Mathematische Annalen

On a local-global principle for quadratic twists of abelian varieties

Francesc Fité[1]

Abstract

Let A and A' be abelian varieties defined over a number field k of dimension $g \geq 1$. For $g \leq 3$, we show that the following local-global principle holds: A and A' are quadratic twists of each other if and only if, for almost all primes $\mathfrak{p}$ of k of good reduction for A and A', the reductions $A_\mathfrak{p}$ and $A'_\mathfrak{p}$ are quadratic twists of each other. This result is known when $g = 1$, in which case it has appeared in works by Kings, Rajan, Ramakrishnan, and Serre. We provide an example that violates this local-global principle in dimension $g = 4$.

1 Introduction

1.1 Main result

Let k be a number field and let A be an abelian variety defined over k of dimension $g \geq 1$. We will denote by A_ψ the twist of A corresponding to a given 1-cocycle $\psi \colon G_k \to \operatorname{Aut}(A_{\overline{\mathbb{Q}}})$, where G_k denotes the absolute Galois group of k. We will say that an abelian variety A' defined over k is a *quadratic twist of* A if it is isogenous over k to A_χ for some (possibly trivial) quadratic character $\chi \colon G_k \to \{\pm 1\} \subseteq \operatorname{Aut}(A_{\overline{\mathbb{Q}}})$. Let Σ_k be the set of nonzero prime ideals of the ring of integers of k. For $\mathfrak{p} \in \Sigma_k$, denote by $k_\mathfrak{p}$ the residue field of k at $\mathfrak{p}$, and if $\mathfrak{p}$ is of good reduction for A, let $A_\mathfrak{p}$ be the reduction of A modulo $\mathfrak{p}$. Let $f_{A_\mathfrak{p}}$ be the the characteristic polynomial of Frobenius relative to $k_\mathfrak{p}$ acting on an ℓ-adic Tate module of $A_\mathfrak{p}$ for some prime ℓ coprime to $\mathfrak{p}$. If $\mathfrak{p}$ is of good reduction for both A and A', we will say that A and A' are *locally quadratic twists at* $\mathfrak{p}$ if $A_\mathfrak{p}$ and $A'_\mathfrak{p}$ are quadratic twists, that is, if either

✉ Francesc Fité
ffite@ub.edu
http://www.ub.edu/nt/ffite/

[1] Departament de Matemàtiques i Informàtica and Centre de Recerca Matemàtica, Universitat de Barcelona, Gran Via de les Corts Catalanes 585, 08007 Barcelona, Catalonia, Spain

$$f_{A_{\mathfrak{p}}}(T) = f_{A'_{\mathfrak{p}}}(T) \quad \text{or} \quad f_{A_{\mathfrak{p}}}(T) = f_{A'_{\mathfrak{p}}}(-T)\,.$$

One easily sees that if A and A' are quadratic twists, then

$$A \text{ and} A' \text{ are locally quadratic twists at almost all primes of } \Sigma_k. \qquad (1.1)$$

Throughout the article, by "almost all primes of Σ_k" we mean "all primes in a (Dirichlet) density 1 subset of Σ_k". Our main object of study will be the converse of the above implication. The following is our main result.

Theorem 1.1 *Let A and A' be abelian varieties defined over k of dimension $g \leq 3$. Suppose that* (1.1) *holds for A and A'. Then A and A' are quadratic twists.*

We complement the above theorem by providing two abelian fourfolds defined over $\mathbb{Q}$ that are locally quadratic twists at all odd primes, but which are not quadratic twists. Let $a_{\mathfrak{p}}(A)$ denote the Frobenius trace of A at $\mathfrak{p}$. The above theorem is not true if one replaces condition (1.1) by the weaker condition that $a_{\mathfrak{p}}(A)$ and $a_{\mathfrak{p}}(A')$ coincide up to sign for almost all $\mathfrak{p}$ in Σ_k. Under this weaker hypothesis, it is easy to find counterexamples, and we give one in dimension $g = 2$. Both examples can be found in §6.

1.2 Previous results

Theorem 1.1 is known if $g = 1$ (at least if A does not have complex multiplication *defined over k*). There are different proofs of this fact in works of Serre [21, p. 324], Kings [13, p. 90-91], and Ramakrishnan [18, Thm. B] (note that in these works the results are generally phrased in terms of Galois representations attached to modular forms). In the CM case, there is a closely related result by Wong [27, Cor. 1].

The dimension $g = 1$ case of Theorem 1.1 can also be retrieved from a general result on ℓ-adic representations due to Rajan [17]. More in general, as we will explain in §2, this result implies that if two abelian varieties A and A' satisfy (1.1), then $A_{\overline{\mathbb{Q}}}$ and $A'_{\overline{\mathbb{Q}}}$ are isogenous. Refining this conclusion to the statement of Theorem 1.1 is the goal of this article.

The above mentioned results are just a few instances of a vast literature on local-global principles concerning abelian varieties over number fields. Our problem is closely related to a recent result of Khare and Larsen [12]. They show that the base changes $A_{\overline{\mathbb{Q}}}$ and $A'_{\overline{\mathbb{Q}}}$ are isogenous if and only if for almost[1] all primes $\mathfrak{p}$ in Σ_k so are the base changes $A_{\mathfrak{p}} \times \overline{k}_{\mathfrak{p}}$ and $A'_{\mathfrak{p}} \times \overline{k}_{\mathfrak{p}}$, where $\overline{k}_{\mathfrak{p}}$ denotes an algebraic closure of $k_{\mathfrak{p}}$. Our methods of proof and those of [12] are rather different (mainly due to the fact that ours is a question sensitive to base change).

In fact, we only prove the local-global principle investigated in this article for certain classes of abelian varietes. The fact that these classes end up encompassing

---

[1] Actually in [12] it suffices to assume that a sufficiently large density of primes of Σ_k has the required property. Obtaining an analogous refinement of Theorem 1.1 seems an interesting question, which we have not attempted to address in this article.

those of dimension $g \leq 3$ may be regarded as an "accident in low dimension". This is reminiscent of other local-global questions concerning abelian varieties over number fields. For example, Katz [11] showed that if $g \leq 2$ and for almost all $\mathfrak{p}$ the cardinality of $A_{\mathfrak{p}}(k_{\mathfrak{p}})$ is divisible by some prime number m, then there exists an abelian variety A' isogenous to A such that m divides the order of the torsion subgroup of $A'(k)$; he also showed that this fails to be true if $g \geq 3$.

