Mathematical Research Letters **8**, 703–712 (2001)

ON THE MODULARITY OF CERTAIN $GL_2(\mathbb{F}_7)$ GALOIS REPRESENTATIONS

J. Manoharmayum

1. Introduction

Let ℓ be a prime, $\overline{\mathbb{F}_\ell}$ an algebraic closure of the finite field with ℓ elements and let

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

be a continuous, irreducible, odd representation. Here, odd means that the image of (a choice of) complex conjugation has distinct eigen-values. Then Serre's conjecture (see [Ser]) asserts that such a representation is modular—that is, there is a newform f of some level, weight and character such that the reduction mod-ℓ of the ℓ-adic representation associated to f is equivalent to $\overline{\rho}$. Serre's conjecture further predicts what the level, weight and character can be taken as. For details, see [Dia] and the references there.

In [Tay], R. Taylor proves the modularity of certain icosahedral representations by working over a soluble extension. Along similar lines, we establish in this article the modularity of certain representations of the absolute Galois group of $\mathbb{Q}$ into $GL_2(\mathbb{F}_7)$. More precisely, we show the following:

Theorem 1.1. *Let*

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

be a continuous, absolutely irreducible odd representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. *Let* χ *be its determinant. Further, assume the following:*

- *The projective image of the inertia group at* 3 *has odd order.*
- *The image of* $\overline{\rho}$ *restricted to the inertia group at* 7 *(for a choice of decomposition group at* 7*) is contained in a Borel subgroup of* $GL_2(\mathbb{F}_7)$.
- *The order of* χ *restricted to the inertia group at* 7 *is even.*

Then $\overline{\rho}$ *is modular.*

We highlight the following case as a corollary:

Corollary 1.2. *Let*

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

be a continuous, absolutely irreducible representation with determinant the cyclotomic character. Suppose further that

Received January 23, 2001.
Revised version received August 29, 2001.

- *the projective image of inertia at* 3 *has odd order, and*
- *the action of the decomposition group at* 7 *on the underlying vector space has a one dimensional invariant subspace.*

Then $\overline{\rho}$ *is modular.*

We now fix some notation. For a number field F and a place v of F, we denote by F_v the v-adic completion of F and we denote the decomposition group at v by D_v. We fix embeddings $\overline{\mathbb{Q}} \longrightarrow \overline{\mathbb{Q}_p}$ for every place p of $\mathbb{Q}$. Given an embedding of a number field F in $\overline{\mathbb{Q}}$, and a place v of F dividing a rational prime p, we then get an identification of D_v with $\mathrm{Gal}(\overline{\mathrm{Q_p}}/\mathrm{F_v})$. We denote by I_v the inertia subgroup of D_v. For a rational finite prime ℓ, we write ϵ_ℓ for the ℓ-adic cyclotomic character. We denote the mod-ℓ cyclotomic character by ω_ℓ. (That is, we take ω_ℓ to be the reduction modulo ℓ of ϵ_ℓ. In [Tay], ω_ℓ is taken to be the Teichmüller lift of $\epsilon_\ell (\mathrm{mod}\ \ell)$.) Given an elliptic curve E over a field K, we write $\rho_{E,\ell}$ (respectively, $\overline{\rho_{E,\ell}}$) for the usual representation of $\mathrm{Gal}(\overline{\mathrm{K}}/\mathrm{K})$ attached to ℓ-power torsion points (respectively, the ℓ-torsion points) of E.

2. A result of Skinner and Wiles

In this section, we describe a very important result of Skinner and Wiles (theorem 5.1 of [S-W]) which is a key ingredient to our argument. We have done so because the paper in its preprint form does not seem to be widely available.

