to check that for $p \in S$ we have $U_p = 0$ in $h_k(4N_S(\bar{\rho}))_{\mathfrak{m}_S(\bar{\rho}, \alpha)_{\pm}}$ whenever $k \geq 2$ and $k \equiv (1 \mp 1)/2 \pmod{2}$. This is standard, see for example corollary 4.2.3 and the proof of lemma 5.1.1 of [CDT].)

We will let

$$\rho_{S, \alpha, \pm}^{(2)} : \text{Gal}(\mathbb{Q}^{ac}/\mathbb{Q}) \longrightarrow GL_2(R_{S, \alpha, \pm}^{(2)})$$

denote the universal deformation of $\bar{\rho}$ to a representation which is unramified outside $S \cup \{2\}$ and which when restricted to $\text{Gal}(\mathbb{Q}_2^{ac}/\mathbb{Q}_2)$ is of the form

$$\begin{pmatrix} \phi_1 & * \\ 0 & \phi_2 \end{pmatrix},$$

where ϕ_2 is unramified and $\phi_2(\text{Frob}_2) \equiv \alpha$ modulo the maximal ideal, and where, thinking of ϕ_1 as a character of \mathbb{Q}_2^{\times} by local class field theory, we have $\phi_1(-1) = \mp 1$ and $\phi_1(x) = x$ for all $x \in (1 + 4\mathbb{Z}_2)$. Similarly we will let

$$\rho_{S, \alpha, \pm}^{\text{ord}} : \text{Gal}(\mathbb{Q}^{ac}/\mathbb{Q}) \longrightarrow (R_{S, \alpha, \pm}^{\text{ord}})$$

denote the universal deformation of $\bar{\rho}$ to a representation which is unramified outside $S \cup \{2\}$ and which when restricted to $\text{Gal}(\mathbb{Q}_2^{ac}/\mathbb{Q}_2)$ is of the form

$$\begin{pmatrix} \phi_1 & * \\ 0 & \phi_2 \end{pmatrix},$$

where ϕ_2 is unramified and $\phi_2(\text{Frob}_2) \equiv \alpha$ modulo the maximal ideal, and where, thinking of ϕ_1 as a character of \mathbb{Q}_2^\times by local class field theory, we have $\phi_1(-1) = \mp 1$. The character $\phi_1 \chi_2^{-1}$ gives a continuous homomorphism, which we will denote S_2 ,

$$(1 + 4\mathbb{Z}_2) \longrightarrow (R_{S,\alpha,\pm}^{\text{ord}})^\times$$

and so makes $R_{S,\alpha,\pm}^{\text{ord}}$ into a Λ -algebra. From the definitions one sees that

$$R_{S,\alpha,\pm}^{(2)} = R_{S,\alpha,\pm}^{\text{ord}} / (S_2(5) - 1).$$

From the universal properties we get maps

- $R_{S,\alpha,+}^{(2)} \longrightarrow h_2(2N_S(\bar{\rho}))_{\mathfrak{m}(\bar{\rho},\alpha)_+}$,
- $R_{S,\alpha,-}^{(2)} \longrightarrow h_2(4N_S(\bar{\rho}))_{-, \mathfrak{m}(\bar{\rho},\alpha)_-}$,
- and $R_{S,\alpha,\pm}^{\text{ord}} \longrightarrow h^0(N_S(\bar{\rho}))_{\pm, \mathfrak{m}(\bar{\rho},\alpha)_\pm}$,

which are in fact surjections. (To see that these maps are surjections note that $U_p = 0$ if $p \in S$, that $T_p = \text{tr} \rho_{\mathfrak{m}(\bar{\rho},\alpha)_\pm}^{(2)}(\text{Frob}_p)$ or $\text{tr} \rho_{\mathfrak{m}(\bar{\rho},\alpha)_\pm}^{\text{ord}}(\text{Frob}_p)$ is in the image for $p \nmid 2N_S(\bar{\rho})$, that $S(p)$ is similarly in the image for $p \nmid 2N_S(\bar{\rho})$ and that U_2 is in the image by Hensel's lemma (as it is an eigenvalue for an element of $\text{Gal}(\mathbb{Q}_2^{ac}/\mathbb{Q}_2)$ above Frob_2 in one of these representations).)

