Journal of Number Theory 164 (2016) 87–102

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Locally potentially equivalent two dimensional Galois representations and Frobenius fields of elliptic curves

Manisha Kulkarni [a], Vijay M. Patankar [b,*], C.S. Rajan [c]

[a] *International Institute of Information Technology Bangalore, Hosur Road, Bangalore, 560100, India*
[b] *School of Physical Sciences, Jawaharlal Nehru University, New Delhi, 110067, India*
[c] *School of Mathematics, Tata Institute of Fundamental Research, Dr. Homi Bhabha Road, Colaba, Bombay, 400005, India*

ARTICLE INFO

Article history:
Received 26 June 2015
Received in revised form 26 December 2015
Accepted 28 December 2015
Available online 3 February 2016
Communicated by Dipendra Prasad

MSC:
primary 11F80
secondary 11G05, 11G15

Keywords:
Galois representations
Elliptic curves
Frobenius fields
Complex multiplication

ABSTRACT

We show that a two dimensional ℓ-adic representation of the absolute Galois group of a number field which is locally potentially equivalent to a $GL(2)$-ℓ-adic representation ρ at a set of places of K of positive upper density is potentially equivalent to ρ.

As an application, for E_1 and E_2 defined over a number field K, with at least one of them without complex multiplication, we prove that the set of places v of K of good reduction such that the corresponding Frobenius fields are equal has positive upper density if and only if E_1 and E_2 are isogenous over some extension of K.

For an elliptic curve E defined over a number field K, we show that the set of finite places of K such that the Frobenius field $F(E, v)$ at v equals a fixed imaginary quadratic field F has

* Corresponding author.
E-mail addresses: manisha.shreesh@gmail.com (M. Kulkarni), vijaypatankar@gmail.com (V.M. Patankar), rajan@math.tifr.res.in (C.S. Rajan).

http://dx.doi.org/10.1016/j.jnt.2015.12.010

positive upper density if and only if E has complex multiplication by F.

1. Introduction

Let K be a global field and $G_K := \mathrm{Gal}(\bar{K}/K)$ denote the absolute Galois group over K of a separable closure $\bar{K}$ of K. Let Σ_K denote the set of finite places of K. For any place v of K, let K_v denote the completion of K at v, and G_{K_v} the corresponding local Galois group. Choosing a place w of $\bar{K}$ lying above v, allows us to identity G_{K_v} with the decomposition subgroup D_w of G_K. As w varies this gives a conjugacy class of subgroups of G_K.

Let ℓ be a rational prime not equal to the characteristic of K and let F be a ℓ-adic local field of characteristic zero. Suppose $\rho : G_K \to GL_n(F)$ is a continuous semisimple representation of G_K. We will assume that ρ is unramified outside a finite set of places of K. At a finite place v of K where ρ is unramified, let σ_v denote the Frobenius conjugacy class in the quotient group $G_K/\mathrm{Ker}(\rho)$. By an abuse of notation, we will also continue to denote by σ_v an element in the associated conjugacy class. Define the localization (or the local component) ρ_v of ρ at v, to be the representation of G_{K_v} obtained by restricting ρ to a decomposition subgroup at v. This is well defined up to isomorphism.

Define two representations r_1 and r_2 of a group Γ to be potentially equivalent, if there exists a subgroup Γ' of finite index in Γ such that $r_1 \mid_{\Gamma'} \simeq r_2 \mid_{\Gamma'}$. Suppose ρ_1 and ρ_2 are representations of G_K as above. Then ρ_1 and ρ_2 are said to be locally potentially equivalent at v, if their localizations $\rho_{1,v}$ and $\rho_{2,v}$ are potentially equivalent.

Let v be a place of K at which both ρ_1 and ρ_2 are unramified. If ρ_1 and ρ_2 are locally potentially equivalent at v, then there exists a natural number k_v such that the conjugacy classes $\rho_1(\sigma_v)^{k_v}$ and $\rho_2(\sigma_v)^{k_v}$ are equal in $GL_n(F)$, i.e., the eigenvalues of $\rho_1(\sigma_v)$ and $\rho_2(\sigma_v)$ differ by roots of unity.

Define the algebraic monodromy group G attached to ρ to be the smallest algebraic subgroup G of GL_n defined over F such that $\rho(G_K) \subset G(F)$.

Our main theorem is to say that locally potentially equivalent (at a sufficiently large set of places) two dimensional Galois representations are potentially equivalent.

Theorem 1. *Suppose $\rho_i : G_K \to GL_2(F),\ i = 1, 2$ are two continuous semisimple ℓ-adic representations of the absolute Galois group G_K of a global field K unramified outside a finite set of places of K, where F is a non-archimedean local field of characteristic zero and residue characteristic ℓ coprime to the characteristic of K.*

Suppose there exists a set T of finite places of K of positive upper density such that for every $v \in T$, $\rho_{1,v}$ and $\rho_{2,v}$ are potentially equivalent.

Assume that the algebraic monodromy group G_1 attached to the representation ρ_1 is isomorphic to GL_2, and that the determinant characters of ρ_1 and ρ_2 are equal.

Then, ρ_1 and ρ_2 are potentially equivalent, viz. there exists a finite extension L of K such that

$$\rho_1|_{G_L} \simeq \rho_2|_{G_L} .$$

We recall the notion of upper density: given a set $S \subset \Sigma_K$ of finite places of K, the *upper density* $ud(S)$ of S is defined as,

$$ud(S) := \text{limsup}_{x\to\infty} \frac{\#\{v \in \Sigma_K \mid Nv \leq x,\ v \in S\}}{\#\{v \in \Sigma_K \mid Nv \leq x\}}.$$

Remark 1. Theorem 1 is a special case of Theorem 2.1 of [5]. It was pointed out by J.-P. Serre that the proof of Theorem 2.1 given in [5] is erroneous. The error in the argument occurs in line 17, page 84 of [5], where it is asserted that under the map $x \mapsto x^m$ of an algebraic group G, a connected component G^ϕ maps *onto* a connected component. This is not true, as can be seen by considering G to be the normalizer of a maximal torus in $SL(2)$ and $m = 2$. Theorem 1 partially salvages this by proving a version of Theorem 2.1 of [5] for $n = 2$.

