COMPOSITIO MATHEMATICA

Constructing elliptic curves from Galois representations

Andrew Snowden and Jacob Tsimerman

Compositio Math. **154** (2018), 2045–2054.

doi:10.1112/S0010437X18007315

FOUNDATION
COMPOSITIO
MATHEMATICA

LONDON
MATHEMATICAL
SOCIETY
EST. 1865

Compositio Math. 154 (2018) 2045–2054
doi:10.1112/S0010437X18007315

Constructing elliptic curves from Galois representations

Andrew Snowden and Jacob Tsimerman

Abstract

Given a non-isotrivial elliptic curve over an arithmetic surface, one obtains a lisse ℓ-adic sheaf of rank two over the surface. This lisse sheaf has a number of straightforward properties: cyclotomic determinant, finite ramification, rational traces of Frobenius elements, and somewhere not potentially good reduction. We prove that any lisse sheaf of rank two possessing these properties comes from an elliptic curve.

1. Introduction

Let C/K be a proper, smooth geometrically irreducible curve, with K a number field, let $f : E \to U \subset C$ be a non-isotrivial family of elliptic curves over a non-empty open subset U of C, and let $L = \mathrm{R}^1 f_*(\overline{\mathbf{Q}}_\ell)$ be the associated rank-two lisse ℓ-adic sheaf on U. The following properties hold.

(a) There is an isomorphism $\bigwedge^2 L \cong \overline{\mathbf{Q}}_\ell(1)$.
(b) There exists a proper smooth model $\mathcal{C}$ of C over $\operatorname{Spec} \mathcal{O}_K[1/N]$, an open subset $\mathcal{U}$ of $\mathcal{C}$ extending U, and a lisse sheaf $\mathcal{L}$ on $\mathcal{U}$ extending L.
(c) For every closed point x of $\mathcal{U}$, the trace of the Frobenius element on $\mathcal{L}_x$ is a rational number.
(d) There exists a point x of $C_{\overline{K}}$ at which $L_{\overline{K}}$ does not have potentially good reduction, i.e., the restriction to the inertia subgroup at x of the representation of $\pi_1^{\text{ét}}(U_{\overline{K}})$ associated to $L_{\overline{K}}$ does not act through a finite order quotient.

To see (d), take x to be a pole of the j-invariant of E.

The purpose of this paper is to prove the following converse of the above statement.

Theorem 1. *Let C/K be as above, and let L be an irreducible rank-two lisse $\overline{\mathbf{Q}}_\ell$-sheaf over an open subset $U \subset C$. Assume conditions (a)–(d) above hold. Then there exists a family of elliptic curves $f : E \to U$ and an isomorphism $L \cong \mathrm{R}^1 f_*(\overline{\mathbf{Q}}_\ell)$.*

Remark 2. The Fontaine–Mazur conjecture predicts that representations of G_K satisfying certain natural conditions should appear in the étale cohomology of algebraic varieties. It seems reasonable to expect some kind of generalization of this conjecture to higher-dimensional bases. Our theorem can be viewed as confirmation of a very simple case of this.

Remark 3. One can prove a version of Theorem 1 where C is replaced with a higher-dimensional variety. We just treat the case of curves to keep the exposition simpler.

Received 12 October 2017, accepted in final form 30 April 2018, published online 29 August 2018.
2010 Mathematics Subject Classification 11G05, 14K15 (primary).
Keywords: Fontaine–Mazur conjecture, Drinfeld modular curve, Langlands program.
AS was supported by NSF grants DMS-1303082 and DMS-1453893 and a Sloan Fellowship.

Remark 4. The theorem is not true if one assumes only (a)–(c). Recall that a *fake elliptic curve* is an abelian surface A such that $\mathrm{End}(A)$ is an order R in a non-split quaternion algebra that is split at infinity. The moduli space of fake elliptic curves corresponding to R is a proper curve. We therefore can construct a family $f : A \to C$ of fake elliptic curves for some C as above. The sheaf $\mathrm{R}^1 f_* \overline{\mathbf{Q}}_\ell$ decomposes as $L^{\oplus 2}$ for some rank-two lisse sheaf L. This L satisfies (a)–(c) but not (d), and thus does not come from a non-isotrivial family of elliptic curves. (Note that one can take f so that L is not isotrivial, in which case L does not come from any family of elliptic curves.)

Question 5. Suppose that for each prime number ℓ we have an irreducible rank-two $\mathbf{Q}_\ell$ sheaf L_ℓ satisfying (a)–(c) such that $\{L_\ell\}$ forms a compatible system (meaning that the $\mathcal{U}$ in part (b) can be chosen uniformly and that the traces of Frobenius elements are independent of ℓ). Does the system come from a family of elliptic curves? Note that the fake elliptic curve counterexample does not apply here: if ℓ ramifies in $R \otimes \mathbf{Q}$ then $\mathrm{R}^1 f_* \mathbf{Q}_\ell$ does not decompose as $L^{\oplus 2}$.

1.1 Summary of the proof

The basic idea is to use Drinfeld's results on the global Langlands program to construct an elliptic curve over $\mathcal{C}_{\mathbf{F}_v}$ for most places v of $\mathcal{O}_K$, and then piece these together to get one over $\mathcal{C}$. More precisely, we proceed as follows.

