On the modularity of $\mathbb{Q}$-curves

Jordan S. Ellenberg and Chris Skinner

12 Apr 2000

Abstract

A $\mathbb{Q}$-curve is an elliptic curve over a number field K which is geometrically isogenous to each of its Galois conjugates. Ribet [16] asked whether every $\mathbb{Q}$-curve is modular, and showed that a positive answer would follow from Serre's conjecture on mod p Galois representations. We answer Ribet's question in the affirmative, subject to certain local conditions at 3.

MSC classification: 11G18 (14G35,14H52)

1 Introduction

Let K be a number field, Galois over $\mathbb{Q}$. A $\mathbb{Q}$-*curve* over K is an elliptic curve E/K which is isogenous over K to each of its Galois conjugates. Our interest in $\mathbb{Q}$-curves is motivated by the following theorem of Ribet.

Theorem ([16, §5]). *Suppose $E/\bar{\mathbb{Q}}$ is an elliptic curve that is also a quotient of $J_1(N)/\bar{\mathbb{Q}}$. Then E is a $\mathbb{Q}$-curve over some number field.*

A $\mathbb{Q}$-curve which is a quotient of $J_1(N)/\bar{\mathbb{Q}}$ is called *modular*; Ribet has conjectured that in fact every $\mathbb{Q}$-curve is modular. The modularity of various $\mathbb{Q}$-curves has been verified by Roberts and Washington [17], by Hasegawa, Hashimoto, and Momose [11], and by Hida [12]. In this article we establish the modularity of a large class of $\mathbb{Q}$-curves, including infinitely many curves not treated in the aforementioned papers (but not including every curve treated there.)

Suppose E/K is a $\mathbb{Q}$-curve, and E^σ is a Galois conjugate of E. Then there exists a non-zero K-isogeny $\mu : E^\sigma \to E$, and so if p is a prime dividing the square-free part of the degree of μ then the $\mathrm{Gal}(\bar{K}/K)$ module $E[p]$ is reducible. The arguments employed in [11] and [12] use this reducibility to associate to E a p-adic representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ whose reduction mod p has dihedral image, and is therefore modular (in the sense that it arises from a modular form). Consequently, the results in [11] and [12] depend on the existence of a prime $p \geq 5$ dividing the square-free part of the degree of some K-rational isogeny between E and one of its Galois conjugates. Moreover, their results require E to satisfy certain local conditions at p.

In contrast, the arguments we employ in the present paper make use of the mod 3 and 3-adic representations attached to a $\mathbb{Q}$-curve. We thus obtain a theorem which does not require the existence of a rational isogeny of large degree (but which does require local conditions at 3.) This allows us, for instance, to prove the modularity of the $\mathbb{Q}$-curve

$$E = E_{A,B,C} : y^2 = x^3 + 2(1+i)Ax^2 + (B + iA^2)x \tag{1.1}$$

discussed by Darmon in [4] in connection with the generalized Fermat equation

$$A^4 + B^2 = C^p. \tag{1.2}$$

We will discuss in a later paper the consequences of the present result regarding solutions of (1.2).

In order to state the main theorems of this paper we introduce a few definitions. Let E/K be a $\mathbb{Q}$-curve, and for each $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ let $\mu_\sigma : E^\sigma \to E$ be a non-zero isogeny. Then we define $b_E \in H^2(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \pm 1)$ by

$$b_E(\sigma, \tau) = \mathrm{sgn}(\mu_\sigma \mu_\tau^\sigma \mu_{\sigma\tau}^{-1}).$$

Denote by $(b_E)_3$ the restriction of b_E to $H^2(\mathrm{Gal}(\bar{\mathbb{Q}}_3/\mathbb{Q}_3), \pm 1)$. Furthermore, we associate to E an ℓ-adic Galois representation $\rho_{E,\ell}$ of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ and a quadratic character $\bar{\psi}_{E,3}$ of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ (cf. Proposition 2.3 and Definition 2.16).

Theorem. *Suppose E/K is a $\mathbb{Q}$-curve with potentially ordinary or multiplicative reduction at a prime of K over 3, and such that $(b_E)_3$ is trivial. Then E is modular.*

Theorem. *Suppose E/K is a $\mathbb{Q}$-curve such that, for some (whence every) prime $\ell > 3$, the projective representation $\mathbb{P}\rho_{E,\ell}$ associated to $\rho_{E,\ell}$ is unramified at 3. Then E is modular.*

We can weaken the condition on $\rho_{E,\ell}$ in the second theorem above, at the expense of introducing some technical conditions.

Denote by $q_{3,\infty}$ the unique class in $H^2(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \pm 1)$ ramified exactly at 3 and ∞. We prove the following theorem.

Theorem. *Suppose E/K is a $\mathbb{Q}$-curve which acquires semistable reduction over a field tamely ramified over $\mathbb{Q}_3$. Suppose further that $(b_E)_3$ is trivial, and that the four classes $(\bar{\psi}_{E,3}, -1)$, $b_E q_{3,\infty}(\bar{\psi}_{E,3}, -1)$, $q_{3,\infty}(\bar{\psi}_{E,3}, 3)$, and $b_E(\bar{\psi}_{E,3}, 3)$ are all nontrivial in $H^2(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \pm 1)$. Finally, suppose that $\deg \mu_\sigma$ can be chosen to be prime to 3 for all $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Then E is modular.*

We remark that the $\mathbb{Q}$-curve (1.1) satisfies the hypotheses of both the second and third theorems above.

There are infinitely many $\mathbb{Q}$-curves which are not proved to be modular by the theorems in this paper. An instructive example is the curve

$$\begin{aligned} E : y^2 \;\; = \;\; & x^3 + (-994708512\sqrt{5257}\sqrt{73} - 414461880\sqrt{5257} - 4973542560\sqrt{73} - 1089620282520)x \\ & +36601957546560\sqrt{5257}\sqrt{73} + 5349307626327168\sqrt{5257} \\ & +55021459817878848\sqrt{73} + 32065347994985088 \end{aligned} \tag{1.3}$$

which is the specialization to $a = 2^2 \cdot 3^2 \cdot 73$ of the family of $\mathbb{Q}$-curves described by Quer in [13, §6]. One checks that

- The reduction of E over 3 is potentially supersingular;
- $\mathbb{P}\rho_{E,\ell}$ is ramified at 3 (because $E/\mathbb{Q}(\sqrt{-2})$ does not have good reduction at 3);
- There is an isogeny of degree 3 between E and one of its Galois conjugates.

Thus, E does not satisfy the hypotheses of any of the theorems above. The 3-adic representation $\rho_{E,3}$ is residually irreducible, but the image of the restriction $\rho_{E,3}|G_3$ does not have trivial centralizer. To prove that such a representation is modular is beyond the reach of existing technology in deformation theory, including the recent result of Breuil, Conrad, Diamond, and Taylor.

The modularity of a $\mathbb{Q}$-curve E is equivalent to the modularity of any one of the $\rho_{E,\ell}$'s. (The modularity of the latter means that it is a representation associated to a modular form.) Most of the present paper is devoted to proving the modularity of the $\rho_{E,3}$'s. This is essentially done by showing that under the hypotheses stated in the theorem these representations satisfy the main theorems of either [2], [21], or [22].

The authors wish to thank Brian Conrad, Fred Diamond, Matthew Emerton, Jordi Quer, Ken Ribet, Richard Taylor, and Andrew Wiles for helpful discussions.

Some Notation

If K is a quadratic extension of $\mathbb{Q}$, we write χ_K for the quadratic character of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ associated to K. Any two quadratic characters χ and χ' of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ give classes in $H^1(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \pm 1)$. We write (χ, χ') for their cup product. This is an element in $H^2(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \pm 1)$. If d is an element of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, we write (χ, d) to mean the cup product $(\chi, \chi_{\mathbb{Q}(\sqrt{d})})$.

We write elements in $H^2(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \pm 1)$ multiplicatively. Thus if $c_1, c_2 \in H^2(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \pm 1)$, then $c_1 c_2$ is the class such that $(c_1 c_2)(\sigma, \tau) = c_1(\sigma, \tau) c_2(\sigma, \tau)$ for all $\sigma, \tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

We take an embedding $\nu : \bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_\ell$ to be fixed for each ℓ, and denote the resulting decomposition subgroup (resp. inertia subgroup) of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ by G_ℓ (resp. I_ℓ). To be completely precise, we need to define *two* such embeddings: one in order to define decomposition subgroups of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, and the other in order to make sense of the scalar action of $\bar{\mathbb{Q}}$ on ℓ-adic vector spaces like $T_\ell A \otimes_{\mathbb{Z}_\ell} \bar{\mathbb{Q}}_\ell$. Write $\iota : \bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_\ell$ for the second embedding. We may think of ν as fixed through the course of the paper; on the other hand, we will occasionally want to vary ι.

We also take an embedding $\bar{\mathbb{Q}} \hookrightarrow \mathbb{C}$ to be fixed. This determines a complex conjugation c.

We denote by $G_\ell^t, I_\ell^t, I_e ll^w$ the tame quotient of the decomposition group, the tame inertia group, and the wild inertia group respectively.

For ℓ a rational prime, we denote by $\chi_\ell : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{Z}_\ell^*$ the cyclotomic character, and by $\bar{\chi}_\ell : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_\ell^*$ the mod ℓ cyclotomic character. If $\rho : G \to \mathrm{GL}_2(F)$ is a representation of a group G over a field F, we write $\mathbb{P}\rho$ for the composition of ρ with the natural projection $\mathrm{GL}_2(F) \to \mathrm{PGL}_2(F)$.

