PACIFIC JOURNAL OF MATHEMATICS
Vol. 181, No. 3, 1997

ICOSAHEDRAL GALOIS REPRESENTATIONS

RICHARD TAYLOR

To the memory of Olga Taussky-Todd

Introduction.

Let K be a number field. We will let G_K denote its absolute Galois group; and for each finite prime $\wp$ of K we will let $G_\wp \subset G_K$ denote a decomposition group for $\wp$, $I_\wp \lhd G_\wp$ the inertia subgroup and $\mathrm{Frob}_\wp \in G_\wp/I_\wp$ the arithmetic Frobenius element. These are all uniquely defined up to conjugation in G_K. We will also let $N\wp$ denote the cardinality of the residue field of $\wp$. If $\rho : G_K \to GL_d(\mathbb{C})$ is a continuous representation then it has finite image. Following Artin [2] we introduce the L-function

$$L(\rho, s) = \prod_\wp \det(1 - \rho^{I_\wp}(\mathrm{Frob}_\wp)(N\wp)^{-s})^{-1},$$

where the product is over all finite primes of K and where $\rho^{I_\wp}$ denotes the representation of $G_\wp/I_\wp$ on the $I_\wp$ invariants of ρ. This definition is easilly seen to independent of the choices of $G_\wp$, $I_\wp$ and $\mathrm{Frob}_\wp$. The product converges for the real part of s greater than 1. Brauer [3] showed that $L(\rho, s)$ has meromorphic continuation to the whole complex plane and satisfies a certain functional equation relating the values at s and $1 - s$. Artin [2] conjectured that $L(\rho, s)$ is holomorphic except for a possible pole at $s = 1$ when the trivial representation is a constituent of ρ. Because any such representation is semi-simple and because $L(\rho_1 \oplus \rho_2, s) = L(\rho_1, s)L(\rho_2, s)$ we see that it suffices to treat the case where ρ is irreducible. It is now generally expected (the "strong Artin conjecture") that in the case where ρ is irreducible there should be a cuspidal automorphic representation $\pi(\rho)$ of $GL_n(\mathbb{A}_K)$ such that $L(\pi(\rho), s) = L(\rho, s)$. This implies Artin's original conjecture, but appears to be strictly stronger. In the case $\dim \rho = 1$ the existence of $\pi(\rho)$ follows from class field theory ([1]) and the holomorphy of $L(\rho, s)$ was known ([13]) before Artin made his more general conjecture. The case $\dim \rho = d$ is still open for any $d \geq 2$, even if $K = \mathbb{Q}$.

For the rest of this article we will restrict attention to two dimensional continuous irreducible representations $\rho : G_K \to GL_2(\mathbb{C})$. Such representations can be classified according to the image of the associated projective

representation $\mathrm{proj}(\rho) : G_K \to PGL_2(\mathbb{C})$. It is known that the image of $\mathrm{proj}(\rho)$ is either the dihedral group D_{2n} of order $2n$ for some $n \geq 2$, the alternating group A_4, the symmetric group S_4 or the alternating group A_5. In the case that the image of $\mathrm{proj}(\rho)$ is dihedral then Artin proved that $L(\rho, s)$ is holomorphic. (In this case $\rho = \mathrm{Ind}_L^K \chi$, where L/K is a quadratic extension and χ is a one dimensional representation of G_L. Artin showed that $L(\rho, s) = L(\chi, s)$.) In this case the strong Artin conjecture is also known to be true, for instance by the theory of theta series.

Langlands [18], using his theory of base change, succeeded in treating the strong Artin conjecture when the image of $\mathrm{proj}(\rho)$ is A_4. He also treated some cases where $K = \mathbb{Q}$ and the image of $\mathrm{proj}(\rho)$ is S_4. Tunnell [24] combining Langlands techniques with some results on automorphic L-functions treated the general case where the image is S_4. These methods relied essentially on the solubility of A_4 and S_4 and seem to offer little insight into the so called icosahedral case where the image of $\mathrm{proj}(\rho)$ is A_5.

In this article we will describe an approach to the strong Artin conjecture for odd, irreducible, icosahedral representations $\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{C})$. By odd we mean that $\det \rho(c) = -1$, with c denoting complex conjugation. I first outlined this approach to Wiles in 1992 when I learnt of his progress on the Shimura-Taniyama conjecture. Since then some progress has been made on this approach and it is perhaps time to describe the overall strategy in print. In the first section we will recall some background material. In the next section we will sketch the basic strategy, and in the last two sections we will fill out this sketch somewhat.

