ELSEVIER

Available online at www.sciencedirect.com

ScienceDirect

Journal of Number Theory 128 (2008) 589–618

JOURNAL OF Number Theory

www.elsevier.com/locate/jnt

On the modularity of supersingular elliptic curves over certain totally real number fields

Frazer Jarvis [*], Jayanta Manoharmayum

Department of Pure Mathematics, University of Sheffield, Sheffield S3 7RH, UK

Received 7 July 2006; revised 30 March 2007

Available online 20 December 2007

Communicated by Gebhard Böckle

Abstract

We study generalisations to totally real fields of the methods originating with Wiles and Taylor and Wiles [A. Wiles, Modular elliptic curves and Fermat's Last Theorem, Ann. of Math. 141 (1995) 443–551; R. Taylor, A. Wiles, Ring-theoretic properties of certain Hecke algebras, Ann. of Math. 141 (1995) 553–572]. In view of the results of Skinner and Wiles [C. Skinner, A. Wiles, Nearly ordinary deformations of irreducible residual representations, Ann. Fac. Sci. Toulouse Math. (6) 10 (2001) 185–215] on elliptic curves with ordinary reduction, we focus here on the case of supersingular reduction. Combining these, we then obtain some partial results on the modularity problem for semistable elliptic curves, and end by giving some applications of our results, for example proving the modularity of all semistable elliptic curves over $\mathbb{Q}(\sqrt{2})$.

MSC: 11F41; 11F80; 11G05

1. Introduction

Let E denote an elliptic curve over a totally real number field F. We say that E is *modular* if there is a Hilbert modular form f over F of parallel weight 2 (i.e., the corresponding automorphic representation has weight 2 at every infinite place) such that the Galois representation associated to E via its ℓ-adic Tate module is isomorphic to an ℓ-adic representation associated to f (see [1] and [20]).

[*] Corresponding author.
E-mail addresses: a.f.jarvis@shef.ac.uk (F. Jarvis), j.manoharmayum@shef.ac.uk (J. Manoharmayum).

0022-314X/$ – see front matter © 2007 Elsevier Inc. All rights reserved.
doi:10.1016/j.jnt.2007.10.003

The approach is now standard, and originated in [24] and [23]; one considers the case $\ell = 3$, uses the Langlands–Tunnell theorem to show that the *reduction* $\bar{\rho}_{E,3}$ is modular, and then proves that every (suitably constrained) lift to characteristic 0 is modular.

Historically, the easier case has been where $\bar{\rho}_{E,3}$ is irreducible. In this case, the deformation theory is now well understood, and this was the only case needed by Wiles and Taylor and Wiles [23,24]. Over totally real fields, Fujiwara circulated a manuscript [9] some years ago, proving an important generalisation of the method of Taylor–Wiles, and announcing a proof of the modularity of certain elliptic curves over totally real fields. However, there are several hypotheses appearing in his main theorem which we hope partially to eliminate in this work. Subsequently, Skinner and Wiles [19] have proven the modularity in many 'nearly ordinary' cases.

In the case where $\bar{\rho}_{E,3}$ is reducible, Skinner and Wiles [17] have developed new techniques to demonstrate modularity of elliptic curves (and more general Galois representations) over totally real fields, although these results depend on certain hypotheses on cyclotomic extensions of F. Since the first version of this article was written (2002–2003), Kisin has also found stronger results (see [11,12]).

1.1. Reduction to the semistable case

We first remark that the modularity of all elliptic curves over totally real fields may be reduced to proving the modularity of all semistable elliptic curves over totally real fields. The argument is simple; by an explicit version of the semistable reduction theorem (see, for example, [21, Lemma 2.2]), an elliptic curve E over a totally real field F attains semistable reduction over a finite soluble totally real Galois extension F'/F. (Note that F'/F will be ramified at any prime of F at which E has additive reduction.) The modularity of $E_{/F}$ then follows from the modularity of $E_{/F'}$ using base-change techniques. This argument is well known to experts, so we omit it here.

For this reason, we restrict attention to semistable curves, and try to prove modularity. In view of some of the applications in mind, we focus in this paper on the easiest case, where the ramification conditions on the field are as strong as possible, but the methods should apply more generally. Because of the results already obtained in the reducible and ordinary cases, we focus on the supersingular case in this paper.

1.2. Applications

As we are able to prove the modularity of more elliptic curves than was previously known, we can therefore improve certain results in the literature. Following Wiles's methods [24], we try to find fields for which we can prove modularity of all semistable curves. Wiles [24, Chapter 5] uses a switch between the primes 3 and 5, which depends on the finiteness of $X_0(15)(\mathbb{Q})$; however $X_0(15)(F)$ will generally not be finite. Other restrictions on the field also become apparent in generalising directly his methods. However, we are able to prove modularity of all semistable elliptic curves for the quadratic fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{17})$. That we can prove such results for the first of these fields is a piece of good fortune; the first author and Paul Meekin [10] have shown that a generalisation of Fermat's Last Theorem to $\mathbb{Q}(\sqrt{2})$ would follow from such a result. They also show that $\mathbb{Q}(\sqrt{2})$ is the only real quadratic field for which an implication of the form 'modularity implies Fermat' can be derived directly.

1.3. Notation

The absolute Galois group of a field F is written either as $\mathrm{Gal}(\overline{F}/F)$ or G_F. The separable algebraic closure of F is denoted by $\overline{F}$. Given an extension of fields $K \supset F$ and some representation $\rho : G_F \to \mathrm{GL}_2(*)$, we denote the restriction of ρ to the absolute Galois group of K by either $\rho|_{G_K}$ or, simply, by $\rho|_K$. If F is a number field, we denote the decomposition and inertia groups at a place v by D_v and I_v, respectively.

Throughout, ℓ is an odd prime. We denote the ℓ-adic cyclotomic character by ϵ_ℓ, and its reduction, the mod ℓ cyclotomic character, by $\bar{\epsilon}_\ell$. We denote by ω_2 the second fundamental character of $\mathbb{Q}_\ell$. Recall that $\omega_2 : I_\ell \to \mathbb{F}_{\ell^2}^\times$ is the unique character of the inertia subgroup I_ℓ given by the rule

$$\tau \to \frac{\tau(\ell^{1/(\ell^2-1)})}{\ell^{1/(\ell^2-1)}}.$$

The notation suppresses the dependence on ℓ, and it would be more appropriate to write $\omega_{2,\ell}$ instead; the context should be generally clear. One should recall that the notion of fundamental character is not functorial; the restriction of ω_2 to a local inertia group I_v is not the second fundamental character of F_v when the ramification degree of $F_v/\mathbb{Q}_\ell$ is greater than 1. We remark that there is an injection $\mathbb{F}_{\ell^2}^\times \hookrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)$; it follows that we can view ω_2 as a 2-dimensional representation Ω_2 over $\mathbb{F}_\ell$. This representation is irreducible over $\mathbb{F}_\ell$, but if we extend scalars to a coefficient field of even degree over $\mathbb{F}_\ell$, then Ω_2 becomes reducible, isomorphic over this quadratic extension to the direct sum of the characters ω_2 and ω_2^ℓ.

For an elliptic curve E over a field F, we denote by $E[n]$ the kernel of the multiplication by n map $E \xrightarrow{\times n} E$. If n is coprime to the characteristic of F,

$$\bar{\rho}_{E,n} : G_F \to \mathrm{Aut}\, E[n](\overline{F}) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

is the mod n representation. If ℓ is a prime different from the characteristic of F, we set

$$\rho_{E,\ell} : G_F \to \varprojlim \mathrm{Aut}\, E\big[\ell^n\big](\overline{F}) \cong \mathrm{GL}_2(\mathbb{Z}_\ell).$$

1.4. Summary of results

Let F be a totally real number field, and let ℓ be an odd prime. Suppose that for all $v \mid \ell$, the ramification index of $F_v/\mathbb{Q}_\ell$ is at most $\ell - 1$. Consider continuous, irreducible representations

$$\rho : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$$

with determinant the ℓ-adic cyclotomic character, and having the same absolutely irreducible residual representation $\bar{\rho}$. We assume that all Artinian quotients of ρ are finite flat at primes above ℓ, and we assume further that

$$\bar{\rho}|_{I_v} \sim \Omega_2|_{I_v} \quad \text{for every } v \mid \ell,$$

where Ω_2 is the second fundamental character of $\mathbb{Q}_\ell$, as in the notation section above, regarded as a 2-dimensional representation—as our coefficient field has residue field containing $\mathbb{F}_{\ell^2}$, the representation splits as $\omega_2 \oplus \omega_2^\ell$. This is the form of the local Galois representations associated to an elliptic curve with good supersingular reduction at v, where F_v is *unramified* over $\mathbb{Q}_\ell$. (If F_v is not unramified, however, the local Galois representation may take a different form; see Section 7 for an example.) The main applications of the results of the paper will be to such elliptic curves.

Our main result is then:

Theorem 1.1. *Let ρ be a representation of the above form. Suppose that $\bar\rho$ has a modular lift which is finite flat at primes above ℓ. Assume that*

$$\bar\rho|_{\mathrm{Gal}(\overline{F}/F(\zeta_\ell))}$$

is absolutely irreducible, and furthermore assume that

- *if $\ell = 5$ and $\operatorname{Proj}\bar\rho|_{\mathrm{Gal}(\overline{F}/F(\zeta_\ell))} \cong A_5$, then $[F(\zeta_\ell) : F] = 4$.*

Then ρ is also modular.

We give two applications of the above. The first relates to Serre's conjecture for mod 7 representations; we extend the result in [13], and show that:

Theorem 1.2. *Let $\bar\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_7)$ be an absolutely irreducible, continuous, odd representation. Suppose that the projective image of inertia at 3 has odd order and that the determinant of $\bar\rho$ restricted to the inertia group at 7 has even order. Then $\bar\rho$ is modular.*

This theorem has been used by Dieulefait and the second author [7] to give a new criterion for the modularity of rigid Calabi–Yau threefolds. Of course, it is largely subsumed within recent work of Khare and Wintenberger; however, we need no hypothesis at 2.[1]

Our second application relates to the modularity of elliptic curves over totally real fields. For general totally real fields, we prove modularity subject to quite a few restrictions. For the full result, see Section 9. A particularly neat corollary is the following.

Theorem 1.3. *Every semistable elliptic curve over $\mathbb{Q}(\sqrt{2})$ is modular.*

This has implications for the study of certain Diophantine equations, and notably the Fermat equation, over $\mathbb{Q}(\sqrt{2})$ (see [10]).

2. Local deformations and cohomology groups

Our objective in this section is to give good upper bounds on the size of certain local cohomology groups. We do this for representations of a certain shape (which can be achieved after an unramified base change). But before that, we begin by setting out our notation. Apart from ℓ being the residue characteristic and λ being a uniformizer (instead of p and π), our choice of notation is meant to be consistent with [2].

[1] Note added in proof: Khare and Wintenberger also no longer need a hypothesis at 2, so our result is now contained within their very much stronger result.

Throughout this section, we fix a finite field k of characteristic $\ell \geqslant 3$. We denote by A its Witt ring $W(k)$ and by K the fraction field of A. We fix a finite totally ramified Galois extension K' of K and denote by A' its ring of integers. We assume that the absolute ramification index $e = [K' : K]$ is less than or equal to $\ell - 1$. The reason for this is that there is then a good notion of Honda system associated to group schemes. We also fix throughout a uniformizer λ such that $\lambda^e = \epsilon\ell$ with $\epsilon \in A^\times$ (as K' is a tamely ramified extension). Write $\mathfrak{m}$ for the maximal ideal of A'.

We denote by σ the Frobenius automorphism of A, and by D_k the Dieudonné ring. Recall that D_k is the A-algebra generated by F and V subject to the usual relations $FV = \ell = VF$, $F\alpha = \sigma(\alpha)F$, $V\alpha = \sigma^{-1}(\alpha)V$ (for $\alpha \in A$). If there is no cause for confusion, we will abbreviate D_k to simply D.

Various tensor products appear in this section. The unspecified $- \otimes -$ will simply mean $- \otimes_{\mathbb{Z}_\ell} -$.

We shall be working with finite Honda systems over A'. For the various properties, see Conrad [2,3].

We now fix a second finite field $\mathbb{F}$ of characteristic ℓ and a continuous representation

$$\bar{\rho} : G_{K'} \to \mathrm{GL}_2(\mathbb{F}).$$

We will shortly impose a further restriction, but for the moment we assume that the representation is finite—that is, there is a finite flat group scheme over A' whose associated Galois module (from the generic fibre) gives precisely our representation $\bar{\rho}$. This allows us to introduce certain cohomology groups $H^1_f(G_{K'}, \mathrm{ad}\,\bar{\rho})$ and $H^1_f(G_{K'}, \mathrm{ad}^0\,\bar{\rho})$. We recall the definitions (see [5] for details): elements of $H^1_f(G_{K'}, \mathrm{ad}\,\bar{\rho})$ are the deformations of $\bar{\rho}$ to $\mathbb{F}[\epsilon]/(\epsilon^2)$ which are finite, and $H^1_f(G_{K'}, \mathrm{ad}^0\,\bar{\rho})$ is the subspace of $H^1_f(G_{K'}, \mathrm{ad}\,\bar{\rho})$ with determinant (of the deformation) equal to the determinant of $\bar{\rho}$.