2 $\mathbb{Q}$-curves and Galois representations

In this section we describe the ℓ-adic and mod ℓ Galois representations attached to a $\mathbb{Q}$-curve. We also define Galois cohomology classes c_E, b_E and $\bar{\psi}_{E,\ell}$ which are naturally attached to a $\mathbb{Q}$-curve E. The definitions and results of this section, with the exception of Proposition 2.13, are not original to this paper. The basic framework is laid down in Ribet's foundational paper [16]. The interested reader should also consult Quer's preprint [13], which alerted us to the relevance of the class b_E.

Let K be a number field Galois over $\mathbb{Q}$.

Definition 2.1. A $\mathbb{Q}$-*curve* E/K is an elliptic curve E/K, such that, for each $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, there exists a non-zero K-isogeny

$$\mu_\sigma : E^\sigma \to E.$$

We may, and do, suppose that μ_σ is the identity morphism for all $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/K)$.

Remark 2.2. Throughout this paper, it will be understood that all $\mathbb{Q}$-curves are elliptic curves *without complex multiplication.* This assumption is not restrictive from our point of view, since $\mathbb{Q}$-curves with complex multiplication are known to be modular [20].

Let ℓ be a rational prime, and define

$$\phi_{E,\ell} : \mathrm{Gal}(\bar{K}/K) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$$

to be the representation of $\mathrm{Gal}(\bar{K}/K)$ on the ℓ-adic Tate module $T_\ell E$ of E. (We have fixed an isomorphism $T_\ell E \cong \mathbb{Z}_\ell^2$.) In the following proposition we describe an extension of $\phi_{E,\ell}$ to a representation of the whole group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

Proposition 2.3. *There exists a representation*

$$\rho_{E,\ell} : G_\mathbb{Q} \to \bar{\mathbb{Q}}_\ell^* \, \mathrm{GL}_2(\mathbb{Q}_\ell)$$

such that $\mathbb{P}\rho_{E,\ell}|_{\mathrm{Gal}(\bar{K}/K)} \cong \mathbb{P}\phi_{E,\ell}$. *This representation is odd, continuous, and ramified at only finitely many primes.*

Proof. For each non-zero isogeny $\mu : E' \to E$, we write μ^{-1} to mean

$$(1/\deg \mu)\mu^\vee \in \mathrm{Hom}(E', E) \otimes_\mathbb{Z} \mathbb{Q},$$

where $\mu^\vee$ is the dual isogeny.

Let σ and τ be elements of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Following [16, §6], we define

$$c_E(\sigma, \tau) = \mu_\sigma \mu_\tau^\sigma \mu_{\sigma\tau}^{-1} \in (\mathrm{Hom}(E, E) \otimes_Z \mathbb{Q})^* = \mathbb{Q}^*.$$

Then c_E determines a class in $H^2(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \mathbb{Q}^*)$. Tate showed that $H^2(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \bar{\mathbb{Q}}^*)$ is trivial, where $\bar{\mathbb{Q}}^*$ is acted on trivially by $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$; [18, Thm. 4]. It follows that there exists a continuous map $\alpha : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \bar{\mathbb{Q}}^*$ such that

$$c_E(g, h) = \alpha(g)\alpha(h)\alpha(gh)^{-1} \tag{2.4}$$

We can now define an action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on $\bar{\mathbb{Q}}_\ell \otimes_{\mathbb{Z}_\ell} T_\ell E$ by

$$\rho_{E,\ell}(g)(1 \otimes x) = \alpha^{-1}(g) \otimes \mu_g(x^g). \tag{2.5}$$

It is clear from the above definition that $\mathbb{P}\rho_{E,\ell}|_{\mathrm{Gal}(\bar{K}/K)} \cong \mathbb{P}\phi_{E,\ell}$. In particular, $\rho_{E,\ell}|_{\mathrm{Gal}(\bar{K}/K)}$ and $\phi_{E,\ell}$ differ by the continuous character $\alpha|_{\mathrm{Gal}(\bar{K}/K)}$. It follows that $\rho_{E,\ell}$ is continous and unramified away from finitely many primes. It remains to show that $\rho_{E,\ell}$ is odd; that is, that $\det \rho_{E,\ell}(c) = -1$, where c is our fixed complex conjugation.

Define a map $\epsilon_E : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \bar{\mathbb{Q}}^*$ by

$$\epsilon_E(\sigma) = \alpha^2(\sigma)/(\deg \mu_\sigma),$$

and let $\epsilon_{E,\ell}$ be the composition of ϵ_E with the chosen embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_\ell$. That this map is a character follows from the observation that

$$c_E(\sigma, \tau)^2 = \frac{(\deg \mu_\sigma)(\deg \mu_\tau)}{\deg \mu_{\sigma\tau}}.$$

It also follows immediately from (2.5) that

$$\det \rho_{E,\ell} = \epsilon_{E,\ell}^{-1}\chi_\ell. \tag{2.6}$$

Write μ for μ_c. We may write the complexification $E/\mathbb{C}$ as the quotient of $\mathbb{C}$ by a lattice Λ. Then μ is given by multiplication by a complex number z such that $z\bar{\Lambda} \subset \Lambda$. The composition $\mu\mu^c$ is then given by zz^c, a positive real number. Since the degree of $\mu\mu^c$ is $(\deg \mu)^2$, we conclude that

$$\mu\mu^c = \deg \mu.$$

Therefore,

$$\epsilon_E(c) = \alpha^2(c)/\deg \mu = c_E(c,c)/\deg \mu = \mu\mu^c/\deg \mu = 1,$$

and

$$\det \rho_{E,\ell}(c) = \epsilon_{E,\ell}(c)\chi_\ell(c) = -1.$$

Since $\alpha^2(c) = c_E(c,c) = \mu\mu^c = \deg \mu$, the proposition follows from the definition of $\epsilon_{E,\ell}$ and (2.6). □

Remark 2.4. It will occasionally be useful to work directly with the homomorphism

$$\hat{\rho}_{E,\ell} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \bar{\mathbb{Q}}^* \,\mathrm{GL}_2(\mathbb{Q}_\ell)$$

defined by (2.5). More precisely: suppose M is a number field such that $\hat{\rho}_{E,\ell}$ takes values in $M^* \,\mathrm{GL}_2(\mathbb{Q}_\ell)$. Let λ be the prime of M defined by $\iota : \bar{\mathbb{Q}} \to \bar{\mathbb{Q}}_\ell$, and let $\lambda = \lambda_1, \ldots, \lambda_r$ be the set of all primes of M dividing ℓ. Write ρ_{E,λ_i} for the composition of $\hat{\rho}_{E,\ell}$ with the map

$$M^* \,\mathrm{GL}_2(\mathbb{Q}_\ell) \to M^*_{\lambda_i} \,\mathrm{GL}_2(\mathbb{Q}_\ell).$$

So $\rho_{E,\lambda}$ is just another name for $\rho_{E,\ell}$.

Remark 2.5. While $\rho_{E,\ell}$ and ϵ_E depend on our choice of α, the projective representation $\mathbb{P}\rho_{E,\ell}$ depends only on the isomorphism class of E/K. Moreover, $\mathbb{P}\rho_{E,\ell}$ is independent of the choice of ι.

Remark 2.6. We can choose α in such a way that the image of ϵ_E has 2-power order, by the following argument. Let $n = 2^a m$ be the order of the image of ϵ_E, where m is odd. If $m \neq 1$, replace α by $\alpha\epsilon_E^{(m-1)/2}$; this has the effect of replacing ϵ_E by ϵ_E^m, whose image has 2-power order.

The reason for introducing the representations $\rho_{E,\ell}$ is found in the following proposition.

Proposition 2.7. *A $\mathbb{Q}$-curve E/K is modular if there exists a (normalized) eigenform f and a prime ℓ such that*

$$\rho_{E,\ell} \cong \rho_{f,\ell}.$$

Here, f is a holomorphic Hecke eigenform on the complex upper-half plane and $\rho_{f,\ell}$ is the Galois representation $\rho_{f,\ell} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\bar{\mathbb{Q}}_\ell)$ such that if $f(z) = \sum_{n=1}^\infty a(n)e(nz)$ $(a(1) = 1)$, then $\operatorname{trace} \rho_{f,\ell}(\mathrm{Frob}_p) = a(p)$ for almost all primes p.

