COMPATIBLE FAMILIES OF ELLIPTIC TYPE

DAVID E. ROHRLICH

In axiomatizing their study of Frobenius distributions [5], Lang and Trotter introduce the notion of an adelic Galois representation *of elliptic type*, and they ask in passing whether every such representation arises from an elliptic curve (see pp. 5 and 19 of [5]). Formulated in the language of ℓ-adic representations [7], their question is as follows. Put $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, let p denote a prime, and write σ_p for any Frobenius element at a prime ideal of $\overline{\mathbb{Q}}$ over p. Let $\{\rho_\ell\}$ be a two-dimensional strictly compatible family of integral ℓ-adic representations of G with exceptional set S, and for $p \notin S$ put $a(p) = \mathrm{tr}\,\rho_\ell(\sigma_p)$ with any $\ell \neq p$. Also, let $\omega_\ell : G \to \mathbb{Z}_\ell^\times$ denote the ℓ-adic cyclotomic character. Although ρ_ℓ is *a priori* a map into $\mathrm{GL}(2, \mathbb{Q}_\ell)$, after a conjugation in $\mathrm{GL}(2, \mathbb{Q}_\ell)$ we may regard it as a map $G \to \mathrm{GL}(2, \mathbb{Z}_\ell)$.

Question of Lang and Trotter. *Suppose that $\{\rho_\ell\}$ satisfies three conditions:*

> **LT1.** *For $p \notin S \cup \{\ell\}$, $\det \rho_\ell(\sigma_p) = p$. In other words, $\det \rho_\ell = \omega_\ell$.*
> **LT2.** *For $p \notin S$, $|a(p)| < 2\sqrt{p}$.*
> **LT3.** *The image of ρ_ℓ is an open subgroup of $\mathrm{GL}(2, \mathbb{Z}_\ell)$ for every ℓ and is equal to $\mathrm{GL}(2, \mathbb{Z}_\ell)$ for all but finitely many ℓ.*

Does it follow that $\{\rho_\ell\}$ is isomorphic to the strictly compatible family $\{\rho_{E,\ell}\}$ afforded by the ℓ-adic Tate modules $T_\ell(E)$ of some elliptic curve E over $\mathbb{Q}$?

Here two strictly compatible families $\{\rho_\ell\}$ and $\{\rho'_\ell\}$ are understood to be isomorphic if for each ℓ the representations ρ_ℓ and ρ'_ℓ are isomorphic over $\mathbb{Q}_\ell$.

If we further stipulate that E should not have complex multiplication then the question is simply whether certain necessary conditions for $\{\rho_\ell\} \cong \{\rho_{E,\ell}\}$ are also sufficient. Indeed **LT1** and **LT2** hold for any elliptic curve over $\mathbb{Q}$, the former being a consequence of the Galois-equivariance of the Weil pairing and the latter an instance of Hasse's Riemann hypothesis for elliptic function fields (a strict inequality here because $\sqrt{p} \notin \mathbb{Q}$). As for **LT3**, if E does not have complex multiplication then the fact that $\rho_{E,\ell}$ is open for all ℓ and surjective for all but finitely many ℓ is Serre's theorem [8].

Elliptic curves with complex multiplication do not fall within the purview of the Lang-Trotter question, but we can include them simply by omitting **LT3**. The question is then whether families of the form $\{\rho_{E,\ell}\}$ are characterized by **LT1** and **LT2** alone. We shall see that an affirmative answer follows from the Fontaine-Mazur conjecture [1] combined with a "catalyst."

The version of the Fontaine-Mazur conjecture that is relevant here is the two-dimensional case stated on pp. 190–191 of [1]. As usual, we call a two-dimensional representation ρ of G even or odd according as $\det \rho$ is trivial or nontrivial on the conjugacy class of complex conjugation. And we shall refer to ρ as an Artin representation if it factors through $\mathrm{Gal}(K/\mathbb{Q})$ for some finite Galois extension K of $\mathbb{Q}$, even if the field of scalars of ρ is not necessarily $\mathbb{C}$.

