Artin representations associated to modular forms of weight one: Deligne-Serre's theorem

Sara Arias de Reyna

Statement of the main result

In this chapter, we address the question of how to attach Galois representations to weight one (classical) modular forms. The main result, proved by Deligne and Serre in the seventies (cf. [DS74]), is the existence of a complex Galois representation of $G_{\mathbb{Q}}$ attached to each weight one eigenform. This result builds upon the existence of ℓ-adic Galois representations attached to eigenforms of weight ≥ 2, but requires new insight to successfully make use of these representations in order to construct the desired one. In what follows, we will give some ideas of the strategy of the proof and how all ingredients fit together; the interested reader can look at the original work of Deligne and Serre to read all the details of the proof.

Theorem 0.1 (Deligne–Serre)**.** *Let $N \geq 1$ be an integer and $\varepsilon : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ a Dirichlet character such that $\varepsilon(-1) = -1$. Let f be a modular form of weight $k = 1$, level N, character ε. Assume that f is an eigenform for all T_p with $p \nmid N$, with eigenvalue a_p. Then there exists a continuous, semi-simple representation*

$$\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$$

such that $\mathrm{Tr}(\rho_f(\mathrm{Frob}_p)) = a_p$ and $\det(\rho_f(\mathrm{Frob}_p)) = \varepsilon(p)$ for all $p \nmid N$.

Moreover, ρ_f is irreducible if and only if f is cuspidal.

Remark 0.2.

1. In the statement of the theorem, the element $\mathrm{Frob}_p \in G_{\mathbb{Q}}$ denotes some lift of the Frobenius element in $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$, after fixing an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. Implicit in the statement is the fact that the image of $\rho_f(\mathrm{Frob}_p) \in G_{\mathbb{Q}}$ does not depend on the choice of the lift.

2. Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$ be a continuous representation (with respect to the Krull topology in $G_{\mathbb{Q}}$ and the Euclidean topology on $\mathbb{C}$). Then the image of ρ in $\mathrm{GL}_2(\mathbb{C})$ is finite. Indeed, the key fact is that $\mathrm{GL}_2(\mathbb{C})$ contains open neighbourhoods of Id which contain no subgroup other than $\{\mathrm{Id}\}$. Let E be such an open set. Then since ρ is continuous, $\rho^{-1}(E)$ is an open neighbourhood of $\mathrm{id} \in G_{\mathbb{Q}}$. Being open with respect to the Krull topology means that there exists $K/\mathbb{Q}$ finite normal extension of fields such that $G_K \subset \rho^{-1}(E)$. Thus $\rho(G_K) \subset \rho(\rho^{-1}(E)) \subset E$. Since the only subgroup contained in E is the trivial subgroup, we obtain that $\rho(G_K) = \{\mathrm{Id}\}$. In particular, $G_K \subset \ker \rho$, and the image of ρ is isomorphic to $G_{\mathbb{Q}}/\ker \rho \hookrightarrow G_{\mathbb{Q}}/G_K \simeq \mathrm{Gal}(K/\mathbb{Q})$, which is a finite set.

3. The semisimplicity condition, together with the fact that the set $\{\mathrm{Frob}_p : p \text{ is a prime}\}$ of lifts of Frobenius is dense in $G_{\mathbb{Q}}$, implies that the representation ρ_f is uniquely determined by the condition $\mathrm{Tr}(\rho_f(\mathrm{Frob}_p)) = a_p$ for all $p \nmid N$.

Remark 0.3. If f is not a cuspidal form, it is easy to prove the existence of the Galois representation ρ_f. Indeed, in this case f is an *Eisenstein series*, and it was already known to Hecke that there exist Dirichlet characters χ_1, χ_2 of $(\mathbb{Z}/N\mathbb{Z})^\times$ such that $\chi_1\chi_2 = \varepsilon$ and $\chi_1(p) + \chi_2(p) = a_p$ for all $p \nmid N$. Thus, it suffices to consider the (reducible) representation $\rho_f = \chi_1 \oplus \chi_2$. Thus we will focus on proving the existence of the Galois representation ρ_f in the case when f is cuspidal.

Through the rest of the chapter, we denote by $M_k(\Gamma_1(N))$ the space of modular forms of weight k with respect to $\Gamma_1(N)$. For each prime number p, we denote by T_p the p-th Hecke operator acting on $M_k(\Gamma_1(N))$. Sometimes we will consider Hecke operators acting on different spaces $M_k(\Gamma_1(N))$, $M_{k'}(\Gamma_1(N))$; we will take care of specifying at each point on which space does T_p act and hope it does not cause confusion.

Essentially, we can divide the proof of the existence of ρ_f into four main steps:

1. Raise the level of f by multiplication with an Eisenstein series (preserving the property of being an eigenform modulo ℓ); and use the existence result of Galois representations in weight ≥ 2 (Theorem 1.1) to prove the existence of a Galois representation attached to f with coefficients in $\mathbb{F}_\ell$ for a suitable infinite set of primes $\ell \nmid N$;
2. Lift to $\mathbb{C}$, assuming a bound on the size of the image of the Galois representations in the previous step, which is independent on ℓ;
3. Provide a bound on the size of the image of the Galois representations in the first step which is independent on ℓ.

We devote one section to describe each of the steps in detail. In the last section we will also show that the representation ρ_f is irreducible when f is cuspidal, thus completing the proof of Theorem 0.1.

1 Step 1: Deligne-Serre lifting lemma and eigenforms mod ℓ

Throughout this section, we fix a cuspidal modular form f as in the statement of Theorem 0.1. If we normalise f so that the first Fourier coefficient equals 1, the Fourier expansion of f is $f(z) = \sum_{n=1}^{\infty} a_n q^n$, where as usual we denote $q := e^{2\pi i z}$. In other words, the Fourier coefficient a_n coincides with the eigenvalues of T_n at f when $\gcd(n, N) = 1$. Denote by K_f the field generated over $\mathbb{Q}$ by the set $\{a_n : n \in \mathbb{N}\}$, and by $\mathcal{O}_f$ the ring of integers of K_f.