1.3 Outline of the article

The methods employed to prove Theorem 1.1 all involve the study of the ℓ-adic representation $\varrho_{A,\ell}$ attached to the abelian variety A. Let us briefly summarize them. We will say that a subset $\mathcal{A}$ of the set of abelian varieties defined over the number field k satisfies the *local-global QT principle* if any pair of abelian varieties in $\mathcal{A}$ that satisfy (1.1) are quadratic twists.

In §2, we record some background results. We start by deriving some consequences of Faltings isogeny theorem; this implies, for example, that if A and A' satisfy (1.1), then A and A' share the same endomorphism field K. We then show that the result by Rajan mentioned above implies that the local-global QT principle holds for those abelian varieties A such that $\text{End}(A_{\overline{\mathbb{Q}}}) = \mathbb{Z}$. We conclude §2 by describing some connections with the theory of Sato–Tate groups. Our proof of Theorem 1.1 is independent of the Sato–Tate conjecture, but it does benefit from the classification of Sato–Tate groups of abelian varieties of dimension ≤ 3.

Suppose that A and A' satisfy (1.1). The main results of §3 are two variants of Rajan's theorem that build on [22]: Theorem 3.1 applies when $\varrho_{A,\ell}$ has an unrepeated strongly absolutely irreducible factor; Theorem 3.3 shows that, under a certain technical assumption, the base changes A_K and A'_K are quadratic twists. A common strategy in later sections consists on first applying Theorem 3.3, and then using arguments specific to the situation of interest to descend the validity of the local-global QT principle from K to k.

In §4, we consider families of abelian varieties for which the methods described in the previous paragraph fail to apply. Those include abelian varieties that are geometrically isogenous to the power of an elliptic curve. In this case, the Tate module tensor decompositions obtained in [5] allow to translate our problem concerning ℓ-adic representations of degree $2g$ into one concerning Artin representations of degree g. This reduction by half in the degree of the representations turns out to be crucial. Indeed, the corresponding local-global principle for Artin representations is almost immediate when g is odd, and, while it can fail for even g, it does hold for $g = 2$. This can be seen by means of reinterpreting Ramakrishnan's theorem [18, Thm. B] in the context of Artin representations. Hence, Ramakrishnan's theorem, originally conceived to treat the dimension $g = 1$ case of our problem, ends up playing an important role in its generalization in dimension $g = 2$. In §4.3, we show that produtcs of geometrically pairwise nonisogenous elliptic curves with complex multiplication satisfy the local-global QT principle. In this section, we use Hecke's equidistribution theorem [10] at several points; this is natural and intuitive, but it would have sufficed to use instead results from [22].

In §5, we complete the proof of Theorem 1.1. The proof takes into account the different possibilities for $\mathrm{End}(A_{\overline{\mathbb{Q}}})\otimes\mathbb{Q}$. Many cases were covered in previous sections. Other cases, as mentioned above, involve invoking Theorem 3.1 or Theorem 3.3, and then providing a few adhoc arguments. As an example of the latter, we mention the case in which A is isogenous to the product of an elliptic curve E and and abelian surface B such that $\mathrm{Hom}(E_{\overline{\mathbb{Q}}}, B_{\overline{\mathbb{Q}}}) = 0$. If E does not have CM, then Theorem 1.1 immediately follows from Theorem 3.1. However, if E has CM, Theorem 3.1 essentially only provides two quadratic characters χ and ψ such that $A' \sim E_\chi \times B_\psi$. That one can take $\chi = \psi$ is the content of Proposition 5.6.

1.4 Notation and terminology

Throughout the article, k is a number field, and A and A' are abelian varieties defined over k of dimension $g \geq 1$. All algebraic extensions of k are assumed to be contained in a fixed algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. If L/k is one such field extension, then we will write G_L to denote the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$, and A_L to denote the base change $A \times_k L$. We denote by $\mathrm{End}^0(A)$ the endomorphism algebra of A, and refer to $\mathrm{End}^0(A_{\overline{\mathbb{Q}}})$ as the geometric endomorphism algebra of A. However, due to a widely used convention, when we say that A has complex multiplication (CM), we in fact mean that $A_{\overline{\mathbb{Q}}}$ has CM. Whenever it becomes necessary to ask that the CM be defined over k, we will explicitly specify it. If E is a field and $\theta\colon G_k \to \mathrm{GL}_r(E)$ is a representation, then $\theta|_L$ denotes the restriction of θ to G_L, and $\theta^\vee$ denotes the contragredient representation of θ. We will say that θ is *absolutely irreducible* if $\theta \otimes \overline{E}$ is irreducible, where $\overline{E}$ denotes an algebraic closure of E. We will say that θ is *strongly absolutely irreducible* if $\theta|_L$ is absolutely irreducible for every finite extension L/k.

2 Generalities

We will derive some properties that A and A' must satisfy in case (1.1) holds. First we record some elementary consequences of Faltings isogeny theorem [2]; then we describe some implications of a theorem of Rajan; finally we explain the connection of our problem to the theory of Sato–Tate groups and derive some consequences of their classification for abelian surfaces.

2.1 Consequences of faltings isogeny theorem

For a prime number ℓ, let $V_\ell(A)$ denote the rational ℓ-adic Tate module of A. There is a continuous action of G_k on $V_\ell(A)$ which gives rise to an ℓ-adic representation $\varrho_{A,\ell}\colon G_k \to \mathrm{Aut}(V_\ell(A))$. For $\mathfrak{p} \in \Sigma_k$, denote by $\mathrm{Fr}_{\mathfrak{p}}$ an arithmetic Frobenius element at $\mathfrak{p}$. By the work of Weil, if $\mathfrak{p}$ is of good reduction for A and does not divide ℓ, then

$$L_{\mathfrak{p}}(A, T) := \det\left(1 - \varrho_{A,\ell}(\mathrm{Fr}_{\mathfrak{p}})T\right)$$

is a polynomial of degree $2g$ with integer coefficients which does not depend on the choice of ℓ. One easily verifies that $\varrho_{A_\chi,\ell} \simeq \chi \otimes \varrho_{A,\ell}$ for any quadratic character χ, and Faltings isogeny theorem then gives that A' is a quadratic twist of A by χ if and only if $\varrho_{A',\ell} \simeq \chi \otimes \varrho_{A,\ell}$. Together with the fact that $L_{\mathfrak{p}}(A, T)$ coincides with the reverse Weil polynomial $T^{2g} f_{A_{\mathfrak{p}}}(1/T)$ of the reduction $A_{\mathfrak{p}}$, this has the following consequence.

