Radical Characterizations of Elliptic Curves

Chris Hall and Antonella Perucca

Abstract

Let K be a number field, and let E be an elliptic curve over K. A famous result by Faltings of 1983 can be reformulated for elliptic curves as follows: if S is a set of primes of good reduction for E having density one, then the K-isogeny class of E is determined by the function $\mathfrak{p} \to \#E(k_\mathfrak{p})$, which maps a prime in S to the size of the group of points over the residue field. In this paper, we prove that it suffices to look at the set of primes dividing the size.

1 Introduction

Let A, A' be abelian varieties over a number field K, and let S be the set of common finite primes $\mathfrak{p} \subset K$ of good reduction. A well-known theorem of Faltings implies that A, A' are K-isogenous if and only if they have the same L-series (cf. proposition 17). The L-series of A is determined, in part, by the function $\nu : \mathfrak{p} \in S \mapsto \#A(k_\mathfrak{p})$, and in this paper we consider other functions which one can use to characterize K-isogeny.

If A, A' are elliptic curves, then Faltings's theorem implies A, A' have the same L-series if and only if $\#A(k_\mathfrak{p}) = \#A'(k_\mathfrak{p})$ for every $\mathfrak{p} \in S$ (cf. lemma 20). A weaker condition that one could ask for is that these integers have the same radical, that is, $\ell \mid \#A(k_\mathfrak{p})$ if and only if $\ell \mid \#A'(k_\mathfrak{p})$, for every prime ℓ and every $\mathfrak{p} \in S$.

Theorem 1. *Suppose A, A' are elliptic curves over a number field K, and let S be a density-one set of finite primes in K over which A, A' have good reduction. If $\Lambda \subseteq \mathbb{N}$ is an infinite set of primes, then the following are equivalent:*

1. *A, A' are K-isogenous;*
2. *$\ell \mid \#A(k_\mathfrak{p})$ if and only if $\ell \mid \#A'(k_\mathfrak{p})$, for every $\ell \in \Lambda$ and $\mathfrak{p} \in S'$.*

We prove theorem 1 in section 5. The proof makes crucial use of the theory developed by Serre in [4] as well as the results of Frey and Jarden [2] on the Galois modules $A[\ell]$. If A is an elliptic curve and $A' = A \times A$, then 2. holds but 1. does not. Nonetheless, the strategy behind our proof seems reasonable for pairs of square free abelian varieties, that is, abelian varieties A, A' each of which whose isogeny factors are distinct. We assume A, A' are elliptic curves because our proof uses explicit knowledge of the structure of the image of the ℓ-adic representation for $\ell \gg 0$. A possible direction of further research is studying the following:

Open problem. Let A, A' be square-free abelian varieties defined over a number field, which are non-isogenous. Let $m, m' \geq 0$. Determine whether the following set has a positive density for $\ell \gg 0$:

$$S_\ell = \{\mathfrak{p} \in K : v_\ell\left(\#A(k_\mathfrak{p})\right) = m,\, v_\ell\left(\#A'(k_\mathfrak{p})\right) = m'\}\,.$$

1.1 Notation

The following notation occurs frequently throughout the paper:

- ℓ : rational prime
- K : a number field
- G_K : absolute Galois group of K
- A, A' : abelian varieties (over K)
- $E = \mathrm{End}(A) \otimes \mathbb{Q}$
- K_ℓ : splitting field of the ℓ-torsion of A
- L/K : a finite extension
- S_L : set of non-archimedean primes $\mathfrak{p} \subseteq L$
- $S_L(A) \subseteq S_L$: primes of good reduction for A
- $S_L(A, A')$: common primes of good reduction for A, A'
- G_S : Galois group of the maximal extension in $\bar{K}$ unramified over $S \subseteq S_K$

Unless explicitly stated otherwise, we assume all abelian varieties and morphisms are defined over K.

2 Arithmetic of elliptic curves

2.1 Local L-functions

Suppose A is an elliptic curve and $\mathfrak{p} \in S_K(A)$, and consider the following definitions

$$q_\mathfrak{p} := \#k_\mathfrak{p}, \quad a_\mathfrak{p} := 1 - \#A(k_\mathfrak{p}) + q_\mathfrak{p}, \quad \Lambda_\mathfrak{p}(T, A) := 1 - a_\mathfrak{p} T + q_\mathfrak{p} T^2.$$

The special fiber $A_\mathfrak{p}$ is an elliptic curve over $k_\mathfrak{p}$, and $\Lambda_\mathfrak{p}(T, A)$ is the numerator of its so-called Hasse-Weil zeta function.

We call $\Lambda_\mathfrak{p}(T, A)$ the *local L-function* of A at $\mathfrak{p}$. One basic property it has is that it satisfies the following identity:

$$\Lambda_\mathfrak{p}(1, A) = 1 - a_\mathfrak{p} + q_\mathfrak{p} = \#A(k_\mathfrak{p}).$$

A much deeper property $\Lambda_{\mathfrak{p}}(T, A)$ satisfies, the so-called Riemann hypothesis, is that the reciprocals $\alpha_{\mathfrak{p}}, \beta_{\mathfrak{p}} \in \mathbb{C}^{\times}$ of its zeros satisfy $|\alpha_{\mathfrak{p}}| = |\beta_{\mathfrak{p}}| = \sqrt{q_{\mathfrak{p}}}$ (cf. [6, ch. V, th. 2.3.1]). By using the quadratic formula one can verify the following equivalences:

$$|\alpha_{\mathfrak{p}}| = |\beta_{\mathfrak{p}}| = \sqrt{q_{\mathfrak{p}}} \quad \iff \quad \bar{\alpha}_{\mathfrak{p}} = \beta_{\mathfrak{p}} \quad \iff \quad |a_{\mathfrak{p}}| \leq 2\sqrt{q_{\mathfrak{p}}}.$$

We suppose without loss of generality that $\alpha_{\mathfrak{p}}$ has non-negative imaginary part so that it is well defined.

Recall that the absolute endomorphism ring of $A_{\mathfrak{p}}$ is an order in the algebra $E_{\mathfrak{p}} = \mathrm{End}(A_{\mathfrak{p}}) \otimes \mathbb{Q}$. Moreover, either $E_{\mathfrak{p}}$ is a quadratic imaginary field or it is a quaternion algebra (cf. [6, ch. V, th. 3.1]), and one says $A_{\mathfrak{p}}$ is *ordinary* or *supersingular* respectively.