The proof of Theorem 1 uses an "analytic and algebraic continuation" of the Galois groups, involving specializing to appropriate elements in the algebraic Galois monodromy groups.

The following theorem [5, Theorem 3.1] considers the general situation for n-dimensional ℓ-adic representations, where the traces of the Frobenius conjugacy classes are equal at a sufficiently large set of places. This happens for instance when the Frobenius conjugacy classes differ by a root of unity. It will be used to prove Theorem 1, in the special case when the eigenvalues of $\rho_1(\sigma_v)$ and $\rho_2(\sigma_v)$ at $v \in T$ differ by $\{\pm 1\}$. The proof of this theorem was given as a consequence of [5, Theorem 2.1]. Since there is a gap in the proof of [5, Theorem 2.1], here we give a proof removing the dependence on [5, Theorem 2.1].

Theorem 2. *Suppose $\rho_i : G_K \to GL_n(F),\ i = 1, 2$ are two continuous semisimple ℓ-adic representations of the absolute Galois group G_K of a global field K unramified outside a finite set of places of K, where F is a non-archimedean local field of characteristic zero and residue characteristic ℓ coprime to the characteristic of K.*

Assume that there exists a set T of finite places of K not containing the ramified places of $\rho_1 \times \rho_2$ and the places of K lying above ℓ, such that for every $v \in T$, there exist non-zero integers $m_v > 0$ satisfying the following:

$$(\chi_{\rho_1}(\sigma_v))^{m_v} = (\chi_{\rho_2}(\sigma_v))^{m_v} ,$$

where $\chi_{\rho_1}(\sigma_v)$ (resp. $\chi_{\rho_1}(\sigma_v)$) is the trace of the image of the Frobenius conjugacy class $\rho_1(\sigma_v)$ (resp. $\rho_2(\sigma_v)$).

Suppose the upper density $ud(T)$ of T is positive, and the Zariski closure of $\rho_1(G_K)$ is a connected algebraic group.

Then, ρ_1 and ρ_2 are potentially equivalent, viz. there exists a finite extension L of K such that

$$\rho_1|_{G_L} \simeq \rho_2|_{G_L} .$$

1.1. Frobenius fields of elliptic curves

Let E be an elliptic curve defined over a number field K. The Galois group G_K acts in a natural manner on $E(\bar{K})$. For a rational prime ℓ, the Tate module $T_\ell(E) := \varprojlim_n E[\ell^n]$ is the G_K-module obtained as a projective limit of the G_K-modules $E[\ell^n]$ of ℓ^n-torsion points of E over $\bar{K}$. Let $V_\ell(E) = T_\ell(E) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$. The Tate module is of rank 2 over the ring of ℓ-adic integers $\mathbb{Z}_\ell$, and we have a continuous ℓ-adic representation $\rho_{E,\ell} : G_K \to GL_2(\mathbb{Q}_\ell)$.

Let $\Sigma_r \subset \Sigma_K$ be a finite set of places containing the finite places of bad reduction for E. The Galois module $V_\ell(E)$ is unramified at the finite places of K outside $\Sigma_{r,\ell} = \Sigma_r \cup \{v|\ell\}$. The representations ρ_ℓ form a compatible system of ℓ-adic representations, in that the characteristic polynomial $\phi_v(t)$ of $\rho_\ell(\sigma_v)$ is independent of ℓ and its coefficients are integral. Thus, $\phi_v(t) := t^2 - a_v(E)t + Nv$, with $a_v(E),\ Nv \in \mathbb{Z}$. Here, Nv is the cardinality of the residue field $k_v := \mathcal{O}_K/\mathfrak{p}_v$, where $\mathcal{O}_K$ is the ring of integers of K, and $\mathfrak{p}_v$ is the prime ideal of $\mathcal{O}_K$ corresponding to v.

Define the *Frobenius field* $F(E, v)$ of E at v as the splitting field of $\phi_v(t)$ over $\mathbb{Q}$. Thus, $F(E, v) = \mathbb{Q}(\pi_v) = \mathbb{Q}(\sqrt{a_v(E)^2 - 4Nv})$, where π_v is a root of $\phi_v(t)$. The Hasse bound $|a_v(E)| \leq 2\sqrt{Nv}$ implies that $F(E, v)$ is either $\mathbb{Q}$ or an imaginary quadratic field.

Let F be an imaginary quadratic field. The elliptic curve E is said to have complex multiplication by F, if there is an embedding of F in $\mathrm{End}_{\bar{K}}(E) \otimes \mathbb{Q}$. The elliptic curve E is said to have complex multiplication (CM), if E admits CM by some imaginary quadratic field F.

As an application of and motivation for the Theorem 1, we have the following multiplicity-one type theorem under the assumption that the set of places v for which the Frobenius fields coincide has positive upper density.

Theorem 3. *Let E_1 and E_2 be two elliptic curves over a number field K. Let Σ_r be a finite subset of the set Σ_K of finite places of K containing the places of bad reduction of E_1 and E_2. Assume that at least one of the elliptic curves is without complex multiplication. Let*

$$S(E_1, E_2) := \{v \in \Sigma_K \setminus \Sigma_r \ \mid \ F(E_1, v) = F(E_2, v)\}.$$

Then, E_1 and E_2 are isogenous over a finite extension of K if and only if $S(E_1, E_2)$ has positive upper density.