- We first show that we are free to pass to finite covers of C. The main content here is a descent result that shows that if L comes from an elliptic curve over a cover of C then it comes from an elliptic curve over C. Using this, we replace C with a cover so that $L/\ell^3 L$ is trivial (after replacing L with an integral form).
- We next consider L over $\mathcal{C}_{\mathbf{F}_v}$ and use Drinfeld's results on the global Langlands program to produce a $\mathbf{GL}_2$-type abelian variety A_v realizing L.
- Using hypotheses (c) and (d), we descend the coefficient field of A_v to $\mathbf{Q}$, obtaining an elliptic curve E_v. (It is likely this could be obtained directly from Drinfeld's proof.)
- We next consider a certain moduli space $\mathcal{M}$ of maps $\mathcal{U} \to Y(\ell^3)$. From the previous step (and the triviality of $L/\ell^3 L$), we see that $\mathcal{M}$ has $\mathbf{F}_v$-points for infinitely many v. Since $\mathcal{M}$ is of finite type over $\mathcal{O}_K$, it therefore has a $\overline{K}$-point. This yields an elliptic curve $E_{\overline{K}}$ over $U_{\overline{K}}$ realizing $L_{\overline{K}}$.
- Our hypotheses imply that $L_{\overline{K}}$ is irreducible. A simple representation theory argument thus shows that there is a finite extension K'/K such that E descends to $U_{K'}$ and its Tate module agrees with $L_{K'}$. We have already shown that it suffices to prove the result over a finite cover of C, so we are now finished.

We note that we use Faltings' proof of the Tate conjecture in the third and fifth steps.

1.2 Outline

In § 2 we recall the relevant background material. In § 3, we prove a few descent results for abelian varieties. In § 4, we package Drinfeld's results on the global Langlands program into the form we need; in particular, we use the results of § 3 to produce elliptic curves (as opposed to $\mathbf{GL}_2$-type abelian varieties). In § 5, we construct a mapping space parametrizing maps between two affine curves. Finally, in § 6, we prove Theorem 1.

https://doi.org/10.1112/S0010437X18007315 Published online by Cambridge University Press

2. Background

2.1 Abelian varieties

Let A be an abelian variety over a field K such that $\mathrm{End}_K(A) \otimes \mathbf{Q}$ contains a number field F. Let $V_\ell(A)$ denote the rational Tate module of A at the rational prime ℓ. This is a module over $F \otimes \mathbf{Q}_\ell = \prod_{w|\ell} F_w$, and thus decomposes as $\bigoplus_{w|\ell} V_w(A)$ where each $V_w(A)$ is a continuous representation of G_K over the field F_w. We recall the following standard results.

Proposition 6. *Let $\sigma \in \mathrm{End}_K(A)$ commute with F. Then the characteristic polynomial of σ on $V_w(A)$ (regarded as an F_w-vector space) has coefficients in F and is independent of w. In particular, each $V_w(A)$ has the same dimension over F_w.*

Proof. See [Shi67, § 11.10] and (for $F = \mathbf{Q}$) [Mil, Proposition 9.23]. □

Proposition 7. *Assume K is a number field and $\mathrm{End}_K(A) \otimes \mathbf{Q} = F$. Let w be a place of F above a prime p. Then $\mathrm{End}_{\mathbf{Q}_p[G_K]}(V_w(A)) = F_w$. In particular, $V_w(A)$ is absolutely irreducible as a representation of G_K over F_w.*

Proof. We have

$$F \otimes \mathbf{Q}_p = \mathrm{End}_{\mathbf{Q}_p[G_K]}(V_p(A)) = \mathrm{End}_{\mathbf{Q}_p[G_K]}\left(\bigoplus_{w|p} V_w(A)\right) \supset \bigoplus_{w|p} \mathrm{End}_{\mathbf{Q}_p[G_K]}(V_w(A)) \supset \bigoplus_{w|p} F_w,$$

where the first equality is the Tate conjecture proved by Faltings [FWGSS92, Theorem 1, p. 211]. Since the endmost spaces have the same dimension, we conclude that the containments are equalities, and so $\mathrm{End}_{\mathbf{Q}_p[G_K]}(V_w(A)) = F_w$. □

2.2 Arithmetic fundamental groups

Let X be an affine normal integral scheme of finite type over $\mathbf{Z}$ and consider $\pi_1^{\text{ét}}(X)$. For each closed point x of X there is a conjugacy class of Frobenius elements F_x. We recall the following generalization of the Chebotarev density theorem.

Proposition 8. *The elements $\{F_x\}_{x \in X}$ are dense in $\pi_1^{\text{ét}}(X)$.*

Proof. This follows from [Ser65, Theorem 7]. □

Corollary 9. *Suppose that ρ_1 and ρ_2 are semi-simple continuous representations $\pi_1^{\text{ét}}(X) \to \mathbf{GL}_n(\overline{\mathbf{Q}}_\ell)$ such that $\mathrm{tr}(\rho_1(F_x)) = \mathrm{tr}(\rho_2(F_x))$ for all x. Then ρ_1 and ρ_2 are equivalent.*

2.3 Ramification of characters

Lemma 10. *Let C be a curve over a number field K, and let U be an open subset. Suppose that $\alpha : \pi_1(U) \to \overline{\mathbf{Q}}_\ell^\times$ is a continuous homomorphism. Then for every point x of $C_{\overline{K}}$, the inertia subgroup of $\pi_1(U_{\overline{K}})$ at x has finite image under α.*

Proof. We are free to replace K with a finite extension, so we may as well assume x is a K-point. The decomposition group at x has the form $\widehat{\mathbf{Z}} \rtimes G_K$, where $\widehat{\mathbf{Z}}$ is the geometric inertia group and G_K acts on it through the cyclotomic character χ. Let T be a topological generator of $\widehat{\mathbf{Z}}$, written multiplicatively. Then for $\sigma \in G_K$ we have $\alpha(T) = \alpha(\sigma T \sigma^{-1}) = \alpha(T^{\chi(\sigma)}) = \alpha(T)^{\chi(\sigma)}$. It follows that $\alpha(T)$ has finite order. □

https://doi.org/10.1112/S0010437X18007315 Published online by Cambridge University Press