As mentioned in the introduction, an essential ingredient in the proof of Theorem 0.1 is the existence result of Galois representations attached to modular eigenforms of weight $k \geq 2$. Let us recall the statement here:

Theorem 1.1 (Deligne)**.** *Let $f \in M_k(\Gamma_1(N))$ be a modular form, with nebentypus ε, which is an eigenform for T_p, for all $p \nmid N$, with eigenvalue a_p. Let K be a finite extension of $\mathbb{Q}$ containing a_p and $\varepsilon(p)$ for all prime $p \nmid N$. Let λ be a finite place of K, of residue characteristic ℓ, and denote by K_λ the completion of K at λ.*

Then there exists a continuous, semi-simple, linear representation

$$\rho_{f,\lambda} : G_{\mathbb{Q}} \to \mathrm{GL}_2(K_\lambda)$$

which is unramified outside $N\ell$ and such that

$$\mathrm{Tr}(\rho_{f,\lambda}(\mathrm{Frob}_p)) = a_p \text{ and } \det(\rho_{f,\lambda}(\mathrm{Frob}_p)) = \varepsilon(p)p^{k-1} \text{ if } p \nmid N\ell.$$

The first key idea in the proof of Theorem 0.1 is the following: for each modular form g of weight k, the product fg is a modular form of weight $k+1$, so it may be possible to apply Theorem 1.1 to it. Of course, difficulties arise immediately: even if f and g were eigenforms for T_p (acting on the spaces of modular forms corresponding to f and g), the product does not have to be an eigenform for T_p (acting on the space of modular forms corresponding to fg). Moreover, even if it were the case that fg is an eigenform for T_p, the eigenvalue would no longer be the eigenvalue a_p of f.

The second key idea is that, instead of working over number fields or their completions, we can look first at the situation over finite fields, taking advantage of the triviality of Eisenstein series modulo ℓ for suitable primes ℓ. Recall that, for each even integer $k > 2$, the *Eisenstein series* of weight k is defined as

$$E_k(z) = \frac{1}{2\zeta(k)} {\sum_{m_1,m_2}}' \frac{1}{(m_1 z + m_2)^k},$$

where the summation runs through all pairs $(m_1, m_2) \in \mathbb{Z} \times \mathbb{Z}$ such that $(m_1, m_2) \neq (0, 0)$. We know that $f \cdot E_k$ is a modular form in $S_{k+1}(\Gamma_1(N))$. Let us write the Fourier expansion $E_k(z) = \sum_{n=0}^{\infty} c_n q^n$ (note that $c_0 = 1$ because of the chosen normalisation). Then a key observation is that, if $(\ell - 1)|k$, we have the congruences

$$c_n \equiv 0 \pmod{\ell} \text{ for all } n \geq 1.$$

Let K be a finite extension of $\mathbb{Q}$ containing the eigenvalues a_p of f for T_p acting on $S_k(\Gamma_1(N))$, for all $p \nmid N$, and choose a prime λ of K of residue characteristic ℓ. By abuse of notation, denote also by λ the maximal ideal of the valuation ring $\mathcal{O}_\lambda$ of the completion K_λ of K at λ. We obtain that

$$f \cdot E_k \equiv f \pmod{\lambda},$$

where (abusing language) we are identifying $f \cdot E_k$ and f with their Fourier expansions as power series in the variable q. Thus $f \cdot E_k$ is not an eigenform, but is *congruent to an eigenform (that is, to f) modulo λ.*

Let us look closer at this last statement. Let ℓ be a prefixed prime and choose k such that $(\ell - 1)|k$. We know that f is an eigenform for all T_p with $p \nmid N$; more precisely, $T_p f = a_p f$

for all $p \nmid N$. Write $f \cdot E_k = \sum_{n=1}^{\infty} b_n q^n$, and recall that the action of the Hecke operator T_p on f and $f \cdot E_k$ can be written in terms of Fourier expansions as follows:

$$T_p f = \sum_{n=1}^{\infty} a_{pn} q^n + \varepsilon(p) \sum_{n=1}^{\infty} a_n q^{pn}.$$
$$T_p(f \cdot E_k) = \sum_{n=1}^{\infty} b_{pn} q^n + \varepsilon(p) p^{k+1-1} \sum_{n=1}^{\infty} b_n q^{pn}.$$

Since $(\ell - 1)|k$, we obtain that $p^k \equiv 1 \pmod{\lambda}$, and thus $T_p f \equiv T_p(f \cdot E_k) \pmod{\lambda}$. This allows us to conclude that

$$T_p(f \cdot E_k) \equiv T_p f \equiv a_p f \equiv a_p f \cdot E_k \pmod{\lambda}.$$

The next step will be to lift $f \cdot E_k \pmod{\lambda}$ to an modular form g of weight $k+1$ which is an eigenform. This is performed via the so called Deligne-Serre lifting Lemma. In [DS74] it is stated in a very general context; here we write a particular version that fits our setting, taken from [Wie].

For any $k \geq 2$, $N \in \mathbb{N}$, denote by $\mathbb{T}_k(N)$ the $\mathbb{Z}$-algebra generated by the set of Hecke operators $\{T_n : n \in \mathbb{N}\}$ inside the algebra of endomorphisms of $M_k(\Gamma_1(N))$. and $\mathbb{T}'(N)$ the $\mathbb{Z}$-algebra generated by the set of Hecke operators $\{T_m : \gcd(m, N) = 1\}$.