Proof. Suppose $\rho_{E,\ell} \cong \rho_{f,\ell}$ for some eigenform f of level N. Then there exists some finite extension L/K such that

$$\phi_{E,\ell}|_{\mathrm{Gal}(\bar{L}/L)} \cong \rho_{f,\ell}|_{\mathrm{Gal}(\bar{L}/L)} \tag{2.7}$$

and the weight of f must be two, as can be seen by comparing determinants. Let $\rho_{N,\ell}$ be the representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on $T_\ell J_1(N) \otimes_{\mathbb{Z}_\ell} \bar{\mathbb{Q}}_\ell$, where $T_\ell J_1(N)$ is the ℓ-Tate module of $J_1(N)$. We have

$$\rho_{N,\ell} \simeq \oplus \rho_{g,\ell} \tag{2.8}$$

where the sum is over all the eigenforms g of level N and weight 2 (this can be deduced from [19, Thm. 7.11]). From (2.7) and (2.8) it follows that $\phi_{E,\ell}$ is a $\mathrm{Gal}(\bar{L}/L)$-quotient of $\rho_{N,\ell}$. It then follows that $\mathrm{Hom}_L(T_\ell J_1(N), T_\ell E)$ is non-zero. By a theorem of Faltings [7] we can conclude from this that $\mathrm{Hom}_L(J_1(N), E)$ is non-zero. □

We next define some cohomological invariants associated to E. Let $b_E \in H^2(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \pm 1)$ be the composition of c_E with the sign map $\mathbb{Q}^* \to \pm 1$. Then b_E can be computed from ϵ_E. Consider the exact sequence in Galois cohomology

$$\mathrm{Hom}(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \bar{\mathbb{Z}}^*) \to \mathrm{Hom}(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \bar{\mathbb{Z}}^*) \xrightarrow{\delta} H^2(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \pm 1) \tag{2.9}$$

arising from the short exact sequence of Galois modules (with trivial action)

$$0 \to \pm 1 \to \bar{\mathbb{Z}}^* \to \bar{\mathbb{Z}}^* \to 0.$$

Proposition 2.8. $b_E = \delta(\epsilon_E)$.

Proof. Let $\chi : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \bar{\mathbb{Z}}^*$ be a character, and for each $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ let $\tilde{\chi}(\sigma)$ be a square root of $\chi(\sigma)$. Then $\delta(\chi)$ is defined by

$$\delta(\chi)(\sigma, \tau) = \frac{\tilde{\chi}(\sigma)\tilde{\chi}(\tau)}{\tilde{\chi}(\sigma\tau)}.$$

To compute $\delta(\epsilon_E)$, we may choose

$$\tilde{\epsilon}_E(\sigma) = \alpha(\sigma)/\sqrt{\deg \mu_\sigma}$$

where the $\sqrt{}$ sign signifies positive square root. We now have

$$\delta(\epsilon_E)(\sigma, \tau) = \frac{\alpha(\sigma)\alpha(\tau)}{\alpha(\sigma\tau)} \frac{\sqrt{\deg \mu_{\sigma\tau}}}{\sqrt{\deg \mu_\sigma}\sqrt{\deg \mu_\tau}} = c_E(\sigma, \tau)/\sqrt{c_E^2(\sigma, \tau)} = b_E(\sigma, \tau).$$

□

Remark 2.9. Note that the class c_E is the inflation of a class in $H^2(\mathrm{Gal}(K/\mathbb{Q}), \pm 1)$. Quer [13, Th. 2.4] has proven the converse: if E/K' is a $\mathbb{Q}$-curve over some extension of K, and if c_E is the inflation of a class in $H^2(\mathrm{Gal}(K/\mathbb{Q}), \pm 1)$, then there exists a $\mathbb{Q}$-curve E_0/K such $E_0 \times_K K'$ is geometrically isogenous to E.

We will need the fact that the representation $\rho_{E,\ell}$ can also be viewed as the ℓ-adic representation attached to a certain abelian variety over $\mathbb{Q}$.

Proposition 2.10. *Let E/K be a $\mathbb{Q}$-curve, and let $\alpha : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \bar{\mathbb{Q}}^*$ be a 1-cochain with coboundary c_E, as in (2.4). Define $\rho_{E,\ell}$ as in (2.5). Let M be the number field generated by the $\alpha(g)$ for all $g \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.*

There exists an abelian variety $A_\alpha/\mathbb{Q}$ satisfying the following conditions.

- *There exists an injection $M \hookrightarrow End(A_\alpha/\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Q}$;*
- *Let $\lambda_1, \dots, \lambda_r$ be the primes of M lying over ℓ. Then the rational Tate module $V_\ell A_\alpha$ decomposes as*

  $$V_\ell A_\alpha = \bigoplus_i V_{\lambda_i} A_\alpha$$

  and $V_{\lambda_i} A_\alpha$ is isomorphic, as $M_{\lambda_i}[\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})]$-module, to ρ_{E,λ_i}. In particular, $V_\lambda A_\alpha \cong \rho_{E,\ell}$.

Proof. The desired A_α is the one constructed by Ribet in [16, §6]. We briefly recall this construction. First, enlarge K if necessary so that α is the inflation of a function on $\mathrm{Gal}(K/\mathbb{Q})$. Let $\mathcal{R}$ be the algebra generated by elements λ_σ for each $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, with the multiplication table

$$\lambda_{\sigma\tau} c_E(\sigma, \tau) = \lambda_\sigma \lambda_\tau.$$

Then $\mathcal{R}$ acts on the abelian variety

$$\mathrm{Res}_{\mathbb{Q}}^K E \times_{\mathbb{Q}} K \cong \bigoplus_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} E^\sigma$$

by the rule

$$\lambda_\sigma(P) = \mu_\sigma^\tau(P) \tag{2.10}$$

for any $P \in E^{\tau\sigma}(\bar{K})$. This action descends to an action of $\mathcal{R}$ on $\mathrm{Res}_{\mathbb{Q}}^K E$.

Our choice of α defines a homomorphism $\omega : \mathcal{R} \to M$. Now define

$$A_\alpha = \mathrm{Res}_{\mathbb{Q}}^K E \otimes_{\mathcal{R}} M$$

in the category of abelian varieties up to isogeny. To be more precise, let $\pi \in \mathcal{R}$ be the projector onto M; then A_α is the image of $m\pi$, where m is an integer large enough to make $m\pi$ an actual endomorphism (not only a rational endomorphism) of $\mathrm{Res}_{\mathbb{Q}}^K E$.

Then A_α admits the desired injection $M \hookrightarrow \mathrm{End}(A_\alpha) \otimes_{\mathbb{Z}} \mathbb{Q}$, and the rational λ_i-adic Tate module $V_{\lambda_i} A_\alpha$ is a 2-dimensional vector space over M_{λ_i} (see [15, Th. 2.1.1]); one then has from (2.10) that $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on $V_{\lambda_i} A_\alpha$ via ρ_{E,λ_i}. □

Remark 2.11. We emphasize that the construction of A_α is independent of ℓ.

Proposition 2.12. *Let $\ell > 2$. Suppose ℓ does not divide* $\deg \mu_g$ *for any $g \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, and suppose α is chosen so that ϵ_E has 2-power order (Remark 2.6.) Let $\lambda = \lambda_1, \dots, \lambda_i$ be the set of primes of M dividing ℓ.*

Then the full ring of integers of $M \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \cong \oplus_i M_{\lambda_i}$ acts on $T_\ell A_\alpha$, and the ℓ-divisible group $T_\ell A_\alpha$ breaks up as a direct sum of ℓ-divisible groups

$$\bigoplus_i T_{\lambda_i} A_\alpha \tag{2.11}$$

where the λ_i range over the primes of M dividing ℓ. Moreover, $T_{\lambda_i} A_\alpha$ is a free $\mathcal{O}_{M_{\lambda_i}}$-module of rank 2.

Proof. Let $\mathbb{Z}[\alpha]$ be the ring generated by the $\alpha(g)$. Then it follows by the definition of A_α that $\mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathbb{Z}[\alpha]$ acts on $T_\ell A_\alpha$. Since $\deg \mu_g$ is an ℓ-adic unit, and since $\alpha(g)/\sqrt{\deg \mu_g}$ is a 2-power root of unity, we can obtain $\mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathbb{Z}[\alpha]$ by successively adjoining square roots of ℓ-adic units to $\mathbb{Z}_\ell$; it follows that $\mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathbb{Z}[\alpha]$ is étale over $\mathbb{Z}_\ell$, and therefore

$$\mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathbb{Z}[\alpha] \cong \bigoplus_i \mathcal{O}_{M_{\lambda_i}}.$$

The decomposition of $T_\ell A_\alpha$ now follows immediately from the decomposition (2.11). □

We now want to define a mod ℓ representation attached to E. We begin with a general result about Galois representations.

Proposition 2.13. *Let L be a totally ramified extension of $\mathbb{Q}_\ell$ and F an unramified extension of L. Let ρ be a continuous representation of* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ *(or any compact group) with image in $F^* \mathrm{GL}_2(\mathbb{Q}_\ell)$. Then ρ is conjugate in $GL_2(F)$ to a representation with image in $\mathcal{O}_F^* \mathrm{GL}_2(\mathcal{O}_L)$.*

Proof. Let S, T be a basis for $F^{\oplus 2}$ with respect to which the image of ρ lies in $F^* \mathrm{GL}_2(\mathbb{Q}_\ell)$, and let $\mathcal{L}_0$ be the lattice $\mathcal{O}_F S + \mathcal{O}_F T$ generated by S, T. There are only finitely many images of $\mathcal{L}_0$ under the action of the compact group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Each such image $\mathcal{L}_i$ is of the form

$$x(\mathcal{O}_F(aS + bT) + \mathcal{O}_F(cS + dT))$$

with $x \in F^*$ and $a, b, c, d \in \mathbb{Q}_\ell$. Let $\mathcal{L}$ be the lattice generated by all the $\mathcal{L}_i$; then $\mathcal{L}$ is preserved by the action of $\rho(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}))$. Because F/L is unramified, we may write $x = yu$, with $y \in L^*$ and $u \in \mathcal{O}_F^*$. So each $\mathcal{L}_i$ can be rewritten as

$$y(\mathcal{O}_F(aS + bT) + \mathcal{O}_F(cS + dT)).$$

Let $\mathcal{L}'_i$ be the lattice in L^2 defined by

$$\mathcal{L}'_i = y(\mathcal{O}_L(aS + bT) + \mathcal{O}_L(cS + dT)),$$

and let

$$\mathcal{L}' = \mathcal{O}_L(\alpha S + \beta T) + \mathcal{O}_L(\gamma S + \delta T),$$

with $\alpha, \beta, \gamma, \delta \in L$, be the lattice generated by all the $\mathcal{L}'_i$. Then $\mathcal{L} = \mathcal{L}' \otimes_{\mathcal{O}_L} \mathcal{O}_F$. Let $S' = \alpha S + \beta T$ and $T' = \gamma S + \delta T$, and write

$$\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(F)$$

with respect to the basis elements S' and T'.