1. Notation and background.

In this section we shall establish some notation and recall some basic facts about modular forms. We will let $\mathcal{H}$ denote the upper half complex plane. By a modular form of weight k and level N we shall mean a holomorphic function $f : \mathcal{H} \to \mathbb{C}$ such that

1. $f((az+b)/(cz+d)) = (cz+d)^k f(z)$ for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N)$,
2. for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ and for thr real part of z in any bounded interval $f((az+b)/(cz+d)) \to 0$ as the imaginary part of z tends to infinity.

Here $\Gamma_1(N)$ denotes the set of $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ such that $c \equiv d - 1 \equiv 0 \bmod N$. We will let $S_k(N)$ denote the finite dimensional complex vector space of modular forms of weight k and level N. This space has a natural

action of $(\mathbb{Z}/N\mathbb{Z})^\times$ by $\overline{d} \mapsto \langle \overline{d} \rangle$, where $f|\langle \overline{d} \rangle(z) = (cz+d)^{-k} f((az+b)/(cz+d))$ for any $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ with $c \equiv 0 \bmod N$ and $d \equiv \overline{d} \bmod N$. Any $f \in S_k(N)$ can be expressed

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

where $q = e^{2\pi i z}$.

If $p \not| N$ is a prime number we define an operator T_p on $S_k(N)$ by

$$f|T_p(z) = \sum_{n=1}^{\infty} c_{np}(f) q^n + \sum_{n=1}^{\infty} c_n(f|\langle p \rangle) q^{np}.$$

If $p|N$ is a prime then we define an operator U_p on $S_k(N)$ by

$$f|U_p(z) = \sum_{n=1}^{\infty} c_{np}(f) q^n.$$

For any $n \in \mathbb{Z}_{\geq 1}$ we define an operator $T(n)$ on $S_k(N)$ by the formulae

1. $T(mn) = T(m)T(n)$ if $(m,n) = 1$,
2. $T(p^r) = U_p^r$ if $p|N$,
3. $\sum_{r=0}^{\infty} T(p^r) X^r = (1 - T_p X + p^{k-1} \langle p \rangle X^2)^{-1}$ if $p \not| N$.

We have the useful formula $c_1(f|T(n)) = c_n(f)$. Finally we define $S_p = p^{k-2}\langle p \rangle = (T(p)^2 - T(p^2))/p$ if $p \not| N$.

We let $\mathbb{T}_k(N)$ denote the $\mathbb{Z}$-algebra generated by $\langle \overline{d} \rangle$ for $\overline{d} \in (\mathbb{Z}/N\mathbb{Z})^\times$, by T_p for $p \not| N$ and by U_p for $p|N$ all acting on $S_k(N)$. It is also the $\mathbb{Z}$-algebra generated by the $T(n)$ for all $n \in \mathbb{Z}_{\geq 1}$ acting on $S_k(N)$. It is commutative and finitely generated as an abelian group. The pairing

$$\begin{array}{ccc} S_k(N) \times (\mathbb{T}_k(N) \otimes_{\mathbb{Z}} \mathbb{C}) & \longrightarrow & \mathbb{C} \\ (f \quad , \quad T \otimes \lambda) & \longmapsto & \lambda c_1(f|T), \end{array}$$

is perfect. For any ring R we define $S_k(N,R) = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_k(N), R)$. If $R \subset \mathbb{C}$ then $S_k(N,R)$ is simply the space of $f \in S_k(N)$ with $c_n(f) \in R$ for all n. An element $f \in S_k(N,R)$ is called an eigenform if the map $f : \mathbb{T}_k(N) \to R$ is a ring homomorphism. For $R \subset \mathbb{C}$, f is an eigenform if and only if f (as an element of $S_k(N)$) is a common eigenvector for all the elements of $\mathbb{T}_k(N)$.

Suppose $l|N$. Then Hida introduced the idempotent $e = \lim_{n \to \infty} U_l^{n!} \in \mathbb{T}_k(N) \otimes \mathbb{Z}_l$. It has the property that U_l is a unit in $e(\mathbb{T}_k(N) \otimes \mathbb{Z}_l)$ and is topologically nilpotent in $(1-e)(\mathbb{T}_k(N) \otimes \mathbb{Z}_l)$. Now suppose $l \not| N$. Then Hida showed that there exists a finite torsion free $\Lambda = \mathbb{Z}_l[[X]]$-algebra $\mathbb{T}^0(N)$ with

distinguished elements $T(n)$ for all $n \in \mathbb{Z}_{\geq 1}$ such that for any $k \geq 1$ and any $r \geq 0$there is a map

$$\mathbb{T}^0(N)/((1+X)^{l^r} - (1+p)^{l^r(k-1)})\mathbb{T}^0(N) \twoheadrightarrow e(\mathbb{T}_k(Nl^{1+r}) \otimes \mathbb{Z}_l)$$

which takes $T(n)$ to $T(n)$ for all n and which is an isomorphism after tensoring with $\mathbb{Q}_l$ if $k \geq 2$. (See [15]. We remark that there are various normalisations one can use here. In our normalisation if p is a prime $\equiv 1 \bmod Nl$ and if $p = (1+l)^s$ in $\mathbb{Z}_l$ then $pS_p = (1+X)^s$ in $\mathbb{T}^0(N)$.) If $l \geq 5$ then it is known that $\mathbb{T}^0(N)$ is free over Λ and that for $k \geq 2$ the above maps are isomorphisms before tensoring with $\mathbb{Q}_l$ (see [14]). If $k = 1$ then it is known that in general the above surjection is not an isomorphism even after tensoring with $\mathbb{Q}_l$ (see [19]).