Remark 2. In [4], Lang and Trotter made a conjecture about the asymptotic behaviour of the set of places v for which the associated Frobenius field is a given imaginary quadratic field F. Analogously it would be interesting to know about the asymptotic behaviour of the set of places v for which the Frobenius fields of two non-isogenous elliptic curves coincide. In fact, based on heuristic arguments, the following conjecture is *suggested* on page 38 [4] for non-CM elliptic curves over the field of rational numbers.

Conjecture 1. *Let E_1 and E_2 be two elliptic curves over the rationals without complex multiplication. Then, E_1 is not potentially isogenous to E_2 if and only if*

$$S(x, E_1, E_2) := \#\{p \leq x \mid F(E_1, p) = F(E_2, p)\} = O(\sqrt{x}/\log x).$$

Conjecture 1 does not seem to have been studied in the literature. Theorem 3 provides a certain non-numerical answer to this conjecture.

Remark 3. In [1], an algorithm is presented to decide when two Abelian varieties are isogenous, and also to detect elliptic curves with CM.

Using Theorem 3, we prove:

Theorem 4. *Let E be an elliptic curve over a number field K. Let F be an imaginary quadratic field. Let Σ_r be a finite subset of the set Σ_K containing the places of bad reduction of E. Let $S(E, F) := \{v \in \Sigma_K \setminus \Sigma_r \mid F(E, v) = F\}$. Then, $S(E, F)$ has positive upper density if and only if E has complex multiplication by F.*

As a consequence, we prove:

Corollary 1. *Let E be an elliptic curve over a number field K. Let $F(E)$ be the compositum of the Frobenius fields $F(E, v)$ as v varies over places of good ordinary reduction for E. Then, $F(E)$ is a number field if and only if E is an elliptic curve with complex multiplication.*

Corollary 1 also follows from a set of exercises in Serre's book [10, Chapter IV, pages 13–14]. Thus, Theorem 4 can be considered as a strengthening of this corollary.

Remark 4. Theorem 4 as above is related to the Theorem 1 in [3], which in turn also seems to be motivated by observations by J.-P. Serre as mentioned above. Theorem 4 seems to be stronger but less general than Theorem 1 in [3]. We thank D. Rohrlich for pointing this out and providing a reference to [3].

2. Proof of Theorem 2

In this section, we give a proof of Theorem 2. The argument is essentially the one given in [5], but we remove the dependence on [5, Theorem 2.1].

2.1. An algebraic Chebotarev density theorem

We recall an algebraic version of the Chebotarev density theorem of [6], see also [9]. Here F stands for a non-archimedean local field of characteristic 0.

Theorem 5. *(See [6, Theorem 3].) Let M be an algebraic group defined over F. Suppose*

$$\rho : G_K \to M(F)$$

is a continuous representation unramified outside a finite set of places of K. Let G be the Zariski closure inside M of the image $\rho(G_K)$, and G^0 be the connected component of identity of G. Let $\Phi = G/G^0$ be the group of connected components of G.

Suppose X is a closed subscheme of M defined over F and stable under the adjoint action of M on itself. Let

$$C := X(F) \cap \rho(G_K).$$

Let Σ_u denote the set of finite places of K at which ρ is unramified, and $\rho(\sigma_v)$ denote the Frobenius conjugacy class in $M(F)$ for $v \in \Sigma_u$. Then the set

$$S := \{v \in \Sigma_u \mid \rho(\sigma_v) \subset C\}$$

has a density given by

$$d(S) = \frac{|\Psi|}{|\Phi|},$$

where Ψ is the set of those $\phi \in \Phi$ such that the corresponding connected component G^ϕ of G is contained in X.

2.2. Proof of Theorem 2

If $\chi_{\rho_1}(\sigma_v)$ vanishes, then the hypothesis holds for any integer m_v. On the other hand, if $\chi_{\rho_1}(\sigma_v)$ is non-zero, then $\chi_{\rho_1}(\sigma_v)$ and $\chi_{\rho_2}(\sigma_v)$ differ by a root of unity belonging to F. Since the group of roots of unity in the non-archimedean local field F is finite, there is an integer m independent of v, such that for $v \in T$,

$$\chi_{\rho_1}(\sigma_v)^m = \chi_{\rho_2}(\sigma_v)^m$$

Let

$$X_m := \{(g_1, g_2) \in GL_n \times GL_n \mid \mathrm{Trace}(g_1)^m = \mathrm{Trace}(g_2)^m \ \}.$$

X_m is a Zariski closed subvariety of $GL_n \times GL_n$ invariant under conjugation. Let G (resp. G_1) be the Zariski closure in $GL_n \times GL_n$ (resp. GL_n) of the image $(\rho_1 \times \rho_2)(G_K)$ (resp.

$\rho_1(G_K)$). By Theorem 5, the density condition on T implies the existence of a connected component G^ϕ of G contained inside X_m.

Let L be some finite extension of K such that the image $(\rho_1 \times \rho_2)(G_L)$ is Zariski dense in the connected component G^0 of identity in G. Since G_1 is assumed to be connected, the subgroup $\rho_1(G_L)$, of finite index in $\rho_1(G_K)$, continues to be Zariski dense in G_1. It follows that the projection map from any connected component G^ψ of G to G_1 is surjective. In particular, there is an element of the form $(1, y) \in G^\phi(\overline{F})$.