Lemma 2.1 *If A and A' are quadratic twists, then they are locally quadratic twists at every prime $\mathfrak{p}$ which is of good reduction for both.*

Throughout this article we will denote by K/k the *endomorphism field* of A, that is, the minimal extension K/k such that $\mathrm{End}(A_K) \simeq \mathrm{End}(A_{\overline{\mathbb{Q}}})$. It is a finite and Galois extension.

Lemma 2.2 *Suppose that* (1.1) *holds for A and A'. Then $\mathrm{End}^0(A_L)$ and $\mathrm{End}^0(A'_L)$ have the same dimension for every finite extension L/k. In particular, A and A' share the same endomorphism field.*

Proof The lemma follows from the isomorphism

$$
\mathrm{End}(A_L) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \simeq \left(V_\ell(A) \otimes V_\ell(A)^\vee \right)^{G_L} \simeq \left(V_\ell(A') \otimes V_\ell(A')^\vee \right)^{G_L}
$$
$$
\simeq \mathrm{End}(A'_L) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell .
$$

The central isomorphism follows from (1.1) and the Chebotarev density theorem. $\square$

2.2 Rajan's theorem

Let E_λ denote a finite extension of $\mathbb{Q}_\ell$, and let $\varrho, \varrho' : G_k \to \mathrm{GL}_r(E_\lambda)$ be continuous, semisimple representations unramified outside a finite set $S \subseteq \Sigma_k$. Consider the set

$$
\mathrm{SM}(\varrho, \varrho') := \{\mathfrak{p} \in \Sigma_k - S \mid \mathrm{Tr}(\varrho(\mathrm{Fr}_{\mathfrak{p}})) = \mathrm{Tr}(\varrho'(\mathrm{Fr}_{\mathfrak{p}}))\} .
$$

With the above notations, Rajan [17, Thm. 2, part i)] shows the following.

Theorem 2.3 *(Rajan) Let F/k be a finite extension such that the Zariski closures of $\varrho(G_F)$ and $\varrho'(G_F)$ are connected. If the upper density of $\mathrm{SM}(\varrho|_F, \varrho'|_F)$ is positive, then there exists a finite Galois extension L/k containing F/k such that $\varrho|_L \simeq \varrho'|_L$.*

Rajan's theorem relates to the local-global QT principle by means of next lemma.

Lemma 2.4 *Suppose that there exists a density 1 subset $\Sigma \subseteq \Sigma_k$ such that for every $\mathfrak{p} \in \Sigma$ there exists $\epsilon_{\mathfrak{p}} \in \{\pm 1\}$ such that $\mathrm{Tr}(\varrho'(\mathrm{Fr}_{\mathfrak{p}})) = \epsilon_{\mathfrak{p}} \cdot \mathrm{Tr}(\varrho(\mathrm{Fr}_{\mathfrak{p}}))$. Then for every finite extension F/k, the set $\mathrm{SM}(\varrho|_F, \varrho'|_F)$ has a positive upper density.*

Proof We first claim that there exists a density 1 subset $\Sigma' \subseteq \Sigma_F$ such that for every $\mathfrak{p} \in \Sigma'$ there exists $\chi_{\mathfrak{p}} \in \{\pm 1\}$ such that $\mathrm{Tr}(\varrho'(\mathrm{Fr}_{\mathfrak{p}})) = \chi_{\mathfrak{p}} \cdot \mathrm{Tr}(\varrho(\mathrm{Fr}_{\mathfrak{p}}))$. Indeed, the hypothesis implies that $\varrho \otimes \varrho \simeq \varrho' \otimes \varrho'$. In particular, we have $\varrho \otimes$

$\varrho|_F \simeq \varrho' \otimes \varrho'|_F$. Hence the claim. But this implies that, if the lemma were false, then $\text{Tr}(\varrho(\text{Fr}_\mathfrak{p})) = -\text{Tr}(\varrho'(\text{Fr}_\mathfrak{p}))$ for all $\mathfrak{p}$ in a density 1 subset of Σ_F. The Chebotarev density theorem would then imply that $\text{Tr}(\varrho|_F) = -\text{Tr}(\varrho'|_F)$, which contradicts $\text{Tr}(\varrho(\text{id})) = \text{Tr}(\varrho'(\text{id}))$. $\qquad\square$

Rajan's theorem has the following consequence (see [17, Thm. 2, part iii)]).

Corollary 2.5 *(Rajan) Suppose that the hypotheses of Theorem 2.3 hold, and that moreover ϱ is strongly absolutely irreducible. Then there exists a finite Galois extension L/k and a character $\chi : \text{Gal}(L/k) \to \overline{\mathbb{Q}}^\times$ such that $\varrho' \simeq \chi \otimes \varrho$.*

Proof By Theorem 2.3 there exists a finite Galois extension L/k such that $\varrho|_L \simeq \varrho'|_L$. Since ϱ is strongly absolutely irreducible, Schur's lemma shows that the space

$$\text{Hom}_{G_L}(\varrho', \varrho) \simeq (\varrho' \otimes \varrho^\vee)^{G_L}$$

is 1-dimensional. Let χ denote the character of the action of $\text{Gal}(L/k)$ on this space. Then

$$\text{Hom}_{G_k}(\varrho', \chi \otimes \varrho) \simeq \text{Hom}_{G_k}\left(\varrho' \otimes \varrho^\vee, (\varrho' \otimes \varrho^\vee)^{G_L}\right) \neq 0.$$

Since $\chi \otimes \varrho$ is irreducible and has the same dimension as ϱ', we have $\varrho' \simeq \chi \otimes \varrho$. $\square$

We will apply Theorem 2.3 when ϱ and ϱ' are the ℓ-adic representations attached to A and A'. The following is a consequence of Rajan's theorem.

Corollary 2.6 *Suppose that (1.1) holds for A and A'. Then there exists a finite Galois extension L/k such that A_L and A'_L are isogenous.*

Proof There exists a finite extension F/k such that the Zariski closures of $\varrho_{A,\ell}(G_F)$ and $\varrho_{A',\ell}(G_F)$ are connected. By Lemma 2.4, the representations $\varrho_{A,\ell}|_F$ and $\varrho_{A',\ell}|_F$ satisfy the hypotheses of Theorem 2.3. Hence, there exists a finite Galois extension L/k containing F/k such that $\varrho_{A,\ell}|_L \simeq \varrho_{A',\ell}|_L$, and so A_L and A'_L are isogenous. $\square$

We now use the above corollaries to show that the local-global QT principle holds for abelian varieties with trivial geometric endomorphism ring.