The quotient $Y_1(N)^{an} = \Gamma_1(N)\backslash\mathcal{H}$ can be algebraised to a smooth irreducible curve $Y_1(N)/\mathbb{C}$ with smooth compactification $X_1(N)$. We let *cusps* denote the reduced divisor $X_1(N) - Y_1(N)$. If $N \geq 5$ then $Y_1(N)$ is the (fine) moduli space for elliptic curves with a point of exact order N. In this case the pull back along the zero section of of the relative differentials of the universal elliptic curve over $Y_1(N)$ gives a line bundle $\omega/Y_1(N)$. This line bundle has a natural extension to $X_1(N)$ which we shall also denote ω. Then $S_k(N) = H^0(X_1(N), \omega^{\otimes k}(-cusps))$. All these objects have natural models over $\mathbb{Z}$, except that the extension of ω to $X_1(N)$ may only be defined over $\mathbb{Z}[1/N]$ (see [17]).

Suppose that $l \not| N$ and let $\overline{SS} \subset Y_1(N) \otimes \overline{\mathbb{F}}_l$ denote the finite set of points which parametrise supersingular elliptic curves. For each $\overline{x} \in \overline{SS}$ choose $T_{\overline{x}} \in \mathcal{O}_{Y_1(N)\otimes W(\overline{\mathbb{F}}_l),\overline{x}}$ such that $\mathcal{O}^{\wedge}_{Y_1(N)\otimes W(\overline{\mathbb{F}}_l),\overline{x}} \cong W(\overline{\mathbb{F}}_l)[[T_{\overline{x}}]]$. If $r \in l^{\mathbb{Q}} \cap [1, 1/l)$ we let $SS_{<r}$ denote the union over $\overline{x} \in \overline{SS}$ of the lifts x of $\overline{x}$ with $|T_{\overline{x}}(x)|_l < r$. If $r \in l^{\mathbb{Q}} \cap (1, 1/l]$ we let $X_1(N)_{>r}$ denote the $\overline{\mathbb{Q}}_l$ points x of $X_1(N)$ which either do not reduce to a point of $\overline{SS}$ or reduce to $\overline{x} \in \overline{SS}$ but $|T_{\overline{x}}(x)|_l > r$. Both $SS_{>r}$ and $X_1(N)_{<r}$ are admissible open subspaces of the rigid space attached to $X_1(N) \otimes K$ for a suitable finite extension $K/\mathbb{Q}_l$ (depending on r). If $r_1 < r_2$ then $X_1(N) = X_1(N)_{>r_1} \cup SS_{<r_2}$ is an admissible cover. These definitions do not depend on the choice of the parameters $T_{\overline{x}}$.

In this paragraph suppose again that $N \geq 5$ and that $l \not| N$. Also suppose that $r \in l^{\mathbb{Q}} \cap (1, l^{-l/(1+l)}]$. If $l \not| n$ then there is a natural Hecke operator $T(n)$ on $H^0(X_1(N)_{>r}, \omega^{\otimes k})$ with the usual effect on q-expansions. The theory of the canonical subgroup (see [16]) allows us to define an action of U_l on $H^0(X_1(N)_{>r}, \omega^{\otimes k})$ and hence of the Hecke operators $T(n)$ for all n. It also gives a map

$$S_k(Nl, K)^{(\mathbb{Z}/l\mathbb{Z})^\times} \hookrightarrow H^0(X_1(N)_{>r}, \omega^{\otimes k})$$

which is equivariant for all the Hecke operators $T(n)$. (Here $(\mathbb{Z}/l\mathbb{Z})^\times$ acts via $(\mathbb{Z}/l\mathbb{Z})^\times \hookrightarrow (\mathbb{Z}/Ml\mathbb{Z})^\times$.) At least if $l \geq 5$ then e is naturally defined on

$H^0(X_1(N)_{>r}, \omega^{\otimes k})$ and

$$eH^0(X_1(N)_{>r}, \omega^{\otimes k}) \cong \mathrm{Hom}_\Lambda(\mathbb{T}^0(N), K)^{(\mathbb{Z}/l\mathbb{Z})^\times}.$$

Here Λ acts on K by letting X act by multiplication by $(1+l)^{k-1}-1$ and $\overline{d} \in (\mathbb{Z}/l\mathbb{Z})^\times$ sends f to $p^{2-k}f \circ S_p$ where p is a prime with $p \equiv 1 \bmod N$ and where $p \equiv \overline{d} \bmod l$. (See [11]. These results remain true for $k=1$, as seems to be well known to experts, but see [4] for a proof.)