We now work over complex numbers. Fix an embedding of F in $\mathbb{C}$, and consider the algebraic group G and the variety X_m over $\mathbb{C}$. Let J be a maximal compact subgroup of $G(\mathbb{C})$, which we can take it to be of the form $J = (U(n) \times U(n)) \cap G(\mathbb{C})$, where $U(n)$ is the unitary group corresponding to a standard hermitian form in n-variables. Since G is reductive, there is a bijection between the connected components of J and G, where we let $J^\psi = J \cap G^\psi$ be the connected component of J corresponding to the connected component G^ψ of G. We can assume that there is an element of the form $(1, y) \in J^\phi \cap X^m$.

Now there is only one element in an unitary group $U(n)$ with trace n and it is the identity matrix. Hence, any element in the unitary group $U(n)$ having n as the absolute value of its trace is a scalar matrix ζI_n with $|\zeta| = 1$. Since $(1, y) \in X_m$, we conclude that y is of the form $\zeta_0 I_n$, for some m-th root of unity ζ_0.

Hence the connected component $G^\phi = G^0(1, \zeta_0 I_n)$. In particular, every element $(u_1, u_2) \in G^0$, can be written as

$$(u_1, u_2) = (z_1, \zeta_0^{-1} z_2),$$

where $(z_1, z_2) \in G^\phi \cap X_m$. Since ζ_0 is a m-th root of unity, we have

$$\mathrm{Trace}(u_1)^m = \mathrm{Trace}(z_1)^m = \mathrm{Trace}(z_2)^m = \mathrm{Trace}(\zeta^{-1} z_2)^m = \mathrm{Trace}(u_2)^m.$$

Hence $G^0 \subset X_m$. Let p_i, $i = 1, 2$ be the two projections from G^0 to $GL(n)$. The statement $G^0 \subset X_m$ can be reformulated as saying that

$$\chi_{p_1}^m = \chi_{p_2}^m,$$

restricted to G^0, where χ_{p_1} and χ_{p_2} are the characters associated to p_1 and p_2 respectively.

We now argue as in [7]. The characters χ_{p_1} and χ_{p_2} differ by an m-th root of unity. Since the characters are equal at identity, they are equal on a connected neighbourhood of identity in G^0. Since a neighbourhood of identity is Zariski dense in a connected algebraic group, and the characters are regular functions on the group, it follows that the characters are equal on G^0. Thus it follows that the representations p_1 and p_2 of G^0 are equivalent.

Since $\rho_i = p_i \circ \rho$ for $i = 1, 2$, the representations $\rho_1|_L$ and $\rho_2|_L$ are equivalent. This proves that ρ_1 and ρ_2 are potentially equivalent.

3. Proof of Theorem 1

In this section we give a proof of Theorem 1. We start with the following lemma about semi-simple algebraic groups.

3.1. A lemma on algebraic groups

Lemma 6. *Let G be a connected reductive algebraic group defined over a field F of characteristic zero. Let $p : G \to GL_2$ be a surjective homomorphism defined over F. Then, $p(G(F))$ contains $SL_2(F)$.*

Proof. The induced map p from the derived group G^d of G to the derived subgroup SL_2 of GL_2 is a surjective homomorphism defined over F.

Since G^d is a connected semi-simple algebraic group over F, there exists a surjective homomorphism $\prod_i G_i \to G^d$ with finite kernel defined over F, where each G_i is a connected, simply connected, simple algebraic group defined over F [2, Theorem 22.10].

This gives a surjective homomorphism ψ from $\prod_i G_i$ to SL_2 over F. Since SL_2 is simple, it follows that for each i, $\psi|_{G_i} : G_i \to SL_2$ is either trivial or an isogeny of algebraic groups. In the latter case, G_i is either a form of SL_2 or PSL_2. Since SL_2 is simply connected, G_i is in fact a form of SL_2 over F. In other words, the induced map $\psi : G_i \to SL_2$ is an isomorphism over $\bar{F}$. However, since ψ is defined over F itself, this proves that $\psi : G_i \to SL_2$ is an isomorphism over F, proving the lemma. □

3.2. An arithmetic lemma

Lemma 7. *Let F be a non-archimedean local field of characteristic zero and residue characteristic l. Suppose d, a are non-zero elements in the ring of integers $\mathcal{O}$ of F. Then there exists $x \in F$ such that $d - ax^2$ is not a square in F.*

Proof. Suppose $d - ax^2$ is a square in F for any value of $x \in F$. Specializing $x = 0$ it follows that $d = b^2$ for some $b \neq 0 \in F$. Writing $x = y/z$ with $z \neq 0$, we get

$$b^2 - ax^2 = ((bz)^2 - ay^2)/z^2.$$

It follows that the homogeneous form $z^2 - ay^2$ is a square in F for any $y, z \in F,\ z \neq 0$.

The form $z^2 - ay^2$ can be considered as the norm form from the quadratic algebra $F(\sqrt{a})$ to F. From the multiplicativity of norms,

$$(z_1^2 - ay_1^2)(z_2^2 - ay_2^2) = (z_1z_2 + ay_1y_2)^2 - a(z_1y_2 + z_2y_1)^2$$

it follows upon equating $z_1z_2 + ay_1y_2 = 0$, that $-a$ is a square in F. The form $z^2 - ay^2$ is equivalent to the norm form $z^2 + y^2$ from the quadratic algebra $F(\sqrt{-1})$ to F, and is a square in F for any $z,\ y \in F$.

If $\sqrt{-1} \in F$, then $F(\sqrt{-1}) \simeq F \times F$, and the norm form is equivalent to the product form $(z, y) \mapsto zy$, and is surjective onto F. This implies that every element of F is a square, and yields a contradiction.