I have taken the liberty of rephrasing the result so as to suit our need better. Let F be a totally real extension of $\mathbb{Q}$, and let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbb{Q}_p$ where p is an odd prime. Suppose we are given two continuous representations

$$\rho_1,\ \rho_2 : \mathrm{Gal}(\overline{\mathrm{F}}/\mathrm{F}) \longrightarrow \mathrm{GL}_2(\mathcal{O})$$

such that:

- (i) The residual representations are absolutely irreducible and isomorphic.
- (ii) The representations are unramified almost everywhere, and the determinant of any choice of complex conjugation is -1.
- (iii) The determinants of ρ_1 and ρ_2 are both equal to the p-adic cyclotomic character times a finite order character.
- (iv) For every place v above p, the restriction

$$\rho_i|_{D_v} \sim \begin{pmatrix} * & * \\ 0 & \delta_v^{(i)} \end{pmatrix},\ i = 1, 2$$

with $\delta_v^{(i)}$ finitely ramified; and, the reductions (modulo maximal ideal) of the characters $\delta_v^{(1)}$ and $\delta_v^{(2)}$ are the same.

We then have the following:

Theorem 2.1. *(theorem 5.1 in* [S-W]*): Suppose the residual representation has the property that the restriction to the decomposition group at a place above* p *has distinct diagonal characters. Then if* ρ_1 *is modular, so is* ρ_2*.*

Remarks.

- (a) The meaning of modularity in the statement is that they are associated to automorphic representations of $GL_{2,F}$.
- (b) If E is an elliptic curve over F which has potentially good ordinary reduction or potentially multiplicative reduction at every place of F above p, then the p-adic representation $\rho_{E,p}$ satisfies the properties (ii) to (iv) listed above.

3. Key proposition

The theorem follows from the following proposition.

Proposition: Let

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

be a continuous, absolutely irreducible, odd representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with determinant χ satisfying the hypotheses of the theorem. Further, assume that

$$\overline{\rho}|_{D_7} \sim \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}.$$

Then there is a totally real, finite extension F of $\mathbb{Q}$ and an elliptic curve E over F having the following properties:

- (i) The two representations of the absolute Galois group G_F of F given by $\overline{\rho_{E,7}}$ and the restriction of $\overline{\rho}$ to G_F are equivalent.
- (ii) E has good ordinary reduction at every prime of F above 3. If $\overline{\rho}|_{I_7}$ is split, then E has good ordinary reduction at every prime of F above 7. If $\overline{\rho}|_{I_7}$ is non-split, then E has potentially multiplicative reduction at every prime of F above 7.
- (iii) The mod-3 representation $\overline{\rho_{E,3}} \ : \ G_F \longrightarrow GL_2(\mathbb{F}_3)$ is surjective.
- (iv) If v is a place of F dividing 3, then

  $$\overline{\rho_{E,3}}|_{D_v} \sim \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$$

  with distinct characters on the diagonal.
- (v) If v is a place of F dividing 7, then

  $$\overline{\rho_{E,7}}|_{I_v} \sim \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$$

  with distinct characters on the diagonal.
- (vi) The extension $\mathbb{Q} \subset F$ has a filtration by cyclic extensions.

The deduction of the theorem given the above proposition is exactly the same as in [Tay]. The crucial ingredients are the lifting results of R. Ramakrishna (see [Ram]), the results of [S-W] and a descent argument of C. Khare (see [Kha]). Nonetheless, we give a brief summary.

Let

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

be a continuous, absolutely irreducible, odd representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ satisfying the hypotheses of the theorem. Twisting by a character, we can assume that

$$\overline{\rho}|_{D_7} \sim \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}.$$

Now let E and F be the elliptic curve and the totally real field given by the proposition above. Note that $\overline{\rho}$ is still absolutely irreducible over F. First, one deduces that $\rho_{E,3}$ is automorphic from properties (ii), (iii) and (iv) by using the results of Langlands and Tunnel, and theorem 5.1 of [S-W] (see Theorem 2.4 of [Tay]). From this, it follows that $\rho_{E,7}$ is automorphic.