We now turn our attention to Galois representations. Let $\mathfrak{m}$ be a maximal ideal of $\mathbb{T}_k(N)$ (resp. $\mathbb{T}^0(N)$) with residue field $k(\mathfrak{m})$ of characteristic l. There is a unique continuous semi-simple representation $\overline{\rho}_\mathfrak{m} : G_\mathbb{Q} \to GL_2(k(\mathfrak{m}))$ which is unramified at all primes $p \not| Nl$ and satisfies $\mathrm{tr}\,\overline{\rho}_\mathfrak{m}(\mathrm{Frob}_p) = T_p$ and $\det \overline{\rho}_\mathfrak{m}(\mathrm{Frob}_p) = pS_p$ at these primes. If $\overline{\rho}_\mathfrak{m}$ is absolutely reducible we call $\mathfrak{m}$ Eisenstein. If $\mathfrak{m}$ is not Eisenstein then there is a unique continuous representation $\rho_\mathfrak{m} : G_\mathbb{Q} \to GL_2(\mathbb{T}_k(N)_\mathfrak{m})$ (resp. $GL_2(\mathbb{T}^0(N)_\mathfrak{m})$) which is unramified at all primes $p \not| Nl$ and satisfies $\mathrm{tr}\,\rho_\mathfrak{m}(\mathrm{Frob}_p) = T_p$ and $\det \rho_\mathfrak{m}(\mathrm{Frob}_p) = pS_p$ at these primes (see [5]). If $\theta : \mathbb{T}_k(N)_\mathfrak{m} \to R$ (resp. $\theta : \mathbb{T}_k(N)_\mathfrak{m} \to R$) is a local map to a noetherian complete local ring R then we will let $\rho_\theta : G_\mathbb{Q} \to GL_2(R)$ denote $\theta \circ \rho_\mathfrak{m}$. If $\theta : \mathbb{T}_k(N) \to \overline{\mathbb{Q}}_l$ is a ring homomorphism then there is a unique continuous irreducible representation $\rho_\theta : G_\mathbb{Q} \to GL_2(\overline{\mathbb{Q}}_l)$ which is unramified at all primes $p \not| Nl$ and satisfies $\mathrm{tr}\,\rho_\theta(\mathrm{Frob}_p) = T_p$ and $\det \rho_\theta(\mathrm{Frob}_p) = pS_p$ at these primes. All the representations described in this paragraph are called modular.

Let us make some remarks on these Galois representations. Firstly if $\rho : G_\mathbb{Q} \to GL_2(\mathbb{C})$ is a continuous representation then the strong Artin conjecture holds for ρ if and only if for some isomorphism $i : \mathbb{C} \xrightarrow{\sim} \overline{\mathbb{Q}}_l$ the composite $i \circ \rho$ is modular.

Secondly we remark that Serre (see [21]) has conjectured that any odd irreducible representation of $G_\mathbb{Q}$ over a finite field is modular.

Thirdly we remark that if $\overline{\rho} : G_\mathbb{Q} \to GL_2(k)$ is absolutely irreducible and modular (k a finite field) then $\overline{\rho} = \overline{\rho}_\mathfrak{m}$ for $\mathfrak{m}$ a maximal ideal of $\mathbb{T}_2(Nl^2)$ where $l \not| N$. If moreover $\overline{\rho}_{I_l}$ is not trivial we may take $\mathfrak{m}$ to be a maximal ideal of $\mathbb{T}_2(Nl)$ such that $U_l \bmod \mathfrak{m}$ is an eigenvalue of $\overline{\rho}_{I_l}(\mathrm{Frob}_l)$ (see [9]). At the possible cost of increasing N we may also assume that $U_p \in \mathfrak{m}$ for all $p|N$ (elementary to verify).

Fourthly we remark that we have the following criterion for modularity which is rather easy to prove. Suppose $A/\mathbb{Q}$ is an abelian variety of dimension d and that there exists an embedding $i : \mathcal{O}_K \hookrightarrow \mathrm{End}\,(A/\mathbb{Q})$, where K is a number field of degree d. Suppose that for one prime λ the representation of $G_\mathbb{Q}$ on the Tate module $T_\lambda A$ is modular. Then for all primes λ' of K the representations of $G_\mathbb{Q}$ on both $T_{\lambda'}A$ and on $A[\lambda']$ are both modular.