2.4 Some lemmas from representation theory

Lemma 11. *Let ρ and ρ' be finite-dimensional representations of a group G with equal determinant. Suppose there exists a normal subgroup H of G such that $\rho|_H$ and $\rho'|_H$ are absolutely irreducible and isomorphic. Then there exists a finite-index subgroup G' of G such that $\rho|_{G'}$ and $\rho'|_{G'}$ are isomorphic.*

Proof. Let V and V' be the spaces for ρ and ρ' and let $f : V \to V'$ be an isomorphism of H representations. One easily verifies that for $g \in G$ the endomorphism $g^{-1}f^{-1}gf$ of V commutes with H, and is therefore given by multiplication by some scalar $\chi(g)$. Thus we have $f^{-1}gf = \chi(g)g$ for all $g \in G$. It follows easily from this that χ is a homomorphism, i.e., $\chi(gg') = \chi(g)\chi(g')$. We thus see that $\chi \otimes \rho$ and ρ' are isomorphic as representations of G. Taking determinants, we see that χ^n is trivial, where n is the dimension of ρ. The result follows by taking G' to be the kernel of χ; this has finite index since the image of χ is contained in the group of nth roots of unity of k. (In fact, the index of G' divides n.) □

Lemma 12. *Let G be a group and H a normal subgroup of G. Consider a two-dimensional irreducible representation $\rho : G \to \mathbf{GL}_2(\overline{\mathbf{Q}}_\ell)$. Assume that for some element $h \in H$, the matrix $\rho(h)$ is a non-trivial unipotent element. Then $\rho|_H$ is irreducible.*

Proof. Suppose not. Then by the existence of h, there exists a unique one-dimensional subspace V invariant under H. But since H is normal in G, it follows that V is invariant under G as well. This contradicts the supposition. □

3. Descent results for abelian varieties

For this section, fix a finitely generated field K. We consider the following condition on a continuous representation $\rho : G_K \to \mathbf{GL}_n(\overline{\mathbf{Q}}_\ell)$.

(∗) There exists an integral scheme X of finite type over $\mathrm{Spec}(\mathbf{Z})$ with function field K and a lisse $\overline{\mathbf{Q}}_\ell$-sheaf L on X with generic fiber ρ such that at every closed point x of X the trace of the Frobenius element on L_x is rational.

In our proof of Theorem 1, we will show that ρ comes from an elliptic curve over some finite extension of K'. We use the following result to conclude that we actually get an elliptic curve over K.

Proposition 13. *Let $\rho : G_K \to \mathbf{GL}_2(\overline{\mathbf{Q}}_\ell)$ be a Galois representation satisfying condition (∗). Suppose that there exists a finite extension K'/K such that $\rho|_{K'}$ comes from a non-CM elliptic curve E. Then ρ comes from an elliptic curve.*[1]

We proceed with a number of lemmas.

Lemma 14. *Let $\rho : G \to \mathbf{GL}_n(\overline{\mathbf{Q}}_\ell)$ a continuous representation of the profinite group G. Suppose there exists an open subgroup H of G such that $\rho(H)$ is contained in $\mathbf{GL}_n(\mathbf{Z}_\ell)$ and contains an open subgroup of $\mathbf{GL}_n(\mathbf{Z}_\ell)$. Suppose also that there is a dense set of elements $\{g_i\}_{i\in I}$ of G such that $\operatorname{tr}\rho(g_i) \in \mathbf{Q}_\ell$ for all $i \in I$. Then $\rho(G)$ is contained in $\mathbf{GL}_n(\mathbf{Q}_\ell)$.*

[1] The non-CM condition is in fact necessary. Let $K = \mathbf{F}_p$, $K'' = \mathbf{F}_{p^2}$ and ℓ be such that p has a square root mod ℓ. Now let ρ have eigenvalues $\pm\sqrt{p}$. Then ρ cannot come from an elliptic curve because the determinant is not the cyclotomic character but $\rho|_{K'}$ corresponds to a supersingular elliptic curve.

https://doi.org/10.1112/S0010437X18007315 Published online by Cambridge University Press

Proof. Let e_{ij} be the $n \times n$ matrix with a 1 in the (i,j) position and 0 elsewhere. By assumption, there exists m such that $\rho(H)$ contains $1 + \ell^m e_{ij}$ for all i,j, and so $e_{ij} \in \mathbf{Q}_\ell[\rho(G)]$. For any $A \in \rho(G)$ we have $A_{i,j} = \mathrm{tr}(e_{ii}Ae_{jj}) \in \mathrm{tr}(\mathbf{Q}_\ell[\rho(G)]) = \mathbf{Q}_\ell$, where the last equality follows from the fact that $\mathrm{tr} \circ \rho : G \to \mathbf{Q}_\ell$ is continuous and $\mathrm{tr}(\rho(g_i)) \in \mathbf{Q}_\ell$ for all i. It thus follows that $\rho(G) \subset \mathbf{GL}_n(\mathbf{Q}_\ell)$ as claimed. □

The following lemma is basically [Tay02, Corollary 2.4].