Theorem 4 and proposition 6 of [Di] show that the map

$$R_{S,\alpha,+}^{(2)} \longrightarrow h_2(2N_S(\bar{\rho}))_{\mathfrak{m}(\bar{\rho},\alpha)_+}$$

is an isomorphism.

Proposition 3.3. *The natural maps*

$$R_{S,\alpha,-}^{(2)} \twoheadrightarrow h_2(4N_S(\bar{\rho}))_{-, \mathfrak{m}(\bar{\rho},\alpha)_-}$$

and

$$R_{S,\alpha,\pm}^{\text{ord}} \twoheadrightarrow h^0(N_S(\bar{\rho}))_{\pm, \mathfrak{m}(\bar{\rho},\alpha)_\pm}$$

are isomorphisms.

Proof. Consider the first of these maps. We have a commutative diagram

$$\begin{array}{ccc} R_{S,\alpha,-}^{(2)}/(2) & \twoheadrightarrow & h_2(4N_S(\bar{\rho}))_{-,m(\bar{\rho},\alpha)_-}/(2) \\ \downarrow & & \downarrow \\ R_{S,\alpha,+}^{(2)}/(2) & \xrightarrow{\sim} & h_2(2N_S(\bar{\rho}))_{m(\bar{\rho},\alpha)_+}/(2), \end{array}$$

where the left hand vertical arrow is an isomorphism from the definitions. Thus

$$R_{S,\alpha,-}^{(2)}/(2) \xrightarrow{\sim} h_2(4N_S(\bar{\rho}))_{-,m(\bar{\rho},\alpha)_-}/(2)$$

and, because $h_2(4N_S(\bar{\rho}))_{-,m(\bar{\rho},\alpha)_-}$ is torsion free over \mathbb{Z}_2 , we deduce that

$$R_{S,\alpha,-}^{(2)} \xrightarrow{\sim} h_2(4N_S(\bar{\rho}))_{-,m(\bar{\rho},\alpha)_-}.$$

Now the composite

$$R_{S,\alpha,-}^{\text{ord}}/(S_2(5) - 1) \twoheadrightarrow h^0(N_S(\bar{\rho}))_{-,m(\bar{\rho},\alpha)_-}/(S_2(5) - 1) \twoheadrightarrow h_2(4N_S(\bar{\rho}))_{-,m(\bar{\rho},\alpha)_-}$$

is an isomorphism and so

$$R_{S,\alpha,-}^{\text{ord}}/(S_2(5) - 1) \xrightarrow{\sim} h^0(N_S(\bar{\rho}))_{-,m(\bar{\rho},\alpha)_-}/(S_2(5) - 1).$$

Because $h^0(N_S(\bar{\rho}))_{-,m(\bar{\rho},\alpha)_-}$ is Λ -torsion free, we deduce that

$$R_{S,\alpha,-}^{\text{ord}} \xrightarrow{\sim} h^0(N_S(\bar{\rho}))_{-,m(\bar{\rho},\alpha)_-}.$$

The same argument also shows that

$$R_{S,\alpha,+}^{\text{ord}} \xrightarrow{\sim} h^0(N_S(\bar{\rho}))_{+,m(\bar{\rho},\alpha)_+}.$$

□

Putting this proposition together with corollary 1.2 and lemma 3.1 we obtain the following corollary.

Corollary 3.4. *Suppose that K/\mathbb{Q}_2 is a finite extension with ring of integers \mathcal{O}_K with maximal ideal \wp_K . Suppose also that*

$$\rho : \text{Gal}(\mathbb{Q}^{ac}/\mathbb{Q}) \longrightarrow GL_2(\mathcal{O}_K)$$

is a continuous representation such that

1. $(\rho \bmod \wp_K)$ has image $SL_2(\mathbb{F}_4)$,

2. $(\rho \bmod \wp_K)(c) \neq 1$,
3. $(\rho \bmod \wp_K)$ is unramified at 5,
4. ρ is unramified at 2 and $\rho(\text{Frob}_2)$ has eigenvalues α and β in \mathcal{O}_K with distinct reduction modulo \wp_K .