Corollary 2.7 *Suppose that $\text{End}(A_{\overline{\mathbb{Q}}}) \simeq \mathbb{Z}$ and that (1.1) holds for A and A'. Then A and A' are quadratic twists.*

Proof By Faltings isogeny theorem, for every finite extension L/k we have an isomorphism

$$\text{End}_{G_L}(V_\ell(A)) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell \simeq \text{End}(A_L) \otimes_{\mathbb{Z}} \overline{\mathbb{Q}}_\ell \simeq \overline{\mathbb{Q}}_\ell,$$

which implies that $\varrho_{A,\ell}$ is strongly absolutely irreducible. By Corollary 2.5, there exists a finite Galois extension L/k and a character χ of $\text{Gal}(L/k)$ such that $\varrho_{A',\ell} \simeq \chi \otimes \varrho_{A,\ell}$. Again by Faltings isogeny theorem, there is an isomorphism

$$\text{Hom}_{G_L}(V_\ell(A), V_\ell(A')) \simeq \text{Hom}(A_L, A'_L) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \simeq \mathbb{Q}_\ell(\chi),$$

where $\mathbb{Q}_\ell(\chi)$ means $\mathbb{Q}_\ell$ equipped with the action of $\mathrm{Gal}(L/k)$ via χ. Hence $\mathrm{Gal}(L/k)$ acts on $\mathrm{Hom}(A_L, A'_L) \simeq \mathbb{Z}$ via χ, and thus χ must be quadratic. □

2.3 The connection with Sato–Tate groups

Throughout this section suppose that A and A' have dimension $g \leq 3$. The Sato–Tate group of A, denoted $\mathrm{ST}(A)$, is a closed real Lie subgroup of $\mathrm{USp}(2g)$, only defined up to conjugacy. It captures important arithmetic information of A and it is conjectured to predict the limiting distribution of the Frobenius elements attached to A. See [1] for its definition in our context; see [23] for a conditional definition in a more general context. Let us denote by $\mathrm{ST}(A)^0$ the connected component of the identity in $\mathrm{ST}(A)$, and by $\pi_0(\mathrm{ST}(A))$ the group of components of $\mathrm{ST}(A)$.

Lemma 2.8 *Suppose that* (1.1) *holds for A and A'. Then*

$$\pi_0(\mathrm{ST}(A)) \simeq \pi_0(\mathrm{ST}(A')) \quad \text{and} \quad \mathrm{ST}(A)^0 \simeq \mathrm{ST}(A')^0 .$$

Proof By Lemma 2.2, A and A' have the same endomorphism field K/k, and by [6, Prop. 2.17], there is an isomorphism $\pi_0(\mathrm{ST}(A)) \simeq \mathrm{Gal}(K/k)$. The second isomorphism follows from Corollary 2.5 and [1, Rem. 3.2]. □

For every $\mathfrak{p} \in \Sigma_k$ of good reduction for A, one defines a semisimple conjugacy class $s_\mathfrak{p}$ of $\mathrm{ST}(A)$ as in [6, Def. 2.9]. The Sato–Tate conjecture for A is the prediction that the sequence $\{s_\mathfrak{p}\}_\mathfrak{p}$, where the indexing set of primes is ordered by norm, is equidistributed with respect to the projection of the Haar measure of $\mathrm{ST}(A)$ on its set of conjugacy classes. The characteristic polynomial $\sum_i a_i T^i \in \mathbb{R}[T]$ of an element of $\mathrm{USp}(2g)$ is monic and palindromic, and it is hence determined by the g-tuple $\mathbf{a} = (a_1, \ldots, a_g)$. If we denote by X_g the set of g-tuples obtained in this way, then there is a bijection $\mathrm{Conj}(\mathrm{USp}(2g)) \simeq X_g$. Let $\mathbf{a}_\mathfrak{p}$ denote the image of $s_\mathfrak{p}$ under the map

$$\mathrm{Conj}(\mathrm{ST}(A)) \to \mathrm{Conj}(\mathrm{USp}(2g)) \simeq X_g .$$

We will denote by μ the projection on X_g, via the above map, of the Haar measure of $\mathrm{ST}(A)$. Define similarly $s'_\mathfrak{p}$, $\mathbf{a}'_\mathfrak{p}$ and μ'.

Let $\pi(x)$ denote the number of primes $\mathfrak{p}$ in Σ_k of good reduction for A such that $\mathrm{Nm}(\mathfrak{p}) \leq x$. The Sato–Tate conjecture implies that

$$\int_{\mathbf{a} \in X_g} f(\mathbf{a})\mu = \lim_{x \to \infty} \frac{1}{\pi(x)} \sum_{\mathrm{Nm}(\mathfrak{p}) \leq x} f(\mathbf{a}_\mathfrak{p}) \tag{2.1}$$

for every $\mathbb{C}$-valued continuous function f on X_g.

Lemma 2.9 *Suppose that* (1.1) *holds for the abelian varieties A and A' of dimension $g \leq 3$. If the Sato–Tate conjecture holds for A and A', then the Sato–Tate groups of A and A' coincide.*

Proof Given $\mathbf{a} \in X_g$ and a g-tuple of nonnegative integer numbers $\mathbf{e} = (e_1, \ldots, e_g)$, let us write $\mathbf{a}^{\mathbf{e}}$ to denote $a_1^{e_1} \cdots a_g^{e_g}$. By [8, Prop. 6.16] and Lemma 2.8, it suffices to show that

$$\int_{\mathbf{a} \in X_g} \mathbf{a}^{\mathbf{e}} \mu = \int_{\mathbf{a} \in X_g} \mathbf{a}^{\mathbf{e}} \mu' \qquad (2.2)$$

for every $\mathbf{e}$. Let $w(\mathbf{e})$ denote $\sum_i i e_i$. Since $-1 \in \mathrm{ST}(A)$, we have that both members of (2.2) are 0 if $w(\mathbf{e})$ is odd. Suppose from now one that $w(\mathbf{e})$ is even. If A and A' are locally quadratic twists at $\mathfrak{p}$, then $s'_{\mathfrak{p}} = \pm s_{\mathfrak{p}}$, and hence $\mathbf{a}'^{\mathbf{e}}_{\mathfrak{p}} = \mathbf{a}^{\mathbf{e}}_{\mathfrak{p}}$. Then (2.2) follows from (2.1).   □

Remark 2.10 Lemma 2.9 will not be used in the sequel. Since the Sato-Tate group of an abelian variety is invariant under quadratic twist, Lemma 2.9 can be recovered from Theorem 1.1 (without assuming the Sato–Tate conjecture).

2.4 Consequences of the classification of Sato–Tate groups

The next two results represent partial progress toward Theorem 1.1 and will be used to simplify some proofs in subsequent sections. We use the notations for Sato–Tate groups introduced in [6] and [8], and present in the data base [14].