LEMMA 15. *Let $\rho : G_K \to \mathbf{GL}_2(\overline{\mathbf{Q}}_\ell)$ be a continuous irreducible Galois representation. Suppose that there is a finite separable extension K'/K such that $\rho|_{G_{K'}}$ comes from a non-CM elliptic curve E. Then there is an abelian variety A/K with $F = \mathrm{End}(A) \otimes \mathbf{Q}$ a number field of degree $\dim(A)$ such that $\rho \cong \overline{\mathbf{Q}}_\ell \otimes_{F_w} V_w(A)$ for some place w of A.*

Proof. Consider $B = \mathrm{Res}_K^{K'} E$, an abelian variety over K of dimension $[K' : K]$ [BLR90, § 7.6]. Write $B = \prod_{i=1}^r B_i$ (up to isogeny) where each B_i is a power of a simple abelian variety. Thus

$$\mathrm{End}_K(B) \otimes \mathbf{Q} = \bigoplus_{i=1}^{r} D_i,$$

where $D_i = \mathrm{End}_K(B_i) \otimes \mathbf{Q}$ is a simple algebra. We have

$$\mathrm{Hom}_{G_K}(\rho, \overline{\mathbf{Q}}_\ell \otimes V_\ell(B)) = \mathrm{Hom}_{G_{K'}}(\rho|_{G_{K'}}, \overline{\mathbf{Q}}_\ell \otimes V_\ell(E)) = \overline{\mathbf{Q}}_\ell,$$

where the latter follows from Faltings' proof of the Tate conjecture [FWGSS92, Theorem 1, p. 211] since E is non-CM. We thus see that ρ occurs uniquely in $\overline{\mathbf{Q}}_\ell \otimes V_\ell(B_i)$ for some i. Let A be this B_i. Since A is a power of a simple abelian variety and ρ occurs uniquely in its Tate module, A must itself be simple. The endomorphism ring D_i must preserve ρ, and thus the action of ρ comes from an algebra homomorphism $\psi : D_i \to \overline{\mathbf{Q}}_\ell$, which is injective since D_i is simple. We thus see that $D_i = F$ is a number field, and ψ corresponds to a place w of F above ℓ. Since $V_w(A) \otimes_{F_w} \overline{\mathbf{Q}}_\ell$ contains ρ and is absolutely irreducible by Proposition 7, it is equal to ρ. Therefore $V_w(A)$ is two dimensional over F_w, and so $[F : \mathbf{Q}] = \dim(A)$ by Proposition 6. □

LEMMA 16. *Proposition 13 holds if K'/K is separable.*

Proof. By Lemma 15, we can find an abelian variety A/K with $\mathrm{End}(A) \otimes \mathbf{Q} = F$ a number field of degree $\dim(A)$, and a place w_0 of F such that $\rho \cong \overline{\mathbf{Q}}_\ell \otimes_{F_{w_0}} V_{w_0}(A)$.

Choose an integral scheme X of finite type over $\mathrm{Spec}(\mathbf{Z})$ with fraction field K and a family of abelian varieties $\mathcal{A} \to X$ extending A. The representation of G_K on $V_w(A)$ factors through $\pi_1^{\text{ét}}(X)$, for all w. Since $V_{w_0}(A)$ satisfies $(*)$, we can replace X with a dense open subscheme such that the Frobenius elements in $\pi_1^{\text{ét}}(X)$ have rational traces on $V_{w_0}(A)$. By Proposition 6, it follows that the Frobenius elements in $\pi_1^{\text{ét}}(X)$ have rational traces on $V_w(A)$ for all w.

By assumption, $\rho|_{G_{K'}} \cong \overline{\mathbf{Q}}_\ell \otimes V_\ell(E)$ for some non-CM elliptic curve E/K'. As above, pick an integral scheme X' of finite type over $\mathrm{Spec}(\mathbf{Z})$ with fraction field K' such that there is an elliptic curve $\mathcal{E} \to X'$ extending E. Further shrinking X, X' we can assume X' maps to X inducing the inclusion $K \subset K'$.

Pick a place $w \mid p$ of F. As we saw above, Frobenius elements of $\pi_1^{\text{ét}}(X)$ have equal traces on $\rho \cong \overline{\mathbf{Q}}_\ell \otimes_{F_{w_0}} V_{w_0}(A)$ and $\overline{\mathbf{Q}}_p \otimes_{F_w} V_w(A)$. Similarly, the traces of Frobenius elements of $\pi_1^{\text{ét}}(X')$ on $V_\ell(E)$ and $V_p(E)$ are equal. We thus see by Corollary 9 that $\overline{\mathbf{Q}}_p \otimes_{F_w} V_w(A)$ is isomorphic

https://doi.org/10.1112/S0010437X18007315 Published online by Cambridge University Press

to $\overline{\mathbf{Q}}_p \otimes_{\mathbf{Q}_p} V_p(E)$ as representations of $\pi_1^{\text{ét}}(X')$. By the Tate conjecture proved by Faltings [FWGSS92, Theorem 1, p. 211], the image of $G_{K'}$ in $\mathbf{GL}(V_p(E))$ contains an open subgroup of $\mathbf{GL}_2(\mathbf{Z}_p)$.