We now impose a restriction on the shape of $\bar{\rho}$:

Assumption 2.1. $\bar{\rho}$ is equivalent to $\Omega_2|_{G_{K'}}$.

Let M be the $D_k \otimes \mathbb{F}$-module

$$(k \otimes \mathbb{F})\mathbf{e}_1 \oplus (k \otimes \mathbb{F})\mathbf{e}_2$$

with F and V actions given by

$$F(\mathbf{e}_1) = 0, \qquad F(\mathbf{e}_2) = \mathbf{e}_1;$$
$$V(\mathbf{e}_1) = 0, \qquad V(\mathbf{e}_2) = -\mathbf{e}_1.$$

(To be more precise, these give the action on our basis elements which one then extends Frobenius semi-linearly.) Let L be the subspace $(k \otimes \mathbb{F})\mathbf{e}_2$. Then (L, M) is the finite Honda system over A associated to $\Omega_2|_{G_K}$. This follows, after base change (see [2, Section 4]), from the description of the Honda system over $\mathbb{Z}_\ell$ associated to Ω_2. (This is presumably well known.) We reserve (L, M) for this particular Honda system throughout.

By the results of [2], calculating $H^1_f(G_{K'}, \mathrm{ad}\,\bar{\rho})$ is the same as calculating extensions of (L, M) by itself in the category of finite Honda systems over A'. As a first step to this calculation, we investigate the extensions of M by itself in the category of $D_k \otimes \mathbb{F}$ modules.

We begin with a technical lemma which enables us to reduce calculations to one of linear algebra.

Lemma 2.2. *Let R be a ring with finite cardinality. If*

$$0 \to R^m \to U \to R^n \to 0$$

is an exact sequence of R-modules, then U is free and isomorphic to R^{n+m}.

Proof. The exact sequence implies that U can be generated by $n+m$ elements. Hence there is a surjective R-module homomorphism $R^{n+m} \twoheadrightarrow U$. As R has finite cardinality, we get $R^{n+m} \cong U$. □

Proposition 2.3. *The group of extensions $\mathrm{Ext}^1_{D_k \otimes \mathbb{F}}(M, M)$ is (non-canonically) isomorphic as an $\mathbb{F}$-vector space to*

- *$(k \otimes \mathbb{F}) \oplus (\mathbb{F}_\ell \otimes \mathbb{F})$ if the degree $[k : \mathbb{F}_\ell]$ is odd, and*
- *$(k \otimes \mathbb{F}) \oplus (\mathbb{F}_{\ell^2} \otimes \mathbb{F})$ if the degree $[k : \mathbb{F}_\ell]$ is even.*

Proof. By Lemma 2.2, we can certainly take any extension class, as an $A \otimes \mathbb{F}$ module, to be

$$M \oplus M = \big((k \otimes \mathbb{F})(\mathbf{e}_1, 0) \oplus (k \otimes \mathbb{F})(\mathbf{e}_2, 0)\big) \oplus \big((k \otimes \mathbb{F})(0, \mathbf{e}_1) \oplus (k \otimes \mathbb{F})(0, \mathbf{e}_2)\big).$$

We need to specify the actions of F and V. In order to do this, we write down matrices using the above choice of basis and compute (remembering to keep track of Frobenius semi-linearity).

To begin with, we can write

$$F = \begin{pmatrix} 0 & 1 & f_1 & f_2 \\ 0 & 0 & f_3 & f_4 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad V = \begin{pmatrix} 0 & -1 & v_1 & v_2 \\ 0 & 0 & v_3 & v_4 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Since $FV = VF = \ell = 0$, we must have the following equalities:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \sigma(v_1) & \sigma(v_2) \\ \sigma(v_3) & \sigma(v_4) \end{pmatrix} + \begin{pmatrix} f_1 & f_2 \\ f_3 & f_4 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix} = 0,$$
$$\begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \sigma^{-1}(f_1) & \sigma^{-1}(f_2) \\ \sigma^{-1}(f_3) & \sigma^{-1}(f_4) \end{pmatrix} + \begin{pmatrix} v_1 & v_2 \\ v_3 & v_4 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = 0.$$

Multiplying out, we find that

$$f_3 = v_3 = 0 \quad \text{and} \quad f_1 = \sigma(v_4), \qquad f_4 = \sigma(v_1).$$

We now reduce the number of variables further by applying appropriate $k \otimes \mathbb{F}$-linear automorphisms of $M \oplus M$. Let A be the endomorphism

$$\begin{pmatrix} 1 & 0 & a_1 & a_2 \\ 0 & 1 & a_3 & a_4 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

To calculate AFA^{-1}, we need to calculate

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} \sigma(a_1) & \sigma(a_2) \\ \sigma(a_3) & \sigma(a_4) \end{pmatrix} + \begin{pmatrix} f_1 & f_2 \\ 0 & f_4 \end{pmatrix}$$

which is

$$\begin{pmatrix} -\sigma(a_3) & a_1 - \sigma(a_4) \\ 0 & a_3 \end{pmatrix} + \begin{pmatrix} f_1 & f_2 \\ 0 & f_4 \end{pmatrix}.$$

We can thus assume that $f_4 = f_2 = 0$, which implies that $v_1 = 0$. Under this assumption, our choice of A is then restricted to

$$a_3 = 0 \quad \text{and} \quad a_1 = \sigma(a_4).$$

To calculate AVA^{-1}, we need to compute

$$\begin{pmatrix} a_1 & a_2 \\ 0 & a_4 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} \sigma^{-1}(a_1) & \sigma^{-1}(a_2) \\ 0 & \sigma^{-1}(a_4) \end{pmatrix} + \begin{pmatrix} 0 & v_2 \\ 0 & v_4 \end{pmatrix}$$

which is

$$\begin{pmatrix} 0 & -a_1 + \sigma^{-1}(a_4) \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & v_2 \\ 0 & v_4 \end{pmatrix}.$$

Since we have $a_1 = \sigma(a_4)$, our choice $v_2 \in k \otimes \mathbb{F}$ can further be restricted to a choice of representative of an element of

$$\frac{k \otimes \mathbb{F}}{(\sigma^2 - 1)(k \otimes \mathbb{F})},$$

while v_4 can be chosen to be an arbitrary element of $k \otimes \mathbb{F}$. The proposition then follows. □

Theorem 2.4. *The dimension of $H^1_f(G_{K'}, \operatorname{ad}\bar{\rho})$ as an $\mathbb{F}$-vector space is at most*

- *$[K' : \mathbb{Q}_\ell] + 2$ if $[k : \mathbb{F}_\ell]$ is even, and*
- *$[K' : \mathbb{Q}_\ell] + 1$ if $[k : \mathbb{F}_\ell]$ is odd.*

Proof. As in [3], we have an $\mathbb{F}$-linear map of vector spaces

$$t : H^1_f(G_{K'}, \operatorname{ad}\bar{\rho}) \to \operatorname{Ext}^1(M, M).$$

In words, the map t is just 'take Dieudonné module of the special fibre of the associated finite flat group scheme.' We already have a bound for the Ext-group, thanks to Proposition 2.3. We now start analysing the kernel of the above linear map.

We begin by describing the structure of the A'-module $M_{A'}$. We recall the definition (due to Fontaine), and refer to [2] for the explicit description we need (see [2, Definition 2.1]). As already set out in the beginning of this section, we have a fixed uniformizer λ of A' satisfying $\lambda^e = \epsilon\ell$ with $\epsilon \in A^\times$.

We have the standard identification of $M^{(1)} = (A, \sigma) \otimes_A M$ with M as an abelian group and twisted A-action. The Dieudonné module structure then gives us two A-linear maps

$$F_0 : M^{(1)} \to M \quad \text{and} \quad V_0 : M \to M^{(1)}.$$

(As in [2], we shall not abbreviate these to F and V.) There are A'-linear maps

$$F^M : A' \otimes_A M^{(1)} \to A' \otimes_A M \quad \text{and} \quad V^M : \mathfrak{m} \otimes_A M \to \ell^{-1}\mathfrak{m} \otimes_A M^{(1)}$$

obtained simply by tensoring with the identity map on A' and the map $x \to \ell^{-1}x$, respectively.

The A'-module $M_{A'}$ is then the quotient of

$$(A' \otimes_A M) \oplus \left(\ell^{-1}\mathfrak{m} \otimes_A M^{(1)}\right)$$

by the submodule

$$\left\{\left(\phi_0^M(u) - F^M(w), \phi_1^M(w) - V^M(u)\right) \,\middle|\, u \in \mathfrak{m} \otimes_A M,\ w \in A' \otimes_A M^{(1)}\right\}$$

where ϕ_0^M, ϕ_1^M are the maps

$$\phi_0^M : \mathfrak{m} \otimes_A M \to A' \otimes_A M \quad \text{and} \quad \phi_1^M : A' \otimes_A M^{(1)} \to \ell^{-1}\mathfrak{m} \otimes_A M^{(1)}$$

induced by the inclusions $\mathfrak{m} \hookrightarrow A'$ and $A' \hookrightarrow \ell^{-1}\mathfrak{m}$.

A basis of $A' \otimes_A M$ as a free $k \otimes \mathbb{F}$-module is given by

$$\lambda^i \otimes \mathbf{e}_j, \quad i = 0, \ldots, e-1,\ j = 1, 2.$$

For $\ell^{-1}\mathfrak{m} \otimes_A M^{(1)}$, we have the $k \otimes \mathbb{F}$ basis

$$\lambda^{-i} \otimes \mathbf{e}_j, \quad i = 0, 1, \ldots, e-1,\ j = 1, 2.$$

Note that for $i \geqslant 1$, the elements $(\lambda^i \otimes \mathbf{e}_1, 0)$ are trivial in $M_{A'}$. Indeed, we have

$$\left(\lambda^i \otimes \mathbf{e}_1, 0\right) = \left(\phi_0^M\left(\lambda^i \otimes \mathbf{e}_1\right) - F^M(0), 0 - V^M\left(\lambda^i \otimes \mathbf{e}_1\right)\right).$$

Furthermore, for $i \geqslant 1$, we have

$$\begin{aligned}\left(0, \lambda^{-i} \otimes \mathbf{e}_1\right) &= \left(0, 0 - V^M\left(\lambda^{e-i} \otimes \mathbf{e}_2\right)\right)\\ &= \left(-\lambda^{e-i} \otimes \mathbf{e}_2, 0\right).\end{aligned}$$

Note also that

$$\begin{aligned}&\left(0, 1 \otimes \mathbf{e}_1\right) = \left(\phi_0^M(0) - F^M(1 \otimes \mathbf{e}_1), \phi_1^M(1 \otimes \mathbf{e}_1) - V^M(0)\right), \quad \text{and}\\ &(0, 1 \otimes \mathbf{e}_2) = (1 \otimes \mathbf{e}_1, 0) + \left(\phi_0^M(0) - F^M(1 \otimes \mathbf{e}_2), \phi_1^M(1 \otimes \mathbf{e}_2) - V^M(0)\right).\end{aligned}$$

Thus any element in $M_{A'}$ can be expressed as an $k \otimes \mathbb{F}$-linear combination of

$$(1 \otimes \mathbf{e}_1, 0), \qquad \bigl(\lambda^i \otimes \mathbf{e}_2, 0\bigr) \quad \text{and} \quad \bigl(0, \lambda^{-m} \otimes \mathbf{e}_2\bigr)$$

with $i = 0, 1, \dots, e-1$ and $m = 1, \dots, e-1$. Since the A'-length of $M_{A'}$ is the same as the A-length of M times e [2, Lemma 2.2], we deduce that the set of generators above is in fact a basis.

Obviously, the A'-submodule of $M_{A'}$ obtained by taking the A'-span of L is precisely $A' \otimes_A A \otimes \mathbb{F}(\mathbf{e}_2, 0)$. Now let (L', M') be the finite Honda system for an element in the kernel of t. Since $M' = M \oplus M$ as a $D_k \otimes \mathbb{F}$-module, we can write $M'_{A'} = M_{A'} \oplus M_{A'}$. We must therefore have, by length considerations,

$$L' = (A' \otimes_A A \otimes \mathbb{F})\bigl((\mathbf{e}_2, 0), 0\bigr) + (A' \otimes_A A \otimes \mathbb{F})\bigl(x, (\mathbf{e}_2, 0)\bigr)$$

for some $x \in M_{A'}$. From our description of a basis of $M_{A'}$, it follows that we can take

$$x = a(1 \otimes \mathbf{e}_1, 0) + y$$

with $a \in k \otimes \mathbb{F}$ and y an element in the $A \otimes \mathbb{F}$-span of $(0, \lambda^{-m} \otimes \mathbf{e}_2)$, $m = 1, \dots, e-1$. By applying a $D_k \otimes \mathbb{F}$-linear automorphism of $M \oplus M$ of the type

$$\begin{pmatrix} 1 & 0 & 0 & * \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

we can assume that $a = 0$. Hence the kernel has dimension, as an $\mathbb{F}$-vector space, at most $(e-1)[k : \mathbb{F}_\ell]$; and this proves the theorem. □

Corollary 2.5. *The dimension of $H^1_f(G_{K'}, \mathrm{ad}^0 \bar{\rho})$ as an $\mathbb{F}$-vector space is at most*

- $[K' : \mathbb{Q}_\ell] + 1$ *if* $[k : \mathbb{F}_\ell]$ *is even, and*
- $[K' : \mathbb{Q}_\ell]$ *if* $[k : \mathbb{F}_\ell]$ *is odd.*

3. The deformation problem

We now set up the deformation problem we want to study. We begin by fixing a totally real extension F of even degree (over $\mathbb{Q}$), an odd prime ℓ, a finite field k of characteristic ℓ, and a continuous homomorphism

$$\bar{\rho} : G_F \to \mathrm{GL}_2(k)$$

which is absolutely irreducible and odd. We assume that the ramification degree of F at all primes over ℓ is less than or equal to $\ell - 1$. Further, we suppose that $\bar{\rho}$ has the following properties:

- The determinant of $\bar{\rho}$ is the mod ℓ cyclotomic character.
- $\bar{\rho}$ restricted to the absolute Galois group of $F(\zeta_\ell)$ is absolutely irreducible.