> **FM.** *Fix a prime p and suppose that $\rho : G \to \mathrm{GL}(2, \overline{\mathbb{Q}}_p)$ is an irreducible representation which is potentially semistable at p and unramified at all but finitely many primes of $\mathbb{Q}$. Assume also that ρ does not have the form $\rho \cong \lambda \otimes \omega_p^n$, where $n \in \mathbb{Z}$ and λ is an even Artin representation of G. Then there exists a primitive cusp form f such that the associated semisimple representation $\rho_{f,p}$ is isomorphic to ρ.*

Here "cusp form" means "cusp form of type (N, k, χ) for some positive integers N and k and Dirichlet character χ modulo N." Furthermore, if we write the Fourier expansion of f as $f(z) = \sum_{n\geqslant 1} a(n)e^{2\pi inz}$ then we have implicitly fixed an embedding into $\overline{\mathbb{Q}}_p$ of the number field generated by the coefficients $a(n)$ and the values of χ. It is then meaningful to specify that for primes $q \nmid Np$ we have $\operatorname{tr} \rho_{f,p}(\sigma_q) = a(q)$ and $\det \rho_{f,p}(\sigma_q) = \chi(q)q^{k-1}$. Since $\rho_{f,p}$ is semisimple it is determined up to isomorphism by these properties.

The catalyst that we need does not appear to have been enunciated in the literature, but it is implicit in the dual use of the word *ordinary* in contemporary arithmetic geometry. For the sake of clarity, let us call a prime $p \notin S$ *classically ordinary* (relative to $\{\rho_\ell\}$) if $p \nmid a(p)$, and *ordinary* (again relative to $\{\rho_\ell\}$) if p satisfies the definition on pp. 97–98 of Greenberg [2]. These notions are complementary in the sense that the former is a condition on ρ_ℓ for $\ell \neq p$ and the latter a condition on ρ_p. Nonetheless, we consider the following hypothesis:

> **ORD.** *Classically ordinary primes are ordinary.*

While **ORD** lacks the legitimacy conferred by an eponym, it seems indispensable in the following application of **FM**:

Theorem 1. *Assume* **FM** *and* **ORD**. *If $\{\rho_\ell\}$ satisfies* **LT1** *and* **LT2** *then there is an elliptic curve E over $\mathbb{Q}$ such that $\{\rho_\ell\} \cong \{\rho_{E,\ell}\}$.*

The proof of Theorem 1 quickly reduces to an elementary remark. Let Λ be the set of primes ℓ such that ρ_ℓ is absolutely irreducible, and let Λ_{surj} be the subset of Λ consisting of those ℓ for which $\rho_\ell(G) = \mathrm{GL}(2, \mathbb{Z}_\ell)$.

Theorem 2. *Suppose that $\{\rho_\ell\}$ satisfies* **LT1** *and* **LT2**. *Then Λ has density 1, and if there exists a prime ℓ_0 such that $\rho_{\ell_0}(G)$ is open in $\mathrm{GL}(2, \mathbb{Z}_{\ell_0})$ then Λ_{surj} has density 1.*

Only the density of Λ is needed in the proof of Theorem 1, but the contingent density of Λ_{surj} can be viewed as a weak form of **LT3**, which in this weak form is therefore a consequence of **LT1** and **LT2**. Thus even without assuming **FM** or **ORD** there is reason to pose the Lang-Trotter question with **LT3** omitted.

Acknowledgment. This note began as a Boston University seminar talk given on October 16, 2006, and it is a pleasure to thank the seminar audience for indulging and enlightening me. I am particularly indebted to Avner Ash, Ben Howard, Jeehoon Park, Robert Pollack, Matthias Schütt, and Glenn Stevens, whose knowledgeable comments were collectively a much better talk than the one that was delivered. Further orientation was provided by Ralph Greenberg, Kiran Kedlaya, and Matt Emerton, whom it is also a pleasure to thank. Finally, I owe Robert Pollack a separate and special expression of gratitude for pointing out a serious error in my attempt to apply the work of Kisin [3] in an earlier version of this note.