Proposition 2. *Suppose $\mathfrak{p} \in S_K(A)$ does not lie over 2 or 3. Then either $A_{\mathfrak{p}}$ is ordinary and $[E_{\mathfrak{p}} : \mathbb{Q}] = 2$ or $A_{\mathfrak{p}}$ is supersingular and exactly one of the following holds:*

1. *$[E_{\mathfrak{p}} : \mathbb{Q}] = 4$ and $\Lambda_{\mathfrak{p}}(T) \in \{ (1 \pm \sqrt{q_{\mathfrak{p}}} T)^2 \}$;*
2. *$[E_{\mathfrak{p}} : \mathbb{Q}] = 2$ and $\Lambda_{\mathfrak{p}}(T) \in \{ 1 \pm \sqrt{q_{\mathfrak{p}}} T + q_{\mathfrak{p}} T^2 \}$;*
3. *$[E_{\mathfrak{p}} : \mathbb{Q}] = 2$ and $\Lambda_{\mathfrak{p}}(T) = 1 + q_{\mathfrak{p}} T^2$.*

Moreover, $A_{\mathfrak{p}}$ is ordinary if and only if $\mathfrak{p} \nmid a_{\mathfrak{p}}$.

Proof. This follows from [7, th. 4.1]. □

Recall $E = \mathrm{End}(A) \otimes \mathbb{Q}$.

Corollary 3. *Suppose $[E : \mathbb{Q}] = 2$ and $E \subseteq K$. If $\mathfrak{p} \in S_K(A)$ does not lie over 2 or 3, then E splits $\Lambda_{\mathfrak{p}}(T)$.*

Proof. There is an embedding $E \to E_{\mathfrak{p}}$, and thus proposition 2 implies either $E = E_{\mathfrak{p}}$ or $[E_{\mathfrak{p}} : \mathbb{Q}] = 4$ and $\Lambda_{\mathfrak{p}}(T)$ splits over $\mathbb{Q}$. The Cayley-Hamilton theorem implies $\Lambda_{\mathfrak{p}}(\mathrm{Frob}_{\mathfrak{p}}, A) = 0$ in $E_{\mathfrak{p}}$, and thus if $E = E_{\mathfrak{p}}$, then $\Lambda_p(T, A)$ has a zero in E and so splits in E. □

2.2 Cartan Subgroups

Suppose ℓ is odd, and let $C_\ell \subseteq \mathrm{GL}_2(\mathbb{F}_\ell)$ be a *Cartan subgroup*. This means that, up to conjugating by some $g \in \mathrm{GL}_2(\mathbb{F}_\ell)$, for some $d \in \mathbb{F}_\ell^{\times}$ we have

$$C_\ell = \left\{ \begin{pmatrix} a & b \\ bd & a \end{pmatrix} \ : \ a, b \in \mathbb{F}_\ell \right\} \cap \mathrm{GL}_2(\mathbb{F}_\ell).$$

The elements with $b = 0$ correspond to the scalars $\mathbb{F}_\ell^{\times} \subseteq \mathrm{GL}_2(\mathbb{F}_\ell)$, and if $d = \delta^2$ with $\delta \in \bar{\mathbb{F}}_\ell$, then the $\bar{\mathbb{F}}_\ell$-eigenspaces of the non-scalar elements have the form $y = \pm\delta x$, with eigenvalues $a \pm b\delta$.

If $\delta \in \mathbb{F}_\ell$, then C_ℓ is called a *split* Cartan subgroup and it consists of all elements which are diagonal with respect to a fixed basis of $\mathbb{F}_\ell^2$. Thus there is an isomorphism

$C_\ell \simeq \mathbb{F}_\ell^\times \times \mathbb{F}_\ell^\times$, defined up to post-composition with $(x, y) \mapsto (y, x)$, and we have $\#C_\ell = (\ell - 1)^2$.

If $\delta \notin \mathbb{F}_\ell$, then $[\mathbb{F}_\ell(\delta) : \mathbb{F}_\ell] = 2$ and C_ℓ is called a *non-split* Cartan subgroup. The elements of C_ℓ, plus the zero matrix, form a commutative division subring of $M_2(\mathbb{F}_\ell)$ with ℓ^2 element. Thus there is an isomorphism $C_\ell \simeq \mathbb{F}_{\ell^2}^\times$, defined up to post-composition with $x \mapsto x^\ell$, and we have $\#C_\ell = \ell^2 - 1$.

2.3 Galois Theory

Let $K_\ell = K(A[\ell])$, and let G_ℓ be the Galois group of K_ℓ/K. We choose a basis of $A[\ell]$ so that we obtain an isomorphism $\mathrm{Aut}(A[\ell]) \simeq \mathrm{GL}_{2g}(\mathbb{F}_\ell)$, for $g = \dim(A)$, and thus there is a natural embedding $G_\ell \to \mathrm{GL}_{2g}(\mathbb{F}_\ell)$ defined up to conjugacy.

We fix a polarization of A and suppose ℓ does not divide its degree so that one can define the Weil pairing on $A[\ell]$. The pairing takes its values in μ_ℓ, the group of ℓth roots of unity, so its existence implies $\mu_\ell \subseteq K_\ell$. It is also Galois equivariant, that is, the following identity holds for all $\gamma \in G_\ell$:

$$\langle P^\gamma, Q^\gamma \rangle = \langle P, Q \rangle^\gamma, \quad \forall P, Q \in A[\ell]. \tag{1}$$

We write $H_\ell \subseteq G_\ell$ for the Galois group of $K_\ell/K(\mu_\ell)$. There is a natural embedding $G_\ell/H_\ell \to \mathrm{Aut}(\mu_\ell) = \mathbb{F}_\ell^\times$, and we write $\chi_\ell : G_\ell \to \mathbb{F}_\ell^\times$ for the composition of this embedding with the quotient map $G_\ell \to G_\ell/H_\ell$.

Remark 4. *If $g = 1$, then χ_ℓ is the restriction to G_ℓ of* $\det : \mathrm{GL}_2(\mathbb{F}_\ell) \to \mathbb{F}_\ell^\times$.

Remark 5. *The induced homomorphism $\chi_\ell : G_K \to \mathbb{F}_\ell^\times$ is the cyclotomic character.*

Let $E = \mathrm{End}(A) \otimes \mathbb{Q}$.

Proposition 6. *Suppose A is an elliptic curve. If $E \subseteq K$, then one of the following holds for all $\ell \gg 0$:*

1. *$E = \mathbb{Q}$ and $G_\ell = \mathrm{GL}_2(\mathbb{F}_\ell)$;*
2. *$E \neq \mathbb{Q}$ and $G_\ell = C_\ell$ for some Cartan subgroup $C_\ell \subseteq \mathrm{GL}_2(\mathbb{F}_\ell)$.*

Proof. The first part follows from [4, théorème 2]. The second follows from [4, §4.5, corollaire] (cf. section 3). □

The following is a useful independence result:

Proposition 7. *Suppose A is an elliptic curve and L/K is a finite extension, and let $K' = KE$. If $\ell \gg 0$, then $L \cap K_\ell \subseteq K'$.*

Proof. If we write $K'_\ell = K'(A[\ell])$, then $L \cap K'_\ell = K'$ implies $L \cap K_\ell \subseteq K'$. Thus it suffices to show the $L \cap K'_\ell = K'$ for all $\ell \gg 0$, and so we replace K, L by K', LE and suppose $E \subseteq K$. There are only finitely many possibilities for the intersection $L \cap K_\ell$ since L is a finite (separable) extension of K, so some extension K''/K occurs for infinitely many ℓ. In particular, [4, th. 3 and §4.5, cor.] implies $K_{\ell_1} \cap K_{\ell_2} = K$ for $\ell_1 > \ell_2 \gg 0$, so the only possibility is $K'' = K$. That is, $L \cap K_\ell = K$ for every $\ell \gg 0$. □

Suppose A' is another polarized abelian variety, and let K'_ℓ, G'_ℓ, and χ'_ℓ be defined accordingly for A'. Consider the compositum $K_\ell K'_\ell$ as an extension of K and let $\Gamma_\ell \subseteq G_\ell \times G'_\ell$ be its Galois group.