Note that any Hecke eigenform $f = \sum_{n=0}^{\infty} a_n q^n$, normalised so that $a_1 = 1$, gives rise to a ring homomorphism

$$\Psi_f : \mathbb{T}_k(N) \to \overline{\mathbb{Q}}$$
$$T_p \mapsto a_p$$

In fact, the map $f \in M_k(\Gamma_1(N)) \mapsto \Psi_f \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_k(N), \mathbb{C})$ is a bijection.

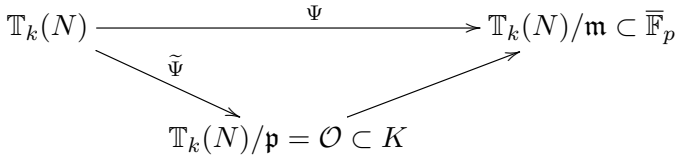
In our setting, we are working with modular forms $f \in M_k(\Gamma_1(N))$ which are eigenforms for the operators T_p where $p \nmid N$, but a priori they are not eigenforms for T_p when $p|N$. However, if f is a *newform* which is an eigenform for all $T \in \mathbb{T}'(N)$, then it is also an eigenform for all $T \in \mathbb{T}(N)$, and it makes sense to talk about the ring homomorphism Ψ_f.

The lifting lemma of Deligne and Serre will follow as a consequence of the structure of the Hecke algebra $\mathbb{T}_k(N)$. More precisely, every maximal strictly ascending chain of prime ideals of $\mathbb{T}_k(N)$ has the form $(0) \subset \mathfrak{p} \subset \mathfrak{m}$, where $\mathbb{T}_k(N)/\mathfrak{m}$ is a finite field of positive characteristic and $\mathbb{T}_k(N)/\mathfrak{p}$ is an order in a number field.

Lemma 1.2 (Deligne-Serre Lifting Lemma)**.** *Let $k \geq 2$, $N \in \mathbb{N}$. Let $\Psi : \mathbb{T}_k(N) \to \overline{\mathbb{F}}_p$ be a ring homomorphism. Then there exists $g = \sum_{n=0}^{\infty} a_n q^n \in M_k(\Gamma_1(N))$, eigenform for all Hecke operators, and a prime $\mathfrak{p}|p$ in an order $\mathcal{O}$ of a number field containing the set $\{a_n : n \in \mathbb{N}\}$, such that for all $n \in \mathbb{N}$, the reduction of a_n mod $\mathfrak{p}$ coincides with $\Psi(n)$.*

Sketch of proof. Let $\mathfrak{m} \subset \mathbb{T}_k(N)$ be the kernel of Ψ. Since the image of Ψ is a subring in a finite field (and thus a field), $\mathfrak{m}$ is a maximal ideal. Let $\mathfrak{p} \subset \mathfrak{m}$ be a nonzero minimal prime

ideal. Then Ψ factors as



where $\mathcal{O} = \mathbb{T}_k(N)/\mathfrak{p}$ is an order in some number field, say K. Then $g(z) := \sum_{i=0}^{\infty} \widetilde{\Psi}(n) q^n$ is a modular form in $M_k(N)$ satisfying the required conditions. □

Corollary 1.3. *Let ℓ be a prime, let $k, k', N \in \mathbb{N}$ with $k' \geq 2$, $k \equiv k' \pmod{\ell - 1}$. Let $f = \sum_{n=0}^{\infty} a_n q^n \in M_k(\Gamma_1(N))$ be a Hecke eigenform for all T_p with $p \nmid N$, normalised, and $g \in M_{k'}(N) = \sum_{n=0}^{\infty} a'_n q^n$ be modular form. Call $K_f := \mathbb{Q}(\{a_n : n \in \mathbb{N}\})$ (resp. $K_g := \mathbb{Q}(\{a'_n : n \in \mathbb{N}\})$), $\mathcal{O}_f$ (resp. $\mathcal{O}_g$) the ring of integers of K_f (resp. K_g). Assume there exists primes $\lambda \subset \mathcal{O}_f$ and $\lambda' \subset \mathcal{O}_g$ above ℓ such that, for all $n \in \mathbb{N}$ with $\gcd(n, N) = 1$, the reduction of a_n mod λ coincides with the reduction of a'_n mod λ'.*

Then there exists $h = \sum_{n=0}^{\infty} b_n q^n \in M_{k'}(\Gamma_1(N))$, eigenform for all Hecke operators, normalised, and a prime $\lambda'' | \ell$, such that for all $n \in \mathbb{N}$ with $\gcd(n, N) = 1$, the reduction of a_n mod λ coincides with the reduction of b_n modulo λ''.

Proof. Replacing N by a divisor, we may assume, without loss of generality, that $f \in M_k(N)$ is a newform. Thus, it is a Hecke eigenform for *all* T_p, p prime. Denote by $\Psi_f : \mathbb{T}_k(N) \to \mathbb{C}$ the ring homomorphism characterised by $\Psi(f)(T_p) = a_p$. By hypothesis $k \equiv k' \pmod{\ell - 1}$, and $a_p \pmod{\lambda} = a'_p \pmod{\lambda'}$, thus the quotient map $\overline{\Psi}_f : T_k(N) \to T_k(N)/\lambda$ gives rise to a ring morphism

$$\begin{aligned} \overline{\Psi} : \mathbb{T}_{k'}(N) &\to \mathbb{T}_{k'}(N)/\lambda' \\ T_p &\mapsto a'_p \pmod{\lambda'}. \end{aligned}$$

Note that each $T_p \in \mathbb{T}_{k'}(N)$ maps to $a_p \pmod{\lambda}$, via an identification of $\mathbb{Z}[\{a_n : n \in \mathbb{N}\}]/(\lambda \cap \mathbb{Z}[\{a_n : n \in \mathbb{N}\}])$ with $\mathbb{Z}[\{a'_n : n \in \mathbb{N}\}]/(\lambda' \cap \mathbb{Z}[\{a'_n : n \in \mathbb{N}\}])$ as a subring of both $\mathbb{T}_k(N)/\lambda\mathbb{T}_k(N)$ and $\mathbb{T}_{k'}(N)/\lambda\mathbb{T}_{k'}(N)$. The hypothesis $k \equiv k' \pmod{\ell - 1}$ is necessary to ensure that $\overline{\Psi}$ respects the ring structure of $\mathbb{T}_{k'}(N)$.