It follows that the conditions of Lemma 14 are fulfilled for $V_w(A) \otimes_{F_w} \overline{\mathbf{Q}}_p$, and so $V_w(A) \otimes_{F_w} \overline{\mathbf{Q}}_p$ is defined over $\mathbf{Q}_p$; that is, there exists some representation V of G_K over $\mathbf{Q}_p$ such that $V_w(A) \otimes_{F_w} \overline{\mathbf{Q}}_p \cong \overline{\mathbf{Q}}_p \otimes_{\mathbf{Q}_p} V$. Since $V_w(A)$ and $V \otimes_{\mathbf{Q}_p} F_w$ have the same character, and are irreducible, it follows that they are isomorphic. We thus see that $\mathrm{End}_{\mathbf{Q}_p[G_K]}(V_w(A)) \cong \mathrm{End}_{\mathbf{Q}_p}(F_w)$, where on the right side we are taking endomorphisms of F_w as a vector space. By Proposition 7 we have that $\mathrm{End}_{\mathbf{Q}_p[G_K]}(V_w(A)) \cong F_w$, and so $\mathrm{End}_{\mathbf{Q}_p}(F_w) = F_w$, which implies $F_w = \mathbf{Q}_p$. We thus see that all places of F are split, and so $F = \mathbf{Q}$. Thus A is actually an elliptic curve, and the proof is complete. □

Lemma 17. *Proposition 13 holds if K'/K is purely inseparable.*

Proof. It suffices to treat the case where $(K')^p = K$. Let E/K' be the elliptic curve giving rise to $\rho|_{K'}$. Let $E^{(p)} = E \times_{K',F_0} K'$ where $F_0 : K' \to K'$ is the absolute Frobenius map. Then $E^{(p)}$ is defined over K, and there is a canonical isogeny (relative Frobenius map) $F : E \to E^{(p)}$ defined over K' inducing an isomorphism on rational ℓ-adic Tate modules. Thus $V_\ell(E^{(p)})|_{G_{K'}} \cong \rho|_{G_{K'}}$ and so $V_\ell(E^{(p)}) \cong \rho$ since K'/K is purely inseparable. □

Proposition 13 in general follows from the previous two lemmas. We now prove a slightly different descent result. Recall that for an elliptic curve E and a number field F, one has an abelian variety $E \otimes \mathcal{O}_F$ with multiplication by $\mathcal{O}_F$: as an abelian variety, $E \otimes \mathcal{O}_F$ is simply E^n where $n = [F : \mathbf{Q}]$.

Proposition 18. *Let k be a finite field, let C/k be a proper smooth geometrically irreducible curve, and let $f : A \to U$ be a family of g-dimensional abelian varieties over a non-empty open subset U of C such that $\mathrm{End}(A) \otimes \mathbf{Q}$ contains a number field F of degree g. For a finite place v of F, let $\mathcal{L}_v$ be the v-adic Tate module of A. Assume that for all closed points x of U, the trace of the Frobenius element at x on $\mathcal{L}_{v,x}$ belongs to $\mathbf{Q}$. Also assume that there is some place of C where A does not have potentially good reduction. Then there exists an elliptic curve $E \to U$ such that A is isogenous to $E \otimes \mathcal{O}_F$.*

Proof. Let ℓ be a rational prime that splits completely in F. Then the ℓ-adic Tate module $\mathcal{L}_\ell$ of A decomposes as $\bigoplus_{v|\ell} \mathcal{L}_v$. The $\mathcal{L}_v$ form a compatible system with coefficients in F, so for each closed point $x \in U$ there exists $\alpha \in F$ such that the trace of the Frobenius element at x on $\mathcal{L}_{v,x}$ is the image of α in F_v. By our assumptions, α is a rational number, and so if $v, w \mid \ell$ then the traces of Frobenius elements on $\mathcal{L}_{v,x}$ and $\mathcal{L}_{w,x}$ are the same element of $\mathbf{Q}_\ell \subset F_v, F_w$. It follows that the characters of $\mathcal{L}_v$ and $\mathcal{L}_w$ are equal at Frobenius elements, and so $\mathcal{L}_v \cong \mathcal{L}_w$. Thus $\dim(\mathrm{End}(\mathcal{L}_\ell)) \geqslant g^2$. By Faltings' isogeny theorem, it follows that $\dim(\mathrm{End}(A) \otimes \mathbf{Q}) \geqslant g^2$.

Let $C' \to C$ be a cover such that A has semi-stable reduction, and let x be a point at which A' (the pullback of A) has bad reduction. Let $\mathcal{A}'$ be the Néron model of A' over C', and let T be the torus quotient of the identity component of $\mathcal{A}'_x$. The dimension h of T is at least 1, and at most g. Under the map $\mathrm{End}(A) \otimes \mathbf{Q} \to \mathrm{End}(T) \otimes \mathbf{Q} \subset M_h(\mathbf{Q})$, the field F must inject, and so $h = g$. Thus T is the entire identity component of $\mathcal{A}'_x$, and so the map $\mathrm{End}(A) \otimes \mathbf{Q} \to \mathrm{End}(T) \otimes \mathbf{Q} \subset M_g(\mathbf{Q})$ is injective. Combined with the previous paragraph, we find that $\dim(\mathrm{End}(A) \otimes \mathbf{Q}) = g^2$, and so the map $\mathrm{End}(A) \otimes \mathbf{Q} \to M_g(\mathbf{Q})$ is an isomorphism. The statement now follows by projecting under an idempotent. □

4. Drinfeld's work on the global Langlands program

PROPOSITION 19. *Let k be a finite field, and C/k be a smooth proper geometrically irreducible curve. Let L be an irreducible rank-two lisse $\overline{\mathbf{Q}}_\ell$-sheaf over a non-empty open subset $U \subset C$, such that the following hold.*

(a) *There is an isomorphism $\bigwedge^2 L \cong \overline{\mathbf{Q}}_\ell(1)$.*
(b) *For every closed point x of C, the trace of the Frobenius element on L_x is a rational number.*
(c) *There exists a point x of $C_{\overline{k}}$ at which $L_{\overline{k}}$ does not have potentially good reduction.*

Then there exists an elliptic curve $f : E \to U$ such that $\mathrm{R}^1 f_*(\overline{\mathbf{Q}}_\ell) \cong L$.