For a prime v of F above 7, one can deduce using property (v) that $\overline{\rho_{E,7}}|_{I_v}$ is split if and only if $\overline{\rho}|_{D_7}$ is split. We now claim that

$$\rho_{E,7}|_{D_v} \sim \begin{pmatrix} * & * \\ 0 & \delta_v \end{pmatrix}$$

with δ_v unramified. In the split case, this follows because E has good ordinary reduction. In the non-split case, the claim follows because the underlying vector space for the representation $\overline{\rho_{E,7}}$ has a unique one-dimensional quotient on which D_v acts trivially.

Using results of [Ram] (see also [Tay]), one deduces the existence of a lift

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

of $\overline{\rho}$ having the following properties:

- $\rho(\mathrm{mod}\ 7) \ \sim \ \overline{\rho}$,
- ρ has determinant the cyclotomic character ϵ_7 times a finite order character, and
- the restriction of ρ to a decomposition group at 7 is of the form

$$\begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}$$

  with χ_2 unramified.

We can now apply theorem 5.1 of [S-W] to deduce that $\rho|_{G_F}$ is automorphic. Further, the modular form associated to ρ is invariant under Galois action. Using cyclic base change results of Langlands, one then deduces that ρ is automorphic—and hence the theorem (see [Kha], and also [Tay]).

4. Twists of modular curves

In this section, we let

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

be a continuous representation with determinant the mod-7 cyclotomic character ω_7. We begin by describing how one attaches to $\overline{\rho}$ a Galois twist of $X(7)$ (the modular curve with full level 7-structure). We refer to [Elk] for details of the various geometric properties of $X(7)$.

We shall think of $\overline{\rho}$ as a 2-dimensional $\mathbb{F}_7$ vector space scheme $\mathcal{W}$ defined over $\mathbb{Q}$ together with a perfect alternating pairing $\mathcal{W} \times \mathcal{W} \longrightarrow \boldsymbol{\mu}_7$ where $\boldsymbol{\mu}_7$ is the group scheme of seventh roots of unity. One then has a fine moduli space classifying pairs $(E, i)/S$ where E is an elliptic curve over S and i is a symplectic isomorphism from $\mathcal{W}/S$ to $E[7]/S$ (here $E[7]$ is the kernel of multiplication by 7 and the alternating pairing on $E[7]$ is the Tate pairing). We denote by $Y(\overline{\rho})$ the resulting fine moduli space, and write $X(\overline{\rho})$ for its compactification (this also has a moduli interpretation in terms of generalised elliptic curves). We note that the construction can be carried out over $\mathbb{Z}[1/N]$ where N is the product of primes where $\overline{\rho}$ is ramified.

The curve $X(\overline{\rho})$ is a smooth non-hyperelliptic curve of genus 3, and is a Hurwitz curve. The canonical divisor embeds $X(\overline{\rho})$ as a smooth quartic in $\mathbb{P}^2$. Further, every automorphism of $X(\overline{\rho})$ comes from an automorphism of $\mathbb{P}^2$ (under the canonical embedding). For the vector space scheme $\mathcal{W} = \boldsymbol{\mu}_7 \times \mathbb{Z}/7\mathbb{Z}$ with pairing given by, say,

$$(\zeta^{a_1}, b_1) \times (\zeta^{a_2}, b_2) \longrightarrow \frac{\zeta^{a_1 b_2}}{\zeta^{a_2 b_1}}$$

where ζ is a fixed primitive seventh root of unity, the corresponding quartic is the Klein quartic $x^3y + y^3z + z^3x = 0$. One has a morphism $j : X(\overline{\rho}) \to_{/\mathbb{Q}} \mathbb{P}^1$ of degree 168 which is given by the j-invariant (and we think of the $\mathbb{P}^1$ as the j-line). The ramification points of j correspond to the cusps and elliptic curves with j-invariants 0 and 1728. The cusps are the points of inflexion (and every tangent at a cusp has multiplicity 3). The elliptic curves with j-invariant 0 are the points which are cut out by bitangents.