Proposition 2.11 *Suppose that* (1.1) *holds for the abelian surfaces A and A', and:*

   (i) The Sato–Tate group of A is distinct from $C_{4,1}$, F_{ac}.
   (ii) There exists a character χ of G_k such that $\varrho_{A',\ell} \simeq \chi \otimes \varrho_{A,\ell}$.

Then A and A' are quadratic twists.

Proof By comparing determinants of $\varrho_{A,\ell}$ and $\varrho_{A',\ell}$ we see that $\chi^4 = 1$. It will suffice to prove that in fact $\chi^2 = 1$. Suppose that the order of χ were 4. Let $\Sigma \subseteq \Sigma_k$ denote the density 1 set of primes $\mathfrak{p}$ of good reduction for A and A', of absolute residue degree 1, and such that A and A' are locally quadratic twists at $\mathfrak{p}$. Define $z_{2,0}$ as the upper density of the set of primes $\mathfrak{p} \in \Sigma$ such that the coefficient $b_{\mathfrak{p}}$ of T^2 in $L_{\mathfrak{p}}(A, T)$ is 0. For every $\mathfrak{p} \in \Sigma$ such that $\chi(\mathrm{Fr}_{\mathfrak{p}})$ has order 4, condition ii) implies that $b_{\mathfrak{p}}$ is zero. In particular, we see that $z_{2,0} \geq 1/2$. It is proven in the course of [20, Thm. 3] that $z_{2,0}$ is the proportion of connected components C of the Sato–Tate group of A such that, for all $\gamma \in C$, the coefficient of T^2 in the characteristic polynomial of γ is 0. Interpreted as this proportion, the quantity $z_{2,0}$ can be read from [6, Table 8] (see columns 'c' and 'z_2'; note that $z_{2,0}$ is the central term of z_2). By inspection of the table, one finds that $C_{4,1}$ and F_{ac} are the only two Sato–Tate groups of abelian surfaces for which $z_{2,0} \geq 1/2$.   □

The next lemma accounts for cases uncovered by the previous proposition. For its proof it is convenient to introduce the following notion. For a finite Galois extension F/k, A will be said to have *Frobenius traces concentrated in F* if $\mathrm{Tr}(\varrho_{A,\ell}(\mathrm{Fr}_{\mathfrak{p}})) = 0$ for every $\mathfrak{p} \in \Sigma_k$ of good reduction for A which does not split completely in F/k.

Lemma 2.12 *Let A and A' be abelian surfaces defined over k. Let K/k denote the endomorphism field of A. Suppose that:*

  (i) *The Sato–Tate group of A is $C_{4,1}$, F_{ac}.*
  (ii) *There is a character ψ of G_k such that $\psi|_K$ is quadratic and $\varrho_{A',\ell} \simeq \psi \otimes \varrho_{A,\ell}$.*

Then A and A' are quadratic twists.

Proof Let E/k be the cyclic extension cut out by ψ. By hypothesis $ii)$, we have that $[E : E \cap K] \leq 2$. Hypothesis $i)$ implies that A has Frobenius traces concentrated in K. If $E \subseteq K$, then this implies that

$$\varrho_{A',\ell} \simeq \psi \otimes \varrho_{A,\ell} \simeq \varrho_{A,\ell}, \tag{2.3}$$

and hence A and A' are in fact isogenous. Suppose from now on that $[E : E \cap K] = 2$. We may assume that ψ is quartic as otherwise there is nothing to show. Then $\mathrm{Gal}(EK/k)$ is a group of order 8 with two normal subgroups of order 2 yielding quotients isomorphic to C_4. This uniquely determines the isomorphism class of $\mathrm{Gal}(EK/k)$, which must be $C_2 \times C_4$. In this case, one readily sees that there exists a quadratic subextension F/k of EK/k such that $EK = FK$. Let χ denote the nontrivial character of $\mathrm{Gal}(F/k)$. If follows that $\chi|_K = \psi|_K$ and hence $\psi \otimes \varrho_{A,\ell} \simeq \chi \otimes \varrho_{A,\ell}$ by the fact that A has Frobenius traces concentrated in K. □

3 Variants of Rajan's theorem

In this section, relying on the results of [22], we will prove variants of Corollary 2.5, which will later play a crucial role in the proof of Theorem 1.1. Resume the notations of §2.2. The following variant of Corollary 2.5 drops the condition that ϱ and ϱ' be strongly absolutely irreducible representations.

Theorem 3.1 *Let $\varrho, \varrho' \colon G_k \to \mathrm{GL}_r(E_\lambda)$ be continuous, semisimple representations unramified outside a finite set $S \subseteq \Sigma_k$. Suppose that there exists a density 1 subset $\Sigma \subseteq \Sigma_k$ such that for every $\mathfrak{p} \in \Sigma$ there exists $\epsilon_{\mathfrak{p}} \in \{\pm 1\}$ such that*

$$\mathrm{Tr}(\varrho'(\mathrm{Fr}_{\mathfrak{p}})) = \epsilon_{\mathfrak{p}} \cdot \mathrm{Tr}(\varrho(\mathrm{Fr}_{\mathfrak{p}})). \tag{3.1}$$

Suppose moreover that

$$\varrho \simeq \varrho_1 \oplus \varrho_2, \quad \varrho' \simeq \varrho'_1 \oplus \varrho'_2, \quad \varrho_i, \varrho'_i \colon G_k \to \mathrm{GL}_{r_i}(E_\lambda),$$

where ϱ_1 is strongly absolutely irreducible, the Zariski closure of its image is connected, and satisfies

$$\mathrm{Hom}_{G_F}(\varrho_1, \varrho_2) = \mathrm{Hom}_{G_F}(\varrho_1, \varrho'_2) = 0 \tag{3.2}$$

for every finite extension F/k. Then there exists a quadratic character χ of G_k such that $\varrho' \simeq \chi \otimes \varrho$.