1. Proof of Theorem 1 (granting Theorem 2)

Given a prime ℓ, let $\overline{\rho}_\ell$ denote the representation $G \to \mathrm{GL}(2, \mathbb{F}_\ell)$ obtained from ρ_ℓ by reduction modulo ℓ. We begin the proof of Theorem 1 by fixing an odd prime ℓ_0 and identifying $\overline{\rho}_{\ell_0}(G)$ with the Galois group over $\mathbb{Q}$ of the fixed field of the kernel of $\overline{\rho}_{\ell_0}$. Applying the Chebotarev density theorem to the one-element conjugacy class consisting of the identity $1 \in \overline{\rho}_{\ell_0}(G)$, we find that the set of primes $p \notin S \cup \{\ell_0\}$ such that $\overline{\rho}_{\ell_0}(\sigma_p) = 1$ has positive density. Since we are granting that Λ has density 1, it follows that there is a prime $p \notin S \cup \{2, 3, \ell_0\}$ such that ρ_p is absolutely irreducible and $\overline{\rho}_{\ell_0}(\sigma_p) = 1$. The latter condition implies that $a(p) \equiv 2$ modulo ℓ_0, and as ℓ_0 is odd we deduce that $a(p) \neq 0$. Since $p \geqslant 5$ it follows from **LT2** and the nonvanishing of $a(p)$ that $p \nmid a(p)$. In other words, p is classically ordinary, hence ordinary by **ORD**, and therefore a theorem of Fontaine and Perrin-Riou [6] assures us that ρ_p is semistable at p. Furthermore, ρ_p is not the twist of an even Artin representation by some power of ω_p, for then $\det \rho_p$ would be even, contrary to **LT1**. Thus **FM** is in force, and we can write $\rho_p \cong \rho_{f,p}$ for some primitive cusp form f. In fact from **LT1** we deduce that f is of weight 2 with trivial character. And since $\operatorname{tr} \rho_p(\sigma_q) = a(q)$ for primes $q \notin S \cup \{p\}$, we obtain the further information that the Fourier coefficients of f are rational integers, whence $\rho_{f,p} \cong \rho_{E,p}$ for some elliptic curve E over $\mathbb{Q}$. Thus $\rho_p \cong \rho_{E,p}$. The proof of Theorem 1 is now completed by the following lemma.

Lemma. *Let $\{\rho_\ell\}$ and $\{\rho'_\ell\}$ be two strictly compatible families of ℓ-adic representations of G, and suppose that $\rho_p \cong \rho'_p$ for some prime p. Suppose in addition that ρ'_ℓ is irreducible for every prime ℓ. Then $\{\rho_\ell\} \cong \{\rho'_\ell\}$.*

Proof. The argument is standard, but we nonetheless recall it. Fix a prime ℓ, and let S and S' be the exceptional sets of the two families. For primes $q \notin S \cup S' \cup \{\ell, p\}$ the strict compatibility of the two families gives $\operatorname{tr} \rho_\ell(\sigma_q) = \operatorname{tr} \rho_p(\sigma_q)$ and $\operatorname{tr} \rho'_\ell(\sigma_q) = \operatorname{tr} \rho'_p(\sigma_q)$, and since $\operatorname{tr} \rho_p = \operatorname{tr} \rho'_p$ by hypothesis we deduce that $\operatorname{tr} \rho_\ell(\sigma_q) = \operatorname{tr} \rho'_\ell(\sigma_q)$. It follows that $\operatorname{tr} \rho_\ell = \operatorname{tr} \rho'_\ell$. Let ρ_ℓ^{ss} denote the semisimplification of ρ_ℓ. By assumption, ρ'_ℓ is irreducible and *a fortiori* semisimple, and since a semisimple representation in characteristic 0 is determined up to isomorphism by its trace we obtain $\rho_\ell^{ss} \cong \rho'_\ell$. This implies in particular that ρ_ℓ^{ss} is irreducible and so coincides up to isomorphism with ρ_ℓ itself. We conclude that $\rho_\ell \cong \rho'_\ell$. □

2. Proof of Theorem 2

As before, write $\overline{\rho}_\ell$ for the reduction of ρ_ℓ modulo ℓ. In the following lemma ℓ denotes a fixed prime.

Lemma 1. *Consider prime numbers $p, p' \notin S$, and put $d = a(p)^2 - 4p$ and $d' = a(p')^2 - 4p'$.*

(a) If $\ell \nmid 2pp'dd'$ and

$$\left(\frac{d}{\ell}\right) = -\left(\frac{d'}{\ell}\right)$$

then $\overline{\rho}_\ell$ is absolutely irreducible.