Let us denote by $\mathcal{K}$ the proper scheme over $\mathbb{Z}$ defined by the Klein quartic $x^3y+y^3z+z^3x$. Note that the special fibre of $\mathcal{K}$ is geometrically irreducible—this can be seen, for example, by setting $z = 1$ and viewing the resulting polynomial as a polynomial over $\mathbb{F}_7[x]$ and then applying Eisenstein's criterion. I am grateful to the referee for pointing out the following:

Lemma 4.1. *For a prime p, there is a finite subset of $\mathcal{K}_{/\overline{\mathbb{F}_p}}(\overline{\mathbb{F}_p})$ such that the following is true: Let P be a point on the generic fibre defined over a finite extension K of $\mathbb{Q}_p$ and let E be the elliptic curve, defined over K, corresponding to P (via pull-back of the universal elliptic curve). If the reduction mod p of P, which is possible by properness, is not in the finite subset then E has good ordinary reduction.*

Proof. Both $\mathcal{K}$ and $X(7)$ are smooth and proper over $\mathrm{Spec}(\mathbb{Z}[1/7])$, and hence they are isomorphic over $\mathrm{Spec}(\mathbb{Z}[1/7])$. The lemma follows in this case as there only finitely many supersingular and degenerate elliptic curves over $\overline{\mathbb{F}_p}$.

For the prime 7, we use an argument based on a suggestion by the referee (and which works in the other cases as well). Let

$$\Phi_6 = xy^5 + yz^5 + zx^5 - 5x^2y^2z^2$$

and

$$\Phi_{14} = \sum\nolimits_c (x^{14} - 34x^{11}y^2z - 250x^9yz^4 + 375x^8y^4z^2 + 18x^7y^7 - 126x^6y^3z^5)$$

be the polynomials given in 1.13 and 1.17 of [Elk] (the subscript c indicates sum over cyclic permutations). Define a rational map $\phi : \mathcal{K}- \to \mathbb{P}^1$ over $\mathrm{Spec}(\mathbb{Z}_7)$ by sending $(x : y : z)$ to $(\Phi_{14}^3 : \Phi_6^7)$. The fact that this is well defined follows from the calculations in [Elk]. In particular, equation 2.13 of [Elk] shows that the map ϕ on the generic fibre is precisely the j-invariant map.

We claim that ϕ is a morphism outside a finite set of closed points of dimension zero (i.e. a finite set of points on the special fibre). This will be so if we can show that $\mathcal{K}$ is regular in codimension 1 (see corollaire 8.2.12 of [EGA]). Using theorem 20.2 of [Mat], we see that the ring $\mathbb{Z}_7[x, y, z]/(x^3y+y^3z+z^3x)$ is a unique factorisation domain—and this establishes regularity in codimension one.

We now check that ϕ gives a non-constant rational map on the special fibre. Now Φ_6 is irreducible over $\mathbb{F}_7$. (This can be seen, as in the case of $x^3y + y^3z + z^3x$, by setting $z = 1$ and working over $\mathbb{F}_7[y]$.) Thus it suffices to check that $x^3y + y^3z + z^3x$ does not divide Φ_6 or Φ_{14}, and that Φ_6 does not divide Φ_{14}. These follow because Φ_6 modulo z is xy^5, and Φ_{14} modulo z is $x^{14}+y^{14}+18x^7y^7$.

It now follows that ϕ is generically finite on the special fibre. We can thus claim that the set of points on the special fibre of $\mathcal{K}$ consisting of points where ϕ is not defined and inverse images of a finite number of points on the special fibre of $\mathbb{P}^1$ is a finite set. Again using the fact that there are only finitely many supersingular j-invariants over $\overline{\mathbb{F}_7}$, we can choose a finite set of points on the special fibre of $\mathcal{K}$ such that for any point on the generic fibre whose reduction is outside this set, the corresponding elliptic curve has integral j-invariant and the reduction mod 7 of the j-invariant does not correspond to a supersingular j-invariant.