We can apply Deligne-Serre's lifting lemma to $\overline{\Psi}$, and conclude that there exists a modular form $h = \sum_n b_n q^n \in M_k(\Gamma_1(N))$, which is a normalised eigenform for all Hecke operators, and a prime λ'' of an order $\mathcal{O}$ of a number field, such that $b_n \pmod{\lambda''} \equiv a'_n \pmod{\lambda'} \equiv a_n \pmod{\lambda}$.

□

Remark 1.4. Let ℓ be a prime, $f \in M_k(\Gamma_1(N))$ as in the hypothesis and $h \in M_{k'}(\Gamma_1(N))$ as in the conclusion of Corollary 1.3. Let ε (resp. ε'') be the nebentypus of f (resp. h). The fact that the diamond operators $\langle p \rangle$ with $p \nmid N$ belong to the Hecke algebra $T'_k(N)$ (resp. $T'_{k'}(N)$) imply that the values $\{a_n : \gcd(n, N) = 1\}$ (resp. $\{b_n : \gcd(n, N) = 1\}$) determine ε (resp. ε'') uniquely, c.f. [DI95, proof of Proposition 3.5.1]. Thus from the equalities $b_n \pmod{\lambda''} \equiv a_n \pmod{\lambda}$ for all n with $\gcd(n, N) = 1$ we obtain that $\varepsilon''(p) \pmod{\lambda''} \equiv \varepsilon(p) \pmod{\lambda}$ for all $p \nmid N$.

Applying Corollary 1.3 to a prefixed prime ℓ and $f \in S_1(N)$, $g = f \cdot E_k \in S_{k+1}(N)$ (where $k \equiv 0 \pmod{\ell-1}$), we obtain that there exists a modular form $h \in M_{k+1}(N)$ which is a Hecke eigenform for all Hecke operators. Furthermore, if we denote by $h(z) = \sum_{n=0}^{\infty} b_n q^n$ its Fourier expansion, we know that for each prime λ of $\mathcal{O}_f$ there exists a prime $\lambda'' \subset \mathbb{Z}[\{b_n : n \in \mathbb{N}\}]$ such that $a_n \pmod{\lambda} \equiv b_n \pmod{\lambda''}$ for all $n \in \mathbb{N}$ with $\gcd(n, N) = 1$ and $\varepsilon(p) \pmod{\lambda} \equiv \varepsilon''(p) \pmod{\lambda''}$ for all $p \nmid N$, where ε (resp. ε'') denote the nebentypus of f (resp. of h). Choose one such prime λ''.

We can apply Theorem 1.1 to the modular form h and the prime $\lambda''|\ell$, and conclude that there exists a Galois representation $\rho_{h,\lambda''} : G_{\mathbb{Q}} \to \mathrm{GL}_2(K_{\lambda''})$, which is semi-simple, unramified outside $N\ell$, and such that $\mathrm{Tr}(\rho_{h,\lambda''}(\mathrm{Frob}_p)) = b_p$ and $\det(\rho_{h,\lambda''}(\mathrm{Frob}_p)) = \varepsilon(p)p^k$ if $p \nmid N\ell$.

Reducing modulo λ'', we obtain a Galois representation $\overline{\rho}_{h,\lambda''} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_{\lambda''})$, where $\mathbb{F}_{\lambda''}$ is the residue field of $K_{\lambda''}$. Moreover, $\overline{\rho}_{h,\lambda''}$ satisfies that it is semi-simple, unramified outside $N\ell$ and $\mathrm{Tr}(\overline{\rho}_{h,\lambda''}(\mathrm{Frob}_p)) \equiv b_p \pmod{\lambda''} \equiv a_p \pmod{\lambda}$, $\det(\overline{\rho}_{h,\lambda''}(\mathrm{Frob}_p)) \equiv \varepsilon(p) \pmod{\lambda''}$ whenever $p \nmid N\ell$. Note that the properties of the representation $\overline{\rho}_{h,\lambda''}$ can be expressed in terms of our original modular form f; at this point we can forget about the chosen lift h and everything related to it. We emphasize this fact by defining

$$\overline{\rho}_{f,\ell} := \overline{\rho}_{h,\lambda''} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$$

(recall that we chose a prime λ'' above ℓ, so it is fixed). Note that the semisimplicity condition implies that $\rho_{f,\ell}$ can be defined over the field generated by the coefficients of the characteristic polynomials $\mathrm{charpoly}(\overline{\rho}_{f,\ell}(\mathrm{Frob}_p))$, for $p \nmid N\ell$. In particular, $\rho_{f,\ell}$ can be defined over the field $\mathbb{F}_\lambda$ generated over $\mathbb{F}_\ell$ by the elements $\{a_n \pmod{\lambda} : \gcd(n, N\ell) = 1\}$.

This procedure can be applied at all primes $\ell \nmid N$. In this way, we obtain a *family* of Galois representations $\overline{\rho}_{f,\ell} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ indexed by the prime ℓ. In the next section, we explain how to use this family to obtain a representation $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$.

2 Lift to $\mathbb{C}$

Let f be a modular form satisfying the hypothesis of Theorem 0.1. We keep the notations from the previous section; in particular, $K_f = \mathbb{Q}(\{a_n : n \in \mathbb{N}\})$. In the previous section we saw that, for each prime $\ell \nmid N$, we have a Galois representation $\overline{\rho}_{f,\ell} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\lambda)$, where $\lambda|\ell$ is a prime of $\mathcal{O}_f$ and $\mathbb{F}_\lambda$ is the residue field $\mathcal{O}_f/\lambda$, such that $\mathrm{Tr}(\rho_{f,\ell}(\mathrm{Frob}_p)) \equiv a_p \pmod{\lambda}$ and $\det(\rho_{f,\ell}(\mathrm{Frob}_p)) \equiv \varepsilon(p) \pmod{\lambda}$ if $p \nmid N\ell$.