- If $\ell = 5$ and $\operatorname{Proj} \bar{\rho}|_{\mathrm{Gal}(\bar{F}/F(\zeta_\ell))}$, then $[F(\zeta_\ell) : F] = 4$.
- Let x be a prime of F above ℓ and let I_x the inertia group of F_x. Then

$$\bar{\rho}|_{I_x} \sim \Omega_2|_{I_x}$$

where Ω_2 is the second fundamental character.

We assume that the characteristic polynomial of $\bar{\rho}(\sigma)$ is split over k for any $\sigma \in G_F$. We fix a finite extension K of $\mathbb{Q}_\ell$ with ring of integers $\mathcal{O}$, maximal ideal (λ) and residue field k.

Let $\mathcal{C}_\mathcal{O}$ be the category of complete, local, Noetherian $\mathcal{O}$-algebras with residue field k. Given $(A, \mathfrak{m}_A) \in \mathcal{C}_\mathcal{O}$, we call a continuous homomorphism

$$\rho_A : G_F \to \mathrm{GL}_2(A)$$

a *finite flat deformation* of $\bar{\rho}$ if

- ρ_A is odd and unramified outside finitely many primes,
- $\rho_A \pmod{\mathfrak{m}_A} = \bar{\rho}$,
- ρ_A is finite flat at primes $v \mid \ell$ (i.e., the restriction of ρ_A to G_{F_v}, for $v \mid \ell$, has the property that for all $n \geqslant 1$, the F_v-group scheme associated to the G_{F_v}-module $\rho_A \bmod \mathfrak{m}_A^n$ is the generic fibre of a finite flat group scheme over $\mathcal{O}_{F,v}$), and
- ρ_A has determinant the ℓ-adic cyclotomic character.

Two such deformations are said to be strictly equivalent if one can be conjugated to the other by a matrix which reduces to the identity modulo the maximal ideal $\mathfrak{m}_A$.

Now let Σ be a finite set of (finite) primes of F not containing any places over ℓ (and it could be empty). We say a finite flat deformation is of type Σ if the representation is unramified outside primes in Σ and outside the set of primes where $\bar{\rho}$ is ramified. There is then a universal finite flat deformation of $\bar{\rho}$ of type Σ which we shall denote by (R_Σ, ρ_Σ).

Given a finite flat deformation $\rho : G_F \to \mathrm{GL}_2(\mathcal{O}/\lambda^n)$ of type Σ, one defines the Galois cohomology group $H^1_\Sigma(G_F, \mathrm{ad}^0 \rho)$ to be the deformations of ρ to $(\mathcal{O}/\lambda^n)[\epsilon]/\epsilon^2$ which are of type Σ. Recall that $\mathrm{ad}^0 \rho$ can be identified with the group of 2×2 trace zero matrices over $\mathcal{O}/\lambda^n$ with G_F action via conjugation (by ρ). The cohomology group $H^1_\Sigma(G_F, \mathrm{ad}^0 \rho)$ is then precisely $H^1_{\mathcal{L}_\Sigma}(G_F, \mathrm{ad}^0 \rho)$ where the local conditions $\mathcal{L}_\Sigma = \{L_x\}$ are given by

- $L_x = H^1(G_{F_x}/I_x, \mathrm{ad}^0 \rho^{I_x})$ if $x \nmid \ell$, $x \notin \Sigma$ and $\bar{\rho}$ is unramified at x,
- $L_x = H^1(G_{F_x}, \mathrm{ad}^0 \rho)$ if $x \nmid \ell$, and either $x \in \Sigma$ or $\bar{\rho}$ is ramified at x,
- $L_x = H^1_f(G_{F_x}, \mathrm{ad}^0 \rho)$ if $x \mid \ell$.

The universal deformation ring R_Σ can be topologically generated as an $\mathcal{O}$-algebra by $\dim_k H^1_\Sigma(G_F, \mathrm{ad}^0 \bar{\rho})$ elements. If $\pi : R_\Sigma \twoheadrightarrow \mathcal{O}$ is an $\mathcal{O}$-algebra homomorphism with corresponding representation ρ, we have a canonical isomorphism

$$\mathrm{Hom}\big(\ker \pi/(\ker \pi)^2, K/\mathcal{O}\big) \cong H^1_\Sigma\big(G_F, \mathrm{ad}^0 \rho \otimes K/\mathcal{O}\big).$$

The pairing $\mathrm{ad}^0\,\bar\rho \times \mathrm{ad}^0\,\bar\rho \to k$ obtained by taking the trace is perfect. Using this pairing, one defines $H^1_{\Sigma^\perp}(G_F, \mathrm{ad}^0\,\bar\rho(1))$ to be given by local conditions $\{L_x^\perp\}$ where $L_x^\perp$ is the orthogonal complement to L_x with respect to the perfect pairing

$$H^1\bigl(G_{F_x}, \mathrm{ad}^0\,\bar\rho\bigr) \times H^1\bigl(G_{F_x}, \mathrm{ad}^0\,\bar\rho(1)\bigr) \to H^2\bigl(G_{F_x}, k(1)\bigr) \simeq k.$$

From now onwards, we assume the following:

Assumption 3.1. For each prime x of F dividing ℓ, the Honda system associated to $\bar\rho|_{F_x}$ has the particular form specified in Assumption 2.1.

Now we make some calculations of these cohomology groups, using similar arguments to those of Wiles.

Theorem 3.2. *As an $\mathcal{O}$-algebra,*

$$\dim_k H^1_{\Sigma^\perp}\bigl(G_F, \mathrm{ad}^0\,\bar\rho(1)\bigr) + \sum_{x\in\Sigma} \dim_k H^0\bigl(G_{F_x}, \mathrm{ad}^0\,\bar\rho(1)\bigr)$$

elements are sufficient to generate the universal deformation ring R_Σ topologically.

Proof. This is almost exactly the same as the proof of Corollary 2.43 in [5]. Using Theorem 2.19 of [5] (a full proof is given in [14, p. 440]), one finds that $\dim_k H^1_\Sigma(G_F, \mathrm{ad}^0\,\bar\rho)$ is the sum of terms:

- $\dim_k H^1_{\Sigma^\perp}(G_F, \mathrm{ad}^0\,\bar\rho(1))$.
- $\sum_{x|\ell} \dim_k H^1_f(G_{F_x}) - \sum_{x|\ell} \dim_k H^0(G_{F_x}) - \sum_{x|\infty} \dim_k H^0_\Sigma(G_{F_x})$, where $H^*_*(G_{F_x})$ means the cohomology group $H^*_*(G_{F_x}, \mathrm{ad}^0\,\bar\rho)$. This term is less than or equal to 0 by Corollary 2.5.
- $\dim_k H^1(G_{F_x}, \mathrm{ad}^0\,\bar\rho) - \dim_k H^0(G_{F_x}, \mathrm{ad}^0\,\bar\rho)$, which equals $\dim_k H^0(G_{F_x}, \mathrm{ad}^0\,\bar\rho(1))$, for each $x \in \Sigma$. □

Theorem 2.49 of [5] still holds in our present setting; the proof, with trivial modifications, remains valid. The result being of significant importance, we give a brief sketch of the proof.

Theorem 3.3. *Let* $r = \dim_k H^1_\emptyset(G_F, \mathrm{ad}^0\,\bar\rho(1))$. *For every positive integer n, we can find a finite set primes Σ_n such that the following hold*:

- *Every prime in Σ_n has norm congruent to* 1 *modulo ℓ^n.*
- *The sets Σ_n all have size equal to r.*
- *If $x \in \Sigma_n$, then $\bar\rho$ is unramified at x and the Frobenius* (*at x*) *has distinct eigenvalues.*
- *The universal deformation ring R_{Σ_n} can be topologically generated as an $\mathcal{O}$-algebra by r elements.*

Proof. As in the proof of Theorem 2.49 of [5], one reduces the result to showing that for $\psi \in H^1_\emptyset(G_F, \mathrm{ad}^0\,\bar\rho(1)) - \{0\}$, we can find $\sigma \in G_F$ such that

- σ acts trivially on $F(\zeta_{\ell^n})$,
- $\operatorname{ad}^0 \bar{\rho}(\sigma)$ has an eigenvalue not equal to 1, and
- $\psi(\sigma) \notin (\sigma - 1)\operatorname{ad}^0 \bar{\rho}(1)$.

(We remark that Theorem 3.2 is crucial in getting the right number of generators from this reduction.)

Let F_n be the minimal extension of $F(\zeta_{\ell^n})$ on which $\operatorname{ad}^0 \bar{\rho}$ acts trivially. The degree of the extension F_1/F_0 is at most $\ell - 1$; the degree $[F_n : F_1]$ is of ℓ-power order. It follows that

$$H^1\big(\operatorname{Gal}(F_n/F_0), \operatorname{ad}^0 \bar{\rho}(1)\big)^{G_F} \cong \operatorname{Hom}\big(\operatorname{Gal}(F_n/F_1), \operatorname{ad}^0 \bar{\rho}(1)^{G_F}\big)$$

is trivial (since $\bar{\rho}$ restricted to the absolute Galois group of $F(\zeta_\ell)$ is absolutely irreducible).

Now consider $H^1(\operatorname{Gal}(F_0/F), \operatorname{ad}^0 \bar{\rho}(1)^{G_{F_0}})$. If this is non-trivial, the order of $\operatorname{Gal}(F_0/F)$ must be divisible by ℓ and $\operatorname{Gal}(F_0/F)$ must have $\operatorname{Gal}(F(\zeta_\ell)/F)$ as a quotient. Note that $\operatorname{Gal}(F_0/F)$ is isomorphic to the projective image of $\bar{\rho}$, and so from the list in Theorem 2.47 of [5] we see that the case $\ell = 5$ and $\operatorname{Proj} \bar{\rho}|_{\operatorname{Gal}(\bar{F}/F(\zeta_\ell))}$ cannot occur. In the other cases the projective image of $\bar{\rho}$ is a semi-direct extension of $\operatorname{PSL}_2(\mathbb{F}_{\ell^r})$ by a group of order prime to ℓ, and so $H^1(\operatorname{Gal}(F_0/F), \operatorname{ad}^0 \bar{\rho}(1))$ again vanishes on applying Lemma 2.48 of [5].

A straightforward application of the inflation–restriction sequence then implies that the group $H^1(\operatorname{Gal}(F_n/F), \operatorname{ad}^0 \bar{\rho}(1))$ is trivial, and it follows that $\psi(G_{F_n})$ is non-trivial.

Now $\bar{\rho}$ restricted to $G_{F(\zeta_{\ell^n})}$ is still absolutely irreducible. Thus the order of $\operatorname{Gal}(F_n/F(\zeta_{\ell^n}))$ is not a power of ℓ. The group $\operatorname{Gal}(F_n/F(\zeta_{\ell^n}))$ also acts (non-trivially) on $\{0\} \neq \psi(G_{F_n}) \subset \operatorname{ad}^0 \bar{\rho}$. Therefore we can find a non-trivial element $g \in \operatorname{Gal}(F_n/F(\zeta_{\ell^n}))$ of order prime to ℓ and fixing a non-zero element of $\psi(G_{F_n})$. Let $\tilde{g} \in G_{F(\zeta_{\ell^n})}$ be a lift of g. As $\psi(G_{F_n}) \not\subset (g-1)\operatorname{ad}^0 \bar{\rho}(1)$, we can find $h \in G_{F_n}$ such that

$$\psi(h\tilde{g}) = \psi(h) + \psi(\tilde{g}) \notin (\tilde{g} - 1)\operatorname{ad}^0 \bar{\rho}(1).$$

Finally, take $\sigma = h\tilde{g}$. Then σ acts trivially on $F(\zeta_{\ell^n})$, and $(\sigma - 1)\operatorname{ad}^0 \bar{\rho}(1) = (\tilde{g} - 1)\operatorname{ad}^0 \bar{\rho}(1) \not\ni \psi(\sigma)$. Since the order of σ is prime to ℓ (and is not 1), it follows that $\operatorname{ad}^0 \bar{\rho}(\sigma)$ has an eigenvalue not equal to 1. □

4. Hecke algebras and ℓ-adic modular forms

We fix a totally real field F of even degree and an odd rational prime ℓ. We write D for the division algebra with centre F and ramified exactly at the set of infinite places of F. Write Z for the algebraic group defined by $Z(R) = (D \otimes_F R)^\times$ if R is an F-algebra. We also fix the following:

- A maximal order $\mathcal{O}_D$, and isomorphisms $\mathcal{O}_{D,x} \cong M_2(\mathcal{O}_{F,x})$ for all finite places x of F. These isomorphisms give us an identification of $\operatorname{GL}_2(\mathbb{A}_F^\infty)$ with $(D \otimes_{\mathbb{Q}} \mathbb{A}^\infty)^\times$.
- A uniformiser ϖ_x of $\mathcal{O}_{F,x}$ for each finite place x.