If $\sqrt{-1} \notin F$, then the image of the non-zero elements of the field $F(\sqrt{-1})$ by the norm map is a subgroup of index 2 in F^* by local class field theory. The hypothesis implies that this is contained in the group $(F^*)^2$ which is of index at least 4 since F is a non-archimedean, local field of characteristic zero. This is a contradiction and establishes the lemma. □

3.3. A lemma on traces

Lemma 8. *Let F be any field and $A \in GL_2(F)$. Then any element of F is the trace of a matrix of the form AX with $X \in SL_2(F)$.*

Proof. Up to multiplying by a unimodular matrix, A can be assumed to be a diagonal matrix with diagonal entries a and 1. If we take $X = \begin{pmatrix} 0 & y \\ z & w \end{pmatrix}$, with $yz = -1$, then the trace of AX is w. Hence the lemma. □

3.4. Proof of Theorem 1

The non-semisimple elements in GL_2 are contained inside a proper Zariski closed set given by the vanishing of the discriminant of its characteristic polynomial. By Theorem 5, it follows that at a set of places of density one, the Frobenius conjugacy classes $\rho_1(\sigma_v)$ are semisimple. In particular, we can assume by going to a subset of T (denoted again by T) with the same upper density, that for $v \in T$, $\rho_1(\sigma_v)$ is semisimple.

The eigenvalues of $\rho_1(\sigma_v)$ and $\rho_2(\sigma_v)$ lie in quadratic extensions of F, say $F_1(v)$ and respectively, $F_2(v)$. Let $F(v)$ be the compositum of $F_1(v)$ and $F_2(v)$. Thus $F(v)$ is a Galois extension of F and contained in a biquadratic extension of F.

By hypothesis, at a place $v \in T$, $\rho_1(\sigma_v)^{n_v} = \rho_2(\sigma_v)^{n_v}$.

For $v \in T$, let $\pi_{1,v},\ \pi'_{1,v}$ and $\pi_{2,v},\ \pi'_{2,v}$ be respectively the roots of the characteristic polynomials of $\rho_1(\sigma_v)$ and $\rho_2(\sigma_v)$. Up to reordering, we have $\pi_{2,v} = u\pi_{1,v}$ and $\pi'_{2,v} = u'\pi'_{1,v}$ for some roots of unity $u,\ u' \in F(v)$.

Since there are only finitely many quadratic extensions of F, the collection of fields $F(v)$ as v varies lie in a fixed local field F'. In particular, the group of roots of unity $\mu_{F'}$ belonging to F' is finite, say of order N. Thus, $\mu_{F'} = \mu_N$, the group of roots of unity of order N.

In order to prove Theorem 1 over F, it is sufficient to work over any finite extension of F. Henceforth we will assume that F contains the N-th roots of unity.

For roots of unity $u,\ u' \in \mu_N \subset F$, let

$$T(u, u') := \{v \in T \mid \pi_{2,v} = u\pi_{1,v} \quad \text{and} \quad \pi'_{2,v} = u'\pi'_{1,v}\}.$$

Since, the upper density of T is positive, it follows that $T(u,u')$ has positive upper density for some $u,u' \in \mu_N$. We consider two cases.

3.4.1. $u = u'$

Let m be the order of u. In this case, we obtain

$$T(u,u) := \{v \in T \mid (Tr(\rho_{1,\ell}(\sigma_v)))^m = (Tr(\rho_{2,\ell}(\sigma_v)))^m\}.$$

Suppose $T(u,u)$ has positive upper density. It follows from Theorem 2 that ρ_1 and ρ_2 are potentially equivalent.

3.4.2. $u \neq u'$

We show in this case, that the set of places $T(u,u')$ is of density zero. We have,

$$\begin{pmatrix} 1 & 1 \\ u & u' \end{pmatrix} \begin{pmatrix} \pi_{1,v} \\ \pi'_{1,v} \end{pmatrix} = \begin{pmatrix} t_1 \\ t_2 \end{pmatrix},$$

where $t_1 := Tr(\rho_1(\sigma_v))$ and $t_2 := Tr(\rho_2(\sigma_v))$. The determinant of this matrix is $u' - u \neq 0$, and we get:

$$\pi_{1,v} = \frac{u't_1 - t_2}{u' - u}$$
$$\pi'_{1,v} = \frac{-ut_1 + t_2}{u' - u}$$

Substituting into the equation

$$\pi_{1,v}\pi'_{1,v} = \det(\rho_1(\sigma_v)) = \det(\rho_2(\sigma_v))$$

and simplifying, we get

$$-t_1^2 - t_2^2 + (u+u')t_1t_2 = (u-u')^2 d, \tag{1}$$

where $d := \det(\rho_1(\sigma_v)) = \det(\rho_2(\sigma_v))$, since we have assumed that the determinant characters are equal. The equality of determinants also implies that $uu' = 1$.

The above equation simplifies to

$$t_1^2 + t_2^2 - at_1t_2 = bd, \tag{2}$$

where $a = (u+u') \in F$ and $b = -(u-u')^2 \neq 0 \in F$.

Let $\rho = \rho_1 \times \rho_2 : G_K \to GL_2(F) \times GL_2(F)$ be the product representation and G be the algebraic monodromy group corresponding to ρ. Since $\rho(G_K) \subset GL_2(F) \times GL_2(F)$ is Zariski dense in G, the connected components of G, being Zariski open subsets in G, are rational over F.

Let X_u be the subvariety of $GL_2 \times GL_2$ defined by Equation (2); it is a closed, invariant subvariety of $GL_2 \times GL_2$.

Suppose that the set of places $T(u, u')$ has positive upper density. By Theorem 5, there exists a connected component G^ϕ that is contained in X_u. Since G^ϕ is rational over F, its set of rational points $G^\phi(F) = (A, B)G^0(F)$, for some matrices $A, B \in GL_2(F)$.