We finish this section by recalling some recent lifting theorems of Wiles [25], Taylor-Wiles [23] and Diamond [8]. Suppose that $l \nmid N$ and $l \neq 2$. Let $\mathfrak{m}$ be a maximal ideal of $\mathbb{T}_2(N)$ (resp. $\mathbb{T}_2(Nl)$, resp. $\mathbb{T}^0(N)$) which contains U_p for all $p|N$. Suppose that $\overline{\rho}_{\mathfrak{m}}|_{\mathbb{Q}(\sqrt{(-1)^{(l-1)/2}l})}$ is absolutely irreducible and that $\overline{\rho}_{\mathfrak{m}}|_{G_l}$ does not act by scalars. Let R be a complete noetherian local $W(k(\mathfrak{m}))$-algebra with finite residue field and let $\rho : \mathbb{G}_{\mathbb{Q}} \to GL_2(R)$ be a continuous representation lifting $\overline{\rho}$ and unramified outside Nl. Suppose also that:

- $\det \rho|_{I_l}$ is the cyclotomic character and for each open ideal $\mathfrak{a}$ of R there is a finite flat group scheme $G/\mathbb{Z}_l$ such that $\rho \bmod \mathfrak{a}$ is equivalent to the action of G_l on $G(\overline{\mathbb{Q}}_l)$.
- resp. $\rho|_{G_l} \sim \begin{pmatrix} \chi_1\epsilon & * \\ 0 & \chi_2 \end{pmatrix}$ with χ_1 tamely ramified and χ_2 unramified.
- resp. $\rho|_{G_l} \sim \begin{pmatrix} * & * \\ 0 & \chi_2 \end{pmatrix}$ with χ_2 unramified.

Then there exists a unique homomorphism $\theta : \mathbb{T}_2(N)_{\mathfrak{m}} \to R$, resp. $\mathbb{T}_2(Nl) \to R$, resp. $\mathbb{T}^0(N) \to R$ such that $\rho \sim \rho_\theta$, $\theta(U_p) = 0$ if $p|N$ and in the second and third cases $\theta(U_l) = \chi_2(\mathrm{Frob}_l)$.

2. The basic strategy.

Let $\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{C})$ be an odd, icosahedral representation. Because ρ has finite image we may suppose (possibly after conjugation), that the image of ρ is contained in $GL_2(E)$ for some number field E. Let λ be a prime of E with residue characteristic l. Then we may suppose (possibly after another conjugation) that $\rho : G_{\mathbb{Q}} \to GL_2(\mathcal{O}_{E,(\lambda)})$ (where $\mathcal{O}_{E,(\lambda)}$ denotes the localisation of the ring of integers of E at λ). Let $\overline{\rho}$ denote the reduction of ρ modulo λ. In [4] Kevin Buzzard and I prove the following theorem.

Theorem 1. *Suppose that $l \geq 5$, that ρ is unramified at l and that the order of $\overline{\rho}(G_l)$ is divisible by a prime other than l. Suppose also that $\overline{\rho}$ is modular. Then the strong Artin conjecture holds for ρ.*

It may be useful to discuss the various assumptions in this theorem. The assumptions that ρ be unramified at l can be weakened (see forthcoming work of Buzzard). Whether it is reasonable to hope it can be removed entirely is not clear to me. Perhaps it can be avoided by using base change. The assumption that the order of $\overline{\rho}(G_l)$ is divisible by a prime other than l seems to be of a technical nature. The assumption that $l \geq 5$ also seems to be of a technical nature. This restriction comes not from the paper [4], but from the papers cited therein. My expectation is that this restriction is only

serious if $l = 2$ and then it is only serious in two of the references. Firstly the reference to [23], which is currently being investigated by Mark Dickinson for his Harvard PhD. Secondly the reference to [20], which is currently being investigated by Ribet and his student David Jones. In the latter case it seems likely that the difficulty can be avoided by imposing an additional local assumption that 2 divides the order of $\overline{\rho}(I_p)$ for some $p \neq 2$. Let me formulate as a conjecture a generalisation of this theorem which I am hopeful will be proven in the near future.

Conjecture 1. *Suppose that ρ is unramified at l, that the order of $\overline{\rho}(G_l)$ is divisible by a prime other than l and that if $l = 2$ then 2 divides the order of $\overline{\rho}(I_p)$ for some $p \neq l$. Suppose also that $\overline{\rho}$ is modular. Then the strong Artin conjecture holds for ρ.*

The final assumption in the theorem and conjecture, that $\overline{\rho}$ is modular, is a special case of a conjecture Serre's conjecture [21]. In general it is probably very deep. However in the special case $l = 2$, Shepherd-Barron and I have the following partial result ([22]).