Fix a number field $K \supseteq K_f$, and let $\mathcal{L}$ denote the (infinite) set of primes ℓ which are totally split in $K/\mathbb{Q}$. For each $\ell \in \mathcal{L}$ and each $\lambda|\ell$ prime of $\mathcal{O}_f$, we have that $\mathbb{F}_\lambda$ is the prime field with ℓ elements.

In the rest of the section, we will make the following assumption, which will be proved in Section 3.

Assumption 2.1. *There exists $A \in \mathbb{R}_{>0}$ such that, for all $\ell \in \mathcal{L}$,*

$$|\overline{\rho}_{f,\ell}(G_{\mathbb{Q}})| \leq A.$$

The fact that the image of $\overline{\rho}_{f,\ell}$ is bounded independently of ℓ will play a very important role in lifting it to characteristic zero. Indeed, we will exploit the following well-known result:

Proposition 2.2. *Let $\ell > 5$ be a prime, $\mathbb{F}_\lambda$ a finite field of characteristic ℓ and let $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\lambda)$ be such that $\ell \nmid |\overline{\rho}_\ell(G_{\mathbb{Q}})|$. Then there exists a representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(K_\lambda)$, where K_λ is the fraction field of the ring of Witt vectors of $\mathbb{F}_\lambda$, such that $\rho \pmod{\lambda}$ coincides with $\overline{\rho}$. Moreover, ρ is unramified outside the ramification set of $\overline{\rho}$.*

Proof. Let K be the fixed field of $\overline{\mathbb{Q}}$ by $\ker \rho$, and let $G = \mathrm{Gal}(K/\mathbb{Q})$ (which is a finite group). We may regard $\overline{\rho}$ as a representation of G. It is a standard result that if G is a finite group with $\ell \nmid |G|$, then any representation of G with coefficients in $\mathbb{F}_\lambda$ can be lifted to a representation with coefficients in the ring of Witt vectors of $\mathbb{F}_\lambda$. This result follows from the fact that the reduction mod λ of an absolutely irreducible representation of G is absolutely irreducible, together with the formula relating $|G|$ and the degrees of all irreducible representations of G, and complete reducibility (cf. [Fei67, (4.4) of §4]). The last assertion follows from the fact that ρ factors through $\mathrm{Gal}(K/\mathbb{Q})$. □

Remark 2.3. We may (and will) assume, without loss of generality, that for all natural numbers $n \leq A$, the n-th roots of unity belong to K. Indeed, let A be a constant such that, for all $\ell \in \mathcal{L}$, $|\overline{\rho}_{f,\ell}(G_{\mathbb{Q}})| \leq A$. For each $n \in \mathbb{N}$, denote by μ_n the group of n-th roots of unity contained in a fixed algebraic closure $\overline{K}$ of K, and consider the field $K' = K(\bigcup_{n \leq A} \mu_n)$. Then $K' \supseteq K_f$, and we can consider the set $\mathcal{L}'$ of primes of K' which are totally split in $K'/\mathbb{Q}$. Note that $\mathcal{L}' \subset \mathcal{L}$ is still an infinite set of primes.

For each $\ell > A$ belonging to $\mathcal{L}$, choose a lift $\rho_{f,\ell} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_\ell)$, which exists by Proposition 2.2. We know that, for any $p \nmid N\ell$, $\mathrm{Tr}(\rho_{f,\ell}(\mathrm{Frob}_p)) \equiv a_p \pmod{\ell}$ and $\det(\rho_{f,\ell}(\mathrm{Frob}_p)) = \varepsilon(p) \pmod{\ell}$. Our aim now is to prove that, in fact, $\rho_{f,\ell}$ can be defined over a number field (at least for some prime ℓ), by means of Chebotarev's Density Theorem. Consider the (finite) set of polynomials

$$Y := \{(1 - \alpha T)(1 - \beta T) \in K[T] : \alpha, \beta \in K \text{ are roots of unity of order} \leq A\}.$$

Lemma 2.4. *Let $\ell \in \mathcal{L}$, $p \nmid N\ell$ a prime, and denote by $M := \rho_{f,\ell}(\mathrm{Frob}_p) \in \mathrm{GL}_2(\mathbb{Z}_\ell)$. Then the characteristic polynomial of M coincides with $1 - a_p T + \varepsilon(p)T^2$ (and in particular belongs to $Y \subset K[T]$).*

Proof. Since $|\overline{\rho}_{f,\ell}(G_{\mathbb{Q}})| \leq A$, we have that the reduction mod ℓ of the matrix M has order $n \leq A$. Therefore the reduction mod ℓ of the characteristic polynomial $P_M(T)$ of M is of the shape $(1 - T\theta_1)(1 - T\theta_2)$, where θ_1, θ_2 are n-th roots of unity in $\overline{\mathbb{F}}_\ell$. Thus, there exists some $P_\ell(T) \in Y$ (depending on ℓ) such that $P_M(T) \equiv P_\ell(T) \pmod{\ell}$.