Proof By Theorem 2.3, there exists a finite extension L/k such that $\varrho|_L \simeq \varrho'_L$. By (3.2), we have $\varrho_i|_L \simeq \varrho'_i|_L$, and then the argument in the proof of Corollary 2.5 yields a character χ_1 satisfying $\varrho'_1 \simeq \chi_1 \otimes \varrho_1$. For a $\mathfrak{p} \in \Sigma$, we may rewrite (3.1) as

$$(\chi_1(\mathrm{Fr}_{\mathfrak{p}}) - \epsilon_{\mathfrak{p}}) \cdot \mathrm{Tr}(\varrho_1(\mathrm{Fr}_{\mathfrak{p}})) - \epsilon_{\mathfrak{p}} \cdot \mathrm{Tr}(\varrho_2(\mathrm{Fr}_{\mathfrak{p}})) + \mathrm{Tr}(\varrho'_2(\mathrm{Fr}_{\mathfrak{p}})) = 0 \,.$$

Let G_i (resp. G'_i) denote the Zariski closure of $\varrho_i(G_k)$ (resp. of $\varrho'_i(G_k)$) in GL_{r_i}. Denote by X_1 the finite set $\mathrm{im}(\chi_1) \pm 1 \subseteq \overline{\mathbb{Q}}$. Choose a *nonzero* x_1 in X_1 and x_2 in $\{\pm 1\}$. Let W_{x_1,x_2} denote the subvariety of $G_1 \times G_2 \times G'_2$ cut by the equation

$$x_1 \cdot \mathrm{Tr}(g_1) + x_2 \cdot \mathrm{Tr}(g_2) + \mathrm{Tr}(g'_2) = 0 \quad \text{for } g_1 \in G_1, \, g_2 \in G_2, \, g'_2 \in G'_2.$$

Note that $W_{x_1,x_2} \cap G_1$ is a closed subvariety of G_1. It is properly contained in G_1, as otherwise we would obtain a relation among the traces of ϱ_1, ϱ_2, and ϱ'_2 that would contradict (3.2). Hence, the connectedness of G_1 implies that $\dim(W_{x_1,x_2} \cap G_1) < \dim(G_1)$. Let H be the (finite) union of the closed proper subvarieties $W_{x_1,x_2} \cap G_1$ attached to choices of the x_1, x_2 as above. Then, by [22, Thm. 10, Thm. 8] the density of the set of primes $\mathfrak{p} \in \Sigma$ for which $\varrho_1(\mathrm{Fr}_{\mathfrak{p}})$ belongs to H is zero. We conclude that for every prime $\mathfrak{p}$ in a subset of Σ, still of density 1, we have $\chi_1(\mathrm{Fr}_{\mathfrak{p}}) = \epsilon_{\mathfrak{p}}$, which in particular implies that χ_1 is quadratic. Therefore, for every $\mathfrak{p}$ in a density 1 subset of Σ_k, we have $\mathrm{Tr}(\varrho'(\mathrm{Fr}_{\mathfrak{p}})) = \chi_1(\mathrm{Fr}_{\mathfrak{p}}) \cdot \mathrm{Tr}(\varrho(\mathrm{Fr}_{\mathfrak{p}}))$, and the theorem follows from the semisimplicity of ϱ and ϱ'. □

We will typically apply Theorem 3.1 when ϱ and ϱ' are $\varrho_{A,\ell}$ and $\varrho_{A',\ell}$, and A has dimension ≤ 3 and all endomorphisms defined over k (in this situation, the Zariski closure of $\varrho(G_k)$ is connected; see [6, Prop. 2.17]). The following is the most basic application.

Corollary 3.2 *Let A and A' be elliptic curves defined over k for which (1.1) holds. Then A and A' are quadratic twists.*

Proof As recalled in §1, the result is known if $\varrho_{A,\ell}$ is irreducible. If A is an elliptic curve with CM defined over k, then $\varrho_{A,\ell}$ satisfies the hypotheses of Theorem 3.1. □

The following result asserts that the local-global QT principle holds over the endomorphism field under a mild technical hypothesis.

Theorem 3.3 *Suppose that (1.1) holds for A and A', and that, if K/k denotes the endomorphim field of A, then the Zariski closures of $\varrho_{A,\ell}(G_K)$ and $\varrho_{A',\ell}(G_K)$ are connected. Then there exists a quadratic character χ of G_K such that $A'_K \sim A_{K,\chi}$ and such that the field extension L/K cut out by χ satisfies that L/k is Galois.*

Proof Suppose that A_K and A'_K are not isogenous, as otherwise the result is clear. Since the Zariski closures of $\varrho_{A,\ell}(G_K)$ and $\varrho_{A,\ell}(G_K)$ are connected, we can choose a prime ℓ such that

$$\varrho_{A,\ell}|_K \simeq \bigoplus_i \varrho_i^{\oplus n_i}\,, \qquad \varrho_{A',\ell}|_K \simeq \bigoplus_i {\varrho'_i}^{\oplus n'_i}\,,$$

where the ϱ_i (resp. ϱ_i') are strongly absolutely irreducible representations of G_K pairwise nonisomorphic even after restriction to a finite extension of K. After reordering the ϱ_i, Corollary 2.6 provides a finite extension L'/K such that $\varrho_i|_{L'} \simeq \varrho_i'|_{L'}$. In particular $n_i = n_i'$. There exists a density 1 subset $\Sigma \subseteq \Sigma_K$ such that for every $\mathfrak{p} \in \Sigma$ there exists $\chi_{\mathfrak{p}} \in \{\pm 1\}$ such that $\mathrm{Tr}(\varrho_{A',\ell}(\mathrm{Fr}_{\mathfrak{p}})) = \chi_{\mathfrak{p}} \cdot \mathrm{Tr}(\varrho_{A,\ell}(\mathrm{Fr}_{\mathfrak{p}}))$. The argument in the proof of Corollary 2.5 shows that there exists a character χ_1 of G_K such that $\varrho_1' \simeq \chi_1 \otimes \varrho_1$. For every $\mathfrak{p} \in \Sigma$, we thus have

$$n_1(\chi_1(\mathrm{Fr}_{\mathfrak{p}}) - \chi_{\mathfrak{p}}) \cdot \mathrm{Tr}(\varrho_1(\mathrm{Fr}_{\mathfrak{p}})) - \chi_{\mathfrak{p}} \cdot \sum_{i \geq 2} n_i \, \mathrm{Tr}(\varrho_i(\mathrm{Fr}_{\mathfrak{p}})) + \sum_{i \geq 2} n_i \, \mathrm{Tr}(\varrho_i'(\mathrm{Fr}_{\mathfrak{p}})) = 0.$$

Arguing as in the proof of Theorem 3.1, we see that $\varrho_{A',\ell}|_K \simeq \chi_1 \otimes \varrho_{A,\ell}|_K$ and that χ_1 is quadratic. If L/K is the quadratic extension cut out by χ_1, then there is an isogeny from A_L to A_L'. Hence L/k is the minimal extension over which all homomorphisms from $A_{\overline{\mathbb{Q}}}$ to $A_{\overline{\mathbb{Q}}}'$ are defined, and so L/k is Galois. □

4 Products of elliptic curves

In this section we consider abelian varieties which are $\overline{\mathbb{Q}}$-isogenous to products of elliptic curves. In §4.2 we examine the case of $\overline{\mathbb{Q}}$-isogenous factors. In this situation, Theorem 3.1 fails to apply, but the local-global QT principle will follow by combining the Tate module tensor decompositions obtained in [5] with a theorem of Ramakrishnan that we recall in §4.1. Finally, in §4.3 we consider the case of a product of pairwise geometrically nonisogenous elliptic curves with CM.