Proof. By Drinfeld's theorem ([Dri83, Main theorem, Remark 5], see also [Dri78]) there is a cuspidal automorphic representation π of $\mathbf{GL}_2(\mathbf{A}_{k(C)})$ which is compatible with L. Since inertia at x does not have finite order, π must be special at x. It follows by another theorem of Drinfeld [Dri77, Theorem 1] that there exists a number field E and a $\mathbf{GL}_2(E)$-type abelian variety A over U which is compatible with π and thus also with L, in the sense that the ℓ-adic Tate module L' of A is isomorphic with L when tensored up to $\overline{\mathbf{Q}}_\ell$; that is, $L' \otimes_E \overline{\mathbf{Q}}_\ell \cong L$. By Proposition 18, we may take A to be an elliptic curve. □

Remark 20. By following Drinfeld's proof carefully, one may directly see that we can take E to be the field generated by the Frobenius traces of L, and is thus $\mathbf{Q}$, which can replace the use of Proposition 18.

5. Mapping spaces

Let S be a noetherian scheme. For $i = 1, 2$, let C_i be a proper smooth scheme over S with geometric fibers irreducible curves, let Z_i be a closed subscheme of C_i that is a finite union of sections $S \to C_i$, and let U_i be the complement of Z_i in C_i. Fix $d \geqslant 1$.

PROPOSITION 21. *There exists a scheme $\mathcal{M}$ of finite type over S and a map $\phi : (U_1)_{\mathcal{M}} \to (U_2)_{\mathcal{M}}$ with the following property: if k is a field, $s \in S(k)$, and $f : U_{1,s} \to U_{2,s}$ is a map of curves over k of degree d (meaning the corresponding function field extension has degree d), then there exists $t \in \mathcal{M}(k)$ over s such that $f = \phi_t$.*

Proof. Let P be the image of a section $S \to C_1$. Define $\widetilde{P}$ to be the dth nilpotent thickening of P. Precisely, if P is defined by the ideal sheaf $\mathcal{I}_P$ then $\widetilde{P}$ is defined by $\mathcal{I}_P^d$. Let Q be the image of a section $S \to C_2$, and define $\widetilde{Q}$ similarly. Let $0 \leqslant e \leqslant d$ be an integer. For an S-scheme S', let $\mathcal{C}_{P,Q,e}(S')$ be the set of maps $f : \widetilde{P}_{S'} \to \widetilde{Q}_{S'}$ such that $f^*(\mathcal{I}_Q) \subset \mathcal{I}_P^e$. As these are finite schemes over S, this functor is represented by a scheme $\mathcal{C}_{P,Q,E}$ of finite type over S.

Write $Z_1 = \coprod_{i=1}^n P_i$ and $Z_2 = \coprod_{j=1}^m Q_j$. (Here $\coprod$ denotes disjoint union.) By a *ramification datum* we mean a tuple $\rho = (\rho_1, \ldots, \rho_n)$ where each ρ_i is either null (denoted $\emptyset$), or a pair (k_i, e_i), where $1 \leqslant k_i \leqslant m$ and $0 \leqslant e_i \leqslant d$, such that the following condition holds: for any $1 \leqslant j \leqslant m$, we have $\sum_{k_i=j} e_i = d$ (the sum taken over i for which $\rho_i \neq \emptyset$). Obviously, there are only finitely many ramification data. For a ramification datum ρ, define $\mathcal{C}_\rho = \prod_{\rho_i \neq \emptyset} \mathcal{C}_{P_i, Q_{k_i}, e_i}$. Finally, define $\mathcal{C} = \coprod_\rho \mathcal{C}_\rho$, where the union is taken over all ramification data ρ.

For an S-scheme S', let $\mathcal{A}(S')$ be the set of morphisms $(C_1)_{S'} \to (C_2)_{S'}$ having degree d in each geometric fiber. The theory of the Hilbert scheme shows that $\mathcal{A}$ is represented by a scheme

https://doi.org/10.1112/S0010437X18007315 Published online by Cambridge University Press

of finite type over S. For $1 \leqslant i \leqslant n$, let $\mathcal{B}_i(S')$ be the set of all maps $(\widetilde{P}_i)_{S'} \to (C_2)_{S'}$. This is easily seen to be a scheme of finite type over S. Let $\mathcal{B} = \coprod_{i=1}^n \widetilde{\mathcal{B}}_i$.

We have restriction maps $\mathcal{A} \to \mathcal{B}$ and $\mathcal{C} \to \mathcal{B}$. Define $\mathcal{M}$ to be the fiber product $\mathcal{A} \times_{\mathcal{B}} \mathcal{C}$, which is a scheme of finite type over S. We can write $\mathcal{M} = \coprod_\rho \mathcal{M}_\rho$, where $\mathcal{M}_\rho = \mathcal{A} \times_{\mathcal{B}} \mathcal{C}_\rho$. If $s \in S(k)$ then $\mathcal{M}_{\rho,s}(k)$ is the set of degree d maps $f : C_{1,s} \to C_{2,s}$ satisfying the following conditions at the P_i: if $\rho_i = \emptyset$ then there is no condition at P_i; otherwise, $f(P_i) = Q_{k_i}$ and the ramification index $e(P_i \mid Q_{k_i})$ is at least e_i. (In fact, the ramification index is exactly e_i, since the total ramification is d and the e_i with $k_i = j$ add up to d.) It is clear that such a map carries $U_{1,s}$ into $U_{2,s}$, and that any map $U_{1,s} \to U_{2,s}$ of degree d comes from a point of some $\mathcal{M}_{\rho,s}$. Thus every map $f : U_{1,s} \to U_{2,s}$ comes from some k-point of $\mathcal{M}_s$. Finally, note that the universal map $(C_1)_{\mathcal{M}} \to (C_2)_{\mathcal{M}}$ carries $(U_1)_{\mathcal{M}}$ to $(U_2)_{\mathcal{M}}$, as this can be checked at field points of $\mathcal{M}$. This proves the proposition. □

6. Proof of Theorem 1

Keep notation as in Theorem 1, and put $S = \operatorname{Spec}(\mathcal{O}_K[1/N])$.