We now introduce a model $\mathcal{V}$ of $X_1(7)$ over $\mathbb{Z}_7$: namely, we take $\mathcal{V}$ to be $\mathbb{P}^1$ with the 'elliptic curve with points of order 7' at $(a : b)$ being given by

$$u^2 + (1 + t - t^2)uv + (t^2 - t^3)u = v^3 + (t^2 - t^3)v^2$$

where $t = a/b$ (see example 13.4 of [Sil]). This has discriminant $t^7(1 - t)^7(t^3 - 8t^2 + 5t + 1)$. Thus we can find finitely many closed points on the special fibre of $\mathcal{V}$ such that a point on the generic fibre whose reduction is not on this finite set gives an elliptic curve with good reduction.

We thus have a rational map $\psi : \mathcal{K}- \to \mathcal{V}$ which is defined over $\mathbb{Z}_7$ and extending the 'natural forgetful' map from $X(7)$ to $X_1(7)$, and defined outside finitely many closed points (since $\mathcal{K}$ is regular in codimension one, we can use corollaire 8.2.12 of [EGA]). Further, ψ is generically finite on the special fibre because ϕ factors through ψ. The lemma now follows. □

5. Proof of the proposition

Let

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

be an absolutely irreducible, continuous, odd representation with determinant χ and satisfying the hypotheses of the proposition. Observe that χ restricted to the unique cyclic degree three extension of $\mathbb{Q}_7^{\mathrm{nr}}$ is the mod 7 cyclotomic character. An outline of the constructions we will be carrying out is as follows. At each step, we will need to keep track of ramification indices at primes above 3 and 7.

- F_0 will be an extension over which the representation has cyclotomic determinant, and is 'nice' at primes above 7. This allows us to introduce a quartic curve in $\mathbb{P}^2$.
- F_1 will be an extension such that for the completion at a prime of interest, we can find points on the curve which lie on a line having some specific properties. These lines will then be approximated by a line defined over F_1.
- F will be the extension of F_1 generated by the points of intersection, and these will give the elliptic curves we want.

Now for the constructions in detail. Let F_0 be the splitting field of $\chi\omega_7^{-1}$ adjoined $\zeta+\zeta^{-1}$ where ζ is a non-trivial seventh root of unity. Note that F_0 is a totally real, abelian extension of $\mathbb{Q}$ and has odd inertial index at 3 and inertial index 3 at 7. Further, $\overline{\rho}$ restricted to F_0 has determinant the mod-7 cyclotomic character, and hence

$$\overline{\rho}|_{D_v} \sim \begin{pmatrix} \omega_7 & * \\ 0 & 1 \end{pmatrix}$$

for any place v of F_0 over 7. Further, these will still be non-split if $\overline{\rho}|_{I_7}$ is non-split. We denote $X(\overline{\rho}|_{G_{F_0}})$ simply by X and fix throughout a model in $\mathbb{P}^2_{/F_0}$.

For each prime v of F_0 dividing 3, let K'_v be the splitting field of $\overline{\rho}|_{D_v}$, and let k'_v be its residue field. We may assume that our model for X is the Klein quartic $x^3y+y^3z+z^3x=0$ in $\mathbb{P}^2$ over K'_v. (Strictly speaking, our model is only isomorphic to the Klein quartic via an element of $PGL_3(K'_v)$.) Our objective is to find a line which cuts X at four distinct points corresponding to elliptic curves with good ordinary reduction.

We can find a line $\overline{L_v}$ defined over some finite extension k_v of k'_v intersecting X at four distinct points which are not in the finite sets given by the lemma in section 4, and these points can be assumed defined over k_v. Now let K_v be the finite unramified extension of K'_v with residue field k_v, and let L_v be a line defined over K_v which reduces to $\overline{L_v}$. It now follows that L_v intersects X at four distinct points corresponding to four elliptic curves defined over K_v with good ordinary reduction. Since the ramification index of K_v is odd, we conclude that $\sqrt{-3}$ is not in K_v.