(b) If in addition $\ell \nmid a(p)a(p')$ then the restriction of $\overline{\rho}_\ell$ to every subgroup of index 2 in G is also absolutely irreducible.

Proof. (a) Put $V = \mathbb{F}_\ell^2$, so that V is the space of $\overline{\rho}_\ell$, and suppose on the contrary that there exists a one-dimensional G-stable subspace W of $\overline{\mathbb{F}}_\ell \otimes_{\mathbb{F}_\ell} V$. We will obtain a contradiction by proving that W is both defined over $\mathbb{F}_\ell$ (in other words, of the form $\overline{\mathbb{F}}_\ell \otimes_{\mathbb{F}_\ell} U$ for some subspace U of V) and not defined over $\mathbb{F}_\ell$.

The characteristic polynomials of $\rho_\ell(\sigma_p)$ and $\rho_\ell(\sigma_{p'})$ are $x^2 - a(p)x + p$ and $x^2 - a(p')x + p'$, whence the eigenvalues of $\overline{\rho}_\ell(\sigma_p)$ and $\overline{\rho}_\ell(\sigma_{p'})$ are the images in $\overline{\mathbb{F}}_\ell$ of the numbers

$$\lambda_\pm = \frac{a(p) \pm \sqrt{d}}{2} \tag{1}$$

and

$$\lambda'_\pm = \frac{a(p') \pm \sqrt{d'}}{2} \tag{2}$$

respectively. Applying the hypothesis to (1) and (2), we see that in one case the two eigenvalues are distinct elements of $\mathbb{F}_\ell$ while in the other case the eigenvalues are distinct elements of $\overline{\mathbb{F}}_\ell$ not belonging to $\mathbb{F}_\ell$. Now the fact that in both cases the eigenvalues are distinct implies that the corresponding eigenspaces are one-dimensional, and since W is stable under G it follows that W is an eigenspace both of $\overline{\rho}_\ell(\sigma_p)$ and of $\overline{\rho}_\ell(\sigma_{p'})$. The rationality properties of the eigenvalues of $\overline{\rho}_\ell(\sigma_p)$ and $\overline{\rho}_\ell(\sigma_{p'})$ now imply the contradictory rationality properties of W mentioned above, and we conclude that $\overline{\rho}_\ell$ is indeed absolutely irreducible.

(b) Suppose on the contrary that there is a subgroup H of index 2 in G and a one-dimensional subspace W of $\overline{\mathbb{F}}_\ell \otimes_{\mathbb{F}_\ell} V$ which is stable under H. Then $\overline{\rho}_\ell(g)^2(W) = W$ for every $g \in G$. This holds in particular for $g = \sigma_p$ and $g = \sigma_{p'}$, and for these two choices of g the eigenvalues of $\overline{\rho}_\ell(g)^2$ can be read from (1) and (2): they are the images in $\overline{\mathbb{F}}_\ell$ of the numbers

$$(\lambda_\pm)^2 = \frac{(a(p)^2 - 2p) \pm a(p)\sqrt{d}}{2}$$

and

$$(\lambda'_\pm)^2 = \frac{(a(p')^2 - 2p') \pm a(p')\sqrt{d'}}{2}$$

respectively. Since $a(p)$ and $a(p')$ are by hypothesis nonzero modulo ℓ, we see once again that in both cases the two eigenvalues are distinct. Hence the fact that the one-dimensional subspace W is stable under $\overline{\rho}_\ell(\sigma_p)^2$ and $\overline{\rho}_\ell(\sigma_{p'})^2$ implies that W is an eigenspace of both maps. But as before, one set of eigenvalues belongs to $\mathbb{F}_\ell$ and the other does not, so we have a contradiction. □

In the next lemma we view $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ as a vector space over $\mathbb{F}_2$. Given a prime $p \notin S$, we have $a(p)^2 - 4p < 0$ by **LT2** and hence in particular $a(p)^2 - 4p \neq 0$, so if we set $d = a(p)^2 - 4p$ then we can consider the coset $d\mathbb{Q}^{\times 2}$ in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$.