Lemma 8. *Γ_ℓ lies in the subgroup of $(\gamma, \gamma') \in G_\ell \times G'_\ell$ satisfying $\chi_\ell(\gamma) = \chi'_\ell(\gamma')$.*

Proof. As noted in remark 5, the induced characters $\chi_\ell : G_K \to \mathbb{F}_\ell^\times$ and $\chi'_\ell : G_K \to \mathbb{F}_\ell^\times$ are both the cyclotomic character, that is, they are the same character. Therefore the compositions of the projections $\Gamma_\ell \to G_\ell, \Gamma_\ell \to G'_\ell$ with the respective restrictions of χ_ℓ, χ'_ℓ are the same map $\Gamma_\ell \to \mathbb{F}_\ell^\times$, that is, $\chi_\ell(\gamma) = \chi'_\ell(\gamma')$ for each $(\gamma, \gamma') \in \Gamma_\ell$. □

3 Complex Multiplication

Throughout this section we assume A is an elliptic curve and that both $[E : \mathbb{Q}] = 2$ and $E \subseteq K$. Thus E is a quadratic imaginary field and $\mathrm{End}_K(A) \otimes \mathbb{Q} = E$ (cf. [5, §II.2, th. 2.2]). Unless stated otherwise, we also suppose that A, A' are $\bar{K}$-isogenous so that $\mathrm{End}(A') \otimes \mathbb{Q} = E$ and define $S = S_K(A, A')$.

Suppose $\ell \geq 3$ is unramified in E, and fix a prime $\lambda \in S_E$ lying over ℓ and let $\bar{\lambda} \in S_E$ be its $\mathrm{Gal}(E/\mathbb{Q})$-conjugate. The modules $A[\lambda]$ and $A[\bar{\lambda}]$ are well-defined, and we have the following isomorphism of Galois modules:

$$A[\ell] \simeq \begin{cases} A[\lambda] \times A[\bar{\lambda}] & \ell \text{ split in } E \\ A[\lambda] & \ell \text{ inert in } E \end{cases}. \tag{2}$$

We note that $A[\lambda]$ is a $\mathbb{F}_\lambda[G_K]$-module satisfying $\dim_{\mathbb{F}_\lambda}(A[\lambda]) = 1$, thus $\mathrm{Aut}_{\mathbb{F}_\lambda}(A[\lambda]) = \mathbb{F}_\lambda^\times$. Moreover, if $\ell \gg 0$, then the projections $A[\ell] \to A[\lambda], A[\bar{\lambda}]$ lift to endomorphisms of A. In particular, for almost all ℓ, the action of G_ℓ must commute with the projections $A[\ell] \to A[\lambda], A[\bar{\lambda}]$ and respective actions of $\mathbb{F}_\lambda^\times, \mathbb{F}_{\bar{\lambda}}^\times$. The subgroup $C_\ell \subseteq \mathrm{Aut}(A[\ell])$ of all elements with this property is a Cartan subgroup. More precisely, C_ℓ is split if and only if ℓ splits in K, and then $C_\ell = \mathrm{Aut}(A[\lambda]) \times \mathrm{Aut}(A[\bar{\lambda}]) = \mathbb{F}_\lambda^\times \times \mathbb{F}_{\bar{\lambda}}^\times$. Otherwise C_ℓ is non-split and ℓ is inert in K, and then $C_\ell = \mathbb{F}_\lambda^\times$.

Let $K_\lambda = K(A[\lambda])$ and $G_\lambda \subseteq \mathrm{Aut}(A[\lambda])$ be the Galois group of K_λ/K.

Proposition 9. *If $\lambda \gg 0$, then there is a canonical isomorphism $G_\lambda = \mathbb{F}_\lambda^\times$.*

Proof. Suppose ℓ is large so that proposition 6 implies $G_\ell = C_\ell$. If C_ℓ is non-split, then $G_\lambda = G_\ell = C_\ell = \mathbb{F}_\lambda^\times$, so suppose C_ℓ is split and thus $C_\ell = \mathbb{F}_\lambda^\times \times \mathbb{F}_{\bar{\lambda}}^\times$ and $K_\ell = K_\lambda K_{\bar{\lambda}}$. There are natural embeddings $G_\ell \subseteq G_\lambda \times G_{\bar{\lambda}}$ and $G_\lambda \times G_{\bar{\lambda}} \subseteq C_\ell$ and their composition is a bijection, hence $G_\lambda \times G_{\bar{\lambda}} = C_\ell$ and thus $G_\lambda = \mathbb{F}_\lambda^\times$. □

If we write $S_\ell \subseteq S$ for the subset of $\mathfrak{p}$ not lying over ℓ, then K_ℓ/K is unramified over S_ℓ and hence so is K_λ/K. That is, the composed character $G_K \to G_\lambda \subseteq \mathbb{F}_\lambda^\times$ factors through $G_K \to G_{S_\ell}$, and we write $\psi_\lambda : G_{S_\ell} \to \mathbb{F}_\lambda^\times$ for the corresponding character. For split C_ℓ, let $\psi_{\bar{\lambda}} : G_{S_\ell} \to \mathbb{F}_{\bar{\lambda}}^\times$ be defined similarly, and otherwise let $\psi_{\bar{\lambda}} : G_{S_\ell} \to \mathbb{F}_\lambda^\times$ be the composition of ψ_λ and the ℓth power map $\mathbb{F}_\lambda^\times \to \mathbb{F}_\lambda^\times$.

Lemma 10. *If $\mathfrak{p} \in S_\ell$ and if $\phi_\mathfrak{p} \in G_{S_\ell}$ is an element in the conjugacy class of the Frobenius, then $(\psi_\lambda + \psi_{\bar{\lambda}})(\phi_\mathfrak{p}) \equiv a_\mathfrak{p} \pmod{\ell}$ and $\psi_\lambda \psi_{\bar{\lambda}}(\phi_\mathfrak{p}) \equiv q_\mathfrak{p} \pmod{\ell}$.*

Proof. As noted in remark 5, the composition of $G_K \to G_{S_\ell} \to G_\ell$ and $\det : G_\ell \to \mathbb{F}_\ell^\times$ is the cyclotomic character χ_ℓ. Moreover, $\phi_\mathfrak{p}$ acts in $\bar{k}_\mathfrak{p}$ as $x \mapsto x^{q_\mathfrak{p}}$, thus $\chi_\ell(\phi_\mathfrak{p}) \equiv q_\mathfrak{p} \pmod{\ell}$. Similarly, the restriction $\mathrm{Tr} : G_\ell \to \mathbb{F}_\ell$ is well defined and $\mathrm{Tr}(\phi_\mathfrak{p}) \equiv a_\mathfrak{p} \pmod{\ell}$.