We now turn to primes w of F_0 above 7. Suppose first that the representation restricted to inertia at 7 is split. Our model for X will no longer have good reduction at w, but thanks to the lemma in section 4, we can still find a finite unramified extension of $F_{0,w}$ and a line defined over it which intersects X at four distinct points, all defined over the extension, and corresponding to elliptic curves with good ordinary reduction. This can be done, for example, by taking

a line which cuts the special fibre of the Klein model at four distinct points and then lifting it.

Suppose now that the restriction restricted to inertia at 7 is non-split. In this case, we assume the following:

For each prime w of F_0 above 7, there is a finite Galois extension of $F_{0,w}$ of odd inertial index and a line defined over it which intersects X at four distinct points, all defined over this extension, corresponding to elliptic curves with potentially multiplicative reduction.

We shall establish the validity of this assumption in the next section.

We take K_w to be the Galois extension of $F_{0,w}$ and L_w to be the line thus obtained. Then L_w intersects X at four distinct points corresponding to elliptic curves with good ordinary reduction or potentially multiplicative reduction, and these points are defined over K_w. Note that, by our construction, the ramification index of K_w is still odd.

For each infinite place ∞ of F_0, we can assume that our model for X is the Klein quartic $x^3y + y^3z + z^3x = 0$. One can check that the line $L_\infty := \{(-3x : y : x)\}$ intersects X at four distinct real points.

Let F_1 be a totally real, soluble extension of F_0 such that

- $F_{1,v'}$ is isomorphic to K_v for every place v' of F_1 dividing v, with v place of F_0 dividing 3, and
- $F_{1,w'}$ is isomorphic to K_w for every place w' of F_1 dividing w with w a place of F_0 dividing 7.

For the existence of such an extension, see lemma 2.2 of [Tay]. Since the space of lines in $\mathbb{P}^2$ is a rational variety, we can take a line L over F_1 which is close enough to L_v, L_w and L_∞ for every place v', w' as in the previous paragraph and every infinite place respectively (with corresponding topologies) such that the following holds.

Let F' be the extension of F_1 generated by the points of intersection of L with X, and let F to be the Galois closure of F' over F_0. Take E to be the elliptic curve given by one of the points of intersection of L with X. Then we can guarantee:

- F is totally real, and any prime of F_1 above 3 and 7 splits completely in F.
- E satisfies properties (i) and (ii) of the proposition.
- $\overline{\rho_{E,3}}$ is surjective (using Hilbert irreducibility).

The extension $F_1 \subset F$ is soluble because the Galois closure of F' over F_1 has as Galois group a subgroup of the symmetric group on four letters. Since K_v does not contain $\sqrt{-3}$, property (iv) follows. Property (v) follows because the ramification index of F over $\mathbb{Q}$ at 7 is still odd. □

6. Some mod 7 representations of 7-adic fields

In this section, we let K be a finite extension of $\mathbb{Q}_7$, and let

$$\overline{\rho} : G_K \longrightarrow \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$$

be a $GL_2(\mathbb{F}_7)$ repesentation of G_K, the absolute Galois group of K, with determinant given by the cyclotomic character. Recall that once we fix an identification of the determinant with the cyclotomic character, we can define the modular curves $X(\overline{\rho})$. Further, fixing such an identification is the same as fixing a primitive seventh root of unity; once we have done that, we can think of the non-diagonal entry as a cocycle in $H^1(G_K, \boldsymbol{\mu}_7)$.

Proposition 6.1. *Fix an identification of the determinant with the cyclotomic character and let $X(\overline{\rho})$ in $\mathbb{P}^2_{/K}$ be the canonical model. We can then find a line L over K with the following properties:*

- *L intersects $X(\overline{\rho})$ in four distinct points defined over a Galois extension with odd inertial index.*
- *The elliptic curves corresponding to the intersection points all have potentially multiplicative reduction.*

Proof. Using the canonical identification of $K^\times/K^{\times 7}$ with $H^1(G_K, \boldsymbol{\mu}_7)$, one deduces the existence of a Tate curve over K having Tate parameter q which gives a K-rational point on $X(\overline{\rho})$. The Tate curves with Tate parameters $7^{7n}q$ will then also give K-rational points, and their j-invariants tend to ∞. Using a compactness argument, we conclude that has $X(\overline{\rho})$ a K-rational cusp.