Lemma 2. *Let $\mathcal{P}$ be a set of primes which contains S and has density* 0*. There is a sequence $\{p_i\}_{i=1}^\infty$ of primes $p_i \notin \mathcal{P}$ such that the cosets of the numbers $d_i = a(p_i)^2 - 4p_i$ are linearly independent in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$.*

Proof. We shall construct the sequence $\{p_i\}$ inductively. To start the induction, choose any prime $p_1 \notin \mathcal{P}$. As just noted, the quantity $d_1 = a(p_1)^2 - 4p_1$ is negative and hence not in $\mathbb{Q}^{\times 2}$. Thus the vector $d_1\mathbb{Q}^{\times 2}$ is nonzero.

Now suppose that for some $n \geqslant 1$ we have chosen primes $p_1, p_2, \ldots, p_n \notin \mathcal{P}$ such that the cosets of $d_1, d_2, \ldots, d_n$ in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ are linearly independent. Then the Chebotarev density theorem ensures that the set of primes $p \nmid 2d_1 d_2 \cdots d_n$ such that

$$\left(\frac{d_1}{p}\right) = \left(\frac{d_2}{p}\right) = \cdots = \left(\frac{d_n}{p}\right) = -1 \tag{3}$$

has density 2^{-n} and in particular positive density. Hence we can choose a prime $p_{n+1} \notin \mathcal{P}$ such that (3) holds with $p = p_{n+1}$. Put $d_{n+1} = a(p_{n+1})^2 - 4p_{n+1}$. We must show that the vector $d_{n+1}\mathbb{Q}^{\times 2}$ is not in the span of the vectors $d_i\mathbb{Q}^{\times 2}$ $(1 \leqslant i \leqslant n)$.

Suppose on the contrary that for some choice of exponents $\epsilon_i \in \{0, 1\}$ $(1 \leqslant i \leqslant n)$ and some choice of $v \in \mathbb{Q}^\times$ we have

$$d_{n+1} = d_1^{\epsilon_1} d_2^{\epsilon_2} \cdots d_n^{\epsilon_n} \cdot v^2. \tag{4}$$

Then the quantity $\epsilon = \epsilon_1 + \epsilon_2 \cdots + \epsilon_n$ is odd, because $d_1, d_2, \ldots, d_n < 0$ and also $d_{n+1} < 0$ while $v^2 > 0$. Thus on setting

$$d = d_1^{\epsilon_1} d_2^{\epsilon_2} \cdots d_n^{\epsilon_n}$$

we have

$$\left(\frac{d}{p_{n+1}}\right) = (-1)^\epsilon = -1,$$

because by construction, (3) holds with $p = p_{n+1}$. It follows that p_{n+1} remains prime in $\mathbb{Q}(\sqrt{d})$ and hence is not a norm from $\mathbb{Q}(\sqrt{d})$. This is a contradiction, for we can rewrite (4) in the form $p_{n+1} = (u^2 - dv^2)/4$ with $u = a(p_{n+1})$. □

Let Π be the set of primes $p \notin S$ such that $a(p) = 0$. If Π has density 0 then let $\mathcal{L}$ denote the set of primes ℓ such that $\overline{\rho}_\ell | H$ is absolutely irreducible for every subgroup H of index 2 in G. If the upper density of Π is strictly positive then we define $\mathcal{L}$ by requiring only that $\overline{\rho}_\ell$ itself be absolutely irreducible. In both cases $\mathcal{L} \subset \Lambda$, so the first assertion of Theorem 2 is a consequence of the next lemma:

Lemma 3. *$\mathcal{L}$ has density* 1.

Proof. We apply Lemma 2 with

$$\mathcal{P} = \begin{cases} \Pi \cup S & \text{if } \Pi \text{ has density } 0, \\ S & \text{otherwise,} \end{cases}$$

obtaining sequences $\{p_i\}$ and $\{d_i\}$ with $p_i \notin \mathcal{P}$ and $d_i = a(p_i)^2 - 4p_i$ such that for every $n \geqslant 1$ the Galois group of $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \ldots, \sqrt{d_n})$ over $\mathbb{Q}$ is $(\mathbb{Z}/2\mathbb{Z})^n$. Let

$$c_n = \begin{cases} 2\prod_{i=1}^n p_i d_i a(p_i) & \text{if } \Pi \text{ has density } 0, \\ 2\prod_{i=1}^n p_i d_i & \text{otherwise.} \end{cases}$$