If C_ℓ is split, then $C_\ell = \mathbb{F}_\lambda^\times \times \mathbb{F}_{\bar{\lambda}}^\times$ and $G_\ell = (\psi_\lambda(G_K), \psi_{\bar{\lambda}}(G_K)) \subseteq C_\ell$, and $\det, \mathrm{Tr}$ are respectively given by the maps $(x, y) \mapsto xy$ and $(x, y) \mapsto x + y$. Otherwise, $C_\ell = \mathbb{F}_\lambda^\times$ and $G_\ell = \psi_\lambda(G_K) \subseteq C_\ell$, and $\det, \mathrm{Tr}$ are respectively the norm and trace maps $\mathbb{F}_\lambda^\times \to \mathbb{F}_\ell^\times$ and $\mathbb{F}_\lambda \to \mathbb{F}_\ell$. □

For each $\mathfrak{p} \in S_K(A)$, corollary 3 implies the reciprocals $\alpha_\mathfrak{p}, \bar{\alpha}_\mathfrak{p}$ of the zeros of $\Lambda_\mathfrak{p}(T)$ lie in E (and thus in K), so for $\mathfrak{p}$ not dividing ℓ, lemma 10 implies we have the following identities:

$$\Lambda_\mathfrak{p}(T) \equiv (1 - \alpha_\mathfrak{p} T)(1 - \bar{\alpha}_\mathfrak{p} T) \equiv (1 - \psi_\lambda(\phi_\mathfrak{p})T)(1 - \psi_{\bar{\lambda}}(\phi_\mathfrak{p})T) \pmod{\lambda}. \tag{3}$$

Suppose A' is $\bar{K}$-isogenous to A. Then a similar congruence holds for $\Lambda'_\mathfrak{p}(T)$ and $\mathfrak{p} \in S_K(A')$, and in particular, we have the following identities for $\mathfrak{p} \in S$:

$$\{\alpha_\mathfrak{p}, \bar{\alpha}_\mathfrak{p}\} \equiv \{\psi_\lambda(\phi_\mathfrak{p}), \psi_{\bar{\lambda}}(\phi_\mathfrak{p})\}, \quad \{\alpha'_\mathfrak{p}, \bar{\alpha}'_\mathfrak{p}\} \equiv \{\psi'_\lambda(\phi_\mathfrak{p}), \psi'_{\bar{\lambda}}(\phi_\mathfrak{p})\} \pmod{\lambda}. \tag{4}$$

Let $\varepsilon_\lambda : G_{S_\ell} \to \mathbb{F}_\lambda^\times$ be the character $\varepsilon_\lambda := \psi'_\lambda / \psi_\lambda$ so that $A[\lambda] \otimes \varepsilon_\lambda \simeq A'[\lambda]$.

Lemma 11. *If A, A' are $\bar{K}$-isogenous, then for some $m \geq 1$ and all $\lambda \gg 0$, the order of ε_λ is at most m.*

Proof. Suppose L/K is a finite Galois extension and over which A, A' are isogenous, and let $S'_\ell \subseteq S_\ell$ be the subset of $\mathfrak{p}$ which are unramified in L so that $\psi_\lambda, \psi'_\lambda, \varepsilon_\lambda$ all factor through characters $G_{S'_\ell} \to \mathbb{F}_\lambda^\times$. For each $\mathfrak{p} \in S'_\ell$, choose $\mathfrak{q} \in S_L$ dividing $\mathfrak{p}$ and let $\phi_\mathfrak{p}, \phi_\mathfrak{q} \in G_{S'_\ell}$ be the corresponding Frobenius elements. Then we have the following identities:

$$\psi_\lambda(\phi_\mathfrak{p})^{[k_\mathfrak{q} : k_\mathfrak{p}]} \equiv \psi_\lambda(\phi_\mathfrak{q}), \quad \psi'_\lambda(\phi_\mathfrak{p})^{[k_\mathfrak{q} : k_\mathfrak{p}]} \equiv \psi'_\lambda(\phi_\mathfrak{q}) \pmod{\lambda}.$$

Suppose $\iota : A \to A'$ is an L-isogeny. If ℓ does not divide $\deg(\iota)$, then ι induces an isomorphism $A[\lambda] \simeq A'[\lambda]$ of G_L-modules and thus the restrictions $\psi_\lambda : G_L \to \mathbb{F}_\lambda^\times$ and $\psi'_\lambda : G_L \to \mathbb{F}_\lambda^\times$ are isomorphic. Therefore, since L/K is Galois and so $[k_\mathfrak{q} : k_\mathfrak{p}] \mid [L : K]$, we have the following identities:

$$\varepsilon_\lambda(\phi_\mathfrak{p})^{[L:K]} \equiv (\psi_\lambda(\phi_\mathfrak{p}) / \psi'_\lambda(\phi_\mathfrak{p}))^{[L:K]} \equiv 1 \pmod{\lambda}.$$

That is, ε_λ has order dividing $[L : K]$ for every $\lambda \gg 0$. □

Corollary 12. *Suppose A, A' are $\bar{K}$-isogenous, and let $S = S_K(A, A')$. If $\lambda \gg 0$, then ε_λ factors through the quotient $G_{S_\ell} \to G_S$.*

Proof. Let m be as in lemma 11, and suppose $\lambda \gg 0$ so that the order of ε_λ is at most m. Since ε_λ takes values in $\mathbb{F}_\lambda^\times$, it has order prime to ℓ, and thus ε_λ is at worst tamely ramified over $\mathfrak{p}$ dividing ℓ. Therefore it suffices to show the restriction of ε_λ to the tame inertia group $I_\ell \subseteq G_{S_\ell}$, defined up to conjugacy, is trivial (cf. [4, §1.6]). Equivalently, it suffices to show that the corresponding invariant, which is an element in $\mathbb{Q}/\mathbb{Z}$ with denominator coprime to ℓ, is zero (cf. [4, §1.7]).