We write A for a topological $\mathbb{Z}_\ell$-algebra which is one of the following: a finite extension of $\mathbb{Q}_\ell$, the ring of integers in such an extension, or a quotient of such a ring of integers.

Definition 4.1. For a compact open subgroup $U \subset (D \otimes_{\mathbb{Q}} \mathbb{A}^{\infty})^{\times}$ and a topological ring A as above, we define $S_A(U)$ to be the space of continuous functions

$$f : D^{\times} \backslash \big(D \otimes_{\mathbb{Q}} \mathbb{A}^{\infty}\big)^{\times} / U.Z\big(\mathbb{A}_F^{\infty}\big) \to A.$$

We define S_A to be the direct limit of $S_A(U)$ as U varies over open compact subsets of $(D \otimes_{\mathbb{Q}} \mathbb{A}^{\infty})^{\times}$.

For a compact open U, the finite double coset decomposition

$$\big(D \otimes_{\mathbb{Q}} \mathbb{A}^{\infty}\big)^{\times} = \coprod D^{\times} t_i U.Z\big(\mathbb{A}_F^{\infty}\big)$$

shows that

$$\begin{aligned} S_A(U) &\to \bigoplus_i A \\ f &\to \big(f(t_i)\big)_i \end{aligned}$$

is an isomorphism. In particular, for any A-algebra B, we have

$$S_A(U) \otimes_A B \cong S_B(U).$$

We denote by $[t_i]$ the function in $S_A(U)$ which is 1 on $D^{\times} t_i U.Z(\mathbb{A}_F^{\infty})$ and 0 elsewhere.

Definition 4.2. For an ideal $\mathfrak{n}$ of $\mathcal{O}_F$ and quotients H_x of $(\mathcal{O}_{F,x}/\mathfrak{n}_x)^{\times}$, we set $H = \prod_x H_x$. We define $U_H(\mathfrak{n})$ to be the compact open subgroup $\prod_x U_H(\mathfrak{n})_x \subset (D \otimes_{\mathbb{Q}} \mathbb{A}^{\infty})^{\times}$ where

$$U_H(\mathfrak{n})_x = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_{F,x}) \cong \mathcal{O}_{D,x}^{\times} \;\middle|\; c \in \mathfrak{n}_x,\ ad^{-1} = 1 \text{ in } H_x \right\}.$$

Now let $\mathfrak{n}$ and H_x be as in the above definition. We recall the definitions of the various Hecke operators on $S_A(U_H(\mathfrak{n}))$:

- If x does not divide $\ell\mathfrak{n}$, we denote the Hecke operators

$$\left[U_H(\mathfrak{n}) \begin{pmatrix} \varpi_x & 0 \\ 0 & 1 \end{pmatrix} U_H(\mathfrak{n})\right] \quad \text{and} \quad \left[U_H(\mathfrak{n}) \begin{pmatrix} \varpi_x & 0 \\ 0 & \varpi_x \end{pmatrix} U_H(\mathfrak{n})\right]$$

  by T_x and S_x, respectively.
- If x divides $\mathfrak{n}$, we set

$$\langle h \rangle = \left[U_H(\mathfrak{n}) \begin{pmatrix} \tilde{h} & 0 \\ 0 & 1 \end{pmatrix} U_H(\mathfrak{n})\right]$$

  for $h \in H_x$ and $\tilde{h}$ a choice of lift of h to $\mathcal{O}_{F,x}^{\times}$.

- If x divides $\mathfrak{n}$, the Hecke operators

$$\left[U_H(\mathfrak{n})\begin{pmatrix}\varpi_x & 0\\ 0 & 1\end{pmatrix}U_H(\mathfrak{n})\right] \quad\text{and}\quad \left[U_H(\mathfrak{n})\begin{pmatrix}1 & 0\\ 0 & \varpi_x\end{pmatrix}U_H(\mathfrak{n})\right]$$

are denoted by $\mathbf{U}_{\varpi_x}$ and $\mathbf{V}_{\varpi_x}$, respectively. We also denote by S_x the Hecke operator

$$\left[U_H(\mathfrak{n})\begin{pmatrix}\varpi_x & 0\\ 0 & \varpi_x\end{pmatrix}U_H(\mathfrak{n})\right].$$

Definition 4.3. Let $\mathfrak{n}$, H_x and A be as in the preceding paragraphs. We define the *Hecke algebra* $\mathbb{T}_A(U_H(\mathfrak{n}))$ to be the A-subalgebra of $\mathrm{End}_A(S_A(U_H(\mathfrak{n})))$ generated by T_x (for x not dividing $\ell\mathfrak{n}$) and $\mathbf{U}_{\varpi_x}$ (for $x \mid \mathfrak{n}$ but not dividing ℓ).

A maximal ideal $\mathfrak{m}$ of $\mathbb{T}_A(U_H(\mathfrak{n}))$ is said to be *Eisenstein* if it contains $T_x - 2$ and $S_x - 1$ for all but finitely many primes with $\mathbf{N}x \pmod{\ell} = 1$.

The Hecke algebra $\mathbb{T}_A(U_H(\mathfrak{n}))$ is always commutative. Also, $\mathbb{T}_{\mathbb{Z}_\ell}(U_H(\mathfrak{n}))$ is semi-local and ℓ-adically complete, and we have the identification

$$\mathbb{T}_{\mathbb{Z}_\ell}\big(U_H(\mathfrak{n})\big) \cong \prod \mathbb{T}_{\mathbb{Z}_\ell}\big(U_H(\mathfrak{n})\big)_{\mathfrak{m}}$$

where the product is over all maximal ideals $\mathfrak{m}$.

If either ℓ is invertible in A, or if $\mathbb{Q}(\zeta + \zeta^{-1}) \not\subset F$ where ζ is a primitive ℓth root of unity, we have a perfect pairing on $S_A(U_H(\mathfrak{n}))$ defined by

$$(f_1, f_2)_{U_H(\mathfrak{n})} = \sum_i f_1(t_i) f_2(t_i)\left(\#\frac{U_H(\mathfrak{n}).Z(\mathbb{A}_F^\infty) \cap t_i^{-1} D^\times t_i}{F^\times}\right)^{-1}$$

where

$$\big(D \otimes_{\mathbb{Q}} \mathbb{A}^\infty\big)^\times = \coprod D^\times t_i U_H(\mathfrak{n}).Z\big(\mathbb{A}_F^\infty\big).$$

We call this the *standard pairing*. The Hecke operators are not necessarily self-adjoint with respect to this pairing; the general behaviour of operators is given by

$$\big(\big[U_{H'}(\mathfrak{n}')gU_H(\mathfrak{n})\big]f_1, f_2\big)_{U_{H'}(\mathfrak{n}')} = \big(f_1, \big[U_H(\mathfrak{n})g^{-1}U_{H'}(\mathfrak{n}')\big]f_2\big)_{U_H(\mathfrak{n})}.$$

Now fix a finite set of primes Σ, none lying above ℓ, and let $\mathfrak{n}_\Sigma = \prod_{x\in\Sigma} x^2$. Let K be a finite extension of $\mathbb{Q}_\ell$ which contains all embeddings $F \hookrightarrow \overline{\mathbb{Q}}_\ell$, and let $\mathcal{O}$ be its ring of integers. We fix a decomposition

$$\big(D \otimes_{\mathbb{Q}} \mathbb{A}^\infty\big)^\times = \coprod D^\times g_i U_1(\mathfrak{n}_\Sigma).Z\big(\mathbb{A}_F^\infty\big) \amalg \coprod D^\times h_i U_1(\mathfrak{n}_\Sigma).Z\big(\mathbb{A}_F^\infty\big)$$

where the g_i's and h_i's are such that

$$\ell \not| \#\frac{U_1(\mathfrak{n}_\Sigma).Z(\mathbb{A}_F^\infty)\cap g_i^{-1}D^\times g_i}{F^\times} \quad\text{and}\quad \ell \,\Big|\, \#\frac{U_1(\mathfrak{n}_\Sigma).Z(\mathbb{A}_F^\infty)\cap h_i^{-1}D^\times h_i}{F^\times}.$$

We denote by $S_{\mathcal{O}}(U_1(\mathfrak{n}_\Sigma))^*$ the $\mathcal{O}$-submodule of $S_{\mathcal{O}}(U_1(\mathfrak{n}_\Sigma))$ generated by the $[g_i]$ and $\ell[h_i]$.

Lemma 4.4. *Keep the notation of the preceding paragraph, and suppose that the ramification index at all primes over ℓ of F is at most $\ell - 1$. Then ℓ exactly divides the order of $(U_1(\mathfrak{n}_\Sigma).Z(\mathbb{A}_F^\infty)\cap h_i^{-1}D^\times h_i)/F^\times$.*

Proof. One easily reduces the statement to showing that finite subgroups of $D^\times$ having ℓ-power order must have order exactly 1 or ℓ (use the two exact sequences in the proof of Lemma 1.1 of [22]). Further, there can be a non-trivial finite subgroup of ℓ-power order if and only if $\zeta+\zeta^{-1}$ is in F. Since any group of order ℓ^2 is abelian, the only possible non-trivial finite subgroup has to have order exactly ℓ. □

Lemma 4.5. *With the notation as above, let $f \in S_{\mathcal{O}}(U_1(\mathfrak{n}_\Sigma))$. Then $T_x(f) \in S_{\mathcal{O}}(U_1(\mathfrak{n}_\Sigma))^*$ for any prime $x \notin \Sigma$ with $\mathbf{N}x \equiv -1 \pmod{\ell}$.*

Proof. Let $U^{(0)}$ be the subgroup of $U_1(\mathfrak{n}_\Sigma)$ consisting of elements whose xth component is congruent to $\left(\begin{smallmatrix} * & 0\\ * & *\end{smallmatrix}\right) \pmod{\varpi_x}$. Let $\zeta \in h^{-1}D^\times h \cap U_1(\mathfrak{n}_\Sigma).Z(\mathbb{A}_F^\infty)$ have order exactly ℓ in the quotient $(h^{-1}D^\times h\cap U_1(\mathfrak{n}_\Sigma).Z(\mathbb{A}_F^\infty))/F^\times$. We need to compute $T_x(f)(h)$ and check that it is a multiple of ℓ. Starting with a double coset decomposition given by $\coprod_{i=0}^{\ell-1}\zeta^i * U^{(0)}$ and using the fact that $\zeta \notin U^{(0)}$, we get a disjoint decomposition

$$U_1(\mathfrak{n}_\Sigma) = \coprod_{i=1}^{\ell}\coprod_{j=1}^{(\mathbf{N}x+1)/\ell}\zeta^i u_j U^{(0)}.$$

This shows that, by index considerations,

$$U_1(\mathfrak{n}_\Sigma)\begin{pmatrix}\varpi_x & 0\\ 0 & 1\end{pmatrix}U_1(\mathfrak{n}_\Sigma) = \coprod_{i=1}^{\ell}\coprod_{j=1}^{(\mathbf{N}x+1)/\ell}\zeta^i u_j\begin{pmatrix}\varpi_x & 0\\ 0 & 1\end{pmatrix}U_1(\mathfrak{n}_\Sigma).$$

Since $h\zeta^i = d_i h$ for some $d_i \in D^\times$, we have

$$\begin{aligned} T_x(f)(h) &= \sum_{i=1}^{\ell}\sum_{j=1}^{(\mathbf{N}x+1)/\ell} f\left(h\zeta^i u_j\begin{pmatrix}\varpi_x & 0\\ 0 & 1\end{pmatrix}\right)\\ &= \sum_{i=1}^{\ell}\sum_{j=1}^{(\mathbf{N}x+1)/\ell} f\left(hu_j\begin{pmatrix}\varpi_x & 0\\ 0 & 1\end{pmatrix}\right)\\ &= \ell\sum_{j=1}^{(\mathbf{N}x+1)/\ell} f\left(hu_j\begin{pmatrix}\varpi_x & 0\\ 0 & 1\end{pmatrix}\right). \end{aligned}$$

The lemma follows. □

Now we discuss various properties of the modular forms and Hecke operators.

Theorem 4.6. *Keeping the assumptions of the two preceding lemmas, we have the following*:

(1) *The $\mathcal{O}$-module $S_{\mathcal{O}}(U_1(\mathfrak{n}_\Sigma))^*$ is invariant under the action of Hecke operators.*
(2) *The pairing on $S_K(U_1(\mathfrak{n}_\Sigma))$ induces a perfect pairing*

$$S_{\mathcal{O}}\big(U_1(\mathfrak{n}_\Sigma)\big) \times S_{\mathcal{O}}\big(U_1(\mathfrak{n}_\Sigma)\big)^* \to \mathcal{O}.$$

(3) *Let $\mathfrak{m}$ be a non-Eisenstein maximal ideal of the Hecke algebra $\mathbb{T}_{\mathcal{O}}(U_1(\mathfrak{n}_\Sigma))$. Then $S_{\mathcal{O}}(U_1(\mathfrak{n}_\Sigma))_{\mathfrak{m}} = S_{\mathcal{O}}(U_1(\mathfrak{n}_\Sigma))^*_{\mathfrak{m}}$. As a consequence, the pairing on $S_K(U_1(\mathfrak{n}_\Sigma))$ induces a perfect pairing on $S_{\mathcal{O}}(U_1(\mathfrak{n}_\Sigma))_{\mathfrak{m}}$.*

Proof. The first part is easily checked using the given pairing on $S_K(U_1(\mathfrak{n}_\Sigma))$. The second part follows from Lemma 4.4. The third part is a direct consequence of Lemma 4.5. □

5. Deformations in the minimal case

In this section, we show that the universal deformation ring in the minimal case is isomorphic to a Hecke algebra, and we show that these are complete intersection rings of relative dimension zero over $\mathbb{Z}_p$.