By Lemma 6, the image of the induced map from $G^0(F)$ to $GL_2(F)$ by the first projection contains $SL_2(F)$. Hence the image of $G^\phi(F)$ with respect to the first projection contains the translate $ASL_2(F)$ of $SL_2(F)$. By Lemma 8, the element $t_1 \in F$ can be an arbitrary element of F.

Hence, Equation (2) continues to have rational solutions $t_2 \in F$ for any element $t_1 \in F$. Considering Equation (2) as a quadratic equation in t_2, it follows that the discriminant

$$(at_1)^2 - 4(t_1^2 - bd) = 4bd + (a^2 - 4)t_1^2$$

takes square values in F for any $t_1 \in F$. Here $4bd \neq 0$. Now $a = u + u'$ is a sum of roots of unity and $u \neq u'$. By embedding F inside $\mathbb{C}$, we conclude that $a^2 \neq 4$.

By Lemma 7, it is not possible that the polynomial $4bd + (a^2 - 4)t_1^2$ takes square values for all $t_1 \in F$. This yields a contradiction, and hence we conclude that there is no such connected component G^ϕ contained inside X_u. But then the upper density of $T(u, u')$ is zero. This proves Theorem 1. □

Remark 5. The proofs of both Theorems 2 and 1, work with the algebraic monodromy group associated to the Galois representations, and then specializing to certain elements in the group to obtain extra information. In a sense, this argument can be thought of as a proof involving analytic continuation of Galois monodromy.

4. Proof of Theorem 3

In this section we prove Theorem 3. We first recall some facts about ordinary and supersingular elliptic curves over finite fields.

4.1. Ordinary and supersingular reduction

Let E be an elliptic curve over a finite field k with $q = p^n$ elements. The curve E is said to be *supersingular* if the group $E[p^r](\bar{k})$ of p^r-torsion points is $\{0\}$, and is defined to be *ordinary* otherwise [11, Chapter V, Section 3]. It is known that E being ordinary is equivalent to $a(E, k)$ being nonzero and coprime to p. The Weil bound implies that $F(E, k)$ is either $\mathbb{Q}$ or an imaginary quadratic field.

Define the *Frobenius field* $F(E, k)$ of E over k as the splitting field of the characteristic polynomial of the Frobenius endomorphism $x \mapsto x^q$ of E acting on $V_\ell(E)$. We gather some well known facts relating certain properties of the Frobenius field attached to an elliptic curve to it being an ordinary elliptic curve [11, Chapter V, Section 3], [12]:

Proposition 1. *Let E be an elliptic curve over a finite field k with $q = p^n$ elements.*

1. *If E is ordinary, then $F(E,k)$ is an imaginary quadratic field in which p splits completely. Further, $F(E,k) = \mathrm{End}(E) \otimes \mathbb{Q}$.*
2. *If E is supersingular over $\mathbb{F}_p$ and $p \geq 5$, then $a(E,\mathbb{F}_p) = 0$. Hence, $F(E,\mathbb{F}_p) = \mathbb{Q}(\sqrt{-p})$ and p ramifies in $\mathbb{Q}(\sqrt{-p})$.*

4.2. Image of Galois

In [10,8], Serre initiated the study of the image $\rho_{E,\ell}(G_K)$ of the Galois group and proved the following theorem:

Theorem 9 *(Serre). Let E be an elliptic curve over a number field K. Let ℓ be a prime. Let $\rho_{E,\ell}$ be the Galois representation attached to E. Let G be the Zariski closure in GL_2 over $\mathbb{Q}_\ell$ of the image of the Galois group $\rho_{E,\ell}(G_K)$. If E does not have complex multiplication, then $G = GL_2$.*

Given a number field K, the set of finite places of K of degree one over $\mathbb{Q}$ is of density one. Hence in working with a set of places of positive upper density, we can restrict to the subset of places of degree 1 over $\mathbb{Q}$. We have the following proposition due to Serre [10, Chapter IV, Exercises, pages 13–14]:

Corollary 2. *Let E be an elliptic curve over a number field K without complex multiplication. Then, the set of places $v \in \Sigma_K$ such that E has supersingular reduction at v has upper density 0.*

Proof. Since E does not have CM, the Zariski closure of the image of Galois is GL_2. At a place v of degree one over $\mathbb{Q}$ having supersingular reduction for E, $a_v(E) = 0$ provided $Nv = p \geq 5$. Since the set $X = \{g \in GL_2 \mid \mathrm{Trace}(g) = 0\}$ is a proper closed conjugation invariant subset of GL_2, the proposition follows from Theorem 5. □

4.3. Proof of Theorem 3

Suppose E_1 and E_2 are isogenous over a finite extension L of K. Consider the curves over L. For any place w of L where both the elliptic curves have good reduction, the reduced curves $E_{1,w}$ and $E_{2,w}$ are isogenous. Hence the characteristic polynomials of the Frobenius conjugacy classes are equal and their associated Frobenius fields $F(E_1,w)$ and $F(E_2,w)$ are isomorphic.

If w is a place of L of degree one over K, then $E_{1,w}$ is isomorphic to $E_{1,v}$ and hence they have the same Frobenius fields. This holds for E_2 as well. Since the set of places v of K for which there exists a place w of L of degree one over K is of positive density in K, it follows that $S(E_1,E_2)$ has positive density and hence positive upper density.