If $\lambda \gg 0$, then ℓ is unramified in K and thus the corollaries of [4, prop. 11, prop. 12] imply that the respective invariants x, x' of $\psi_\lambda, \psi'_\lambda$ are elements of

$$X = \{\ 0,\ 1/(\ell-1),\ 1/(\ell^2-1),\ \ell/(\ell^2-1)\ \}.$$

Swapping A, A' if necessary, we suppose $x \geq x'$. Then the invariant of $\varepsilon_\lambda = \psi_\lambda/\psi'_\lambda$ is $x - x'$ and thus is an element of

$$X' = \{\ 0, 1/(\ell-1),\ 1/(\ell^2-1),\ \ell/(\ell^2-1),\ \ell/(\ell-1),\ 1/(\ell+1)\ \}$$

If m_λ is the order of ε_λ, then $x - x' = a/b$ is a multiple of $1/m_\lambda$, that is, $b \mid m_\lambda$ when $\gcd(a,b) = 1$. Thus if $a \neq 0$, then b is one of $\ell - 1$, $\ell + 1$, or $\ell^2 - 1$. In particular, since $b \leq m_\lambda \leq m$, if $\ell > m+1$, then we must have $a = 0$, that is, the invariant of ε_λ is trivial for $\lambda \gg 0$. □

Let $\mu \subset E$ by the subgroup of roots of unity. We define $\mu \to \mathbb{F}_\lambda^\times$ to be the homomorphism induced by reduction modulo λ; it is injective, if $\ell \geq 5$. If λ is split, we define $\mu \to \mathbb{F}_{\bar\lambda}^\times$ to be reduction modulo $\bar\lambda$.

Corollary 13. *Suppose A, A' are $\bar K$-isogenous. If $\lambda \gg 0$, then ε_λ takes values in μ and $\varepsilon_\lambda = \varepsilon_{\lambda'}$ for all λ' in some infinite $\Lambda \subseteq S_E$.*

Proof. Suppose $\lambda \gg 0$ so that lemma 11 implies ε_λ has order at most m and corollary 12 implies ε_λ factors through $G_{S_\ell} \to G_S$. Hermite's theorem implies the set of characters of G_S of order at most m is finite, hence up to excluding finitely many λ we may suppose $\varepsilon_\lambda = \varepsilon_{\lambda'}$ for all λ' in an infinite $\Lambda' \subseteq S_E$.

Suppose $\mathfrak{p} \in S_\ell$. Up to swapping $\alpha_\mathfrak{p}, \bar\alpha_\mathfrak{p}$ and up to swapping $\alpha'_\mathfrak{p}, \bar\alpha'_\mathfrak{p}$, we apply (4) and assume the following identities hold for all λ' not dividing $\mathfrak{p}$ and in some infinite $\Lambda \subseteq \Lambda'$:

$$\psi_{\lambda'}(\phi_\mathfrak{p}) \equiv \alpha_\mathfrak{p}, \quad \psi'_{\lambda'}(\phi_\mathfrak{p}) \equiv \alpha'_\mathfrak{p}, \quad \varepsilon_{\lambda'}(\phi_\mathfrak{p}) \equiv \alpha_\mathfrak{p}/\alpha'_\mathfrak{p} \pmod{\lambda'}.$$

Since this identity holds for infinitely many λ' and since $\varepsilon_\lambda(\phi_\mathfrak{p}) = \zeta_\mathfrak{p} = \varepsilon_{\lambda'}(\phi_\mathfrak{p})$ for some root of unity $\zeta_\mathfrak{p} \in \bar E$, we must have $\zeta_\mathfrak{p} = \alpha_\mathfrak{p}/\alpha'_\mathfrak{p}$ and thus $\zeta_\mathfrak{p} \in \mu \subset E$. □

Remark 14. *Suppose $\lambda \gg 0$, and let $\Lambda \subseteq S_E$ be as in corollary 13 and $\chi : G_S \to \mu$ be such that $\chi = \varepsilon_\lambda$ for every $\lambda \in \Lambda$. Then $\psi_\lambda \chi = \psi'_\lambda$, or equivalently, $A[\lambda] \otimes \chi \simeq A'[\lambda]$ for every $\lambda \in \Lambda$.*

Suppose $\ell \geq 5$, and consider the following embedding $\mu \subseteq C_\ell$: if C_ℓ is split, then it is the product embedding $\mu \to \mathbb{F}_\lambda^\times \times \mathbb{F}_{\bar\lambda}^\times = C_\ell$ given by $\zeta \mapsto (\zeta, \zeta)$ $(= (\zeta, 1/\zeta) \in \mathbb{F}_\ell^\times \times \mathbb{F}_\ell^\times$ via the field isomorphisms $\mathbb{F}_\lambda = \mathbb{F}_\ell = \mathbb{F}_{\bar\lambda})$; otherwise it is the embedding $\mu \to \mathbb{F}_\lambda^\times = C_\ell$. Thus for any character $\chi : G_K \to \mu$ we can consider the twist $A[\ell] \otimes \chi$ as an $\mathbb{F}_\ell[G_K]$-module.

Lemma 15. *If $A[\lambda] \otimes \chi \simeq A'[\lambda]$, then $A[\ell] \otimes \chi \simeq A'[\ell]$.*

Proof. If ℓ is inert, then there is nothing to prove, so suppose ℓ is split and $A[\lambda] \otimes \chi \simeq A'[\lambda]$. On one hand, $C_\ell = \mathbb{F}_\lambda^\times \times \mathbb{F}_{\bar{\lambda}}^\times$ and the composition of $\chi : G_K \to \mu \subseteq C_\ell$ with the projection $C_\ell \to \mathbb{F}_{\bar{\lambda}}^\times$ and bijection $\mathbb{F}_{\bar{\lambda}} = \mathbb{F}_\lambda$ is χ^{-1}, thus $A[\ell] \otimes \chi$ is isomorphic to the direct sum of $A[\lambda] \otimes \chi$ and $A[\bar{\lambda}] \otimes (1/\chi)$. On the other hand, since $\psi_\lambda \chi = \psi'_\lambda$, lemma 10 implies $\psi_\lambda \psi_{\bar{\lambda}} = \psi'_\lambda \psi'_{\bar{\lambda}}$, thus $\psi'_{\bar{\lambda}} = \psi_{\bar{\lambda}}/\chi$ and so $A[\bar{\lambda}] \otimes (1/\chi) \simeq A'[\bar{\lambda}]$. Together these imply $A[\ell] \otimes \chi \simeq A'[\ell]$. □

Corollary 16. *If A, A' are $\bar{K}$-isogenous, then there is an infinite $\Lambda_\mathbb{Q} \subseteq S_\mathbb{Q}$ and a character $\chi : G_K \to \mu$ such that $A[\ell] \otimes \chi \simeq A'[\ell]$ for every $\ell \in \Lambda_\mathbb{Q}$.*

Proof. Let $\Lambda_\mathbb{Q} = \{\lambda \cap \mathbb{Q} : \lambda \in \Lambda\}$ and combine remark 14 and lemma 15. □

4 Fibers of elliptic curves

4.1 Essentially Equal Functions

We say that a pair of functions f, f' defined on a subset of S_K are *essentially equal* if and only if they are equal on some density-one subset, and then we write $f \approx f'$.