Recall that we are given a continuous representation

$$\bar{\rho} : G_F \to \mathrm{GL}_2(k)$$

satisfying the various properties listed in the beginning of Section 3, and also satisfying Assumption 3.1. In this and the next section, we shall assume the following additional modularity condition.

Assumption 5.1. Let U_0 denote $U_{\{1\}}(\mathfrak{n}_\emptyset)$. Then we assume that there is a continuous homomorphism $\phi : \mathbb{T}_{\mathcal{O}}(U_0) \to k$ with non-Eisenstein kernel which gives our representation $\bar{\rho}$. We write $\mathfrak{m}_\emptyset$ for the kernel.

Our aim is to show that the natural map $R_\emptyset \twoheadrightarrow \mathbb{T}_{\mathcal{O}}(U_0)_{\mathfrak{m}_\emptyset}$ is an isomorphism of complete intersection rings.

Fix a finite set of primes Σ of F not dividing ℓ such that for every $x \in \Sigma$, we have

- $\mathbf{N}x \equiv 1 \pmod{\ell}$,
- $\bar{\rho}$ is unramified at x and has distinct eigenvalues $\alpha_x \neq \beta_x$.

We denote the maximal ℓ-power quotient of $(\mathcal{O}_F/x)^\times$, for $x \in \Sigma$, by Δ_x and set $\Delta_\Sigma = \prod \Delta_x$. We define the following objects (all products are over $x \in \Sigma$):

(1) An ideal $\mathfrak{n}_\Sigma = \prod x^2$.
(2) Compact open subgroups $U_{0,\Sigma} = U_{\{1\}}(\mathfrak{n}_\Sigma)$ and $U_{1,\Sigma} = U_{\Delta_\Sigma}(\mathfrak{n}_\Sigma)$.
(3) An ideal $\mathfrak{m}_\Sigma$ of either $\mathbb{T}(U_{0,\Sigma})$ or $\mathbb{T}(U_{1,\Sigma})$ generated by ℓ and
   - $T_x - \operatorname{tr}\bar{\rho}(\mathrm{Frob}_x)$ for $x \nmid \ell\mathfrak{n}_\Sigma$, and
   - $\mathbf{U}_{\varpi_x} - \alpha_x$ for $x \in \Sigma$.

Note that Lemmas 2.1 and 2.2 of [22] remain true in the present situation (and we will write them down again in a moment). We also have the fact that $S_{\mathcal{O}}(U_{1,\Sigma})$ is an $\mathcal{O}[\Delta_\Sigma]$-module via $h \to \langle h\rangle$. But slight care is required for the critical Lemma 2.3 and Corollary 2.4 of [22]: it is no longer obvious that $S_{\mathcal{O}}(U_{1,\Sigma})_{\mathfrak{m}_\Sigma}$ is free over $\mathcal{O}[\Delta_\Sigma]$. Nonetheless, we can still get the 'patching modules' technique of [6] to work.

We first present a trivial reformulation of Theorem 2.1 of [6].

Theorem 5.2. *Fix a positive integer r, a finite field k; set $A = k[[S_1, \dots, S_r]]$ and $B = k[[X_1, \dots, X_r]]$. We denote the maximal ideal of A by $\mathfrak{n}$. We are given: a k-algebra R, a non-zero R-module H which is finite-dimensional over k. For each positive integer n, we suppose that we have k-algebra homomorphisms $\phi_n : A \to B$ and $\psi_n : B \to R$, a B-module H_n and a B-linear homomorphism $\pi_n : H_n \to H$ such that:*

- *ψ_n is surjective and $\psi_n\phi_n = 0$,*
- *π_n induces an isomorphism between $H_n/\mathfrak{n}H_n$ and H, and*
- *there is an unbounded sequence of positive integers $(a_n)_{n\geqslant 1}$ such that $H_n/\mathfrak{n}^{a_n}H_n$ is free over $A/\mathfrak{n}^{a_n}$.*

Then R is a complete intersection, and H is free over R.

We now begin analysing and comparing the $\mathcal{O}[\Delta_\Sigma]$-module structures of $S_{\mathcal{O}}(U_{0,\Sigma})$ and $S_{\mathcal{O}}(U_{1,\Sigma})$. Denote the augmentation ideal of $\mathcal{O}[\Delta_\Sigma]$ by I_{Δ_Σ}. Obviously, functions in $S_{\mathcal{O}}(U_{0,\Sigma})$ are precisely the elements of $S_{\mathcal{O}}(U_{1,\Sigma})$ which are invariant under the action of Δ_Σ; there is a 'norm' map

$$\sum_{h\in\Delta_\Sigma} \langle h\rangle : S_{\mathcal{O}}(U_{1,\Sigma})_{\Delta_\Sigma} \to S_{\mathcal{O}}(U_{0,\Sigma}),$$

where the subscript denotes coinvariants.

Proposition 5.3. *The norm map*

$$\sum_{h\in\Delta_\Sigma} \langle h\rangle : S_{\mathcal{O}}(U_{1,\Sigma}) \to S_{\mathcal{O}}(U_{0,\Sigma})$$

has kernel $I_{\Delta_\Sigma} S_{\mathcal{O}}(U_{1,\Sigma})$ and surjects onto $S_{\mathcal{O}}(U_{0,\Sigma})^*$.

The $\mathbb{T}(U_{1,\Sigma})$-module

$$\Bigg(\sum_{h\in\Delta_\Sigma[\ell]} h\Bigg) S_{\mathcal{O}}(U_{1,\Sigma})$$

is free over $\mathcal{O}[\Delta_\Sigma/\Delta_\Sigma[\ell]]$; and the norm map factorizes, in an obvious way, as the composite of

$$\sum_{h\in\Delta_\Sigma[\ell]} \langle h\rangle \quad \textit{and} \quad \sum_{h\in\Delta_\Sigma/\Delta_\Sigma[\ell]} \langle h\rangle.$$

Proof. We have a decomposition

$$\big(D \otimes_{\mathbb{Q}} \mathbb{A}^{\infty}\big)^{\times} = \coprod D^{\times} t_i U_{0,\Sigma}.Z\big(\mathbb{A}_F^{\infty}\big).$$

For $h \in \Delta_\Sigma$, we have a lift $\tilde{h} \in (\mathbb{A}_F^{\infty})^{\times}$ which gives the coset decomposition

$$U_{0,\Sigma} = \coprod_{h \in \Delta_\Sigma} \begin{pmatrix} \tilde{h} & 0 \\ 0 & 1 \end{pmatrix} U_{1,\Sigma}.$$

There is an obvious transitive action of Δ_Σ on this coset decomposition.

For each t_i, we define

$$\mathrm{Stab}_i = \left\{ h \in \Delta_\Sigma \;\middle|\; D^{\times} t_i U_{1,\Sigma}.Z\big(\mathbb{A}_F^{\infty}\big) = D^{\times} t_i \begin{pmatrix} \tilde{h} & 0 \\ 0 & 1 \end{pmatrix} U_{1,\Sigma}.Z\big(\mathbb{A}_F^{\infty}\big) \right\}.$$

Obviously, the definition is independent of the representatives t_i and depends only the double coset decomposition. We get the double coset decomposition

$$\big(D \otimes_{\mathbb{Q}} \mathbb{A}^{\infty}\big)^{\times} = \coprod_{i} \coprod_{h \in \Delta_\Sigma/\mathrm{Stab}_i} D^{\times} t_i \begin{pmatrix} \tilde{h} & 0 \\ 0 & 1 \end{pmatrix} U_{1,\Sigma}.Z\big(\mathbb{A}_F^{\infty}\big).$$

In particular, we see that the set

$$\bigcup_i \big\{ \langle h \rangle [t_i] \;\big|\; h \in \Delta_\Sigma/\mathrm{Stab}_i \big\}$$

is a basis for the free $\mathcal{O}$-module $S_{\mathcal{O}}(U_{1,\Sigma})$.

It is now clear that the image of the map

$$\sum_{h \in \Delta_\Sigma} \langle h \rangle : S_{\mathcal{O}}(U_{1,\Sigma}) \to S_{\mathcal{O}}(U_{0,\Sigma})$$

is free over $\mathcal{O}$ with basis $\{|\mathrm{Stab}_i|[t_i]\}_i$. The fact that the kernel is the image of the augmentation ideal is obvious once we show that it is enough to consider elements in the kernel having the form

$$x = \sum_{h \in \Delta_\Sigma/\mathrm{Stab}_i} a_h \langle h \rangle [t_i] \quad \text{with } a_h \in \mathcal{O} \quad \text{and} \quad \sum_{h \in \Delta_\Sigma/\mathrm{Stab}_i} a_h = 0.$$

It suffices to consider such x because we can write $x = \sum x_i$, where x_i lies in the kernel and has the form $|\mathrm{Stab}_i|(\sum a_h)[t_i]$.

We now show that the image of the norm map is $S_{\mathcal{O}}(U_{0,\Sigma})^*$ by proving that the order of Stab_i is equal to the power of ℓ that divides the order of $(t_i^{-1} D^{\times} t_i \cap U_{0,\Sigma}.Z(\mathbb{A}_F^{\infty}))/F^{\times}$.

We claim that the order of $(t_i^{-1}D^\times t_i \cap U_{1,\Sigma}.Z(\mathbb{A}_F^\infty))/F^\times$ is not divisible by ℓ. Indeed, let $\alpha \in t_i^{-1}D^\times t_i \cap U_{1,\Sigma}.Z(\mathbb{A}_F^\infty)$ be such that $\alpha^\ell \in F^\times$. Fix a place $x \in \Sigma$. We can write the xth component of $\alpha \in U_{1,\Sigma}.Z(\mathbb{A}_F^\infty)$ as $u_x z_x$ where $z_x \in K_x$ and $u_x \in \mathrm{GL}_2(\mathcal{O}_x)$ satisfies

$$u_x \equiv \begin{pmatrix} h & * \\ 0 & 1 \end{pmatrix} \pmod{\varpi_x}$$

with h having order prime to ℓ. Raising u_x to the ℓth power, one deduces that u_x reduces to the identity mod ϖ_x, and hence that u_x is trivial. This then implies that $\alpha \in F^\times$.

Let m be the prime to ℓ part of the order of $(t_i^{-1}D^\times t_i \cap U_{0,\Sigma}.Z(\mathbb{A}_F^\infty))/F^\times$. We define a map $\theta : \mathrm{Stab}_i \to (t_i^{-1}D^\times t_i \cap U_{0,\Sigma}.Z(\mathbb{A}_F^\infty))/F^\times$ as follows: If $h \in \mathrm{Stab}_i$, we must have $t_i^{-1}dt_i = hu_1a = x$ (say) for some $d \in D^\times$, $u_1 \in U_{1,\Sigma}$ and $a \in (\mathbb{A}_F^\infty)^\times$. Thus $x \in t_i^{-1}D^\times t_i \cap U_{0,\Sigma}.Z(\mathbb{A}_F^\infty)$, and we set $\theta(h) = x^m \pmod{F^\times}$. By the claim established in the previous paragraph, it follows that θ is a well-defined injective homomorphism from Stab_i to the ℓ-primary part of $(t_i^{-1}D^\times t_i \cap U_{0,\Sigma}.Z(\mathbb{A}_F^\infty))/F^\times$. Since by Lemma 4.4 the order of the ℓ-primary part of $(t_i^{-1}D^\times t_i \cap U_{0,\Sigma}.Z(\mathbb{A}_F^\infty))/F^\times$ is exactly ℓ or 1, it is then simple to verify that θ is an isomorphism between Stab_i and the ℓ-primary part of $(t_i^{-1}D^\times t_i \cap U_{0,\Sigma}.Z(\mathbb{A}_F^\infty))/F^\times$. It follows that the image of the norm map is exactly $S_{\mathcal{O}}(U_{0,\Sigma})^*$.

The last part of the proposition follows since $\mathrm{Stab}_i \subset \Delta_\Sigma[\ell]$. □

The following is Lemma 2.2 of [22]. The proof given in [22] works verbatim in our case (thanks to Theorem 4.6).

Lemma 5.4. *There is an isomorphism $S_{\mathcal{O}}(U_{0,\emptyset})_{\mathfrak{m}_\emptyset} \to S_{\mathcal{O}}(U_{0,\Sigma})_{\mathfrak{m}_\Sigma}$ inducing an isomorphism $\mathbb{T}(U_{0,\Sigma})_{\mathfrak{m}_\Sigma} \to \mathbb{T}(U_{0,\emptyset})_{\mathfrak{m}_\emptyset}$.*

Using the fact that the rings in consideration are semi-local, reduced and complete (they are finite flat $\mathbb{Z}_\ell$-algebras), and Theorem 4.6, we get the following:

Corollary 5.5.