Then $c_n \neq 0$. We put $\mathcal{M}_n = \mathcal{M}_n^+ \cup \mathcal{M}_n^-$, where $\mathcal{M}_n^\pm$ is the set of primes $\ell \nmid c_n$ such that

$$\left(\frac{d_1}{\ell}\right) = \left(\frac{d_2}{\ell}\right) = \cdots = \left(\frac{d_n}{\ell}\right) = \pm 1. \tag{5}$$

By the Chebotarev density theorem, $\mathcal{M}_n^+$ and $\mathcal{M}_n^-$ each have density 2^{-n}, whence $\mathcal{M}_n$ has density 2^{1-n}. It follows that the complement of $\mathcal{M}_n$ in the set of all primes not dividing c_n has density $1 - 2^{1-n}$. Denote this complement $\mathcal{L}_n$. To prove the lemma it suffices to see that $\mathcal{L}_n \subset \mathcal{L}$, for then $\mathcal{L}$ has lower density $\geqslant 1 - 2^{1-n}$ with n arbitarily large. So suppose that $\ell \in \mathcal{L}_n$. Then $\ell \notin \mathcal{M}_n$, and consequently there are indices i and j $(1 \leqslant i < j \leqslant n)$ such that

$$\left(\frac{d_i}{\ell}\right) = -\left(\frac{d'_j}{\ell}\right).$$

Applying Lemma 1 with $p = p_i$, $p' = p_j$, $d = d_i$, and $d' = d'_j$, we conclude that $\ell \in \mathcal{L}$. □ □

It remains to prove the second assertion of Theorem 2. Let $\mathcal{L}^* \subset \mathcal{L}$ be the subset consisting of all $\ell \in \mathcal{L}$ such that $\overline{\rho}_\ell(G)$ either contains $\mathrm{SL}(2, \mathbb{F}_\ell)$ or is contained in the normalizer of a Cartan subgroup of $\mathrm{GL}(2, \mathbb{F}_\ell)$.

Lemma 4. *$\mathcal{L}^*$ has density one. In fact $\mathcal{L} \smallsetminus \mathcal{L}^*$ is finite.*

Proof. In view of Lemma 3 it suffices to prove the second statement. Now if $\ell \in \mathcal{L}$ then $\overline{\rho}_\ell$ is irreducible, and consequently $\overline{\rho}_\ell(G)$ is not contained in a Borel subgroup of $\mathrm{GL}(2, \mathbb{F}_\ell)$. If in addition $\ell \notin \mathcal{L}^*$ then $\overline{\rho}_\ell(G)$ neither contains $\mathrm{SL}(2, \mathbb{F}_\ell)$ nor is contained in the normalizer of a Cartan subgroup of $\mathrm{GL}(2, \mathbb{F}_\ell)$, whence the classification of subgroups of $\mathrm{GL}(2, \mathbb{F}_\ell)$ leaves only one possibility (cf. [8], p. 280, Prop. 15 and p. 282, 2.6): For every $g \in G$ we have

$$P(u_\ell(g)) \equiv 0 \pmod{\ell}, \tag{6}$$

where P is the polynomial $P(u) = u(u-1)(u-2)(u-4)(u^2 - 3u + 1)$ and $u_\ell(g) = (\operatorname{tr} \rho_\ell(g))^2 / \det \rho_\ell(g)$. Suppose that $\mathcal{L} \smallsetminus \mathcal{L}^*$ is infinite, so that (6) holds for infinitely many $\ell \in \mathcal{L}$. Then for $p \notin S$ and infinitely many $\ell \neq p$ we have $P(u_\ell(\sigma_p)) \equiv 0$ mod ℓ. But $u_\ell(\sigma_p) = a(p)^2/p$, so $p^6 P(u_\ell(\sigma_p))$ is a rational integer, and since it is congruent to 0 for infinitely many ℓ it is equal to 0. In other words $Q(a(p)) = 0$, where $Q(x) = x^2(x^2 - p)(x^2 - 2p)(x^2 - 4p)(x^4 - 3px^2 + p^2)$. By inspection, the only rational root of $Q(x) = 0$ is $x = 0$, so $a(p) = 0$ for all $p \notin S$. As we saw already in the proof of Theorem 1, this is impossible. (If we fix an odd prime ℓ_0, then by the Chebotarev density theorem there are infinitely many $p \notin S \cup \{\ell_0\}$ such that $\overline{\rho}_{\ell_0}(\sigma_p) = 1$, and for such p we have $a(p) \equiv 2 \bmod \ell_0$.) We conclude that $\mathcal{L} \smallsetminus \mathcal{L}^*$ is finite. □