We now prove the converse. Suppose that the upper density of $S := S(E_1, E_2)$ is positive. Since E_1 is without complex multiplication, by Proposition 2, the set of places $v \in \Sigma_K$ such that E_{1v} is ordinary has density 1. Let

$$S_1 := \{v \in S \mid E_{1,v} \text{ is ordinary and } \deg_{\mathbb{Q}}(v) = 1\}.$$

Thus, $ud(S_1) = ud(S) > 0$.

By Proposition 1, E has good ordinary reduction at v if and only if $F(E, v)$ is an imaginary quadratic field and p_v splits in $F(E, v)$, where p_v is the prime of $\mathbb{Q}$ that lies below v. This implies that p_v splits in $F(v) = F(E_1, v) = F(E_2, v)$. Consequently, every $v \in S_1$ is a place of good ordinary reduction for both E_1 and E_2.

For $v \in S_1$, let $\pi_{1,v}, \overline{\pi}_{1,v}$ and $\pi_{2,v}, \overline{\pi}_{2,v}$ be respectively the roots of the characteristic polynomials $\phi_v(E_1, t)$ and $\phi_v(E_2, t)$. Thus,

$$\pi_{1,v}\overline{\pi}_{1,v} = \pi_{2,v}\overline{\pi}_{2,v} = p_v$$

As ideals of $F(v) := F(E_1, v) = F(E_2, v)$, we have:

$$(\pi_{1,v})(\overline{\pi}_{1,v}) = (\pi_{2,v})(\overline{\pi}_{2,v}) = (p_v).$$

By unique factorization theorem for ideals, it follows that $\pi_{1,v} = u\pi_{2,v}$ or $\pi_{1,v} = u\overline{\pi}_{2,v}$, where u depends on $v \in S_1$ and is a unit of $F(v)$. Renaming if needed, one can assume that

$$\pi_{1,v} = u\pi_{2,v}. \tag{3}$$

Since the units in $F(v)$ are roots of unity, it follows that the representations $\rho_{E_1,\ell}$ and $\rho_{E_2,\ell}$ are locally potentially equivalent:

$$\rho_{E_1,\ell}(\sigma_v)^{12} = \rho_{E_2,\ell}(\sigma_v)^{12}, \tag{4}$$

for $v \in S_1$.

Since E_1 is assumed to be non-CM, by Theorem 9, the Galois monodromy group $G_1 = GL_2$. Hence by Theorem 1, the representations $\rho_{E_1,\ell}$ and $\rho_{E_2,\ell}$ are potentially equivalent.

By Faltings' theorem, it follows that E_1 and E_2 are isogenous over a finite extension of K. This proves Theorem 3. □

Remark 6. In the above theorem, it is necessary to assume that at least one of the elliptic curves is without complex multiplication and can be seen as follows:

Suppose v is a prime of K of degree one over a rational prime $p \geq 5$, at which an elliptic curve E has good supersingular reduction. The Frobenius field $F(E, v)$ is $\mathbb{Q}(\sqrt{-p})$. Let F_1 and F_2 be non-isomorphic imaginary quadratic fields of class number one. Let E_1 and E_2 be CM elliptic curves over $\mathbb{Q}$ with complex multiplication by F_1 and F_2 respectively.

At the set of primes p of $\mathbb{Q}$ of good reduction for E_1 and E_2, and such that p is inert in both F_1 and F_2, the curves E_1 and E_2 have supersingular reduction. Hence there is a set of places of positive density (in fact having density $\frac{1}{4}$) at which the Frobenius fields are isomorphic, but E_1 and E_2 are non-isogenous.

Remark 7. It can be seen that we can modify and prove the theorem under the assumption that the upper density of the set of finite places v of K for which both the elliptic curves have good ordinary reduction at v is positive.

5. Proof of Theorem 4

Suppose E has complex multiplication by an imaginary quadratic field F. We want to show that the set $S(E,F) := \{v \in \Sigma_K \mid F(E,v) = F\}$ has positive upper density.

Let v be a place of K of good reduction for E with CM by F. From Proposition 1, the following can be seen to be equivalent:

1. E has ordinary reduction modulo v.
2. $F(E,v) = F$.
3. p_v splits in F, where p_v denotes the rational prime of $\mathbb{Q}$ that lies below v.

Let L be the compositum of K and F. Let $Spl(L/\mathbb{Q})$ be the set of all primes p that split completely in L. Let

$$S := \{v \in \Sigma_K \mid v \text{ lies over } p \in Spl(L/\mathbb{Q})\}.$$

Thus, for a finite place $v \in S$, $\deg v$ is 1. Since every prime $p \in Spl(L/\mathbb{Q})$ also splits in F, it follows that $F(E,v) = F$ for $v \in S$. By the very construction, $S \subseteq S(E,F)$. Since every place $v \in S$ is of degree 1 and lies over the primes of $Spl(L/\mathbb{Q})$,

$$ud(S(E,F)) \geq ud(S) \geq ud(Spl(L/\mathbb{Q})) = \frac{1}{[L:\mathbb{Q}]} > 0.$$

In the converse direction, we want to prove that if for some imaginary quadratic field F, $ud(S(E,F)) > 0$, then E has complex multiplication by F. Without affecting the density, we will assume that the places in $S(E,F)$ are of degree one over $\mathbb{Q}$ with residue characteristic at least 5.

Case 1: Suppose E has complex multiplication by an imaginary quadratic field $F' = \mathbb{Q}(\sqrt{-d})$. We want to prove that $F' = F$. Let $S = S(E,F)$. We can assume after removing a finite set of places from S that for $v \in S$, E has good reduction modulo v and p_v is not ramified in F'.

Suppose p_v is inert in F'. By Proposition 1, E has supersingular reduction modulo v and $F(E,v) = \mathbb{Q}(\sqrt{-p_v}) = F$. The set of such v is finite.