Lemma 22. *The restriction of L to any open subgroup of $\pi_1^{\text{ét}}(U_K)$ is irreducible.*

Proof. Suppose not. Then there exists an open normal subgroup H of $G = \pi_1^{\text{ét}}(U_K)$ such that $L|_H$ is reducible. It is semi-simple by Lemma 12, and therefore a sum of two characters. Since characters have finite ramification by Lemma 10, we have contradicted assumption (d). □

Choose $r \gg 0$ so that $X = X(\ell^r)$ has genus at least 2 and $Y = Y(\ell^r)$ is a fine moduli space; in fact, $r = 3$ suffices for any ℓ. We replace $\mathcal{L}$ with a rank-two $\mathcal{O}_E$-sheaf, where $E/\mathbf{Q}_\ell$ is a finite extension. Proposition 13 and Lemma 22 show that it suffices to prove the proposition after passing to a finite cover of C. By passing to an appropriate cover, we can therefore assume that $\mathcal{L}/\ell^r$ is trivial. The image of the Galois representation $\rho : \pi_1^{\text{ét}}(\mathcal{U}) \to \mathbf{GL}_2(\mathcal{O}_E)$ has order $M \cdot \ell^\infty$ (in the sense of profinite groups) for some positive integer M. By enlarging N, we can assume that $M \cdot \ell \mid N$ and that the complement of U in C spreads out to a divisor on $\mathcal{C}$ that is smooth over S.

We make the following definitions.

- Let D be an integer greater than $(g(C) - 1)/(g(X) - 1)$, where $g(-)$ denotes genus. Let $\mathcal{M}_d$ be the space of maps $\mathcal{U} \to Y$ of degree d, in the sense of Proposition 21, and let $\mathcal{M} = \coprod_{d=1}^D \mathcal{M}_d$.
- Let $\mathcal{T}$ be the (integral) ℓ-adic Tate module of the universal elliptic curve over Y, and let $\mathcal{T}' = \mathcal{T} \otimes \mathcal{O}_E$. Also let $\mathcal{L}_n = \mathcal{L}/\ell^n\mathcal{L}$ and let $\mathcal{T}'_n = \mathcal{T}'/\ell^n\mathcal{T}'$.
- Let $\widetilde{\mathcal{M}}_n$ be the moduli space of pairs (f, ψ) where $f \in \mathcal{M}$ and ψ is an isomorphism of $\mathcal{O}_E$-sheaves $f^*(\mathcal{T}_n) \to \mathcal{L}_n$.

Lemma 23. *The map $\pi : \widetilde{\mathcal{M}}_n \to \mathcal{M}$ is finite.*

Proof. Note that for every field-valued point f of $\mathcal{M}$ there are only finitely many choices for ψ and so the map $\widetilde{\mathcal{M}}_n \to \mathcal{M}$ is quasi-finite. Thus, to prove the lemma it is sufficient to show that π is proper.

We use the valuative criterion. Let R be a discrete valuation ring with fraction field F. Let $f \in \mathcal{M}(R)$ and $(\psi, f) \in \widetilde{\mathcal{M}}_n(F)$. Thus, f corresponds to a map $f : U_R \to Y_R$ and $\psi : f^*(\mathcal{T}_n)_F \to (\mathcal{L}_n)_F$ is an isomorphism. Since $f^*(\mathcal{T}_n)$ and $\mathcal{L}_n$ are finite étale sheaves on U_R, which is a normal scheme, ψ extends uniquely over U_R. □

https://doi.org/10.1112/S0010437X18007315 Published online by Cambridge University Press

Let $\mathcal{M}_n$ be the image of $\widetilde{\mathcal{M}}_n$ in $\mathcal{M}$, which is closed by Lemma 23. We endow it with the reduced subscheme structure. As the $\mathcal{M}_n$ form a descending chain of closed subschemes of $\mathcal{M}$, they stabilize. Let $\mathcal{M}_\infty$ be $\mathcal{M}_n$ for $n \gg 0$.

Lemma 24. *The fiber of $\mathcal{M}_\infty$ over all closed points of S is non-empty.*

Proof. Let s be a closed point of S of characteristic p. By Lemma 12, $\mathcal{L}_{\overline{K}}$ is an irreducible sheaf. Let $\overline{S}$ be the strict Hensilization of S at s, $\overline{s}$ the geometric point corresponding to s, and K_s the fraction field of $\overline{S}$. By [SGA1, XIII, 2.10, p. 289],

$$\pi_1^{\text{ét},(p)}(\mathcal{U}_{\overline{s}}) \cong \pi_1^{\text{ét},(p)}(\mathcal{U}_{\overline{S}}) \twoheadleftarrow \pi_1^{\text{ét}}(U_{K_s}) \supset \pi_1^{\text{ét}}(U_{\overline{K_s}}) = \pi_1^{\text{ét}}(U_{\overline{K}}), \tag{$*$}$$

where $\pi_1^{\text{ét},(p)}$ denotes the prime to p quotient of $\pi_1^{\text{ét}}$. We can regard $\mathcal{L}$ as a representation of $\pi_1^{\text{ét}}(\mathcal{U})$ and then restrict it to a representation of $\pi_1^{\text{ét}}(\mathcal{U}_{\overline{S}})$; since the image of the representation has order $M\ell^\infty$, which is prime to p, it factors through $\pi_1^{\text{ét},(p)}(\mathcal{U}_{\overline{S}})$. We thus obtain a representation of $\pi_1^{\text{ét},(p)}(\mathcal{U}_{\overline{s}})$. The pullback of this representation to $\pi_1^{\text{ét}}(U_{\overline{K}})$ is irreducible. It follows now that $\mathcal{L}_s$ is an irreducible sheaf on $\mathcal{U}_s$.