Recall that $\mathrm{Tr}(M) \equiv a_p \pmod{\ell}$ and $\det(M) \equiv \varepsilon(p) \pmod{\ell}$. Therefore we have the congruence

$$P_\ell(T) \equiv 1 - a_p T + \varepsilon(p)T^2. \tag{1}$$

In this way, we can obtain a family of polynomials $\{P_\ell(T) : \ell \in \mathcal{L}, p \nmid N\ell\} \subset Y$ such that Equation (1) holds for all $\ell \in \mathcal{L}, p \nmid N\ell$. Since $\mathcal{L}$ is an infinite set and Y is finite, there

exists a $P(T) \in Y$ such that $P(T) = P_\ell(T)$ for infinitely many primes ℓ. In particular, the congruences $P(T) \equiv 1 - a_p T + \varepsilon(p)T^2 \equiv P_M(T) \pmod{\ell}$ hold for infinitely many primes ℓ, and must therefore be equalities, proving the assertion of the Lemma.

□

Proposition 2.5. *Let $\ell > A$ be a prime number in $\mathcal{L}$. Then the representation $\rho_{f,\ell}$ can be defined over K. Moreover, if $\ell' > A$ is another prime in $\mathcal{L}$, then $\rho_{f,\ell}$ and $\rho_{f,\ell'}$ are isomorphic as complex representations.*

Proof. Recall that the set $\{\mathrm{Frob}_p : p \nmid N\ell\}$ is dense in $G_\mathbb{Q}$, and $\mathrm{charpoly}(\rho_{f,\ell}(\mathrm{Frob}_p)) \in K[T]$ by the previous lemma. Moreover, the image of $\rho_{f,\ell}$ is finite (since the set of characteristic polynomials $\{\mathrm{charpoly}(\rho_{f,\ell}(\mathrm{Frob}_p)) : p \nmid N\ell\} \subset Y$ is finite). In particular, the representation $\rho_{f,\ell}$ is semi-simple. Thus it can thus be defined over K. The last assertion follows from the fact that, for all $p \nmid N\ell\ell'$, $\mathrm{charpoly}(\rho_{f,\ell}(\mathrm{Frob}_p)) = \mathrm{charpoly}(\rho_{f,\ell'}(\mathrm{Frob}_p))$. □

Define $\rho_f : G_\mathbb{Q} \to \mathrm{GL}_2(K)$ to be the representation $\rho_{f,\ell}$, for any $\ell > A$, belonging to $\mathcal{L}$; the proposition above shows that this definition is independent of the choice of ℓ.

Corollary 2.6. *The representation ρ_f is unramified outside N.*

Proof. By Proposition 2.5, we know that ρ_f is isomorphic to $\rho_{f,\ell}$ for any $\ell > A$, $\ell \in \mathcal{L}$. Fix one such prime: then ρ_f is unramified outside $N\ell$ by construction. Fixing a different prime ℓ', we conclude that ρ_f is unramified outside $N\ell'$; thus it is unramified outside N. □

Remark 2.7. We still need to show that ρ_f is irreducible if and only if it is cuspidal. We will prove this in the next section.

3 Bounds on the image of the mod ℓ Galois representations

The aim of this section is to prove that Assumption 2.1 holds for the family of Galois representations $\{\overline{\rho}_{f,\ell}\}_\ell$ obtained in Section 1. Moreover, we will show that the representation ρ_f obtained in the previous section from a cuspidal modular form f is irreducible. We treat these two issues together, because they both require the use of a result from analytic number theory, that will be introduced in this section.

We start with the proof of Assumption 2.1. First of all, we will see a result of group-theoretic nature, that reduces the problem of bounding the cardinality of semi-simple subgroups $G_\ell \in \mathrm{GL}_2(\mathbb{F}_\ell)$ in a family of $\{G_\ell\}_\ell$ independently of ℓ to checking the property $C(\eta, M)$ defined below.

Definition 3.1 (Property $C(\eta, M)$)**.** Let $\eta, M > 0$. We say a subgroup $G \subseteq \mathrm{GL}_2(\mathbb{F}_\ell)$ satisfies $C(\eta, M)$ if there exists $H \subset G$ such that:

- $|H| \geq (1 - \eta)|G|$;
- The set $\{\det(1 - hT) : h \in H\}$ has at most M elements.

Example 3.2. Let $G \subset \mathrm{GL}_2(\mathbb{F}_\ell)$. Take M to be the cardinality of the set $\{\det(1-gT) : g \in G\}$ (which is a finite set). Then G satisfies the property $C(\eta, M)$ for any $\eta > 0$, taking $H = G$.

Proposition 3.3. *For each prime ℓ, let $G_\ell \subset \mathrm{GL}_2(\mathbb{F}_\ell)$ be a semi-simple subgroup. Assume there exist $\eta < 1/2$, $M \geq 0$ such that: For all prime ℓ, G_ℓ satisfies $C(\eta, M)$. Then there exists $A = A(\eta, M) > 0$ such that, for all ℓ,*

$$|G_\ell| \leq A.$$

Proof. We will distinguish several cases, according to Dickson's classification of subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$:

1. G_ℓ is contained in a Cartan subgroup $\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$;
2. G_ℓ is contained in the normaliser of Cartan subgroup $\left\langle \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}, \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix} \right\rangle$;
3. The projection of G by the map $\mathrm{GL}_2(\mathbb{F}_\ell) \to \mathrm{PGL}_2(\mathbb{F}_\ell)$ is isomorphic to $\mathfrak{A}_4$, $\mathfrak{S}_4$ or $\mathfrak{A}_5$ (exceptional cases).
4. $G_\ell \supset \mathrm{SL}_2(\mathbb{F}_\ell)$ (huge);

The analysis in all cases can be found in [DS74]; here we will just consider a couple of cases, to illustrate the procedure.