Then there exists an odd integer $N \geq 5$ divisible by all primes at which ρ ramifies and a normalised eigenform $f_\alpha \in \mathcal{M}_1^{>2-2/3}(N)$ such that

- $T_p f_\alpha = (\text{tr } \rho(\text{Frob}_p)) f_\alpha$ for all primes $p \nmid 2N$,
- $pS(p) f_\alpha = (\det \rho(\text{Frob}_p)) f_\alpha$ for all primes $p \nmid 2N$,
- $U_2 f_\alpha = \alpha f_\alpha$,
- and $U_p f_\alpha = 0$ for all $p \mid N$.

(We remark that it is presumably not hard to weaken the fourth assumption to simply require that $\rho|_{\text{Gal}(\mathbb{Q}_2^{ac}/\mathbb{Q}_2)}$ is unramified and that α is an eigenvalue of $\rho_{I_2}(\text{Frob}_2)$. We do not do so as we shall not need this result.)

4 The main theorem.

We now turn to the proof of theorem A. By the previous work cited in the introduction, it suffices to check the following special case, which is our only contribution.

Theorem 4.1. *Suppose that K/\mathbb{Q} is a Galois extension with Galois group A_5 . Suppose also that*

- 2 is unramified in K and $\text{Frob}_2 \in \text{Gal}(K/\mathbb{Q})$ has order 3,
- 5 is unramified in K
- and K is not totally real.

If $r : \text{Gal}(\mathbb{Q}^{ac}/\mathbb{Q}) \rightarrow GL_2(\mathbb{C})$ is a continuous representation such that the image of $\text{proj } r$ is $\text{Gal}(K/\mathbb{Q})$ then there is a weight one newform f such that for all prime numbers p the p^{th} Fourier coefficient of f equals the trace of Frobenius at p on the inertia at p coinvariants of r . In particular the Artin L -series for r is the Mellin transform of a weight one newform and is an entire function.

Proof. Twisting r by a character of finite order we may suppose that the image of $\det r$ has two-power order, that r is unramified at 2 and 5, and that $r(\text{Frob}_2)$ has order 3. Choose an isomorphism of fields $\mathbb{Q}_2^{ac} \cong \mathbb{C}$, so that we may think of r as a representation

$$\text{Gal}(\mathbb{Q}^{ac}/\mathbb{Q}) \longrightarrow GL_2(\mathcal{O}_K)$$

for some finite extension K/\mathbb{Q}_2 inside \mathbb{Q}_2^{ac} . By corollary 3.4 we see that we may find an odd integer $N \geq 5$ divisible by all primes at which r ramifies and normalised eigenforms $f_\alpha, f_\beta \in \mathcal{M}_1^{>2-2/3}(N)$ such that

- $T_p f_\alpha = (\text{tr } r(\text{Frob}_p))f_\alpha$ and $T_p f_\beta = (\text{tr } r(\text{Frob}_p))f_\beta$ for all primes $p \nmid 2N$,
- $pS(p)f_\alpha = (\det r(\text{Frob}_p))f_\alpha$ and $pS(p)f_\beta = (\det r(\text{Frob}_p))f_\beta$ for all primes $p \nmid 2N$,
- $U_2 f_\alpha = \alpha f_\alpha$ and $U_2 f_\beta = \beta f_\beta$,
- and $U_p f_\alpha = U_p f_\beta = 0$ for all $p|N$.

Theorem 2.10 tells us that

$$f = (\alpha f_\alpha - \beta f_\beta)/(\alpha - \beta)$$

is classical and theorem A follows from this. □

Lastly let us give some examples. To that end we will call a number field K *suitable* if

- K is Galois over \mathbb{Q} with group A_5 ,
- 2 is unramified in K and $\text{Frob}_2 \in \text{Gal}(K/\mathbb{Q})$ has order 3,
- 5 is unramified in K
- and K is totally complex.