Since $\rho(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}))$ preserves the lattice $\mathcal{O}_F S' + \mathcal{O}_F T'$, we have $\rho(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})) \in \mathrm{GL}_2(\mathcal{O}_F)$. Since S', T' lie in $LS + LT$, we have $\rho(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})) \in F^* GL_2(L)$. Combining these two facts yields the desired result. □

The representation $\rho_{E,\ell}$ produced in Proposition 2.3 takes values in $M_\lambda^* \mathrm{GL}_2(\mathbb{Q}_\ell)$, where M_λ is the extension of $\mathbb{Q}_\lambda$ generated by the values of $\iota(\alpha(\sigma))$ for all $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Recall from the proof of Proposition 2.3 that $\epsilon_{E,\ell}(\sigma) = \alpha^2(\sigma)/\deg \mu_\sigma$ is a Dirichlet character. So M_λ is contained in an extension generated by square roots and roots of unity; it is thus an abelian extension of $\mathbb{Q}_\ell$. It follows from local class field theory that there exists an abelian extension F of $\mathbb{Q}_\ell$ containing M and such that F also contains a subextension L totally ramified over $\mathbb{Q}_\ell$ over which F is unramified. Then F and L satisfy the conditions of Proposition 2.13, so there exists a basis of $F^{\oplus 2}$ with respect to which $\rho_{E,\ell}$ takes images in $\mathcal{O}_F^* \mathrm{GL}_2(\mathcal{O}_L)$.

Definition 2.14. We denote by

$$\bar{\rho}_{E,\ell} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \bar{\mathbb{F}}_\ell^* \, \mathrm{GL}_2(\mathbb{F}_\ell).$$

the representation obtained by choosing a basis of $F^{\oplus 2}$ as above and reducing the resulting representation

$$\rho_{E,\ell} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathcal{O}_F^* \, \mathrm{GL}_2(\mathcal{O}_L)$$

modulo the maximal ideal $\mathfrak{m}_F$ of $\mathcal{O}_F$. The reduced representation $\bar{\rho}_{E,\ell}$ is then well defined up to semisimplification and conjugation by $\mathrm{GL}_2(\bar{\mathbb{F}}_\ell)$.

We observe that

$$\det \bar{\rho}_{E,\ell} = \bar{\epsilon}_{E,\ell} \bar{\chi}_\ell$$

where the overlines indicate the reductions of the ℓ-adic characters to mod-ℓ characters. Let $\bar{\delta}$ be the reduction mod ℓ of the coboundary map δ in (2.9).

From this point on, we assume that $\ell > 2$.

Proposition 2.15. *$b_E = \bar{\delta}(\bar{\epsilon}_{E,\ell})$.*

Proof. Immediate from Proposition 2.8. □

When R is a domain we abuse notation and denote by 'det' the determinant character from $\mathrm{PGL}_2(R)$ to $R^*/(R^*)^2$.

Definition 2.16. Let ℓ be an odd prime. Then we define a quadratic Dirichlet character

$$\bar{\psi}_{E,\ell} = \det \mathbb{P}\bar{\rho}_{E,\ell} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_\ell^*/(\mathbb{F}_\ell^*)^2 \cong \pm 1.$$

The character $\bar{\psi}_{E,\ell}$, like the cohomology class b_E, depends only on the isomorphism class of E/K.

Remark 2.17. The invariants b_E and $\bar{\psi}_{E,\ell}$ are easy to compute in practice. For instance, suppose K is a quadratic extension of $\mathbb{Q}$ and E/K is a $\mathbb{Q}$-curve. Let τ be the non-trivial element of $\mathrm{Gal}(K/\mathbb{Q})$, and let n be the integer such that $\mu\mu^\tau$ is multiplication by n. Then

$$b_E = \begin{cases} 0 & \text{if } n \text{ positive} \\ \chi_K & \text{if } n \text{ negative.} \end{cases}$$

Suppose, for simplicity, that ℓ does not divide n. Let $\eta : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \pm 1$ be the quadratic character ramified only at ℓ. Then

$$\bar{\psi}_{E,\ell} = \begin{cases} \eta & n \in (\mathbb{Q}_\ell^*)^2 \\ \eta\chi_K & n \notin (\mathbb{Q}_\ell^*)^2. \end{cases}$$

3 The potentially supersingular, residually irreducible case

Theorem 3.1. *Suppose K is tamely ramified over 3. Let E/K be a $\mathbb{Q}$-curve such that*

- *E has good supersingular reduction over K_v for one (whence every) prime v of K above 3;*
- *$b_E \in H^2(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \pm 1)$ has trivial projection to $H^2(G_3, \pm 1)$;*
- *Either $\mathbb{P}\rho_{E,\ell}|G_3$ is unramified for some (whence every) $\ell \neq 3$, or $\deg \mu_\sigma$ is not a multiple of 3 for any $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$;*
- *The restriction of $\bar{\rho}_{E,3}$ to $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}[\sqrt{-3}])$ is absolutely irreducible.*

Then E is modular.

Proof. The basic tool will be the theorem of Wiles and Taylor-Wiles [24, 23], as refined by Diamond [6] and by Conrad, Diamond, and Taylor [2]. In particular, our argument follows closely the proof of Theorem 7.2.1 of [2].

We have from Proposition 2.3 that $\rho_{E,3}$ is an odd, continuous representation unramified away from finitely many primes.

Write G_v, I_v for the absolute Galois group and the inertia group of K_v. Write I_3^w for the subgroup of wild inertia in I_3.

Lemma 3.2. *$\bar{\rho}_{E,3}$ is modular.*

Proof. We follow closely the usual argument that the 3-division points of an elliptic curve over $\mathbb{Q}$ form a modular representation–see [8, I.1] for more details.

The image of $\bar{\rho}_{E,3}$ lies in $\bar{\mathbb{F}}_3^* \mathrm{GL}_2(\mathbb{F}_3)$. We suppose without loss of generality that the chosen extension of the 3-adic valuation of $\mathbb{Q}$ to $\mathbb{Q}[\sqrt{-2}]$ is given by the prime $(1+\sqrt{-2})$.

We can define a homomorphism

$$\iota : \bar{\mathbb{F}}_3^* \mathrm{GL}_2(\mathbb{F}_3) \to \mu_\infty \mathrm{GL}_2(\mathbb{Z}[\sqrt{-2}]),$$

where μ_∞ denotes the group of roots of unity, as follows: set

$$\iota \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix},$$

$$\iota \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ -\sqrt{-2} & -1+\sqrt{-2} \end{bmatrix},$$

and, for each scalar $a \in \bar{\mathbb{F}}_3^*$, define $\iota(a)$ to be the preimage, under the chosen embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_3$, of the Teichmüller lift of a.

Let F be a number field such that the image of $\iota \circ \bar{\rho}_{E,3}$ lies in $\mathrm{GL}_2(F)$, and let w be the chosen extension of the 3-adic valuation to F. Then the composition of $\iota \circ \bar{\rho}_{E,3}$ with reduction mod w is $\bar{\rho}_{E,3}$.

The composition $\iota \circ \bar{\rho}_{E,3}$ is a continuous complex representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, odd and irreducible because $\bar{\rho}_{E,3}$ is odd and absolutely irreducible. It follows from the theorem of Langlands and Tunnell that there exists a weight 1 eigenform, of some level and Dirichlet character,

$$g = \sum_{n=1}^{\infty} b_n q^n$$

such that

$$b_p = \mathrm{Tr}(\iota \circ \bar{\rho}_{E,3}(\mathrm{Frob}_p))$$

for almost all p. Let F' be a number field containing all the b_n. If E is a weight 1 Eisenstein series whose Fourier expansion is congruent to 1 mod 3, then gE is a weight 2 cusp form, of some level and Dirichlet character, such that $T_n(gE)$ is congruent mod w to $b_n gE$, for some prime w' of F' above w. It then follows from an argument of Deligne and Serre [5, §6.10] that there exists an eigenform

$$f = \sum_{n=1}^{\infty} a_n q^n$$

of weight 2 with $a_n \in F'$ and $a_n \equiv b_n \bmod w$ for all n. In particular, $a_p = \mathrm{Tr}(\bar{\rho}_{E,3}(\mathrm{Frob}_p))$ for almost all p. So $\bar{\rho}_{E,3}$ is the mod w' representation associated to f. □

We will show that $\rho_{E,3}$ satisfies the conditions of Theorem 7.1.1 of [2].