Assume for example that G_ℓ is contained in a Cartan subgroup $\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$. Let $P(T) \in \mathbb{F}_\ell(T)$ be a fixed polynomial of degree 2 with independent term equal to 1. Since G_ℓ is semi-simple, there are at most two elements in G with this characteristic polynomial. Since G_ℓ satisfies $C(\eta, M)$, there exists a subgroup, say H_ℓ, such that (1) $|H_\ell| \geq (1-\eta)|G_\ell|$ and (2) $|\{\det(1-hT) : h \in H_\ell\}| \leq M$. Inequality (2) implies that $|H_\ell| \leq 2M$. Moreover, replacing this inequality in (1), we obtain the following bound for $|G_\ell|$, which is independent of ℓ:

$$|G_\ell| \leq 2M/(1-\eta).$$

Let us consider also the case in the list of Dickson when G_ℓ has the biggest possible cardinality, that is, when $G_\ell \supseteq \mathrm{SL}_2(\mathbb{F}_\ell)$. Let $r := (G_\ell : \mathrm{SL}_2(\mathbb{F}_\ell))$. Then we can compute the cardinality of G_ℓ as

$$|G_\ell| = r\ell(\ell+1)(\ell-1).$$

Fix a quadratic polynomial $P(T) \in \mathbb{F}_\ell[T]$ with independent term equal to 1. If $P(T)$ has two different roots in $\mathbb{F}_\ell$, we have that there are at most $\ell^2 + \ell$ elements of G_ℓ with characteristic polynomial $P(T)$. If $P(T)$ has a double root in $\mathbb{F}_\ell$, then there are at most ℓ^2 elements of G_ℓ with characteristic polynomial $P(T)$. Finally, if $P(T)$ is irreducible in $\mathbb{F}_\ell[T]$, then there are at most $\ell^2 - 1$ elements of G_ℓ with characteristic polynomial $P(T)$.

Since G_ℓ satisfies $C(\eta, M)$, there exists a subgroup, say H_ℓ, such that (1) $|H_\ell| \geq (1-\eta)|G_\ell|$ and (2) $|\{\det(1-hT) : h \in H_\ell\}| \leq M$. We can bound the cardinality of H_ℓ from above as

$$|H_\ell| \leq M(\ell^2 + \ell)$$

and from below as

$$|H_\ell| \geq (1-\eta)|G_\ell| = (1-\eta)r\ell(\ell+1)(\ell-1)$$

Combining these two inequalities we obtain a bound for ℓ, namely

$$\ell \leq 1 + \frac{M}{1-\eta}$$

Therefore, the case $G_\ell \supset \mathrm{SL}_2(\mathbb{F}_\ell)$ can only occur finitely many times, provided that, for each member of the family $\{G_\ell\}_\ell$, condition $C(\eta, M)$ holds. □

To apply Proposition 3.3 to the setting of this chapter, we need to check that there exist at least one positive number $\eta < 1/2$ and one positive number M such that for all $\ell \in \mathcal{L}$, $\overline{\rho}_{f,\ell}(G_{\mathbb{Q}})$ satisfies $C(\eta, M)$. Actually, we will prove a much stronger result, as stated below:

Proposition 3.4. *For each $\eta < 1/2$ there exists $M(\eta) > 0$, such that for all primes $\ell \in \mathcal{L}$, $\overline{\rho}_{f,\ell}(G_{\mathbb{Q}}) \subset \mathrm{GL}_2(\mathbb{F}_\ell)$ satisfies $C(\eta, M)$.*

The proof is based on the following inequality, that can be obtained as a consequence of a result of Rankin on the poles of $\sum_n |a_n|^2 n^{-s}$ where $f = \sum_{n=1}^{\infty} a_n q^n \in S_k(\Gamma_1(N))$ is a Hecke eigenform for T_p with $p \nmid N$[1]: For $s \to k^+$,

$$\sum_{p \nmid N} |a_p|^2 p^{-s} \leq \log\left(\frac{1}{s-k}\right) + O(1) \tag{2}$$

Before we prove Proposition 3.4, we recall the notion of superior density: if X is a subset of the set $\mathcal{P}$ of prime numbers, then

$$\mathrm{dens.sup}(X) = \limsup_{s \to 1^+} \frac{\sum_{p \in X} p^{-1}}{\log(1/(s-1))}.$$

Sketch of the proof of Proposition 3.4. Let $f = \sum_n a_n q^n \in S(\Gamma_1(N))$ a nonzero eigenform of the T_p for $p \nmid N$. We consider a filtration of the set of eigenvalues $\{a_p : p \nmid N \text{ prime}\}$ by their size (i.e. the absolute value of a_p, once we embed K into $\mathbb{C}$). More precisely, for any positive number c, consider the sets

$$\begin{aligned} Y(c) :=& \{a \in K : |\sigma(a)| \leq c \text{ for all embeddings } \sigma : K \hookrightarrow \mathbb{C}\} \\ X(c) :=& \{p \text{ prime number} : a_p \notin Y(c)\}. \end{aligned}$$

[1]Namely, the result of Rankin states that the product $\left(\sum_n |a_n|^2 n^{-s}\right) \zeta(2s-2k+2) H(s)$, where $H(s)$ is a finite product taking care of the factors for $p \mid N$, can be extended to a meromorphic function in the complex plane, with a single pole at $s = k$.

Note that the sets $\{Y(c)\}_{c>0}$ is an (increasing) sequence of finite sets, and the sets $\{X(c)\}_{c>0}$ form a (decreasing) sequence of sets. For each $c > 0$, the set $\{a_p : p \notin X(c)\} \subset Y(c)$ is also a finite set.

Applying equation (2) to f, we obtain

$$\sum_{p\nmid N} |a_p|^2 p^{-s} \leq \log\left(\frac{1}{s-1}\right) + O(1)$$

when $s \to 1^+$.

Note that, if $a_p \in K$ is an eigenvalue, so is $\sigma(a_p)$ for any field embedding $\sigma : K \hookrightarrow \mathbb{C}$ (indeed, it is an eigenvalue of f^σ). Thus we can apply the inequality above $[K : \mathbb{Q}]$ times (one to each f^σ, $\sigma : K \hookrightarrow \mathbb{C}$ an embedding). Adding them all together we obtain

$$\sum_{\sigma:K\hookrightarrow\mathbb{C}} \sum_{p\nmid N} |\sigma(a_p)|^2 p^{-s} \leq [K : \mathbb{Q}] \log\left(\frac{1}{s-1}\right) + O(1). \tag{3}$$

when $s \to 1^+$.