So now let $X(\overline{\rho})$ be the model in $\mathbb{P}^2_{/K}$ with a K-rational cusp. From the geometry of the Klein curve, the process of taking tangents at cusps yields the following:

- $X(\overline{\rho})$ has three K-rational cusps.
- Under a linear change of coordinates, we can assume that the three cusps are $(1:0:0)$, $(0:1:0)$ and $(0:0:1)$; and, we can assume that $x = 0$ is the tangent (with multiplicity 3) at $(0:0:1)$ and passes through $(0:1:0)$, and so on (i.e. the same with cyclic permutations).

We can thus assume, possibly after scaling, that the defining equation for $X(\overline{\rho})$ is given by $x^3y + y^3z + az^3x = 0$, where a is a non-zero element of the ring of integers of K. It is clear that a line sufficiently close to one of the above tangents will give elliptic curves with potentially multiplicative reduction. But the ramification index of the field over which they are defined might be even—although one of them will certainly be defined over K. We get around this by an explicit calculation.

We work in affine coordinates by setting $z = 1$. Now $x = 0$ is the tangent at $(0, 0)$. We now look at the points of intersection of $x = b$ with $X(\overline{\rho})$, where b is very small. These are given by the roots of $y^3 + b^3y + ab = 0$. Denoting the normalized valuation on K by v, we see that for b sufficiently small with $v(ab)$

not divisible by 3 and $v(b^3) > v(ab)$, the polynomial $y^3 + b^3y + ab$ is irreducible over K. Hence the points of intersection are defined over a Galois extension of K with Galois group a transitive subgroup S_3. Such an extension necessarily has odd inertial index (in fact 1 or 3). This shows the proposition, except for the (inconsequential) fact that we only get three genuine elliptic curves. This is easily removed by a further approximation. □

Acknowledgement

I would like to thank Gebhard Böckle and Chandrashekhar Khare for useful discussions; and thanks also to the referee for his many helpful comments and observations.

References

[Dia] F. Diamond, *The refined conjecture of Serre.* Modular forms, elliptic curves and Fermat's Last Theorem (Hong Kong, 1993), 22–37, Ser. Number Theory, I, Internat. Press, Cambridge MA, 1995.

[EGA] A. Grothendieck and J. A. Dieudonné, *Eléments de Géométrie Algébrique, I: Le langage des schemas,* second edition, 4–18, Springer, Berlin, 1971.

[Elk] N. Elkies, *The Klein quartic in Number Theory*, The eight fold way, 51–101, Math. Sci. Res. Inst. Publ., 35, Cambridge Univ. Press, Cambridge, 1999.

[Kha] C. Khare, *Mod p descent for Hilbert modular forms*, Math. Res. Lett. 7 (2000), no. 4, 455–462.

[Mat] H. Matsumura, *Commutative ring theory.* Cambridge Studies in Advanced Mathematics, 8. Cambridge University Press, 1986.

[Ram] R. Ramakrishna, *Deforming Galois representations and the conjectures of Serre and Fontaine-Mazur,* preprint.

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

[Sil] J. H. Silverman, *The arithmetic of elliptic curves.* Graduate Texts in Mathematics, 106. Springer-Verlag, New York, 1986.

[S-W] C. Skinner and A. Wiles, *Nearly ordinary deformations of irreducible residual representations,* to appear in Ann. Fac. Sci. Toulouse Math. (6).

[Tay] R. Taylor, *On icosahedral Artin representations II,* preprint, available at `http://www.math.harvard.edu/~rtaylor`

Department Mathematik, ETH-Zürich, Rämistrasse, 101 8092 Zürich, Switzerland.
E-mail address: `j.manoharmayum@sheffield.ac.uk`