Theorem 2. *Suppose $l = 2$ and $\overline{\rho}$ is unramified at 3 and 5, then $\overline{\rho}$ is modular.*

Corollary 1. *Suppose that ρ is unramified at 2, 3 and 5. Suppose moreover that $\mathrm{proj}(\rho)(G_2)$ has odd order and that $\mathrm{proj}(\rho)(I_p)$ has even order for some $p \neq 2$. If Conjecture 1 is true then the strong Artin conjecture is true for ρ.*

It may be helpful to comment on the ramification assumptions in Theorem 2. They result from restrictions in the available lifting results for modular Galois representations (see [25], [23], [8]). One can expect them to be weakened in the near future, but it is less clear how soon it will be possible to remove them entirely. In fact using the results of [7] one may already reduce the assumption at 3 from being unramified to being tamely ramified.

In the rest of this paper we will comment briefly on the proofs of theorems 1 and 2. Both rely in an essential way on the work of Wiles [25] as completed by Wiles and the author [23].

3. Mod 2 icosahedral representations.

We have isomorphisms $\overline{\mathbb{F}}_2^{\times} \times SL_2(\overline{\mathbb{F}}_2) \xrightarrow{\sim} GL_2(\overline{\mathbb{F}}_2)$ and $SL_2(\overline{\mathbb{F}}_2) \xrightarrow{\sim} PSL_2(\overline{\mathbb{F}}_2)$. The only subgroups of $GL_2(\overline{\mathbb{F}}_2)$ isomorphic to A_5 are those conjugate to $SL_2(\mathbb{F}_4)$. (For instance by examining the mod 2 modular characters of A_5.) Thus to prove Theorem 2 we must show that any continuous representation $\overline{\rho} : G_{\mathbb{Q}} \to SL_2(\mathbb{F}_4)$ which is unramified at 3 and 5 is modular.

The key construction in [22] is the proof of the existence of a principally polarised abelian surface $(A,\psi)/\mathbb{Q}$, together with an embedding $i : \mathbb{Z}[(1+\sqrt{5})/2] \hookrightarrow \mathrm{End}\,((A,\psi)/\mathbb{Q})$ such that the representation of $G_{\mathbb{Q}}$ on $A[2]$ is equivalent to $\overline{\rho}$. In fact we can ensure that the representation of $G_{\mathbb{Q}}$ on $A[\sqrt{5}]$ has image the whole of $GL_2(\mathbb{F}_5)$ and (by twisting) that A has semi-stable reduction at 3 and 5. To do this one examines the appropriate twisted coarse moduli space, Y say. This space is a cubic surface in $\mathbb{P}^3$ which it is in fact unirational: If X denotes the restriction of scalars from $\mathbb{Q}(\sqrt{5})$ to $\mathbb{Q}$ of Y then we show that X is rational and because Y is a cubic surface collinearity gives a dominant rational map θ from X to Y. As Y is not a fine moduli space, rational points on Y do not necessarily correspond to rationally defined abelian surfaces. However by a rather explicit calculation we show that this is the case for the rational points $\theta(X(\mathbb{Q}))$. We obtain the assertion about the action on $A[\sqrt{5}]$ by combining the above argument with a Hilbert irreducibility argument (as Wiles does in [25]).

Once we have constructed the desired triple (A,λ,i) we show that $T_{\sqrt{5}}A$ is modular and deduce that $A[\sqrt{2}]$ is also. By the results of Wiles [25], Taylor-Wiles [23] and Diamond [8], to show that $T_{\sqrt{5}}A$ is modular it suffices to show that $A[\sqrt{5}]$ is modular.

In fact one can show that if $\overline{\rho}' : G_Q \to GL_2(\mathbb{F}_5)$ is any representation with determinant the cyclotomic character and which is tamely ramified at 3 then $\overline{\rho}'$ is modular. The argument is similar. One finds an elliptic curve $E/\mathbb{Q}$ which realises $\overline{\rho}'$ on its 5 division points. (This seems to be implicit in work going back to Hermite, but we could not find it explicitly in the literature.) Using Hilbert irreducibility we may ensure (following Wiles) that the representation of $G_{\mathbb{Q}}$ on $E[3]$ has image $GL_2(\mathbb{F}_3)$. Then, by [8], T_3E is modular and so $E[5]$ is also. (In 1992 I explained to Wiles how this argument could be used to show that the Shimura-Taniyama conjecture implied Serre's conjecture for representations $G_{\mathbb{Q}} \to GL_2(\mathbb{F}_5)$ with determinant the cyclotomic character. He later combined the argument with Hilbert irreducibility as part of his attack on the Shimura-Taniyama conjecture.)

4. l-adic representations unramified at l.