Recall that, for any ℓ,

$$\phi_{E,\ell} : \mathrm{Gal}(\bar{K}/K) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$$

is the Galois representation attached to E/K as elliptic curve, and that $\mathbb{P}\phi_{E,\ell}$ and $\mathbb{P}\rho_{E,\ell}$ are isomorphic projective representations of $\mathrm{Gal}(\bar{K}/K)$, by Proposition 2.3.

The representation $\rho_{E,\ell}$ produced by Proposition 2.3 depends on a choice of $\alpha : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \bar{\mathbb{Q}}^*$, a cochain whose coboundary is c_E. We begin by observing that α can be chosen so as to impart to $\rho_{E,\ell}$ some useful arithmetic properties.

Lemma 3.3. *There exists a choice of* $\alpha : G_{\mathbb{Q}} \to \bar{\mathbb{Q}}^*$ *such that*

- *for all* $\ell \neq 3$*, the representation* $\rho_{E,\ell}|G_3$ *is tamely ramified;*
- *for all* ℓ*,* $\det \rho_{E,\ell}|G_3 = \chi_\ell|G_3$*;*
- ϵ_E *has* 2*-power order.*

Proof. Since K is tamely ramified, $c_E|G_3$ is the inflation of an element of

$$H^2(G_3^t, \mathbb{Q}^*).$$

The cohomology group

$$H^2(G_3^t, \bar{\mathbb{Q}}^*)$$

is trival, as can be seen by placing G_3^t in the exact sequence

$$0 \to I_3^t \to G_3^t \to G_3/I_3$$

and computing the initial terms of the Hochschild-Serre spectral sequence [18, §6.1]. Therefore, there is a cochain $a_3 : G_3 \to \bar{\mathbb{Q}}^*$ such that

$$c_E(g,h) = \alpha_3(g)\alpha_3(h)\alpha_3(gh)^{-1}$$

for all $g, h \in G_3$, and such that α_3 vanishes on the wild inertia group I_3^w. Now let $\alpha' : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \bar{\mathbb{Q}}^*$ be any cochain whose coboundary is c_E. Then $(\alpha'|G_3)\alpha_3^{-1}$ is a character θ_3 of G_3. Let θ be a character of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ whose restriction to G_3 is θ_3. Then define

$$\alpha = \alpha'\theta^{-1}.$$

So the coboundary of α is c_E, and $\alpha|G_3 = \alpha_3$; in particular, α vanishes on wild inertia. Since E obtains good reduction after a tame extension of K, we know $\phi_{E,\ell}$ is tamely ramified at 3 for all $\ell \neq 3$. It follows from the definition (2.5) that $\rho_{E,\ell}|G_3$ is tamely ramified for all $\ell \neq 3$.

By Proposition 2.8 and (2.6), the assumption that $b_E|G_3$ is trivial means that

$$\epsilon_E|G_3 = \chi^2$$

for some character $\chi : G_3 \to \bar{\mathbb{Q}}^*$. The character $\epsilon_{E,\ell}$ is tamely ramified for any $\ell \neq 3$, because $\rho_{E,\ell}|G_3$ is tamely ramified; it follows that ϵ_E, whence also χ, is tamely ramified. Replacing α by $\alpha\chi$ now yields the first two desired conditions. In particular, $\epsilon_E|G_3$ is trivial. So we can modify α by any power of ϵ_E without affecting the first two conditions. Now we can force ϵ to have 2-power order by the argument of Remark 2.4. □

For the rest of the proof, it is understood that α is chosen so that $\rho_{E,\ell}|G_3$ satisfies the conditions in Lemma 3.3. We now take as fixed some $\ell > 3$. From Proposition 2.10, we have an abelian variety $A_\alpha/\mathbb{Q}$ such that

$$\rho_{E,\ell} \cong V_\lambda A_\alpha$$

where $\lambda|\ell$ is the prime of M (the number field generated by the $\alpha(g)$) determined by ι.

Denote by L the ramified quadratic extension of $\mathbb{Q}_3$, by $G_L \subset G_3$ the absolute Galois group of L, and by I_L the inertia subgroup of G_L. Let ψ be the ramified quadratic character of G_L, and write A_α^ψ/L for the twist of $A_\alpha \times_{\mathbb{Q}} L$ by ψ.

From this point on, we take as fixed some $\ell > 3$.

Lemma 3.4. *Either*

- $\rho_{E,\ell}|G_L$ *and* $P\rho_{E,\ell}|G_3$ *are unramified, and* A_α/L *has good reduction; or*
- $\rho_{E,\ell}|G_L \otimes \psi$ *is unramified, and* A_α^ψ/L *has good reduction.*

Proof. By Lemma 3.3, wild inertia is killed by $\rho_{E,\ell}$. Let τ be a topological generator of I_3^t, and define $m = \rho_{E,\ell}(\tau)$. Since m has finite order, it is diagonalizable.

Note that τ and τ^3 are conjugate in G_3. So m and m^3 are conjugate in $\bar{\mathbb{Q}}_\ell^* \, \mathrm{GL}_2(\mathbb{Q}_\ell)$. Since $\det(m) = \chi_\ell(\tau) = 1$, we conclude that the eigenvalues of m must be either $(1,1), (-1,-1)$ or $(i,-i)$. In the former two cases, we see that $\rho_{E,\ell}|G_L$ is unramified. In the latter case, $(\rho_{E,\ell}|G_L) \otimes \psi$ is unramified.

Suppose the eigenvalues of m are $(1,1)$ or $(-1,-1)$; equivalently, $\mathbb{P}\rho_{E,\ell}|G_3$ is unramified. Recall from Remark 2.5 that $\mathbb{P}\rho_{E,\ell}$ does not depend on the choice of ι. So $\rho_{E,\lambda_i}(\tau)$ is scalar for any i, whence I_L acts trivially on $V_{\lambda_i} A_\alpha$ for any prime λ_i of M dividing ℓ. It then follows from Proposition 2.10 that I_L acts trivially on $V_\ell A_\alpha$, and so A_α/L has good reduction.

Likewise, if the eigenvalues of m are $(i,-i)$, then $\rho_{E,\lambda_i}(\tau^2) = -1$ for all i, so $\rho_{E,\lambda_i}|G_L \otimes \psi$ is unramified for all i, and A_α^ψ/L has good reduction.

□

Suppose $\mathbb{P}\rho_{E,\ell}|G_3$ is unramified. Then $\rho_{E,\ell}|G_L$ is unramified. Since $\det \rho_{E,\ell}|I_3$ is trivial, the image $\rho_{E,\ell}(I_3)$ is either trivial or ±1. So, in fact, either $A_\alpha/\mathbb{Q}_3$ or its ramified quadratic twist has good reduction over $\mathbb{Q}_3$. Therefore, either $\rho_{E,3}|G_3$ or its ramified quadratic twist is associated to a 3-divisible group, and E is modular by [6, Theorem 5.3].

We therefore assume from now on that $(\rho_{E,\ell}|G_L) \otimes \psi$ is unramified, so that A_α^ψ/L has good reduction. In this case, by the hypotheses of our theorem, 3 does not divide $\deg \mu_g$ for any $g \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

In this case, A_α^ψ/L has good reduction. Therefore, if ψ' is a ramified quadratic character of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}[\sqrt{-3}])$, the twist $A_\alpha^{\psi'}/\mathbb{Q}[\sqrt{-3}]$ has good reduction at the prime over 3.

Let θ be the prime of M determined by the chosen embedding $M \hookrightarrow \bar{\mathbb{Q}}_3$. Then, by Proposition 2.12, we can define a finite flat group scheme $A_\alpha[\theta]$ as the 3-torsion (equivalently, the θ-torsion) of the 3-divisible group $T_\theta A_\alpha^{\psi'}/\mathbb{Q}[\sqrt{-3}]$. Because $\bar{\rho}_{E,3}$ is absolutely irreducible when restricted to $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}[\sqrt{-3}])$, and because

$$\rho_{E,3} \otimes \psi' \cong V_\theta A_\alpha^{\psi'},$$

we have an isomorphism of $(\mathcal{O}_{M_\theta}/\theta)[\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}[\sqrt{-3}])]$-modules

$$\bar{\rho}_{E,3} \otimes \psi' \cong A_\alpha^{\psi'}[\theta].$$

Restricting this isomorphism to G_L yields an isomorphism of $(\mathcal{O}_{M_\theta}/\theta)[G_L]$-modules

$$\bar{\rho}_{E,3}|G_L \otimes \psi \cong A_\alpha^{\psi}[\theta].$$

In particular, $(\bar{\rho}_{E,3}|G_L) \otimes \psi$ is flat. Recall that a representation of G_L with finite image is said to be *flat* if the attached finite flat group scheme over L is the generic fiber of a finite flat group scheme over $\mathcal{O}_L$. In the case, the finite flat group scheme in question is $(A_\alpha^\psi)[\theta]$.