Given abelian varieties A, A', let λ, λ' be the functions on $S_K(A)$ which maps $\mathfrak{p} \in S_K(A)$ to the respective local L-function $\Lambda_\mathfrak{p}(T, A), \Lambda_\mathfrak{p}(T, A') \in \mathbb{Z}[T]$ (cf. section 2.1).

Proposition 17. *$\lambda \approx \lambda'$ if and only if A, A' are K-isogenous.*

Proof. See [1, Corollary 2]. □

Given an abelian variety A and finite extension L/K, we consider the function ϕ_L which maps $\mathfrak{p} \in S_L(A)$ to the isomorphism class of the group of points $A(k_\mathfrak{p})$ on the special fiber. Given a function ψ on the set of groups modulo isomorphism, we write $\psi\phi_L$ for the composed function which maps $\mathfrak{p} \in S_L(A)$ to $\psi(A(k_\mathfrak{p}))$. We define ϕ'_L and $\psi\phi'_L$ similarly given an additional abelian variety A'.

The following lemma demonstrates $\approx$ behaves well with respect to base change:

Lemma 18. *If A, A' are abelian varieties and if $\psi\phi_K \approx \psi\phi'_K$, then $\psi\phi_L \approx \psi\phi'_L$.*

Proof. Let $S'_K \subseteq S_K$ and $S'_L \subseteq S_L$ be the respective subsets of primes of degree one. They have Dirichlet density one. If $\mathfrak{q} \in S'_L$ and if $\mathfrak{p} := \mathfrak{q} \cap K$, then the embedding $k_\mathfrak{p} \to k_\mathfrak{q}$ is surjective and

$$\psi\phi_L(\mathfrak{q}) = \psi\phi_K(\mathfrak{p}) = \psi\phi'_K(\mathfrak{p}) = \psi\phi'_L(\mathfrak{q}),$$

and thus $\psi\phi_L(\mathfrak{q}) = \psi\phi'_L(\mathfrak{q})$ for all $\mathfrak{q}$ in the density-one set S'_L. □

Remark 19. *The converse does not hold: if A, A' are not K-isogenous but are L-isomorphic, then $\phi_{A,K} \not\approx \phi_{A',K}$ and $\phi_{A,L} \approx \phi_{A',L}$.*

For each A and ℓ, we write $\nu_{A,K}$ for the function $\mathfrak{p} \in S_K(A) \mapsto \#A(k_\mathfrak{p})$ and regard it as the composition of $\phi_{A,L}$ and the counting function $G \mapsto \#G$. A priori, one could have $\lambda_{A,K} \not\approx \lambda_{A',K}$ and yet still have $\nu_{A,K} \approx \nu_{A',K}$, but the lemma shows this does not occur for $\dim(A) = 1$:

Lemma 20. *If A, A' are elliptic curves over K, then $\nu_{A,K} \approx \nu_{A',K}$ if and only if A, A' are K-isogenous.*

Proof. If we write $\lambda = \lambda_{A,K}$ and define λ', ν, ν' similarly, then we the following equivalences between identities imply $\lambda \approx \lambda'$ if and only if $\nu \approx \nu'$:

$$\lambda(\mathfrak{p}) = \lambda'(\mathfrak{p}) \quad \iff \quad a_\mathfrak{p} = a'_\mathfrak{p} \quad \iff \quad \nu(\mathfrak{p}) = 1 - a_\mathfrak{p} + q_\mathfrak{p} = 1 - a'_\mathfrak{p} + q_\mathfrak{p} = \nu'(\mathfrak{p}).$$

The lemma follows if we apply proposition 17 to deduce that A, A' are K-isogenous if and only if $\lambda \approx \lambda'$.

□

4.2 Radicals

Suppose ℓ is a prime, and let $g = \dim(A)$. Recall that the radical of a finite group G is the square free product of the primes dividing $\#G$. We consider only the ℓ-part of the radical and define ρ_ℓ to be the following map:

$$S_K(A) \to \{0, 1\} : \mathfrak{p} \mapsto \min\{1, v_\ell(\#A(k_\mathfrak{p}))\};$$

Recall that in section 2.3 we defined $K_\ell = K(A[\ell])$ and $G_\ell = \mathrm{Gal}(K_\ell/K)$. The following lemma gives a Galois-theoretic way to analyze ρ_ℓ:

Lemma 21. *Suppose $\mathfrak{p} \in S_K(A)$ does not ramify in K_ℓ and $\mathfrak{q} \in S_{K_\ell}$ lies over $\mathfrak{p}$. If $\phi_\mathfrak{q} \in G_\ell$ is the Frobenius of $\mathfrak{q}$, then $\rho_\ell(\mathfrak{p}) = 1$ if and only if $\det(\phi_\mathfrak{q} - 1) = 0$.*

Proof. The embedding $A(k_\mathfrak{p}) \to A(k_\mathfrak{q})$ identifies $A(k_\mathfrak{p})[\ell]$ with $\ker(\phi_q - 1) \subseteq A[\ell]$, hence $\ell \mid \#A(k_\mathfrak{p})$ if and only if 1 is an eigenvalue of $\phi_\mathfrak{q}$. □

Recall that we defined K'_ℓ and G'_ℓ for A' and that $\Gamma_\ell \subseteq G_\ell \times G'_\ell$ denotes the Galois group of the compositum $K_\ell K'_\ell / K$. Let ρ'_ℓ be defined accordingly for A'.

Lemma 22. *If $\rho_\ell \approx \rho'_\ell$, then $\det(\gamma - 1), \det(\gamma' - 1)$ are both zero or both non-zero for every $(\gamma, \gamma') \in \Gamma_\ell$.*

Proof. Suppose $S \subseteq S_K(A, A')$ has Dirichlet density one and that $\rho_\ell|_S = \rho'_\ell|_S$. Let $S' \subseteq S$ be the subset consisting of the primes $\mathfrak{p}$ which are unramified in $K_\ell K'_\ell$ and whose Frobenius conjugacy class in Γ_ℓ contains (γ, γ'). The density of S' is positive, and for each $\mathfrak{p} \in S'$, lemma 21 implies the values $\rho_\ell(\mathfrak{p})$, $\rho'_\ell(\mathfrak{p})$ respectively identify whether or not $\det(\gamma - 1), \det(\gamma' - 1)$ are non-zero, and thus the hypothesis $\rho_\ell(\mathfrak{p}) = \rho'_\ell(\mathfrak{p})$ implies the determinants are both zero or both non-zero. □

5 Proof of Theorem 1

Let A, A' be elliptic curves over K and ρ_ℓ, ρ'_ℓ the maps defined in section 4.2. In this section we prove the following result:

Theorem 1. *Suppose $S' \subseteq S = S_K(A, A')$ has density one and $\Lambda \subseteq \mathbb{N}$ is an infinite set of primes. If A, A' are elliptic curves over K, then the following are equivalent:*