We will now briefly discuss the proof of theorem 1. In fact it is no more difficult to prove a stronger theorem. We will put ourselves in the following situation. Let $\mathcal{O}$ denote the ring of integers of a finite extension of $\mathbb{Q}_l$, λ its maximal ideal and k its residue field. Let $\rho : \mathbb{G}_{\mathbb{Q}} \to GL_2(\mathcal{O})$ be a continuous representation which is ramified only at a finite set of primes. Let $\overline{\rho}$ denote the reduction of ρ modulo λ. In [4] the following theorem which is stronger than theorem 1 is proven.

Theorem 3. *Suppose that $l \geq 5$ and that*

1. *ρ is unramified at l;*
2. *$\overline{\rho}$ is modular;*
3. *$\overline{\rho}|_{G_{\mathbb{Q}(\sqrt{(-1)^{(l-1)/2}})}}$ is absolutely irreducible;*
4. *$\overline{\rho}(\mathrm{Frob}_l)$ has two distinct eigenvalues.*

Then ρ has a finite image and the strong Artin conjecture is true for ρ.

This theorem also provides some evidence for a conjecture of Fontaine and Mazur (see [10]) that any continuous l-adic representation of $G_{\mathbb{Q}}$ which is ramified at only finitely many primes and is finitely ramified at l (i.e. the image of I_l is a finite group) has finite image. As far as we are aware the only previous evidence for this conjecture was in the case of one dimensional representations. It also gives a hint about how to prove Theorem 1: One should try to only exploit the finiteness of $\rho(I_l)$ not the finiteness of $\rho(G_{\mathbb{Q}})$.

Let α and β be the two eigenvalues of $\rho(\mathrm{Frob}_l)$. We may suppose that α and β lie in $\mathcal{O}$. Because ρ is modular we can find, perhaps after interchanging α and β, a homomorphism $\overline{f}_\alpha : \mathbb{T}_2(Nl) \to k$ such that

1. N is not divisible by l;
2. $\overline{f}_\alpha(T_p) = \operatorname{tr} \overline{\rho}(\mathrm{Frob}_p)$ for $p \not| Nl$;
3. $p\overline{f}_\alpha(S_p) = \det \overline{\rho}(\mathrm{Frob}_p)$ for $p \not| Nl$;
4. $\overline{f}_\alpha(U_l) = \alpha$;
5. $\overline{f}_\alpha(U_p) = 0$ for $p|N$.

We can then produce a second homomorphism $\overline{f}_\beta : \mathbb{T}_2(Nl) \to k$ with the same properties except that $\overline{f}_\beta(U_l) = \beta$. The construction of $\overline{f}_\beta$ is a deep theorem. To stress how surprising the existence of $\overline{f}_\beta$ is, it may be worth remarking that any lifts f_α and f_β of $\overline{f}_\alpha$ and $\overline{f}_\beta$ to homomorphisms $\mathbb{T}_2(Nl) \to \overline{\mathbb{Q}}_l$ will differ on most Hecke operators T_p. Gross [12] gives a construction for all l, but dependent on some unproven functorialities in some rigid cohomology. Coleman and Volloch [6] then gave an unconditional construction but one which excludes the prime $l = 2$.

We can now apply recent lifting results of Wiles, Taylor-Wiles and Diamond (see [8]) to produce homomorphisms F_α and $F_\beta : \mathbb{T}^0(N) \to \mathcal{O}$ such that

1. $F_\alpha(T_p) = \operatorname{tr} \rho(\mathrm{Frob}_p)$ for $p \not| Nl$;
2. $pF_\alpha(S_p) = \det \rho(\mathrm{Frob}_p)$ for $p \not| Nl$;
3. $F_\alpha(U_l) = \alpha$;
4. $F_\alpha(U_p) = 0$ for $p|N$,

and similarly for F_β. Here again we are using $l \neq 2$. This assumption is being used in an important way in at least two places. The lifting theorems

are proved by first reducing the level to a certain minimal case (following Ribet [20] and others), lifting in the minimal case (using the method of Taylor-Wiles [23]) and then extending to the more general case again (using the method of Wiles [25]). Both the first two steps use $l \neq 2$ in a significant way. The first uses an auxiliary prime $p \not\equiv 1$ or $0 \bmod l$. The second requires a numerical coincidence in Galois cohomology for the method to work, which becomes delicate if $l = 2$.