Lemma 5. *Let ℓ be a prime $\geqslant 5$. If $\overline{\rho}_\ell(G)$ contains $\mathrm{SL}(2, \mathbb{F}_\ell)$ then $\rho_\ell(G) = \mathrm{GL}(2, \mathbb{Z}_\ell)$.*

Proof. If $\ell \geqslant 5$ and X is a closed subgroup of $\mathrm{GL}(2, \mathbb{Z}_\ell)$ such that the reduction of X modulo ℓ contains $\mathrm{SL}(2, \mathbb{F}_\ell)$ then X contains $\mathrm{SL}(2, \mathbb{Z}_\ell)$ ([7], p. IV-23, Lemma 3, or see [4], p. 229). In the case $X = \rho_\ell(G)$ our assumption **LT1** then gives $\rho_\ell(G) = \mathrm{GL}(2, \mathbb{Z}_\ell)$. □

The proof of Theorem 2 is completed by the next lemma.

Lemma 6. *The following are equivalent:*

(i) Λ_{surj} *has density* 1.
(ii) *There exists a prime ℓ_0 such that $\rho_{\ell_0}(G)$ is open in* $\mathrm{GL}(2, \mathbb{Z}_{\ell_0})$.
(iii) Π *has density* 0.

Proof. That (i) implies (ii) is trivial, and that (ii) implies (iii) follows from the Chebotarev density theorem (cf. [9], p. 150, Theorem 10, which is much stronger than what is needed here). Now suppose that Π has density 0. In view of Lemma 4 it will suffice to see that $\mathcal{L}^* \subset \Lambda_{\mathrm{surj}}$. In fact by Lemma 5 we need only show that if $\ell \in \mathcal{L}^*$ then $\overline{\rho}_\ell(G)$ is not contained in the normalizer of a Cartan subgroup C of $\mathrm{GL}(2, \mathbb{F}_\ell)$. If on the contrary such a containment does hold, then $\rho_\ell^{-1}(C)$ is a subgroup H of index 2 in G such that $\overline{\rho}_\ell(H)$ is abelian. It follows in particular that $\overline{\rho}_\ell|H$ is not absolutely irreducible. This contradicts the definition of $\mathcal{L}$ in the case where Π has density 0. □

References

[1] J.-M. Fontaine and B. Mazur, *Geometric Galois representations*. In: *Elliptic Curves, Modular Forms, & Fermat's Last Theorem*, J. Coates and S.-T. Yau, eds. International Press, Cambridge MA (1997), pp. 190 – 227.

[2] R. Greenberg, *Iwasawa theory for p-adic representations*. In: *Algebraic Number Theory – in honor of K. Iwasawa*, Advanced Studies in Pure Mathematics 17 (1989), pp. 97 – 137.

[3] M. Kisin, *The Fontaine-Mazur conjecture for* GL_2, to appear.

[4] S. Lang *Elliptic Functions*, Springer-Verlag, GTM vol. 112 (1987).

[5] S. Lang and H. Trotter, *Frobenius Distributions in* GL_2*-Extensions*, Springer-Verlag, LNM vol. 504 (1976).

[6] B. Perrin-Riou (with an appendix by L. Illusie), *Représentations p-adiques ordinaires*. In: *Périodes p-adiques*, Astérisque 223 (1994), pp. 185 – 220.

[7] J-P. Serre, *Abelian* ℓ*-Adic Representations and Elliptic Curves* W. A. Benjamin, 1968.

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

[9] J-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Publ. Math. IHES 54 (1981), 123 – 201.

Department of Mathematics and Statistics, Boston University, Boston, MA 02215
E-mail address: rohrlich@math.bu.edu