If K is such a number field then we can find a continuous homomorphism

$$r : \text{Gal}(\mathbb{Q}^{ac}/\mathbb{Q}) \longrightarrow GL_2(\mathbb{C})$$

such that the image of $\text{proj } r$ is $\text{Gal}(K/\mathbb{Q})$ (see for instance the corollary to theorem 4 of [S2]). For any such r we have just shown that $L(r, s)$ has analytic continuation to the whole complex plane. Thus to give examples of our theorem, one need only give examples of suitable number fields K .

Suppose that S is a finite set of places of \mathbb{Q} including 2, 5 and ∞ . For $v \in S$ let L_v/\mathbb{Q}_v be a finite Galois extension such that $\text{Gal}(L_v/\mathbb{Q}_v)$ embeds into A_5 . Suppose that

- L_2/\mathbb{Q}_2 is unramified of degree 3,
- L_5/\mathbb{Q}_5 is unramified
- and $L_\infty = \mathbb{C}$.

According to [M] the quotient of affine 5 space over \mathbb{Q} by the action of A_5 which simply permutes the variables, is rational. Hence, by for example the discussion on page xiv of [S3] (see in particular theorem 2 and the remark which follows), we see that there is a number field K which is Galois over \mathbb{Q} with group A_5 and such that for $v \in S$ we have $K_v \cong L_v^{60/[L_v:\mathbb{Q}_v]}$. By varying S we see in particular that there are infinitely many suitable number fields.

More concrete examples can be found in the literature. For example, according to Buhler [Buh], the splitting fields of the following are suitable:

$$x^5 + 4x^4 + 25x^3 + 17x^2 + 5x + 2$$

$$x^5 + 6x^4 + 19x^3 + 25x^2 + 11x + 2$$

$$x^5 + 3x^4 + 7x^3 + 6x^2 - 11x - 24$$

$$x^5 + 3x^4 + x^3 - 4x^2 + 17x - 8$$

$$x^5 + 2x^4 + 37x^3 - 7x^2 + 25x - 4.$$

Corrigenda for [Ta2].

One of us (R.T.) would like to take the opportunity to record some corrections to [Ta2]. He would like to thank Kevin Buzzard, Henri Darmon and Nick Shepherd-Barron for pointing these out.

- page 3, line 8: the formula defining T_p should have a factor p^{k-1} multiplying the second sum.
- page 3, line -1/2: between “if and only if” and “ f (as an element...)” insert “ $c_1(f) = 1$ and”.
- page 4, line -7: the $SS_{>r}$ should read $SS_{<r}$ and the $X_1(N)_{<r}$ should read $X_1(N)_{>r}$.
- page 7, line 5: in theorem 1 we need to assume that the image of G_l under the *projective* representation associated to $\bar{\rho}$ has order divisible by a prime other than l .

- page 7, line -8: in conjecture 1 we should have assumed that the image of G_l under the *projective* representation associated to $\bar{\rho}$ has order divisible by a prime other than l .
- page 8, line -14: “together with an embedding $i : \mathbb{Z}[(1 + \sqrt{5})/2] \hookrightarrow \text{End}((A, \psi)/\mathbb{Q})$ such that the representation of $G_{\mathbb{Q}}$ on $A[2]$ is equivalent to $\bar{\rho}$.” should read “together with an embedding $i : \mathbb{Z}[(1 + \sqrt{5})/2] \hookrightarrow \text{End}(A/\mathbb{Q})$ such that the image of i is fixed by the ψ -Rosati involution and the representation of $G_{\mathbb{Q}}$ on $A[2]$ is equivalent to $\bar{\rho}$.”
- page 9, line 5: it should read “ $A[2]$ ”, not “ $A[\sqrt{2}]$ ”.