Because $\det \rho$ is unramified at l we see that F_α and F_β factor through $\mathbb{T}^0(N)/X\mathbb{T}^0(N)$. Thus, at least if $l \geq 5$, they define sections of ω over the rigid space $X_1(N)_{>l^{-l/(1+l)}}$. We introduce $F = (\alpha F_\alpha - \beta F_\beta)/(\alpha - \beta)$ and $F' = (F_\alpha - F_\beta)/(\alpha - \beta)$. Then $F = \sum_{n=1}^{\infty} a_n q^n$ is formally a weight one level N normalised eigenform, while $F' = \sum_{n=1}^{\infty} a_n q^{ln}$. We have that

1. $a_p = \operatorname{tr} \rho(\mathrm{Frob}_p)$ for $p \not| N$ (including $p = l$);
2. $a_p = 0$ for $p|N$.

In [4] we fabricate from F' a rigid section of ω over $SS_{<l^{-1/(1+l)}}$ which we show matches F on $SS_{<l^{-1/(1+l)}} \cap X_1(N)_{>l^{-l/(1+l)}}$. Gluing and applying rigid GAGA we see that F extends to a classical weight one modular form such that $\rho_f \sim \rho$. Thus ρ has finite image and the strong Artin conjecture holds for ρ.

References

[1] E. Artin, *Über eine neue Art von L-Reihen*, Abh. Math. Semin. Univ. Hamburg, **3** (1924), 89-108.

[2] ———, *Zur Theorie der L-Reihen mit allgemeinen Gruppencharakteren*, Abh. Math. Semin. Univ. Hamburg, **8** (1930), 292-306.

[3] R. Brauer, *On Artin's L-series with general group characters*, Ann. Math., **48**(**2**) (1947), 502-514.

[4] K. Buzzard and R. Taylor, *Companion forms and weight one forms*, preprint, 1997.

[5] H. Carayol, *Formes modulaires et représentations galoisiennes à valeurs dans un anneau local complet*, in "p-adic monodromy and the Birch-Swinnerton-Dyer conjecture" (B.Mazur and G.Stevens, eds.), Contemporary Math., **165** (1995), 213-237.

[6] R. Coleman and J.F. Voloch, *Companion forms and Kodaira-Spencer theory*, Invent. Math., **110** (1992), 263-281.

[7] B. Conrad, F. Diamond and R. Taylor, *Modularity of certain potentially crystalline Galois representations*, preprint, 1997.

[8] F. Diamond, *On deformation rings and Hecke rings*, Annals of Math., **144** (1996), 137-166.

[9] S. Edixhoven, *The weight in Serre's conjecture on modular forms*, Invent. Math., **109** (1992), 563-594.

[10] J.-M. Fontaine and B. Mazur, *Geometric Galois representations*, in 'Elliptic curves, modular forms and Fermat's last theorem' (J.Coates and S.-T.Yau eds.), International Press, 1995.

[11] F. Gouvea, *Arithmetic of p-adic modular forms*, Lecture notes in Math., **1304**, Springer, 1988.

[12] B. Gross, *A tameness criterion for Galois representations associated to modular forms mod p*, Duke Math. J., **61** (1990), 445-517.

[13] E. Hecke, *Eine neue Art von Zetafunctionen und ihre Beeitungen zur Vertielung der Primzahlen*, Math. Z., **6** (1920), 11-51.

[14] H. Hida, *Galois representations into $GL_2(\mathbb{Z}_p[[X]])$ attached to ordinary cusp forms*, Invent. Math., **85** (1986), 545-613.

[15] ———, *On p-adic Hecke algebras for GL_2 over totally real fields*, Annals of Math., **128** (1988), 295-384.

[16] N. Katz, *p-adic properties of modular schemes and modular forms*, in 'Modular forms of one variable III' (W.Kuyk and J.-P.Serre eds.), Lecture notes in Math., **350**, Springer 1973.

[17] N. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Annals of Math. Studies, Princeton Univ. Press, Princeton, 1985.

[18] R.P. Langlands, *Base change for $GL(2)$*, Annals of Math. Studies, **96**, Princeton Univ. Press, Princeton, 1980.

[19] B. Mazur and A. Wiles, *On p-adic analytic families of Galois representations*, Comp. Math., **59** (1986), 231-264.

[20] K.A. Ribet, *On modular representations of* $\mathrm{Gal}\,(\bar{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Inv. Math., **100** (1990), 431-476.

[21] J.-P. Serre, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J., **54** (1987), 179-230.

[22] N. Shepherd-Barron and R. Taylor, Mod 2 *and* mod 5 *icosahedral representations*, J. Amer. Math. Soc., **10** (1997), 283-298.

[23] R. Taylor and A. Wiles, *Ring theoretic properties of certain Hecke algebras*, Annals of Math., **141** (1995), 553-572.

[24] J. Tunnell, *Artin's conjecture for representations of octahedral type*, Bull. AMS, **5** (1981), 173-175.

[25] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Annals of Math., **141** (1995), 443-551.

Harvard University
Cambridge, MA 02138, U.S.A.
E-mail address: rtaylor@math.harvard.edu