By Proposition 19, we can find a family of elliptic curves $\mathcal{E} \to \mathcal{U}_s$ and an isomorphism $\mathcal{L}_s|_{\mathcal{U}_s} \cong T(\mathcal{E}) \otimes \mathcal{O}_E$, where $T(\mathcal{E})$ is the relative Tate module of $\mathcal{E}$. It follows that $T(\mathcal{E})/\ell^r$ is the trivial sheaf, and so we can find a basis for $\mathcal{E}[\ell^r]$ over $\mathcal{U}_s$. We thus have a map $f : \mathcal{U}_s \to Y$ such that $T(\mathcal{E}) \cong f^*(\mathcal{T})$. Factor f as $g \circ F^n$, where $g : \mathcal{U}_s \to Y$ is separable and $F : Y_{\kappa(s)} \to Y_{\kappa(s)}$ is the absolute Frobenius element. Note that $F^*(\mathcal{T}) \cong \mathcal{T}$, and so $T(\mathcal{E}) \cong g^*(\mathcal{T})$. Let $\overline{g}$ be the extension of g to a map $C_s \to X$. Since $\overline{g}$ is separable, it has degree $\leqslant D$. Thus $\overline{g}$, and the isomorphism $\mathcal{L} \cong g^*(\mathcal{T}) \otimes \mathcal{O}_E$, define a $\kappa(s)$ points of $\mathcal{M}_n$ for all n, which proves the lemma. □

Proof of Theorem 1. Since $\mathcal{M}_\infty$ is finite type over S and all of its fibers over closed points are non-empty, it follows that the generic fiber of $\mathcal{M}_\infty$ is non-empty. Choose a point x in $\mathcal{M}_\infty(L')$, for some finite extension L'/L, corresponding to a family of elliptic curves $\mathcal{E} \to U_{L'}$. Now, x lifts to $\widetilde{\mathcal{M}}_n(\overline{L})$ for all n. Thus $\mathcal{L}_n$ and $T(\mathcal{E}) \otimes \mathcal{O}_E/\ell^n$ are isomorphic for all n, as sheaves on $U_{\overline{L}}$. It follows that $\mathcal{L}$ and $T(\mathcal{E}) \otimes \mathcal{O}_E$ are isomorphic over $U_{\overline{L}}$ (by compactness). By Lemma 11, $\mathcal{L}[1/\ell]$ and $T(\mathcal{E}) \otimes E$ are isomorphic over $U_{L''}$, for some finite (even quadratic) extension L'' of L'. Passing to the generic fibers, we see that $\rho|_{KL''}$ comes from an elliptic curve, which completes the proof by Proposition 13. □

Acknowledgement

We thank the referee for helpful comments, which improved the exposition of the paper.

References

BLR90 S. Bosch, W. Lütkebohmert and M. Raynaud, *Néron models* (Springer, Berlin, 1990).

Dri77 V. G. Drinfeld, *Elliptic modules II*, Math. USSR-Sb **31** (1977), 159–170.

Dri78 V. G. Drinfeld, *Langland's conjecture for* **GL**(2) *over function fields*, in *Proc. Int. Congress Mathematicians, Helsinki, 1978* (Academia Scientiarum Fennica, 1980), 565–574.

Dri83 V. G. Drinfed, *Two-dimensional ℓ-adic representations of the fundamental group of a curve over a finite field and automorphic forms on* **GL**(2), Amer. J. Math. **105** (1983), 85–114.

FWGSS92 G. Faltings, G. Wüstholz, F. Grunewald, N. Schappacher and U. Stuhler, *Rational points*, Aspects of Mathematics, vol. E6, third edition (Vieweg, Braunschweig, 1992).

Mil J. S. Milne, Abelian varieties, http://www.jmilne.org/math/CourseNotes/AV110.pdf.

Ser65 J.-P. Serre, *Zeta and L functions*, in *Arithmetical algebraic geometry* (Harper and Row, New York, NY, 1965), 82–92.

SGA1 A. Grothendieck and M. Raynaud, *Revêtements étales et groupe fondamental (SGA 1)*, Documents Mathématiques (Paris), vol. 3 (Société Mathématique de France, 2003).

Shi67 G. Shimura, *Algebraic number fields and symplectic discontinuous groups*, Ann. of Math. (2) **86** (1967), 503–592.

Tay02 R. Taylor, *Remarks on a conjecture of Fontaine and Mazur*, J. Inst. Math. Jussieu **1** (2002), 125–143.

Andrew Snowden asnowden@umich.edu
Department of Mathematics, University of Michigan,
Ann Arbor, MI, USA
http://www-personal.umich.edu/∼asnowden/

Jacob Tsimerman jacobt@math.toronto.edu
Department of Mathematics, University of Toronto,
Toronto, CA, Canada
http://www.math.toronto.edu/∼jacobt/

https://doi.org/10.1112/S0010437X18007315 Published online by Cambridge University Press