References

- [A] E.Artin, *Zur Theorie der L-Reihen mit allgemeinen Gruppencharakteren*, Abh. math. Semin. Univ. Hamburg 8 (1930), 292-306.
- [BCDT] C.Breuil, B.Conrad, F.Diamond and R.Taylor, *On the modularity of elliptic curves*, in preparation.
- [Br] R.Brauer, *On Artin's L-series with general group characters*, Ann. Math. (2) 48 (1947), 502-514.
- [BT] K.Buzzard and R.Taylor, *Companion forms and weight one forms*, to appear in Annals of Math.
- [Buh] J.Buhler, *Icosahedral Galois representations*, LNM 654, Springer 1978.
- [Buz] K.Buzzard, *On level lowering for mod 2 representations*, preprint.
- [CDT] B.Conrad, F.Diamond and R.Taylor, *Modularity of certain potentially Barsotti-Tate Galois representations*, J.A.M.S. 12 (1999), 521-567.
- [CF] G.Faltings and C.-L.Chai, *Degeneration of abelian varieties*, Springer 1990.
- [De] P.Deligne, unpublished letter to Serre, dated 28 May 1974.
- [Di] M.Dickinson, *On the modularity of certain 2-adic Galois representations*, in preparation.

- [DO] I.Dolgachev and D.Ortland *Point sets in projective space and theta functions*, Astérisque 165 (1988).
- [E] T.Ekedahl, *An effective version of Hilbert's irreducibility theorem*, in "Séminaire de Théorie des Nombres, Paris 1988-89", Birkhäuser 1990.
- [F] G.Frey, *On Artin's conjecture for odd 2-dimensional representations*, LNM 1585, Springer 1994.
- [G] B.Gross, *A tameness criterion for Galois representations associated to modular forms mod p* , Duke Math. J. 61 (1990), 445-517.
- [He] E.Hecke, *Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen*, Math. Z. 6 (1920), 11-51.
- [Hi] H.Hida, *On p -adic Hecke algebras for GL_2 over totally real fields*, Annals of Math. 128 (1988), 295-384.
- [K] N.Katz, *P -adic properties of modular schemes and modular forms*, in "Modular functions of one variable III", eds. W.Kuyk and J.-P.Serre, LNM 350, Springer 1973.
- [KM] N.Katz and B.Mazur, *Arithmetic moduli of elliptic curves*, Princeton University Press 1985.
- [Lang] S.Lang, *Complex multiplication*, Springer 1983.
- [Langl] R.P. Langlands, *Base change for $GL(2)$* , Annals of Math. Studies **96**, Princeton Univ. Press, Princeton, 1980.
- [M] T.Maeda, *Noether's problem for A_5* , J. of Alg. 125 (1989), 418-430.
- [N] L.Nyssen, *Pseudo-représentations*, Math. Ann. 306 (1996), 257-283.
- [R] R.Rouquier, *Caractérisation des Caractères et pseudo-Caractères*, Jour. of Algebra 180 (1996), 571-586.
- [S1] J.-P.Serre, *Endomorphismes complètement continus des espaces de Banach p -adiques*, Publ. math. IHES 12 (1962), 69-85.
- [S2] J.-P.Serre, *Modular forms of weight one and Galois representations*, in "Algebraic number fields" ed. A.Fröhlich, Academic Press 1977.
- [S3] J.-P.Serre, *Topics in Galois theory*, Jones and Bartlett, 1992.

- [ST] N.Shepherd-Barron and R.Taylor, *Mod 2 and mod 5 icosahedral representations*, J. Amer. Math. Soc. 10 (1997), 283-298.
- [Ta1] R.Taylor, *Galois representations associated to Siegel modular forms of low weight*, Duke Math. J. 63 (1991),281-332.
- [Ta2] R. Taylor, *Icosahedral Galois representations*, Pacific J. Math., Special issue: Olga Taussky-Todd: in memoriam (1997), 337-347.
- [Tu] J. Tunnell, *Artin's conjecture for representations of octahedral type*, Bull. AMS **5** (1981), 173–175.
- [W] A.Wiles, *On ordinary λ -adic representations associated to modular forms*, Invent. Math. 94 (1988), 529-573.