Hence for some $v \in S$, p_v splits in F'. This implies that the Frobenius field at v equals the CM field, i.e. $F(E, v) = F'$. On the other hand, since $v \in S = S(E, F)$, we have $F(E, v) = F$. This proves $F = F'$.

Case 2: Let us now consider the case when E is an elliptic curve over K without complex multiplication. The idea is to construct an elliptic curve, say E', over a suitable number field with complex multiplication by F and to apply Theorem 3 to prove that E and E' are isogenous over some extension of K.

Let $\mathcal{O}_F$ be the ring of integers of F. Let E' be the elliptic curve over $\mathbb{C}$ such that $E'(\mathbb{C}) \simeq \mathbb{C}/\mathcal{O}_F$. The theory of complex multiplication implies that E' is defined over $H := H(F)$, the Hilbert class field of F. Let $L := HK$ be the compositum of H and K.

We wish to apply Theorem 3 to the two elliptic curves E and E' considered as elliptic curves defined over L. Thus, we need to prove that the set of places w of L such that $F(E, w) = F(E', w)$ has positive upper density.

Let us denote by S_K the set of degree 1 places $v \in S(E, F) \subseteq \Sigma_K$. Then, $ud(S_K) = ud(S(E, F))$. Let $S_{\mathbb{Q}}$ be the set of primes p_v of Σ_Q that lie below the places of $v \in S_K$. Then $ud(S_{\mathbb{Q}})$ is also positive.

Let $p \in S_{\mathbb{Q}}$ and let v be a place of K that lies above $p = p_v$. By construction, the Frobenius field at v equals $\mathbb{Q}(\pi_v) = F$. Since, $\pi_v \overline{\pi}_v = Nv = p = p_v$, the primes $p \in S_{\mathbb{Q}}$ split in F.

Let S_F be the set of places of F that lie over the set of places of $S_{\mathbb{Q}}$. Then $S_F := \bigcup_{v \in S_K} \{(\pi_v), (\overline{\pi}_v)\}$. Thus, $ud(S_F)$ is positive.

The prime ideals of S_F are principal. By class field theory, they split completely in the Hilbert class field H of F. This implies that the primes $p \in S_{\mathbb{Q}}$ split completely in H.

Let S_L be the set of primes of L that lie above S_K. Let $w \in S_L$ be a place above $v \in S_K$. Since p_v splits completely in H, it is easy to see that the prime v of K splits completely in L. This implies that $\deg(w) = \deg(v) = 1$, implying $ud(S_L) > 0$.

By considering E as an elliptic curve over L, it follows that $F(E, w) = F(E, v) = F$ where $w \in S_L$ and $v \in S_K$ that lies below w. Similarly, we have $F(E', w) = F$.

Applying Theorem 3 to E and E' considered as elliptic curves over L, it follows that E and E' are isogenous over some finite extension of L, proving the theorem. □

Acknowledgments

The results presented in this paper are motivated by a question raised by Dipendra Prasad. We would like to thank Dipendra Prasad for some useful discussions. We very gratefully acknowledge the valuable feedback from J.-P. Serre, who pointed out an error in [5]. He also gave a different proof of Theorem 3. The second author thanks H. Hida and A. Burungale for some useful discussions. The second author also thanks D. Rohrlich for some useful comments and for pointing out a reference to a paper of C. Khare. The authors thank J. Achter for some useful comments. We also thank Abhinav Kumar for his comments. The second author thanks the School of Mathematics, Tata Institute

of Fundamental Research, Mumbai for its excellent hospitality and work environment. The second author also thanks his past employer, International Institute of Information Technology Bangalore, Bangalore, where part of this work was carried out. We thank the referee for his detailed suggestions and input.

References

[1] Jeffrey D. Achter, Detecting complex multiplication, in: Computational Aspects of Algebraic Curves, in: Lecture Notes Ser. Comput., vol. 13, World Sci. Publ., Hackensack, NJ, 2005, pp. 38–50.
[2] Armand Borel, Linear Algebraic Groups, second edition, Grad. Texts in Math., vol. 126, Springer-Verlag, New York, 1991.
[3] Chandrashekhar Khare, F-split Galois representations are potentially abelian, Proc. Amer. Math. Soc. 131 (10) (2003) 3021–3023.
[4] Serge Lang, Hale Trotter, Frobenius Distributions in GL_2-Extensions, Lecture Notes in Math., vol. 504, Springer-Verlag, Berlin, New York, 1976.
[5] Vijay M. Patankar, C.S. Rajan, Locally potentially equivalent Galois representations, J. Ramanujan Math. Soc. 27 (1) (2012) 77–90.
[6] C.S. Rajan, On strong multiplicity one for ℓ-adic representations, Int. Math. Res. Not. 3 (1998) 161–172.
[7] C.S. Rajan, Recovering modular forms and representations from tensor and symmetric powers, in: Algebra and Number Theory, Hindustan Book Agency, Delhi, 2005, pp. 281–298.
[8] Jean-Pierre Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. 15 (4) (1972) 259–331.
[9] Jean-Pierre Serre, Quelques applications du théorème de densité de Chebotarev, Publ. Math. Inst. Hautes Études Sci. 54 (1981) 323–401.
[10] Jean-Pierre Serre, Abelian ℓ-adic Representations and Elliptic curves, Res. Notes Math., vol. 7, A.K. Peters, Ltd., Wellesley, MA, 1998.
[11] Joseph H. Silverman, The Arithmetic of Elliptic Curves, second edition, Grad. Texts in Math., vol. 106, Springer, Dordrecht, 2009.
[12] William C. Waterhouse, Abelian varieties over finite fields, Ann. Sci. Éc. Norm. Supér. (4) 2 (1969) 521–560.