Lemma 3.5. *The centralizer of $\bar{\rho}_{E,3}(G_3)$ consists entirely of scalars.*

Proof. The result follows from a theorem of Conrad [1, Theorem 4.2.1]. As above, the relevant finite flat group scheme over $\mathcal{O}_L$ is $G = (A_\alpha^\psi)[\theta]$. To apply Conrad's theorem, we need only to verify that G is connected and has connected Cartier dual, and that G satisfies a certain exactness condition on Dieudonné modules. The connectedness of G and its dual follow from the fact that G is a closed subgroup scheme of the 3-torsion subscheme of the supersingular abelian variety A_α^ψ. The exactness condition is automatically satisfied because G is the 3-torsion in the 3-divisible group $T_\theta A_\alpha^\psi$. □

Let F be a finite extension of $\mathbb{Q}_\ell$. Recall that an ℓ-adic representation ρ of the Galois group of F is said to be *Barsotti-Tate* if it arises from the generic fiber of an ℓ-divisible group, and to be *potentially Barsotti-Tate* if some restriction of ρ to a finite-index subgroup of $\mathrm{Gal}(\bar{F}/F)$ is Barsotti-Tate. (See [2, §1.1].) The representation $\rho_{E,3}|G_3$ is potentially Barsotti-Tate, because it is realized on the θ-adic Tate module of A_α, which has potentially good reduction. From now on, we will abuse notation and refer to the local representation $\rho_{E,3}|G_3$ simply as $\rho_{E,3}$.

Let V be a d-dimensional vector space over a finite extension F' of $\mathbb{Q}_\ell$. One can associate to any potentially Barsotti-Tate representation $\rho : \mathrm{Gal}(\bar{F}/F) \to \mathrm{GL}(V)$ a continuous representation

$$WD(\rho) : W_F \to GL(D)$$

of the Weil group of F on a $\bar{\mathbb{Q}}_\ell$-vector space D of dimension d, as in Conrad, Diamond, and Taylor [2, Appendix B]. In the lemma that follows, we will freely use definitions and facts from that paper, especially §1.2, §2.3, and Appendix B.

Lemma 3.6. *The type of $WD(\rho_{E,3})$ is strongly acceptable for $\bar\rho_{E,3}$.*

Proof. We take $F' = M_\lambda$.

Let τ be the restriction of $WD(\rho_{E,3})$ to I_3. It follows from Proposition 2.10 and [2, Prop. B.4.2] that $\rho_{E,3}$ is Barsotti-Tate over L' for any finite extension $L'/\mathbb{Q}_\ell$ such that τ is trivial. Our choice of α in Lemma 3.3 guarantees that $\det \rho_{E,3} = \chi_3$ and $\det \bar\rho_{E,3} = \bar\chi_3$. It follows that $\rho_{E,3}$ is a deformation of $\bar\rho_{E,3}$ of type τ, according to the definition in [2, §1.2].

We know that $(\rho_{E,3}|G_L) \otimes \psi$ is Barsotti-Tate, because it is associated to the 3-divisible group $T_\theta A^\psi_\alpha$. So

$$WD((\rho_{E,3}|G_L) \otimes \psi) = WD(\rho_{E,3}|G_L) \otimes WD(\psi)$$

is unramified, so $\tau|I_L = WD(\psi)|I_L$. We know that $WD(\psi) = \psi|W_L \otimes_{M_\lambda} \bar{\mathbb{Q}}_\ell$ ([2, §B.2]); that is, $WD(\psi)|I_L$ is a non-trivial quadratic character of I_L. We also know that the determinant of τ is trivial on I_3, because the WD functor commutes with exterior products, and the determinant of $\rho_{E,3}$ is the cyclotomic character χ_3; the character $WD(\chi_3)$ is shown to be unramified in [2, §B.2]. We conclude that

$$\tau \cong \tilde\omega_2^2 \oplus \tilde\omega_2^6,$$

where $\tilde\omega_2 : I_3^t \to \bar{\mathbb{Q}}_3^*$ is the Teichmüller lift of ω_2, the fundamental tame character of level 2.

It now follows from Corollary 2.3.2 of [2] that τ is acceptable for $\bar\rho_{E,3}$.

We have by [1, Theorem 4.2.1] that either

- $(\bar\rho_{E,3}|I_3) \otimes_{\mathbb{F}_3} \bar{\mathbb{F}}_3 \cong \omega_2^m \oplus \omega_2^{3m}$, where $m = 1$ or 5;
- $\bar\rho_{E,3}|I_3 \cong \begin{bmatrix} \bar\chi_3^m & * \\ 0 & \bar\chi_3^n \end{bmatrix}$, where $(m, n) = (0, 1)$ or $(1, 0)$ and $*$ is peu ramifié.

In either case, it follows from the criterion of [2, §1.2] that τ is strongly acceptable for $\bar\rho_{E,3}$. □

Now, combining Lemmas 3.5 and 3.6, we can apply [2, Theorem 7.1.1] and conclude that $\rho_{E,3}$, whence E, is modular. □

4 More on residual representations

In [24], Wiles deals with the case where the 3-adic representation associated to an elliptic curve C is residually reducible by executing a "3-5 switch". That is, he replaces C with another elliptic curve C', such that the mod 3 representation attached to C' is absolutely irreducible when restricted to $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}[\sqrt{-3}])$, and such that C and C' have isomorphic mod 5 Galois representations. Aside from a finite set of exceptions, the common mod 5 Galois representation is absolutely irreducible when restricted to $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}[\sqrt{5}])$. This coincidence of mod 5 Galois representations is enough to show that modularity of C' is equivalent to modularity of C, and the modularity of C' follows from the condition on the mod 3 Galois representation of C'. This argument relies on the fact that, given an elliptic curve C, there are plenty of elliptic curves C' whose mod 5 representations are isomorphic to that of C. This fact, in turn, depends on the fact that the modular curve $X(5)/\mathbb{Q}$ is isomorphic to $\mathbb{P}^1/\mathbb{Q}$. In general, the modular curve parametrizing $\mathbb{Q}$-curves with full level 5 structure will not have genus 0, rendering a 3-5 switch impossible.

We are left with two methods of treating the residually reducible cases. One method is to generalize the lifting theorems of Wiles, Taylor Wiles, *et. al.* to the residually reducible situation.

Several theorems in this direction have been proven by Andrew Wiles and the second author [21],[22] in the case where the reduction of E is ordinary or multiplicative. We will apply those theorems to the present situation in Theorem 5.1 below.

Another method is to exploit the fact that, in contrast with the case of elliptic curves over $\mathbb{Q}$, there are often cohomological obstructions to the reducibility of $\bar{\rho}_{E,\ell}$. These obstructions can be computed explicitly in terms of the invariants described in section 2. We begin with a general fact about reducible projective mod ℓ Galois representations.

Proposition 4.1. *Let ℓ be an odd prime, and let*

$$\mathbb{P}\bar{\rho} : \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{PGL}_2(\mathbb{F}_\ell)$$

be a projective mod ℓ Galois representation. Let $\chi : \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \pm 1$ be a quadratic Dirichlet character (possibly trivial). Let G be the subgroup of matrices in $\bar{\mathbb{F}}_\ell^* \operatorname{GL}_2(\mathbb{F}_\ell)$ having determinant 1, and let $\gamma \in H^2(\operatorname{PGL}_2(\mathbb{F}_\ell), \pm 1)$ be the class of the extension

$$1 \to \pm 1 \to G \to \operatorname{PGL}_2(\mathbb{F}_\ell) \to 1.$$

Let $\bar{\psi} = \det \mathbb{P}\bar{\rho}$. Finally, suppose that either

(a) *the image of $\mathbb{P}\bar{\rho}$ lies in the normalizer N of a Cartan subgroup C of $\operatorname{PGL}_2(\mathbb{F}_\ell)$, and the quadratic character $\operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to N/C$ is equal to χ, or*

(b) *the image of $\mathbb{P}\bar{\rho}$ lies in a Borel subgroup of $\operatorname{PGL}_2(\mathbb{F}_\ell)$, and χ is trivial.*

Then either $(\bar{\psi}, \chi\bar{\psi})$ or $\mathbb{P}\bar{\rho}^*\gamma(\bar{\psi}, \chi\bar{\psi})(\chi, \chi)$ is the trivial class in $H^2(\operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \pm 1)$.

Proof. First, suppose the image of $\mathbb{P}\bar{\rho}$ lies in the normalizer N of a Cartan subgroup C of $\operatorname{PGL}_2(\mathbb{F}_\ell)$. Write $\bar{N}$ for the group N/C^2. Let π be the natural projection of N onto $\bar{N}$. Then $\bar{N} \cong (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$; a choice of isomorphism can be fixed by requiring that the first copy of $\mathbb{Z}/2\mathbb{Z}$ be $\pi(C)$ and the second be the kernel of $\det : \bar{N} \to \mathbb{F}_\ell^*/(\mathbb{F}_\ell^*)^2$. We then have

$$\pi \circ \mathbb{P}\bar{\rho} = \bar{\psi} \oplus \chi : \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}. \tag{4.12}$$

We consider two cases.

Case 1: $|C^2|$ is even. Then π factors as

$$N \to \hat{N} \to \bar{N},$$

where $\hat{N}$ is a dihedral group of order 8 whose cyclic subgroup of order 4 is the preimage of $\pi(C)$. So $\pi \circ \mathbb{P}\bar{\rho}$ lifts to a homomorphism from $\operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ to $\hat{N}$, which means that $d(\pi \circ \mathbb{P}\bar{\rho})$ vanishes in the cohomology sequence

$$H^1(\operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \hat{N}) \to H^1(\operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \bar{N}) \xrightarrow{d} H^2(\operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \pm 1).$$

The isomorphism $\bar{N} \cong (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$ then tells us that $d'(\bar{\psi} \oplus \chi)$ vanishes in

$$H^1(\operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), D_4) \to H^1(\operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}) \xrightarrow{d'} H^2(\operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \pm 1),$$

where D_4 is a dihedral group of order 8 whose cyclic subgroup of order 4 is the preimage of the first copy of $(\mathbb{Z}/2\mathbb{Z})$. It is well known that, for any two characters χ_1, χ_2, we have $d'(\chi_1 \oplus \chi_2) = (\chi_1, \chi_1\chi_2)$ [10, Prop. 3.10]. So $(\bar{\psi}, \chi\bar{\psi}) = 0$, as desired.