4.1 Ramakrishnan's theorem

Let L/k be a finite Galois extension, V a $\overline{\mathbb{Q}}$-vector space, and $\theta \colon \mathrm{Gal}(L/k) \to \mathrm{GL}(V)$ an Artin representation. Let

$$\mathrm{ad}_\theta \colon \mathrm{Gal}(L/k) \to \mathrm{Aut}(\mathrm{End}(V)), \qquad \mathrm{ad}_\theta(s)(f) := \theta(s) \circ f \circ \theta(s)^{-1}$$

denote the adjoint representation of θ. It satifies $\mathrm{ad}_\theta \simeq \theta \otimes \theta^\vee$. Note that if ad_θ^0 denotes the restriction of ad_θ on the subspace of trace 0 elements of $\mathrm{End}(V)$, then $\mathrm{ad}_\theta \simeq \mathbf{1} \oplus \mathrm{ad}_\theta^0$, where $\mathbf{1}$ denotes the trivial representation.

The next theorem of Ramakrishnan [18, Thm. B] shows that, in the 2-dimensional case, θ can be recovered from ad_θ^0 up to twist by a character (beware that Ramakrishnan's original theorem applies to general ℓ-adic representations; we will only apply it to Artin representations).

Theorem 4.1 (Ramakrishnan) *If* $\theta, \theta' \colon \mathrm{Gal}(L/k) \to \mathrm{GL}_2(\overline{\mathbb{Q}})$ *are Artin representations with* $\mathrm{ad}_\theta^0 \simeq \mathrm{ad}_{\theta'}^0$, *then there is a character* χ *of* $\mathrm{Gal}(L/k)$ *such that* $\theta' \simeq \chi \otimes \theta$.

Proof It follows from Schur Lemma that θ is irreducible if and only if $\mathbf{1}$ is not an irreducible constituent of ad_θ^0. Hence, θ' is irreducible if and only if θ is irreducible. See [18, Thm. B] for the proof in the case that both θ and θ' are irreducible. If both θ and θ' are reducible, the proof is an elementary exercise left to the reader. □

Remark 4.2 If $\theta, \theta' \colon G_k \to \mathrm{GL}_3(\overline{\mathbb{Q}})$ are Artin representations such that $\mathrm{ad}_\theta^0 \simeq \mathrm{ad}_{\theta'}^0$, it is not necessarily true that there exists a character χ such that $\theta' \simeq \chi \otimes \theta$. To construct an example of this, let L/k be a degree 24 Galois extension with Galois group $\mathrm{D}_4 \times \mathrm{C}_3$, let ν denote a non-selfdual degree 2 irreducible representation of $\mathrm{Gal}(L/k)$, and let ω denote the determinant of ν. One easily verifies that $\theta = \mathbf{1} \oplus \nu$ and $\theta' = \omega \oplus \nu$ provide the desired example.

We will be concerned with the following consequence of the above theorem.

Corollary 4.3 *Let* $\theta, \theta' \colon \mathrm{Gal}(L/k) \to \mathrm{GL}_g(\overline{\mathbb{Q}})$ *be Artin representations. Suppose that* g *is* 2 *or odd. If for every* $s \in \mathrm{Gal}(L/k)$, *there exists* $\chi_s \in \{\pm 1\}$ *such that*

$$\det(1 - \theta'(s)T) = \det(1 - \chi_s \cdot \theta(s)T), \tag{4.1}$$

then there exists a quadratic character $\chi \colon \mathrm{Gal}(L/k) \to \mathbb{Q}^\times$ *such that* $\theta' \simeq \chi \otimes \theta$.

Proof By comparing the leading coefficients of both sides of (4.1), one obtains

$$\det(\theta'(s)) = \chi_s^g \cdot \det(\theta(s)) \tag{4.2}$$

for every s in $\mathrm{Gal}(L/k)$. If g is odd, define the character $\chi := \det(\theta')/\det(\theta)$. Since it satisfies $\chi(s) = \chi_s$ for every s, it is quadratic and $\theta' \simeq \chi \otimes \theta$ as desired. Suppose next that $g = 2$. Then (4.1) implies that $\mathrm{ad}_\theta^0 \simeq \mathrm{ad}_{\theta'}^0$. Hence by Theorem 4.1 there exists a character $\chi \colon \mathrm{Gal}(L/k) \to \overline{\mathbb{Q}}^\times$ such that $\theta' \simeq \chi \otimes \theta$. Taking determinants of this isomorphism and comparing with (4.2), one finds that χ is in fact quadratic. □

Remark 4.4 The above corollary fails to hold for general even values of g. Let L/k denote a biquadratic extension. Let φ and ψ denote two distinct nontrivial characters of $\mathrm{Gal}(L/k)$. It is easy to verify that the degree 6 Artin representations

$$\theta := \mathbf{1}^{\oplus 3} \oplus \varphi \oplus \psi \oplus \varphi\psi, \qquad \theta' := \mathbf{1}^{\oplus 2} \oplus \varphi^{\oplus 2} \oplus \psi^{\oplus 2}.$$

verify (4.1), while there is no character χ of $\mathrm{Gal}(L/k)$ such that $\theta' \simeq \chi \otimes \theta$.

4.2 Tate module tensor decompositions

In this section, we consider some families of geometrically isotypic abelian varieties, that is, abelian varieties that are $\overline{\mathbb{Q}}$-isogenous to the power of an (absolutely) simple one. We will rely on the description of the Tate module of one such variety given in [5, Thm. 1.1]. We next restate that theorem in our particular cases of interest.

Fix a complex conjugation σ in $G_\mathbb{Q}$. Let ϱ be an ℓ-adic representation of G_k unramified outside a finite set $S \subseteq \Sigma_k$. We will denote by ϱ^σ the ℓ-adic representation

defined by $\varrho^\sigma(s) := \varrho(\sigma s \sigma^{-1})$ for every $s \in G_k$. Given a number field F, we will say that ϱ is F-rational if $\det(1 - \varrho(\mathrm{Fr}_{\mathfrak{p}})T) \in F[T]$ for every $\mathfrak{p} \in \Sigma_k - S$. If θ is an Artin representation with coefficients in F, we will denote by $\overline{\theta}$ the representation with coefficients in $\sigma(F)$ defined by $\overline{\theta}(s) := \sigma(\theta(s))$.