(1) *There is an isomorphism $S_{\mathcal{O}}(U_{1,\Sigma})_{\mathfrak{m}_\Sigma,\Delta_\Sigma} \to S_{\mathcal{O}}(U_{1,\emptyset})_{\mathfrak{m}_\emptyset}$. This isomorphism is compatible with the map on Hecke algebras $\mathbb{T}(U_{1,\Sigma})_{\mathfrak{m}_\Sigma} \to \mathbb{T}(U_{0,\emptyset})_{\mathfrak{m}_\emptyset}$ which sends:*
- *T_x to T_x for x not dividing $\ell\mathfrak{n}_\Sigma$,*
- *$\langle h\rangle$ to 1 for $h \in \Delta_\Sigma$, and*
- *$\mathbf{U}_{\varpi_x}$ to A_x for $x \in \Sigma$ where A_x is the unique root of $X^2 - T_xX + \mathbf{N}x$ in $\mathbb{T}(U_{0,\emptyset})_{\mathfrak{m}_\emptyset}$ congruent to $\alpha_x \pmod{\mathfrak{m}_\emptyset}$.*

(2) *The surjection $S_{\mathcal{O}}(U_{1,\Sigma})_{\mathfrak{m}_\Sigma} \twoheadrightarrow S_{\mathcal{O}}(U_{1,\emptyset})_{\mathfrak{m}_\emptyset}$ given by composing the norm map with the isomorphism of the preceding lemma factorizes as the composite of*

$$S_{\mathcal{O}}(U_{1,\Sigma})_{\mathfrak{m}_\Sigma,\Delta_\Sigma} \twoheadrightarrow H_\Sigma \quad \textit{and} \quad H_\Sigma \to S_{\mathcal{O}}(U_{1,\emptyset})_{\mathfrak{m}_\emptyset}$$

where
- *H_Σ is a $\mathbb{T}(U_{1,\Sigma})_{\mathfrak{m}_\Sigma}$-algebra and the maps are compatible with the algebra structures, and*
- *H_Σ is a free $\mathcal{O}[\Delta_\Sigma/\Delta_\Sigma[\ell]]$ module.*

We apply the above corollary to the sets Σ_n produced by Theorem 3.3. Applying the 'patching modules' result of Diamond [6] and Fujiwara [9] (Theorem 5.2 above), we get the following result.

Theorem 5.6. *The natural map*

$$R_\emptyset \to \mathbb{T}(U_0)_{\mathfrak{m}_\emptyset}$$

is an isomorphism of complete intersection rings and the module $S_{\mathcal{O}}(U_0)_{\mathfrak{m}_\emptyset}$ is free over $\mathbb{T}(U_0)_{\mathfrak{m}_\emptyset}$.

6. Non-minimal level

The proof of the result in the non-minimal case given in [22] remains valid in our case. We shall only give a sketch. Throughout this section, we keep the various assumptions (and notation) of the last section.

Fix a homomorphism $\pi_\emptyset : R_\emptyset \twoheadrightarrow \mathcal{O}$. We now let Σ be a finite set of primes of F not containing any primes above ℓ. We denote by π_Σ the surjection $R_\Sigma \twoheadrightarrow \mathcal{O}$ obtained by taking the composite of

$$R_\Sigma \twoheadrightarrow R_\emptyset \twoheadrightarrow \mathcal{O}$$

where the first map is the one given by the universal property of R_Σ and the second map is $\pi_\emptyset$. We shall denote the kernel of π_Σ by $\mathfrak{P}_\Sigma$.

Let $\mathfrak{n}_\Sigma = \prod_{x \in \Sigma} x^2$, and let $U_\Sigma = U_{\{1\}}(\mathfrak{n}_\Sigma)$. Also, let $\mathfrak{m}_\Sigma$ be the maximal ideal of $\mathbb{T}_{\mathcal{O}}(U_\Sigma)$ corresponding to our residual representation $\bar{\rho}$. We denote by $\mathbb{T}_\Sigma$ the localization $\mathbb{T}_{\mathcal{O}}(U_\Sigma)_{\mathfrak{m}_\Sigma}$, and write S_Σ for the $\mathbb{T}_\Sigma$-module $S_{\mathcal{O}}(U_\Sigma)_{\mathfrak{m}_\Sigma}$.

We then have the following.

Theorem 6.1. *The natural map $R_\Sigma \twoheadrightarrow \mathbb{T}_\Sigma$ is an isomorphism of complete intersection rings and S_Σ is free over $\mathbb{T}_\Sigma$.*

To prove the theorem, one needs to check (by Theorem 2.4 of [6]) that the order of $\mathfrak{P}_\Sigma/\mathfrak{P}_\Sigma^2$ divides the order of

$$\Omega_\Sigma \stackrel{\text{def}}{=} \frac{S_\Sigma}{S_\Sigma[\mathfrak{P}] \oplus S_\Sigma[\operatorname{Ann}_{\mathbb{T}_\Sigma}\mathfrak{P}]}.$$

A standard computation shows that the order of $\mathfrak{P}_\Sigma/\mathfrak{P}_\Sigma^2$ divides

$$\#\big(\mathfrak{P}_\emptyset/\mathfrak{P}_\emptyset^2\big) \prod_{x \in \Sigma} \#\big(\mathcal{O}/(1 - \mathbf{N}x)\big(T_x^2 - (1 + \mathbf{N}x)^2\big)\mathcal{O}\big),$$

and we shall prove that this expression is the order of Ω_Σ.

Note that $S_\Sigma[\mathfrak{P}_\Sigma]$ is a free $\mathcal{O}$-module of rank 1. Fix a perfect symmetric $\mathcal{O}$-valued $\mathcal{O}$-bilinear pairing $\{,\}_\Sigma$ on $S_\Sigma[\mathfrak{P}_\Sigma]$, and let $j_\Sigma : S_\Sigma[\mathfrak{P}_\Sigma] \hookrightarrow S_\Sigma$ be the natural inclusion. Also, define a pairing $\langle,\rangle_\Sigma$ on S_Σ by

$$\langle f_1, f_2 \rangle_\Sigma = (f_1, w_\Sigma f_2)$$

where (,) is the standard pairing, and $w_\Sigma \in \mathrm{GL}_2(\mathbb{A}_F^\infty) \cong (D \otimes_{\mathbb{Q}} \mathbb{A}^\infty)^\times$ is the element defined by

$$w_{\Sigma,x} = \begin{cases} \text{identity} & \text{if } x \notin \Sigma, \\ \begin{pmatrix} 0 & 1 \\ \varpi_x^2 & 0 \end{pmatrix} & \text{if } x \in \Sigma. \end{cases}$$

This new pairing is perfect, and the Hecke operators are self-adjoint with respect to $\langle,\rangle_\Sigma$.

Now let x be a prime not dividing $\mathfrak{n}_\Sigma \ell$. There is a well-defined map

$$i_x : S_\Sigma \to S_{\Sigma \cup \{x\}}$$

which is obtained from the map sending $f \in S_{\mathcal{O}}(U_\Sigma)$ to

$$(\mathbf{N}x) f - \begin{pmatrix} 1 & 0 \\ 0 & \varpi_x \end{pmatrix} T_x f + \begin{pmatrix} 1 & 0 \\ 0 & \varpi_x^2 \end{pmatrix} f \in S_{\mathcal{O}}(U_{\Sigma \cup \{x\}}).$$

Under this map, the image of $S_\Sigma[\mathfrak{P}_\Sigma]$ is contained in $S_{\Sigma \cup \{x\}}[\mathfrak{P}_{\Sigma \cup \{x\}}]$. We denote by $\widetilde{i_x}$ the resulting map from $S_\Sigma[\mathfrak{P}_\Sigma]$ to $S_{\Sigma \cup \{x\}}[\mathfrak{P}_{\Sigma \cup \{x\}}]$.

We then have the following.

- Let i_x^* be the adjoint of i_x with respect to the pairings $\langle,\rangle_\Sigma$ and $\langle,\rangle_{\Sigma \cup \{x\}}$. The composite $i_x^* \circ i_x$ is equal to

$$\mathbf{N}x(1 - \mathbf{N}x)\big(T_x^2 - (1 + \mathbf{N}x)^2\big).$$

- $i_x(S_\Sigma[\mathfrak{P}_\Sigma]) = S_{\Sigma \cup \{x\}}[\mathfrak{P}_{\Sigma \cup \{x\}}]$. This follows from Ihara's lemma (see [22, Lemma 3.1]).
- Let j_Σ^* be the adjoint of j_Σ with respect to the pairings $\{,\}_\Sigma$ and $\langle,\rangle_\Sigma$. It induces an isomorphism

$$j_\Sigma^* : \Omega_\Sigma \xrightarrow{\sim} \frac{S_\Sigma[\mathfrak{P}_\Sigma]}{j_\Sigma^* S_\Sigma[\mathfrak{P}_\Sigma]}.$$

- Let $\widetilde{i_x}^*$ be the adjoint of $\widetilde{i_x}$ with respect to the pairings $\{,\}_\Sigma$ and $\{,\}_{\Sigma \cup \{x\}}$. It is an isomorphism, and we have $\widetilde{i_x}^* \circ j_{\Sigma \cup \{x\}}^* = j_\Sigma^* \circ i_x^*$.

It follows that

$$\#\Omega_\Sigma = \#\Omega_\emptyset \prod_{x \in \Sigma} \#\big(\mathcal{O}/(1 - \mathbf{N}x)\big(T_x^2 - (1 + \mathbf{N}x)^2\big)\mathcal{O}\big).$$

The result in the minimal case implies that $\#\Omega_\emptyset = \#(\mathfrak{P}_\emptyset / \mathfrak{P}_\emptyset^2)$, and hence that

$$\# \frac{\mathfrak{P}_\Sigma}{\mathfrak{P}_\Sigma^2} \,\Big|\, \#\Omega_\Sigma.$$

7. Modularity of Galois representations and elliptic curves

We now collect the results of the preceding two sections.

Let F be a totally real, finite extension of $\mathbb{Q}$. Let $\mathcal{O}$ be the ring of integers in a finite extension of $\mathbb{Q}_\ell$ where ℓ is an odd prime, and let k be its residue field. We suppose that we are given continuous representations

$$\rho_i : G_F \to \mathrm{GL}_2(\mathcal{O}), \quad i = 1, 2,$$

satisfying the following properties:

- ρ_i $(i = 1, 2)$ is an odd representation unramified outside finitely many primes;
- $\det \rho_1 = \det \rho_2 = \epsilon_\ell$ where ϵ_ℓ is the ℓ-adic cyclotomic character.
- The residual representations $\bar{\rho}_i : G_F \to \mathrm{GL}_2(k)$ are equivalent and are absolutely irreducible. We denote the residual representation by $\bar{\rho}$.

Theorem 7.1. *With notations as in the preceding paragraph, we make the following assumptions.*

- *The restriction of $\bar{\rho}$ to the absolute Galois group of $F(\zeta_\ell)$ is absolutely irreducible; furthermore, if $\ell = 5$ and* $\mathrm{Proj}\,\bar{\rho}|_{\mathrm{Gal}(\overline{F}/F(\zeta_\ell))}$, *then* $[F(\zeta_\ell) : F] = 4$.
- (*Conditions at ℓ.*) *Let v be any prime of F dividing ℓ, and let I_v be the inertia group of F_v. We assume*:
  1. *$\bar{\rho}|_{I_v} \sim \Omega_2|_{I_v}$, where Ω_2 is the second fundamental character of the inertia group of $\mathbb{Q}_\ell$.*
  2. *Let $\mathfrak{m}$ be the maximal ideal of $\mathcal{O}$, and let $\bar{\rho}_{i,n}$ be the reduction of ρ_i modulo $\mathfrak{m}^n$. Then $\bar{\rho}_{i,n}|_{F_v}$ is finite flat.*
- *The ramification index of F at any prime above ℓ is less than or equal to $\ell - 1$.*

Under these assumptions, the modularity of ρ_1 implies the modularity of ρ_2.

Proof. We can find a totally real, finite soluble extension F'/F such that:

- The extension F'/F is unramified at primes dividing ℓ.
- $\bar{\rho}|_{G_{F'}}$ satisfies Assumption 5.1. (For this, we need to use the modularity of ρ_1 along with the base change results in [18].)

It follows that $\rho_2|_{G_{F'}}$ is modular. Langlands' cyclic base change then shows that ρ_2 is modular. □

In Section 9, we will give some applications to the modularity of elliptic curves. However, let us remark here that Theorem 7.1 will not apply in general to all supersingular curves, as the first condition at ℓ will not be satisfied in general. Indeed, let $F = \mathbb{Q}(\sqrt{3})$, and let E denote the elliptic curve

$$y^2 = x^3 + \sqrt{3}x^2 + x + 1.$$

The curve has discriminant $32(3\sqrt{3}-14)$, and hence has good reduction at the prime $\sqrt{3}$ above 3. On the other hand, it is easy to show that multiplication by 3 on the group law of an elliptic curve

$$y^2 = x^3 + a_2x^2 + a_4x + a_6$$

is given by

$$[3]t = 3t - 8a_2t^3 + \cdots,$$

so that the curve above has supersingular reduction at $\sqrt{3}$, as $v_3(a_2) = v_3(\sqrt{3}\,) > 0$, showing that the formal group at 3 has height 2. As in Serre [15, Proposition 10], the action of tame inertia on the 3-torsion points is given by 2 copies of the fundamental character of level 1, rather than by the fundamental character of level 2.