Case 2: $|C^2|$ is odd.

In this case, the inflation map

$$\pi^* : H^2(\bar{N}, \pm 1) \to H^2(N, \pm 1) \tag{4.13}$$

is an isomorphism. The subgroup of N generated by an involution in C and any element of $N \backslash C$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$; in fact, any such subgroup is the image of an injection $s : \bar{N} \to N$ such that $\pi \circ s$ is the identity. Write ι for the inclusion of N in $\mathrm{PGL}_2(\mathbb{F}_\ell)$. Let M be the subgroup of G lying over $s(\bar{N})$. Then $s^* \iota^* \gamma$ is the class $c \in H^2(\bar{N}, \pm 1)$ corresponding to the extension

$$1 \to \pm 1 \to M \to \bar{N} \to 1.$$

It follows from the fact that a non-scalar element of G whose square is a scalar has exact order 4 that M is the quaternion group of order 8. Now, from (4.12) and [10, Th. 3.11], one gets

$$\mathbb{P}\rho^* \pi^* c = (\bar{\psi} \oplus \chi)^* c = (\bar{\psi}, \chi\bar{\psi})(\chi, \chi),$$

The isomorphism (4.13) implies that $\pi^* s^*$ acts as the identity on $H^2(N, \pm 1)$. In particular, we have $\pi^* c = \iota^* \gamma$. Pulling back both of these by $\mathbb{P}\rho$ (or, more precisely, by the homomorphism $f : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to N$ such that $\iota \circ f = \mathbb{P}\rho$) one obtains the equality

$$\mathbb{P}\rho^* \gamma = \mathbb{P}\rho^* \pi^* c.$$

which yields the desired result.

The only case remaining is that where the image of $\mathbb{P}\rho$ lies in a Borel subgroup but not necessarily in the normalizer of a Cartan. In this case, the semisimplification of $\mathbb{P}\bar{\rho}$ has image lying in a split Cartan subgroup, and we are in the case already discussed. □

We now apply Proposition 4.1 to the case of mod ℓ representations attached to $\mathbb{Q}$-curves.

Proposition 4.2. *Let E/K be a $\mathbb{Q}$-curve and ℓ an odd prime. Let $\chi : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \pm 1$ be a quadratic Dirichlet character (possibly trivial). Let $q_{\ell,\infty} \in H^2(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \pm 1)$ be the Brauer class of the quaternion algebra ramified only at ℓ and ∞. Suppose that either*

(i) *the image of $\mathbb{P}\bar{\rho}_{E,\ell}$ lies in the normalizer N of a Cartan subgroup C of $\mathrm{PGL}_2(\mathbb{F}_\ell)$, and the quadratic character $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to N/C$ is equal to χ, or*

(ii) *the image of $\mathbb{P}\bar{\rho}_{E,\ell}$ lies in a Borel subgroup of $\mathrm{PGL}_2(\mathbb{F}_\ell)$, and χ is trivial.*

Then either $(\bar{\psi}_{E,\ell}, \chi\bar{\psi}_{E,\ell})$ or $b_E q_{\ell,\infty}(\bar{\psi}_{E,\ell}, \chi\bar{\psi}_{E,\ell})(\chi, \chi)$ is the trivial class in $H^2(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \pm 1)$.

Proof. The proposition is an immediate corollary of Proposition 4.1. The only thing to check is that

$$\mathbb{P}\bar{\rho}^*_{E,\ell} \gamma = b_E q_{\ell,\infty}.$$

Let G be as in the statement of Proposition 4.1. For each $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ let $d_\sigma \in \bar{\mathbb{F}}_\ell^*$ be a square root of $\det(\bar{\rho}_{E,\ell}(\sigma))$. Then $g_\sigma = d_\sigma^{-1} \bar{\rho}_{E,\ell}$ is a set-theoretic lift of $\mathbb{P}\bar{\rho}_{E,\ell}$ to G. To this lift one associates a 2-cocycle c given by the rule

$$c(\sigma, \tau) = g_\sigma g_\tau g_{\sigma\tau}^{-1} = d_\sigma^{-1} d_\tau^{-1} d_{\sigma\tau}.$$

But this is just a 2-cocycle representing the class $\bar{\delta}(\det \bar{\rho}_{E,\ell})$, where $\bar{\delta}$ is defined as in Proposition 2.15. From that proposition and from the fact that $\bar{\delta}(\bar{\chi}_\ell) = q_{\ell,\infty}$, one has

$$\bar{\delta}(\det \bar{\rho}_{E,\ell}) = b_E \bar{\delta}(\bar{\chi}_\ell) = b_E q_{\ell,\infty}.$$

The desired result follows. □

Proposition 4.2 guarantees in many cases that the 3-adic representation attached to a $\mathbb{Q}$-curve is residually absolutely irreducible, even when restricted to a quadratic field.

5 The main theorems

We are now ready to state and prove the main results of the paper. Recall that $(b_E)_3$ denotes the restriction of b_E to $H^2(G_3, \pm 1)$.

Theorem 5.1. *Suppose E/K is a $\mathbb{Q}$-curve with potentially ordinary or multiplicative reduction at some (whence every) prime of K over 3, and such that $(b_E)_3$ is trivial. Then E is modular.*

Proof. First, suppose that $\bar{\rho}_{E,3}$ is absolutely reducible when restricted to $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}[\sqrt{-3}])$. For this case we appeal to the main theorems of [21] and [22]. In order for these theorems to apply we need only verify the following properties of the representation $\rho_{E,3}$:

(i) $\rho_{E,3}$ is continuous, irreducible, and odd;

(ii) $\det \rho_{E,3}(\mathrm{Frob}_\ell) = \psi(\ell)\ell^{k-1}$ for some finite character ψ, some integer $k \geq 2$, and almost all primes ℓ;

(iii) $\rho_{E,3}|_{G_3} \cong \begin{bmatrix} \phi_1 & * \\ & \phi_2 \end{bmatrix}$ with $\phi_2|_{I_3}$ finite;

(iv) the reductions $\bar{\phi}_1$ and $\bar{\phi}_2$ are distinct;

(v) $\bar{\rho}_{E,3}$ is modular (in the sense of Lemma 3.2) if it is absolutely irreducible.

Properties (i) and (ii) follow from Proposition 2.3 and (2.6). (Here we have again used that E does not have complex multiplication, this time to ensure that $\phi_{E,3}$, and hence $\rho_{E,3}$, is irreducible.) We next prove that property (iii) holds.

From the possibilities for the reduction type of E it follows that the restriction of $\phi_{E,3}$ to a decomposition group G_v at a prime $v|3$ of K satisfies

$$\phi_{E,3}|_{G_v} \cong \begin{bmatrix} \theta_1 & * \\ & \theta_2 \end{bmatrix}$$

with θ_2 having finite order on inertia. We claim that the same is true of $\rho_{E,3}|_{G_3}$. Suppose otherwise. From the fact that $\rho_{E,3}|_{\mathrm{Gal}(\bar{K}/K)}$ is isomorphic to a twist of $\phi_{E,3}$ it follows that there is a quadratic extension, say L, of $\mathbb{Q}_3$ such that the restriction of $\rho_{E,3}$ to $\mathrm{Gal}(\bar{L}/L)$ is the direct sum of two characters that are interchanged by the action of $\mathrm{Gal}(L/\mathbb{Q}_3)$. Since the product of these two characters, being the restriction of $\det \rho_{E,3}$, is infinitely ramified, so must be one, and hence both, of these characters. But this contradicts the above description of $\phi_{E,3}|_{G_v}$. Write

$$\rho_{E,3}|_{G_3} \cong \left[\begin{array}{cc} \phi_1 & * \\ & \phi_2 \end{array} \right].$$

We next prove that the reductions $\bar{\phi}_1$ and $\bar{\phi}_2$ are distinct on G_3; in other words, that $\rho_{E,3}$ has property (iv). To see this we note that if $\bar{\phi}_1$ and $\bar{\phi}_2$ were not distinct on G_3 then $\det \bar{\rho}_{E,3}|_{G_3}$ would be a square. Suppose this were so. Then from $\det \bar{\rho}_{E,3} = \bar{\epsilon}_3 \bar{\chi}_3$ (see (2.6)) we conclude that $\bar{\epsilon}_3|_{G_3} = \phi^2 \bar{\chi}_3|_{G_3}$ for some character ϕ of G_3. It then follows from Proposition 2.15 that the restriction of b_E to G_3 equals the restriction of $\bar{\delta}(\bar{\chi}_3)$ to G_3. But the latter is non-trivial, hence so is the former, contradicting hypothesis (ii) of the theorem.

It remains to prove that property (v) holds. If $\bar{\rho}_{E,3}$ is absolutely irreducible, then it must be dihedral and in fact induced from a character of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\sqrt{-3}))$ since we are assuming that $\bar{\rho}_{E,3}$ is absolutely reducible on $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\sqrt{-3}))$. It is a classical result that such representations are modular.