If $p \in X(c)$, there exists $\sigma : K \hookrightarrow \mathbb{C}$ such that $|\sigma(a_p)|^2 > c$, and consequently we have that $\sum_{\sigma:K\hookrightarrow\mathbb{C}} |\sigma(a_p)|^2 > c$. Replacing this inequality in (3) and neglecting the contribution of the terms with $p \notin X(c)$, we obtain

$$c \sum_{p\in X(c)} p^{-s} \leq [K : \mathbb{Q}] \log\left(\frac{1}{s-1}\right) + O(1)$$

when $s \to 1^+$. In particular,

$$\text{dens.sup}(X(c)) \leq [K : \mathbb{Q}]/c.$$

Fix a positive number $c > [K : \mathbb{Q}]/\eta$, and consider $X_\eta = X(c)$. Then $\text{dens.sup}(X_\eta) < \eta$, and the set $\{a_p : p \notin X_\eta\}$ is a finite set. Consider the set $\{P(T) \in K[T] : P(T) = X^2 - a_p T + \varepsilon(p) : p \notin X_\eta\}$, which is also a finite set, say of cardinality M. We claim that, for all $\ell \in \mathcal{L}$, the group $G_\ell := \overline{\rho}_{f,\ell}(G_\mathbb{Q})$ satisfies condition $C(\eta, M)$.

Indeed, consider the subgroup $H_\ell \subseteq G_\ell$ defined as be the smallest subgroup, closed under conjugation, and containing the set $\{\overline{\rho}_{f,\ell}(\text{Frob}_\text{p}) : p \notin X_\eta\}$. From the definition and Chebotarev's Density Theorem, it is clear that $|H_\ell| \geq (1-\eta)|G_\ell|$. For the second condition, note that for any $p \notin X_\eta$,

$$\text{charpoly}(\overline{\rho}_{f,\ell}(\text{Frob}_\text{p})) \equiv 1 - a_p T + \varepsilon(p) T^2 \pmod{\lambda},$$

for some prime $\lambda|\ell$. Therefore the set $\{\text{charpoly}(\overline{\rho}_{f,\ell}(\text{Frob}_\text{p})) : p \notin X_\eta\}$ has at most M elements, satisfying thus the second condition in Definition 3.1.

□

To sum up, we have proven that, given a cuspidal modular form as in Theorem 0.1, there exists a Galois representation $\rho_f : G_\mathbb{Q} \to \text{GL}_2(\mathbb{C})$ satisfying Equality (1.1). To conclude the

proof of Theorem 0.1, it suffices to show that ρ_f is irreducible. The reasoning is based on Rankin's estimate (2). Indeed, assume that ρ_f is reducible, thus $\rho_f \simeq \chi_1 \oplus \chi_2$ for some characters $\chi_1, \chi_2 : G_{\mathbb{Q}} \to \mathbb{C}^\times$, unramified outside N. To simplify notation, we identify them with Dirichlet characters modulo N. Equation (1.1) implies that, for each $p \nmid N$,

$$\chi_1(p) + \chi_2(p) = a_p \text{ and } \chi_1(p)\chi_2(p) = \varepsilon(p).$$

Let us compute $\sum_{p\nmid N} |a_p|^2 p^{-s}$ in terms of χ_1 and χ_2; denoting by $\bar{\cdot}$ the complex conjugation, we get

$$|a_p| = a_p\overline{a}_p = (\chi_1(p) + \chi_2(p))(\overline{\chi_1}(p) + \overline{\chi}_2(p)) = 2 + \chi_1(p)\overline{\chi}_2(p) + \overline{\chi_1}(p)\chi_2(p),$$

since $\chi_i\overline{\chi}_i = 1$ for $i = 1, 2$. Note that the character $\chi_1\overline{\chi}_2$ (resp. $\overline{\chi}_1\chi_2$) is not the trivial character; otherwise we would have $\chi_2 = \chi_1$ and $\varepsilon(-1) = \chi_1(-1)^2 = (\pm 1)^2 = 1$, which contradicts the assumptions of Theorem 0.1.

Therefore we can estimate

$$\sum_{p\nmid N} |a_p|^2 p^{-s} = 2\sum_{p\nmid N} p^{-s} + \sum_{p\nmid N} \chi_1(p)\overline{\chi}_2(p)p^{-s} + \sum_{p\nmid N} \overline{\chi}_1(p)\chi_2(p)p^{-s}$$

The last two term are equal to $O(1)$ when $s \to 1^+$, thus we have

$$\begin{aligned}\sum_{p\nmid N} |a_p|^2 p^{-s} &= 2\sum_{p\nmid N} p^{-s} + O(1) \\ &= 2\log\left(\frac{1}{s-1}\right) + O(1),\end{aligned}$$

when $s \to 1^+$, contradicting (2). This concludes the proof of Theorem 0.1.

References

[DI95] Fred Diamond and John Im. Modular forms and modular curves. In *Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994)*, volume 17 of *CMS Conf. Proc.*, pages 39–133. Amer. Math. Soc., Providence, RI, 1995.

[DS74] Pierre Deligne and Jean-Pierre Serre. Formes modulaires de poids 1. *Ann. Sci. École Norm. Sup. (4)*, 7:507–530 (1975), 1974.

[Fei67] Walter Feit. *Characters of finite groups.* W. A. Benjamin, Inc., New York-Amsterdam, 1967.

[Wie] Gabor Wiese. Lectures on modular galois representations modulo prime powers. Lecture notes for the PhD School *Modular Galois Representations Modulo Prime Powers*, Copenhagen 2011.