1. *A, A' are K-isogenous;*
2. *$\rho_\ell(\mathfrak{p}) = \rho'_\ell(\mathfrak{p})$ for every $\ell \in \Lambda$ and $\mathfrak{p} \in S'$.*

The implication $1 \Rightarrow 2$ follows from lemma 20, so we prove $2 \Rightarrow 1$. The structure of the proof is as follows:

1. We reduce to the case $E, E' \subseteq K$ for $E = \mathrm{End}(A) \otimes \mathbb{Q}$ and $E' = \mathrm{End}(A') \otimes \mathbb{Q}$.
2. We show $K(A[\ell]) = K(A'[\ell])$ for all ℓ in an infinite $\Lambda' \subseteq \mathbb{N}$ and deduce A, A' are $\bar{K}$-isogenous and $E = E'$.
3. We construct a character χ such that $A[\ell] \otimes \chi \simeq A'[\ell]$ for all ℓ in an infinite $\Lambda'' \subseteq \Lambda'$.
4. We prove $A[\ell] \simeq A'[\ell]$ for almost all $\ell \in \Lambda''$ and deduce that A, A' are K-isogenous.

The remainder of this section is broken into four pieces, one for each of these steps.

Step 1

Lemma 18 implies the hypotheses of the theorem hold over any finite extension of K, and two applications of the following lemma, one with A, A' swapped, imply that it suffices to prove theorem 1 over $KEE' = (KE)E'$:

Lemma 23. *If A, A' are KE-isogenous, then $E' = E$ and A, A' are K-isogenous.*

Proof. The identity $\mathrm{End}(A) \otimes \mathbb{Q} = \mathrm{End}(A') \otimes \mathbb{Q}$ holds for any pair of $\bar{K}$-isogenous abelian varieties, thus $E = E'$. Moreover, if $E \subseteq K$ then A, A' are K-isogenous, so suppose $E \not\subseteq K$.

Let $S \subseteq S_K(A, A')$ be the density-one subset of $\mathfrak{p}$ which have degree one and which neither ramify in KE or lie over 2 or 3. We will show that $a_\mathfrak{p} = a'_\mathfrak{p}$ for every $\mathfrak{p} \in S$, and then lemma 20 implies A, A' are K-isogenous, so suppose $\mathfrak{p} \in S$.

If $\mathfrak{q} \in S_{KE}$ is a prime lying over $\mathfrak{p}$, then $a_\mathfrak{q} = a'_\mathfrak{q}$ since A, A' are KE-isogenous. If $\mathfrak{p}$ splits in KE, then we have $a_\mathfrak{p} = a_\mathfrak{q}$ and $a'_\mathfrak{q} = a'_\mathfrak{p}$ since $k_\mathfrak{q} = k_\mathfrak{p}$, thus $a_\mathfrak{p} = a'_\mathfrak{p}$. Otherwise, $\mathfrak{p} \in S$ is inert, thus [3, ch. 10 §4 theorem 10] implies A, A' have supersingular reduction over $\mathfrak{p}$. Moreover, since $q_\mathfrak{p}$ is prime and thus not a square, proposition 2 implies $a_\mathfrak{p} = a'_\mathfrak{p} = 0$. Therefore $a_\mathfrak{p} = a'_\mathfrak{p}$ for every $\mathfrak{p} \in S$ as claimed. □

Step 2

We use the notation of section 2.3, thus $K_\ell = K(A[\ell])$, $G_\ell = \mathrm{Gal}(K_\ell/K) \subseteq \mathrm{GL}_2(\mathbb{F}_\ell)$, and $H_\ell = G_\ell \cap \mathrm{SL}_2(\mathbb{F}_\ell)$ is the stabilizer of $K(\zeta_\ell)$. Similarly, we have corresponding objects $K'_\ell, G'_\ell, H'_\ell$. Finally, $\Gamma_\ell \subseteq G_\ell \times G'_\ell$ is the Galois group of $K_\ell K'_\ell/K$.

The kernels of the projections $\Gamma_\ell \to G_\ell$ and $\Gamma_\ell \to G'_\ell$ project onto normal subgroups of G'_ℓ and G_ℓ respectively. For example, lemma 8 implies the intersection of Γ_ℓ with the normal subgroup $\mathrm{SL}_2(\mathbb{F}_\ell) \times \{1\} \subseteq \mathrm{GL}_2(\mathbb{F}_\ell) \times \mathrm{GL}_2(\mathbb{F}_\ell)$ is the kernel of $\Gamma_\ell \to G'_\ell$ and it projects isomorphically onto a normal subgroup of G_ℓ contained in H_ℓ. Moreover, this kernel is trivial if and only if $K_\ell \subseteq K'_\ell$, thus both kernels are trivial if and only if $K_\ell = K'_\ell$.

Lemma 24. *Suppose $E, E' \subseteq K$. If $K_\ell \neq K'_\ell$ and if $\ell \gg 0$, then $\rho_\ell \not\approx \rho'_\ell$.*

Proof. Suppose $K_\ell \neq K'_\ell$ and $\ell \gg 0$, and without loss of generality suppose the kernel of $\Gamma_\ell \to G'_\ell$ is non-trivial and thus projects to a non-trivial normal subgroup of G_ℓ contained in H_ℓ. Since $E \subseteq K$ and ℓ is large, proposition 6 implies $G_\ell = \mathrm{GL}_2(\mathbb{F}_\ell)$ or $G_\ell = C_\ell$ for some Cartan subgroup $C_\ell \subseteq \mathrm{GL}_2(\mathbb{F}_\ell)$.

In the first case, the $g = -1$ lies in every non-trivial normal subgroup of $H_\ell = \mathrm{SL}_2(\mathbb{F}_\ell)$ (cf. [2, lem. 2.2]). In the second case, every $g \in H_\ell$ is semisimple and satisfies $\det(g) = 1$, so either $g = 1$ or $\det(g-1) \neq 0$. Either way, we can find an element $(g, 1)$ in the kernel satisfying $\det(g-1) \neq 0$, and thus lemma 22 implies $\rho_\ell \not\approx \rho'_\ell$. □

Since by assumption $\rho_\ell \approx \rho'_\ell$ for infinitely many ℓ, we conclude that $K_\ell = K'_\ell$ for all ℓ an an infinite $\Lambda' \subseteq \Lambda$.

Proposition 25. *If $K_\ell = K'_\ell$ for infinitely many ℓ, then A, A' are $\bar{K}$-isogenous and $E = E'$.*

Proof. The varieties A, A' are $\bar{K}$-isogenous by [2, theorem A], and thus $E = E'$. □

Step 3

Let $\mu \subset E^\times$ by the subgroup of roots of unity. If $[E : \mathbb{Q}] = 2$, then recall that, for $\ell \geq 5$, there is an embedding $\mu \to C_\ell \subseteq \mathrm{Aut}(A[\ell])$ (cf. section 3).