Serre's argument also shows that in order that the mod 3 representation of the curve E be given (on tame inertia) by the fundamental character of level 2, it is necessary and sufficient that the Newton polygon of the multiplication-by-3 map on the formal group should consist of a single line from $(1,e)$ to $(9,0)$. This is automatic when $e=1$, but if $e>1$, then other situations may arise, as above.

It follows that our main result can apply to all supersingular curves defined over fields F unramified at 3, as well as to many examples of curves defined over more general fields.

8. Applications I

Theorem 8.1. *Let $\bar{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_7)$ be an absolutely irreducible, continuous, odd representation. If the projective image of $\bar{\rho}$ is insoluble, we also assume that*:

- *the projective image of inertia at* 3 *has odd order,*
- *the determinant of $\bar{\rho}$ restricted to the inertia group at* 7 *has even order,*

then $\bar{\rho}$ is modular.

Sketch of proof. Of course, we need only consider the case when the image of $\bar{\rho}$ is insoluble. Moreover by [13], we can assume that the restriction of $\bar{\rho}$ to a decomposition group at 7 is irreducible. Twisting by a quadratic character, we can also assume that $\bar{\rho}|_{I_7}$ is equivalent to $\omega_2 \oplus \omega_2^7$ or $\omega_2^{13} \oplus \omega_2^{7.13}$ where $\omega_2 : I_7 \to \mathbb{F}_{49}^{\times}$ is the second fundamental character. Applying the axiomatic formulation of Ramakrishna's result in [21], together with Theorems 3.2.1, 4.2.1 of [3], one deduces the existence of a continuous, odd representation

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_7)$$

lifting $\bar{\rho}$, unramified outside finitely many primes, determinant the cyclotomic character times a finite order character, and such that the Artinian quotients $\rho \pmod{7^n}$ are finite flat when restricted to the absolute Galois group of $\mathbb{Q}_7(7^{1/4})$. Assuming the existence of a totally real soluble extension $F/\mathbb{Q}$ such that $\bar{\rho}|_{G_F}$ is modular and the ramification index of $F/\mathbb{Q}$ at 7 is at most 6, one deduces the modularity of ρ by Theorem 7.1 and Langlands' cyclic base change.

We now explain how to find such a field F. Firstly, we can find a finite soluble, totally real extension $F_1/\mathbb{Q}$ and a quadratic twist of $\bar{\rho}|_{G_{F_1}}$, which we denote by $\tilde{\rho}$, such that the following conditions are satisfied.

- The determinant of $\tilde{\rho}$ is the mod 7 cyclotomic character.
- Conditions at 3: Let v be any prime of F_1 above 3, and let D_v be a decomposition group at v.
  - $\tilde{\rho}$ is trivial on D_v.
  - The ramification index of $F_{1,v}/\mathbb{Q}_3$ is odd.
- Conditions at 7: Let v be any prime of F_1 above 7, and let D_v, I_v be the decomposition and inertia groups at v. Then, the ramification index of $F_{1,v}/\mathbb{Q}_7$ is exactly 4. Furthermore, we have $\tilde{\rho}|_{I_{F_{1,v}}} \cong (\omega_2 \oplus \omega_2^7)|_{I_{F_{1,v}}}$.

We denote by $X(\tilde{\rho})$ the (completed) moduli space of elliptic curves with mod 7 representation symplectically isomorphic to $\tilde{\rho}$ (see [13] for details). The canonical divisor embeds $X(\tilde{\rho})$ as a quartic curve in $\mathbb{P}^2_{/F_1}$.

For each prime v of F_1 dividing 3∞, we can find a finite unramified extension $F_v/F_{1,v}$ and a line L_v defined over $F_{1,v}$ such that L_v cuts $X(\tilde{\rho})_{/F_v}$ at four distinct points all of which are defined over F_v. Moreover, the elliptic curves corresponding to these four points all have good ordinary reduction when $v \mid 3$. (See the fourth paragraph in Section 5 of [13].) For primes above 7, we have the following lemma:

Lemma 8.2. *Let v be a prime of F_1 above 7. We can find a finite Galois extension $F_v/F_{1,v}$ and an F_v-rational line L_v such that the following holds.*

- *L_v cuts $X(\tilde{\rho})_{/F_v}$ at four distinct points all of which are defined over F_v.*
- *The ramification index of $F_v/\mathbb{Q}_7$ is at most 4. The four points of intersection are all elliptic curves with good supersingular reduction.*

Assuming the above lemma, intersecting $X(\tilde{\rho})$ with a line over F_1 which is v-adically close to L_v for each $v \mid 3.7.\infty$ gives the following: There is a finite, soluble, totally real $F \supset F_1 \supset \mathbb{Q}$, and an elliptic curve $E_{/F}$ satisfying the following conditions.

- $\bar{\rho}_{E,7} \sim \tilde{\rho}|_{G_F}$ and $\bar{\rho}_{E,3} : G_F \twoheadrightarrow \mathrm{GL}_2(\mathbb{F}_3)$ is surjective.
- Conditions at primes v dividing 3: E has good ordinary reduction at every prime above 3 and the ramification index of F at 3 is odd.
- Conditions above 7: F/F_1 is unramified at every prime above 7 and E has good supersingular reduction at every prime above 7.

The elliptic curve E is modular by a result of Skinner and Wiles [19], and therefore $\bar{\rho}$ is also modular. □

Proof of Lemma 8.2. The modular curve $X(\omega_2 \oplus \omega_2^7)_{/\mathbb{Q}_7^{\mathrm{nr}}}$ is isomorphic to $X(\tilde{\rho})$ over $\mathbb{Q}_7^{\mathrm{nr}}(\sqrt[4]{7})$. The elliptic curve $y^2 = x^3 + x$ has j-invariant 1728 and so has supersingular reduction. Taking a cyclic degree 3 isogeny of E if necessary, we can assume that $X(\omega_2 \oplus \omega_2^7)(\mathbb{Q}_7^{\mathrm{nr}})$ contains an elliptic curve E having good supersingular reduction and with j-invariant 1728. Let us denote this point by P. From the geometry of the Klein quartic (see the proposition in Section 2 of [8]), we see that there is a unique involution (in the automorphism group) fixing P. The normalizer of this involution is a Sylow 2-subgroup, and the orbit of P when acted on by the normalizer has size exactly 4. Furthermore, they (the points in the orbit) lie on a unique line.

We can thus find a unique line L passing through P such that:

- L is defined over $\mathbb{Q}_7^{\mathrm{nr}}$,
- L passes through four distinct points of $X(\omega_2 \oplus \omega_2^7)$ whose j-invariants are 1728.

We claim that two of these points are already defined over $\mathbb{Q}_7^{\mathrm{nr}}$. We have the point P with corresponding elliptic curve E. Note that E has complex multiplication by $\mathbb{Z}[i]$ (and the endomorphism ring is already defined over $\mathbb{Q}_7^{\mathrm{nr}}$). We now check that the isogeny $E \xrightarrow{2-2i} E$ gives us another point of intersection (which is obviously defined over $\mathbb{Q}_7^{\mathrm{nr}}$). This can be checked over $\mathbb{C}$, and follows from the following observations.

- The involution $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \in \mathrm{PSL}_2(\mathbb{F}_7)$ fixes
$$\bigl(\{1/7, i/7\}, \mathbb{C}/\mathbb{Z} + i\mathbb{Z}\bigr) \in X(7)(\mathbb{C}).$$
- $\left(\begin{smallmatrix} 2 & 2 \\ -2 & 2 \end{smallmatrix}\right)$ is in the normalizer of $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and sends
$$\bigl(\{1/7, i/7\}, \mathbb{C}/\mathbb{Z} + i\mathbb{Z}\bigr) \quad \text{to } \bigl(\{2 - 2i/7, 2 + 2i/7\}, \mathbb{C}/\mathbb{Z} + i\mathbb{Z}\bigr).$$

Thus each of the four points of intersection are defined over $\mathbb{Q}_7^{\mathrm{nr}}(\sqrt{7})$. The Sylow 2-subgroup which acts transitively on these four points is dihedral; in terms of generators and relations, it is given by
$$\bigl\langle \alpha, \beta \bigm| \alpha^4 = \beta^2 = e,\ \beta\alpha\beta = \alpha^3 \bigr\rangle.$$

The unique involution which stabilizes P is α^2, and it is defined over $\mathbb{Q}_7^{\mathrm{nr}}$. The other three points are given by $\alpha(P)$, $\beta(P)$ and $\alpha\beta(P)$.

We now check that α, β are defined over $\mathbb{Q}_7^{\mathrm{nr}}(\sqrt[4]{7})$. If $\sigma \in G_{\mathbb{Q}_7^{\mathrm{nr}}(\sqrt{7})}$, we have
$$(\sigma * \beta)(P) = \sigma\bigl(\beta\bigl(\sigma^{-1} P\bigr)\bigr) = \beta(P).$$

Therefore, we have $\sigma * \beta = \alpha^{2i(\sigma)}\beta$ where
$$i : G_{\mathbb{Q}_7^{\mathrm{nr}}(\sqrt{7})} \to \mathbb{Z}/2\mathbb{Z}$$

is a continuous homomorphism which necessarily factors through $\mathbb{Q}_7^{\mathrm{nr}}(\sqrt[4]{7})$. Similarly for α. We can thus conclude that all the four points of intersection have good supersingular reduction $\mathbb{Q}_7^{\mathrm{nr}}(\sqrt[4]{7})$.

Finally, it follows that we can find a line defined over an extension of $F_{1,v}$ with absolute ramification index 4 which cuts $X(\tilde{\rho})$ at four distinct supersingular points, all defined over that extension. Take F_v to be the Galois closure of the extension thus constructed, and take L_v to be the line $L_{/F_v}$. $\square$

9. Applications II

The aim of this section is to study the modularity of elliptic curves over certain totally real fields, using Theorem 7.1. Our main results are given by Propositions 9.2 and 9.3. For the particular example of the field $\mathbb{Q}(\sqrt{2})$, we can prove more; the analogue of the switch between $p = 3$ and $p = 5$ used by Wiles [24, §5] holds, and we can use existing results, together with the new results in this paper, to deduce the modularity of all semistable elliptic curves over $\mathbb{Q}(\sqrt{2})$.

In [10], it is explained that this implies a version of Fermat's Last Theorem over $\mathbb{Q}(\sqrt{2})$. Further calculations in [10] show that $\mathbb{Q}(\sqrt{2})$ is the only real quadratic field for which one can hope to generalise the methods of Ribet and Wiles to prove such a result. It seems remarkable to us that there are any fields other than $\mathbb{Q}$ for which all the numerology allows us to prove generalisations of Fermat's Last Theorem.

We begin by proving results for more general fields. We start with a preliminary lemma.

Lemma 9.1. *Let p be equal to 3 or 5, and let F be a totally real number field in which p is unramified. Let E be an elliptic curve over F with good supersingular reduction at some place $v \mid p$. Then*

$$\bar{\rho}_{E,p}|_{\mathrm{Gal}(\overline{F}/F(\sqrt{(-1)^{(p-1)/2}p}))}$$

is absolutely irreducible.

Proof. The presence of a non-trivial complex conjugation shows that irreducibility is the same as absolute irreducibility for odd $\mathrm{GL}_2(\mathbb{F}_p)$-valued representations of totally real fields. The lemma then follows easily when $p = 5$.

We now do $p = 3$. Suppose, for a contradiction, that the conclusion of the lemma fails. Let I_v be a decomposition group at v. Since the image $\bar{\rho}_{E,3}(I_v)$ is cyclic of order 8, it follows that the image $\bar{\rho}_{E,3}(\mathrm{Gal}(\overline{F}/F))$ is the full Sylow 2-subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$. Denoting by K the splitting field of $\bar{\rho}_{E,3}$, it follows that the image $\bar{\rho}_{E,3}(\mathrm{Gal}(K/F(\sqrt{-3})))$ is an abelian group of order 8.

The Sylow 2-subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$ is the group

$$\langle c, \tau \mid c^2 = \tau^8 = 1,\ c\tau = \tau^3 c\rangle,$$

and we may suppose that

$$c = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}.$$

Since the image of $\mathrm{Gal}(K/F(\sqrt{-3}))$ is in $\mathrm{SL}_2(\mathbb{F}_3)$, it must in fact be the subgroup generated by τ^2 and $c\tau$. This subgroup is non-abelian, giving the desired contradiction. □

The next two propositions prove modularity of many elliptic curves over certain totally real fields, using Theorem 7.1.

Proposition 9.2. *Let F be a totally real number field in which 3 is unramified, and let E be an elliptic curve over F with good supersingular reduction at primes above 3. Then E is modular.*

Proof. We proceed in several steps. By the result of Langlands and Tunnell, we know that $\bar{\rho}_{E,3}$ is modular. However, in order to apply Theorem 7.1 we need to produce a modular lift with level coprime to 3.

Step I: By Langlands' cyclic base change, we need only prove the result over a totally real soluble extension. In particular, making an appropriate base change if necessary, we can assume that $\bar{\rho}_{E,3}|_{D_v}$ is trivial for any prime $v \mid 5$.

Step II: We can find an elliptic curve E' over F such that

- $\bar{\rho}_{E,3} \sim \bar{\rho}_{E',3}$,
- $\bar{\rho}_{E',5}$ has insoluble image,
- E' has good ordinary reduction at every prime above 5 and

$$\bar{\rho}_{E',5}|_{D_v} \cong \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \quad \text{for any } v \mid 5$$

  with distinct characters on the diagonal,
- E' has good reduction at primes above 3.