We have shown that $\rho_{E,3}$ has properties (i)-(v) listed above. As mentioned before, the theorem follows.

Now, suppose that $\bar{\rho}_{E,3}$ is absolutely irreducible when restricted to $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}[\sqrt{-3}])$. By the argument above,

$$\rho_{E,3}|_{G_3} \cong \left[\begin{array}{cc} \phi_1 & * \\ & \phi_2 \end{array} \right],$$

where ϕ_2 has finite image on inertia and $\phi_1|_{I_3} = \eta\chi_3|_{I_3}$, with η a finite-order character. After twisting $\rho_{E,3}$ by a finite-order character of $G_{\mathbb{Q}}$, we may assume ϕ_2 is unramified. We have already shown above that $\bar{\phi}_1 \neq \bar{\phi}_2$. Finally, $\bar{\rho}_{E,3}$ is modular by Lemma 3.2 (which does not use the assumption of supersingular reduction in Theorem 3.1.) It now follows from Theorem 5.3 of [6] that $\rho_{E,3}$, whence E, is modular. □

Theorem 5.2. *Suppose E/K is a $\mathbb{Q}$-curve such that, for some (whence every) prime $\ell > 3$, the projective representation $\mathbb{P}\rho_{E,\ell}$ associated to $\rho_{E,\ell}$ is unramified at 3. Then E is modular.*

Proof. If E has potentially ordinary or multiplicative reduction, the modularity follows from Theorem 5.1. We therefore assume that the reduction of E is potentially supersingular.

We have that $\rho_{E,\ell}|I_3$ is a character θ. So

$$\theta^2 = \det \rho_{E,\ell}|I_3 = \epsilon_E|I_3.$$

Choose α such that ϵ_E has 2-power order; then ϵ_E, whence also $\rho_{E,\ell}$, is tamely ramified. We may choose K to be a compositum of quadratic fields [13, Cor. 2.5], in which case it follows that E obtains good reduction over a tamely ramified extension of $\mathbb{Q}_3$.

Let τ be a topological generator of tame inertia, and let $m = \rho_{E,\ell}(\tau)$; then m is a scalar which is conjugate to its cube, so $m = \pm 1$. In either case,

$$\det m = \epsilon_E(\tau) = 1,$$

so ϵ_E is unramified at 3, and $(b_E)_3 = \delta(\epsilon_E|G_3)$ is trivial.

From Proposition 2.10, the action of τ on $T_\ell A_\alpha$ is either 1 or -1. Thus, after modifying α by a quadratic character, we may assume that A_α has good supersingular reduction at 3.

Therefore, $A_\alpha[3]$ extends to a finite flat group scheme over $R = W(\bar{\mathbb{F}}_3)$, to which we can apply Raynaud's classification [14]. Let F be the fraction field of R. Let H be a Jordan-Hölder quotient of $A_\alpha[3]_F$. Then we have from [14, Cor. 3.4.4] that the action of τ on $H(\bar{F})$ has eigenvalues

$$\psi_m(\tau)^{n3^i}(i = 0, \dots, m-1)$$

where ψ_m is a fundamental tame character of I_3, and n is an integer whose base-3 expansion contains only 0's and 1's. In particular, τ^4 acts trivially on $H(\bar{F})$ if and only if τ^2 acts trivially.

Suppose τ^2 acts trivially on $H(\bar{F})$. Then $H(\bar{F})$ is a 1-dimensional $\mathbb{F}_3$-vector space, and H is isomorphic to either $(\mathbb{Z}/3\mathbb{Z})_K$ or $(\mu_3)_K$. It then follows from [14, Cor. 3.3.6] that $A_\alpha[3]/R$ has either $\mathbb{Z}/3\mathbb{Z}$ or μ_3 as a subquotient, which contradicts the supersingularity of A_α.

We may therefore suppose that τ^4 acts non-trivially on the $\bar{F}$-points of every subquotient of $A_\alpha[3]$. In particular, $\bar\rho_{E,3}(\tau^4)$ does not have 1 as an eigenvalue.

Suppose the restriction of $\bar\rho_{E,3}$ to $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}[\sqrt{-3}])$ is absolutely reducible. As in § 3, let L be the ramified quadratic extension of $\mathbb{Q}_3$. Then

$$(\bar\rho_{E,3}|I_L)^{ss} \cong \phi_1 \oplus \phi_2$$

for some characters $\phi_1, \phi_2 : I_L^t \to \bar{\mathbb{F}}_3^*$. Since $(\bar\rho_{E,3}|I_L)$ extends to a representation of G_3, we have that $\{\phi_1, \phi_2\} = \{\phi_1^3, \phi_2^3\}$. The fact that $\bar\rho_{E,3}|\mathbb{Q}[\sqrt{-3}]$ is absolutely reducible means that in fact $\phi_i^3 = \phi_i$ for $i = 1, 2$; in other words, ϕ_1 and ϕ_2 are quadratic characters. In particular, $\bar\rho_{E,3}(\tau^4)$ is unipotent, which is a contradiction.

To sum up: we have shown that under the hypotheses of the theorem, we know that

- E obtains good supersingular reduction over a tame extension of $\mathbb{Q}_3$;
- $(b_E)_3 = 1$; and
- $\bar\rho_{E,3}|\,\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}[\sqrt{-3}])$ is absolutely irreducible.

It now follows from Theorem 3.1 that E is modular. □

Theorem 5.3. *Suppose E/K is a $\mathbb{Q}$-curve which acquires semistable reduction over a field tamely ramified over $\mathbb{Q}_3$. Suppose further that $(b_E)_3$ is trivial, and that the four classes $(\bar\psi_{E,3}, -1)$, $b_E q_{3,\infty}(\bar\psi_{E,3}, -1)$, $q_{3,\infty}(\bar\psi_{E,3}, 3)$, and $b_E(\bar\psi_{E,3}, 3)$ are all nontrivial in $H^2(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \pm 1)$. Finally, suppose that $\deg \mu_\sigma$ can be chosen to be prime to 3 for all $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Then E is modular.*

Proof. We may assume that the reduction of E over 3 is potentially supersingular; otherwise, E is modular by Theorem 5.1.

It follows from Proposition 4.2 that the restriction of $\bar\rho_{E,3}$ to $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}[\sqrt{-3}])$ is absolutely irreducible. It then follows from Theorem 3.1 that E is modular. □

References

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

[2] B. Conrad, F. Diamond, and R. Taylor. Modularity of certain potentially Barsotti-Tate Galois representations. *J. Amer. Math. Soc.*, 12(2):521–567, 1999.

[3] G. Cornell, J. Silverman, and G. Stevens, editors. *Modular forms and Fermat's last theorem.* Springer-Verlag, 1997.

[4] H. Darmon. Serre's conjectures. In V. Kumar Murty, editor, *Seminar on Fermat's Last Theorem*, number 17 in CMS Conference Proceedings, pages 135–153, 1995.

[5] P. Deligne and J.P. Serre. Formes modulaires de poids 1. *Ann. Sci. E.N.S.*, 7:507–530, 1974. Also item 101 in *Oeuvres*, Serre.

[6] F. Diamond. On deformation rings and Hecke rings. *Ann. of Math.*, 144(1):137–166, 1996.

[7] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern *Invent. Math.*, 73:349–366,1983.

[8] S. Gelbart. Three lectures on the modularity of $\bar{\rho}_{E,3}$ and the Langlands reciprocity conjecture. In Cornell et al. [3], pages 155–207.

[9] A. Grothendieck. *Groupes de Monodromie en Géométrie Algébrique (SGA 7).* Number 288 in Lecture Notes in Math. Springer-Verlag, 1972.

[10] H. Grundman, T. Smith, and J. Swallow. Groups of order 16 as Galois groups. *Expo. Math.*, 13:289–319, 1995.

[11] Y. Hasegawa, K.-i. Hashimoto, and F. Momose. Modular conjecture for **Q**-curves and QM-curves. Preprint., 1996.

[12] H. Hida. Modular Galois representations of "Neben" type. Preprint.

[13] J. Quer. **Q**-curves and abelian varieties of $\mathbf{G}L_2$-type. Preprint.

[14] M. Raynaud. Schémas en groupes de type $(p, \ldots, p)$. *Bull. Soc. Math. France*, 102:241–280, 1974.

[15] K. Ribet. Galois actions on division points of abelian varieties with real multiplications. *Amer. J. Math.*, 98(3):751–804, 1976.

[16] K. Ribet. Abelian varieties over **Q** and modular forms. In *Algebra and Topology 1992*, pages 53–79. Korea Adv. Inst. Sci. Tech., 1992.

[17] B. Roberts and L. Washington. The modularity of some **Q**-curves. *Compositio Math.*, 111(1):35–49, 1998.

[18] J.-P. Serre. Modular forms of weight one and galois representations. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 193–268. Academic Press, London, 1977.

[19] G. Shimura. *Introduction to the arithmetic theory of automorphic functions.* Princeton University Press, Princeton, 1971.

[20] G. Shimura. On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields. *Nagoya Math. J.*, 43:199–208, 1973.

[21] C. Skinner and A. Wiles. Residually reducible representations and modular forms. Preprint.

[22] C. Skinner and A. Wiles. Nearly ordinary deformations of irreducible residual representations. Preprint.

[23] R. Taylor and A. Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math.*, 141(3):553–572, 1995.

[24] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math.*, 141(3):443–551, 1995.