Lemma 26. *Suppose $\Lambda' \subseteq S_\mathbb{Q}$ is infinite and $E \subseteq K$ and $K_\ell = K'_\ell$ for all $\ell \in \Lambda'$. Then there exist an infinite $\Lambda'' \subseteq \Lambda'$ and a character $\chi : G_K \to \mu$ such that $A[\ell] \otimes \chi \simeq A'[\ell]$ for all $\ell \in \Lambda''$.*

Proof. If $E = \mathbb{Q}$ and if $\ell \gg 0$, then $G_\ell = G'_\ell \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$, and thus [4, lem. 8] implies, for each $\ell \in \Lambda$, there is a character $\chi_\ell : G_S \to \mu$ such that $A[\ell] \otimes \chi_\ell \simeq A'[\ell]$. Hermite's theorem implies there is a finite partition $\Lambda' = \Lambda'_1 \cup \ldots \cup \Lambda'_r$ such that $\chi_\ell = \chi_{\ell'}$ if and only if $\ell, \ell' \in \Lambda'_i$ for some i, thus there are $\chi : G_K \to \mu$ and an infinite $\Lambda'' \subseteq \Lambda'$ such that $\chi_\ell = \chi$ for all $\ell \in \Lambda''$. If $E \neq \mathbb{Q}$, then we can apply proposition 25 to deduce that A, A' are $\bar{K}$-isogenous and apply corollary 16 to conclude. □

Step 4

If $\chi : G_K \to \mu$ and $\Lambda'' \subseteq \Lambda'$ are as in lemma 26, then the following lemma implies χ must be trivial and hence $A[\ell] \simeq A'[\ell]$ for almost all $\ell \in \Lambda''$:

Lemma 27. *Suppose $E \subseteq K$ and $\chi : G_K \to \mu$ is non trivial. If $A[\ell] \otimes \chi \simeq A'[\ell]$ and if $\ell \gg 0$, then $\rho_\ell \not\approx \rho'_\ell$.*

Proof. Let L/K be the splitting field of χ. By construction, it is a Galois extension and χ identifies $\mathrm{Gal}(L/K)$ with the subgroup $\chi(G_K) \subseteq \mu$.

Let $S'_\ell \subseteq S$ be the subset of $\mathfrak{p}$ which split completely in K_ℓ/K. If $\mathfrak{p} \in S'_\ell$, then $A(k_\mathfrak{p})[\ell] = A[\ell]$ and also $\ell \mid \#k_\mathfrak{p} - 1$ since the existence of the Weil pairing implies $\mu_\ell \subseteq k_\mathfrak{p}$. Hence $\rho_\ell(\mathfrak{p}) = 1$ and we have the congruences

$$\Lambda_\mathfrak{p}(T) \equiv (1-T)^2 \pmod{\ell}.$$

Suppose $\mathfrak{p} \in S'$ and $\ell \geq 5$, and let $\zeta_\mathfrak{p} = \chi(\phi_\mathfrak{p})$, $\bar{\zeta}_\mathfrak{p} = 1/\zeta_\mathfrak{p}$ and let $\alpha_\mathfrak{p}, \bar{\alpha}_\mathfrak{p} \in \bar{\mathbb{F}}_\ell$ be the reciprocals of the eigenvalues of the image of $\phi_\mathfrak{p}$ in G_ℓ. Suppose $A[\ell] \otimes \chi \simeq A'[\ell]$. If $\mu = \mu_2$, then $\bar{\zeta}_\mathfrak{p} = \zeta_\mathfrak{p}$ and $\Lambda'_\mathfrak{p}(T) = \Lambda_\mathfrak{p}(\zeta_\mathfrak{p} T)$, and otherwise, up to swapping $\alpha_\mathfrak{p}, \bar{\alpha}_\mathfrak{p}$ or $\alpha'_\mathfrak{p}, \bar{\alpha}'_\mathfrak{p}$, we have the following congruences for some $\lambda \in S_E$ dividing ℓ:

$$\alpha'_\mathfrak{p} \equiv \psi'_\lambda(\phi_\mathfrak{p}) \equiv \psi_\lambda(\phi_\mathfrak{p})\chi(\phi_\mathfrak{p}) \equiv \zeta_\mathfrak{p}\alpha_\mathfrak{p}, \quad \bar{\alpha}'_\mathfrak{p} \equiv \bar{\zeta}_\mathfrak{p}\bar{\alpha}_\mathfrak{p} \pmod{\lambda}.$$

That is, for any μ and some $\lambda \in S_E$ dividing ℓ, we have the following congruences (cf. (3)):

$$\Lambda_\mathfrak{p}(T) \equiv (1-\alpha_\mathfrak{p}T)(1-\bar{\alpha}_\mathfrak{p}T), \quad \Lambda'_\mathfrak{p}(T) \equiv (1-\zeta_\mathfrak{p}\alpha_\mathfrak{p}T)(1-\bar{\zeta}_\mathfrak{p}\bar{\alpha}_\mathfrak{p}T) \pmod{\lambda}.$$

Therefore, if moreover $\mathfrak{p} \in S'_\ell$, then we have the following congruences:

$$\#A'(k_\mathfrak{p}) = \Lambda'_\mathfrak{p}(1) \equiv (1-\zeta_\mathfrak{p})(1-\bar{\zeta}_\mathfrak{p}) \pmod{\lambda}.$$

In particular, if $\zeta_\mathfrak{p} \neq 1$, then the last term is non zero and so $\rho'_\ell(\mathfrak{p}) = 0$.

To complete the proof we recall that $E \subseteq K$ and observe that proposition 7 implies $L \cap K_\ell = K$ for $\ell \gg 0$, thus the subset $S''_\ell \subseteq S'_\ell$ of $\mathfrak{p}$ such that $\zeta_\mathfrak{p} \neq 1$ has positive density. □

In summary, $A[\ell] \simeq A'[\ell]$ for infinitely many ℓ, hence [2, prop. 1.4] implies A, A' are K-isogenous. Q.E.D.

References

[1] G. Faltings, *Finiteness Theorems for Abelian Varieties over Number Fields*, Arithmetic Geometry, Edited by G. Cornell and J. H. Silverman, Springer-Verlag, New York, 1986, 9–27.

[2] G. Frey and M. Jarden, *Horizontal isogeny theorems*, Forum Math. **14** (2002), no. 6, 931–952.

[3] S. Lang, *Elliptic functions*, second edition, Graduate Texts in Mathematics 112, Springer-Verlag, New York, 1987.

[4] J-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.

[5] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 151, Springer-Verlag, New York, 1994.

[6] J. Silverman, *The arithmetic of elliptic curves*, Second edition, Graduate Texts in Mathematics 106, Springer, Dordrecht, 2009.

[7] W. C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. **4** (1969), no. 2, 521–560.

Chris Hall, University of Wyoming
E-mail: chall14@uwyo.edu

Antonella Perucca, Research Foundation - Flanders (FWO)
E-mail: antonellaperucca@gmail.com