If we can show that E' is modular, then $\rho_{E',3}$ will be a modular lift of $\bar{\rho}_{E,3}$ of the 'right level'; we can then use Theorem 7.1 to conclude that $\rho_{E,3}$ is modular.

In order to show that E' is modular, we want to make use of its 5-adic representation and apply the results in [19]. For this, we need to produce a nearly ordinary modular lift of $\bar{\rho}_{E',5}$. Again, we can work over totally real soluble extensions.

Step III: We can assume that $\bar{\rho}_{E',5}$ is trivial when we restrict to primes above 3. We can then find a second elliptic curve E'' such that

- $\bar{\rho}_{E',5} \sim \bar{\rho}_{E'',5}$,
- $\bar{\rho}_{E'',3} : G_F \to \mathrm{GL}_2(\mathbb{F}_3)$ is surjective,
- E'' has split multiplicative reduction at every prime above 3 and

$$\bar{\rho}_{E'',3}|_{D_v} \cong \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \quad \text{for any } v \mid 3$$

  with distinct characters on the diagonal,
- E'' has good ordinary reduction at primes above 5.

By Theorem 7.1, E'' is modular.

Since $\rho_{E'',5}$ is a nearly ordinary modular lift, it follows that $\rho_{E',5}$ is modular. □

Proposition 9.3. *Let F be a totally real number field in which* 3 *and* 5 *are unramified. Let E be an elliptic curve over F with semistable reduction at primes above* 3 *and* 5. *Further, assume that E has good supersingular reduction at primes above* 5 *and that $\bar{\rho}_{E,5}|_{\mathrm{Gal}(\bar{F}/F(\sqrt{5}))}$ is irreducible. Then E is modular.*

Proof. Going up to a soluble totally real field (without changing ramification at 3 and 5) if necessary, we can assume that $\bar{\rho}_{E,5}|_{D_v}$ is trivial for places $v \mid 3$ where E has good reduction. Then using the twisted modular curve $X(E[5])_{/F}$, we can find an elliptic curve E'/F such that

- $\bar{\rho}_{E',5} \sim \bar{\rho}_{E,5}$,
- E' has the same reduction type as E at primes above 5,
- E' is a Tate curve at primes above 3, and
- $\bar{\rho}_{E',3} : G_F \to \mathrm{GL}_2(\mathbb{F}_3)$ is surjective.

It follows that $\rho_{E',3}$ is modular, and $\rho_{E',5}$ is a modular lift of $\bar{\rho}_{E,5}$ of the 'right level.' Therefore, using either Theorem 5.1 of [19] or Theorem 7.1 of this article, it follows that $\rho_{E,5}$ is modular. □

Having proven some results over general fields, we now specialise to the case $F = \mathbb{Q}(\sqrt{2})$, for which, as we shall see, there is also a version of the switch between 3 and 5 used by Wiles [24, §5]. In particular, this allows us to prove the modularity of all semistable elliptic curves over $\mathbb{Q}(\sqrt{2})$.

Proposition 9.4. *Let E be a semistable elliptic curve over $\mathbb{Q}(\sqrt{2})$. Let p be either* 3 *or* 5*. If $\bar{\rho}_{E,p}$ is irreducible, then*

$$\bar{\rho}_{E,p}|_{\mathrm{Gal}(\bar{F}/F(\sqrt{(-1)^{(p-1)/2}p}))}$$

is absolutely irreducible.

Proof. Suppose the proposition fails to hold. Then p does not divide the order of $\bar{\rho}_{E,p}(\mathrm{Gal}(\bar{F}/F))$, and so the semistability condition implies that $\bar{\rho}_{E,p}$ is unramified at primes not dividing p. Further, by Lemma 9.1, we see that E has good ordinary or multiplicative reduction at p. Therefore, we must have

$$\bar{\rho}_{E,p}|_{I_p} \sim \begin{pmatrix} \bar{\epsilon}_p & 0 \\ 0 & 1 \end{pmatrix}$$

where $\bar{\epsilon}_p$ is the mod p cyclotomic character. (Note also that 3 and 5 are inert in $\mathbb{Q}(\sqrt{2})$.)

Let K be the splitting field of $\bar{\rho}_{E,p}$, and let ζ_p be a primitive pth root of unity. Then K is an everywhere unramified abelian extension of $\mathbb{Q}(\sqrt{2}, \zeta_p)$. The class number of $\mathbb{Q}(\sqrt{2}, \zeta_p)$ is then checked to be equal to 1 for both $p = 3$ and $p = 5$ (we used PARI to verify this), giving the required contradiction. □

Proposition 9.5. *The modular curve $X_0(15)$ has exactly eight $\mathbb{Q}(\sqrt{2})$-rational points. Four of these are cusps. The remaining four are elliptic curves with additive reduction at* 5.

Proof. $X_0(15)$ is an elliptic curve, and, using Cremona's tables [4], we can find an explicit equation for it. The rank of $X_0(15)$ regarded as an elliptic curve over $\mathbb{Q}(\sqrt{2})$ is the sum of its rank over $\mathbb{Q}$ and the rank (over $\mathbb{Q}$) of its quadratic twist. An equation of $X_0(15)$ over $\mathbb{Q}$ is $y^2 + xy + y = x^3 + x^2 - 10x - 10$, and its quadratic twist over $(\sqrt{2})$ is $y^2 = x^3 + x^2 - 641x - 3105$, which is curve 960G3 in Cremona's tables. Both curves have rank 0 over $\mathbb{Q}$, and it follows that $X_0(15)$ has rank 0 over $\mathbb{Q}(\sqrt{2})$. Thus all of its points over $\mathbb{Q}(\sqrt{2})$ are torsion points, and we can count them by considering the number of points in various residue fields of $\mathbb{Q}(\sqrt{2})$ (as in [16, VII.3]). Note that 7 splits in $\mathbb{Q}(\sqrt{2})$, so $\mathbb{Q}(\sqrt{2})$ has a residue field isomorphic to $\mathbb{F}_7$. Now $X_0(15)$ has good reduction at the primes above 7, and $|X_0(15)(\mathbb{F}_7)| = 8$. By [16, VII.3.1(b)], we see that the size of the torsion group over $\mathbb{Q}(\sqrt{2})$ divides 8. However, we know that $X_0(15)$ has 8 points over $\mathbb{Q}$, all of which are torsion, and so these can be the only points on $X_0(15)$ defined over $\mathbb{Q}(\sqrt{2})$. Of these, 4 are cusps, and the remaining 4 correspond to elliptic curves over $\mathbb{Q}$ which have additive reduction at 5 (curves 50A1, 50A2, 50A3 and 50A4 in Cremona's tables). Since 5 is unramified in $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, these curves continue to have additive reduction at 5 over $\mathbb{Q}(\sqrt{2})$, and so are also not semistable. It follows that none of the $\mathbb{Q}(\sqrt{2})$-rational points on $X_0(15)$ correspond to semistable elliptic curves. □

Theorem 9.6. *Any semistable elliptic curve over $\mathbb{Q}(\sqrt{2})$ is modular.*

Proof. Let E be a semistable elliptic curve over $\mathbb{Q}(\sqrt{2})$. By Proposition 9.5, one of $\bar{\rho}_{E,3}$ or $\bar{\rho}_{E,5}$ will be absolutely irreducible. The case where $\bar{\rho}_{E,3}$ is absolutely irreducible and E has good ordinary reduction or multiplicative reduction at 3 follows from Theorem 5.1 of [19] (using Proposition 9.4 to check the hypothesis that $\bar{\rho}_{E,3}|_{\mathrm{Gal}(\bar{F}/F(\sqrt{-3}))}$ is absolutely irreducible). If $\bar{\rho}_{E,3}$ is absolutely irreducible and E has supersingular reduction, then the modularity of E follows from Proposition 9.2. Otherwise $\bar{\rho}_{E,5}$ is irreducible, and modularity follows by switching to an elliptic curve E' as in the proof of Proposition 9.3. By the previous argument, E' is modular, so that $\bar{\rho}_{E',5} \cong \bar{\rho}_{E,5}$ is modular. If E has good ordinary reduction or multiplicative reduction at 5, modularity follows from Theorem 5.1 of [19], again using Proposition 9.4 to check that the hypotheses of this theorem hold. Otherwise, E has good supersingular reduction at 5. As remarked at the end of Section 7, since 5 is unramified in $\mathbb{Q}(\sqrt{2})$, the Galois representation $\bar{\rho}_{E,5}$ has the form given in Theorem 7.1; this theorem now implies that E is modular, as required. □

Remark 9.7. In fact, $\mathbb{Q}(\sqrt{2})$ is not the only real quadratic field for which all the numerology is valid to deduce modularity. Indeed, let $F = \mathbb{Q}(\sqrt{17})$. Note that 3 and 5 are inert in F. Again using PARI, one can verify that the class numbers of $F(\zeta_3)$ and $F(\zeta_5)$ are both 1, so that the analogue of Proposition 9.4 will hold also for F. (We suspect that this might be the only other real quadratic field with this property.) Next, the quadratic twist of $X_0(15)$ to F is curve 4335D3 in Cremona's tables, which has rank 0 (and 4 points defined over $\mathbb{Q}$), so that $X_0(15)$ has rank 0 over F. We can count the $\mathbb{Q}(\sqrt{17})$-rational points by counting the points in residue fields of F whose characteristic is a prime of good reduction for $X_0(15)$. Since 13 and 43 both split in F, and $X_0(15)$ has 16 points in $\mathbb{F}_{13}$ and 40 points in $\mathbb{F}_{43}$, we see that the size of the torsion group of $X_0(15)$ over F divides 8. Now one argues as in the case of $\mathbb{Q}(\sqrt{2})$ to see that all semistable elliptic curves over $\mathbb{Q}(\sqrt{17})$ are modular.

Acknowledgments

The authors thank the EPSRC for its support by means of a Research Grant from 2001–2003, when this work was done.

References

[1] H. Carayol, Sur les représentations ℓ-adiques associées aux formes modulaires de Hilbert, Ann. Sci. École Norm. Sup. 19 (1986) 409–468.

[2] B. Conrad, Finite group schemes over bases with low ramification, Compos. Math. 119 (1999) 239–320.

[3] B. Conrad, Ramified deformation problems, Duke Math. J. 97 (1999) 439–513.

[4] J. Cremona, Algorithms for Modular Elliptic Curves, second ed., Cambridge Univ. Press, Cambridge, 1997.

[5] H. Darmon, F. Diamond, R. Taylor, Fermat's Last Theorem, in: Elliptic Curves, Modular Forms and Fermat's Last Theorem, International Press, Cambridge, MA, 1997, pp. 2–140.

[6] F. Diamond, The Taylor–Wiles construction and multiplicity one, Invent. Math. 128 (1997) 379–391.

[7] L. Dieulefait, J. Manoharmayum, Modularity of rigid Calabi–Yau threefolds over $\mathbb{Q}$, in: Calabi–Yau Varieties and Mirror Symmetry, Toronto, 2001, in: Fields Inst. Commun., vol. 38, Amer. Math. Soc., Providence, RI, 2003, pp. 159–166.

[8] N. Elkies, The Klein quartic in Number Theory, in: The Eightfold Way, in: Math. Sci. Res. Inst. Publ., vol. 35, Cambridge Univ. Press, Cambridge, 1999.

[9] K. Fujiwara, Deformation rings and Hecke algebras in the totally real case, preprint, 1996, revised 2004, 2006.

[10] F. Jarvis, P. Meekin, The Fermat equation over $\mathbb{Q}(\sqrt{2})$, J. Number Theory 109 (2004) 182–196.

[11] M. Kisin, Moduli of finite flat group schemes and modularity, Ann. of Math., in press.

[12] M. Kisin, Modularity of some geometric Galois representations, in: Proceedings of L-functions and Galois representations, Durham 2004, in press.

[13] J. Manoharmayum, On the modularity of certain $\mathrm{GL}_2(\mathbb{F}_7)$ Galois representations, Math. Res. Lett. 8 (2001) 703–712.

[14] J. Neukirch, A. Schmidt, K. Wingberg, Cohomology of Number Fields, Grundlehren Math. Wiss., vol. 323, Springer, 2000.

[15] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. 15 (1972) 259–331.

[16] J. Silverman, The Arithmetic of Elliptic Curves, Grad. Texts in Math., vol. 106, Springer, 1986.

[17] C. Skinner, A. Wiles, Residually reducible representations and modular forms, Publ. Math. Inst. Hautes Études Sci. 89 (2000) 5–126.

[18] C. Skinner, A. Wiles, Base change and a problem of Serre, Duke Math. J. 107 (2001) 15–25.

[19] C. Skinner, A. Wiles, Nearly ordinary deformations of irreducible residual representations, Ann. Fac. Sci. Toulouse Math. (6) 10 (2001) 185–215.

[20] R. Taylor, On Galois representations associated to Hilbert modular forms, Invent. Math. 98 (1989) 265–280.

[21] R. Taylor, On icosahedral Artin representations II, Amer. J. Math. 125 (2003) 549–566.

[22] R. Taylor, On the meromorphic continuation of degree two L-functions, Doc. Math. Extra Vol. (2006) 729–779.

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

[24] A. Wiles, Modular elliptic curves and Fermat's Last Theorem, Ann. of Math. 141 (1995) 443–551.