Theorem 4.5 *([5]) Suppose that $A_{\overline{\mathbb{Q}}}$ is isogenous to the power of either:*

(a) an elliptic curve without CM; or
(b) an abelian surface with quaternionic multiplication (QM); or
(c) an elliptic curve with CM by a quadratic imaginary field M.

Then there exists a number field F such that for every prime ℓ totally split in F:

(i) If a) or b) hold, then

$$\varrho_{A,\ell} \simeq \theta \otimes_{\mathbb{Q}_\ell} \varrho \,,$$

where $\theta\colon G_k \to \mathrm{GL}_g(F)$ is an Artin representation, and $\varrho\colon G_k \to \mathrm{GL}_2(\mathbb{Q}_\ell)$ is a strongly absolutely irreducible F-rational ℓ-adic representation.
(ii) If c) holds, then F contains M and

$$\varrho_{A,\ell}|_{kM} \simeq (\theta \otimes_{\mathbb{Q}_\ell} \chi) \oplus (\overline{\theta} \otimes_{\mathbb{Q}_\ell} \overline{\chi}) \,,$$

where $\theta\colon G_{kM} \to \mathrm{GL}_g(F)$ is an Artin representation and $\chi, \overline{\chi}\colon G_{kM} \to \mathbb{Q}_\ell^\times$ are F-rational continuous characters. Moreover, the ℓ-adic representations $\theta \otimes_{\mathbb{Q}_\ell} \chi$ and $\overline{\theta} \otimes_{\mathbb{Q}_\ell} \overline{\chi}$ are in fact M-rational. Finally, if $k \neq kM$, then

$$\varrho_{A,\ell} \simeq \mathrm{Ind}_{kM}^k(\theta \otimes_{\mathbb{Q}_\ell} \chi) \quad and \quad \overline{\theta} \otimes_{\mathbb{Q}_\ell} \overline{\chi}|_{kM} \simeq \theta^\sigma \otimes_{\mathbb{Q}_\ell} \chi^\sigma|_{kM} \,. \quad (4.3)$$

Remark 4.6 There is a particular situation of case i) of the above theorem in which the representations θ, ϱ admit especially explicit descriptions. Suppose that there exists an elliptic curve B without CM and *defined over k* such that $A_{\overline{\mathbb{Q}}}$ and $B_{\overline{\mathbb{Q}}}^g$ are isogenous (by [4, Thm. 2.21], this happens for example whenever g is odd). Then we may take $F = \mathbb{Q}$, $\varrho = \varrho_{B,\ell}$, and $\theta = \mathrm{Hom}^0(B_{\overline{\mathbb{Q}}}^g, A_{\overline{\mathbb{Q}}})$, in which case the theorem follows from [3, Thm. 3.1].

The above theorem is a crucial input for Theorems 4.9 and 4.11, whose proofs will also need the following auxiliary lemma on the abundance of ordinary primes. Let $\mathfrak{p}$ be a prime of Σ_k of good reduction for A lying over the rational prime p. We say that $\mathfrak{p}$ is *ordinary* if the central coefficient of $L_{\mathfrak{p}}(A, T)$ is not divisible by p, equivalently, if g of the roots of $L_{\mathfrak{p}}(A, T)$ have p-adic valuation 0; we say that $\mathfrak{p}$ is *supersingular* if all the roots of $L_{\mathfrak{p}}(A, T)$ are of the form $\zeta \, \mathrm{Nm}(\mathfrak{p})^{-1/2}$, where ζ is a root of unity and $\mathrm{Nm}(\mathfrak{p})$ is the absolute norm of $\mathfrak{p}$.

Lemma 4.7 *Suppose that $A_{\overline{\mathbb{Q}}}$ is isogenous to the power of an elliptic curve B. If B has CM, say by a quadratic imaginary field M, suppose that $k = kM$. Then the set of primes of ordinary reduction for A has density 1.*

Proof We claim that a prime $\mathfrak{p}$ of Σ_k of good reduction for A is either ordinary or supersingular. Indeed, let q denote $\mathrm{Nm}(\mathfrak{p})$, let $\alpha_{\mathfrak{p}}$ be a root of $L_{\mathfrak{p}}(A, T)$, and let $v \colon \overline{\mathbb{Q}}_p^{\times} \to \mathbb{Q}$ denote the p-adic valuation normalized so that $v(q)$ is 1. By hypothesis, there exists a finite Galois extension K/k such that A_K is isogenous to the power of an elliptic curve over K. If $f \geq 1$ denotes the residue degree of $\mathfrak{p}$ in K/k, then $A_{\mathfrak{p}} \times_{\mathbb{F}_q} \mathbb{F}_{q^f}$ is isogenous to the power of an elliptic curve over $\mathbb{F}_{q^f}$, and hence the valuation $v(\alpha_{\mathfrak{p}}^f)$ is either $0, f$, or $f/2$. In the first two cases, $\mathfrak{p}$ is ordinary, and in the latter case $\mathfrak{p}$ is supersingular. We need to show that the set S of supersingular primes has density 0. If B does not have CM, let θ and ϱ be as in part i) of Theorem 4.5. If $\mathfrak{p} \in S$, then $\mathrm{Tr}(\varrho(\mathrm{Fr}(\mathfrak{p})))$ is divisible by $\sqrt{q}$ and hence is limited to finitely many possibilities. By [22], this implies that S has density 0. If B has CM, let χ be as in part ii) of Theorem 4.5. If $\mathfrak{p} \in S$, then $\chi(\mathrm{Fr}_{\mathfrak{p}}) = \zeta \sqrt{q}$, where ζ is a root of unity whose order is bounded in terms of g. By [22] or [10], and under the assumption $k = kM$, this implies that S has density 0. $\qquad\square$

Remark 4.8 When g is odd and B has no CM, the above lemma admits an even simpler proof. In this case, by Remark 4.6, there is an elliptic curve B *defined over k* and an Artin representation θ such that $\varrho_{A, \ell} \simeq \theta \otimes \varrho_{B, \ell}$. Thus a prime of good reduction of A is ordinary for A if and only if it is ordinary for B. That the set of primes ordinary for B has density 1 is well known.

Theorem 4.9 *Suppose that* (1.1) *holds for A and A', and that:*

- *(i) The dimension g of A is either odd or equal to 2.*
- *(ii) $A_{\overline{\mathbb{Q}}}$ is either an abelian surface with QM or isogenous to the power of an elliptic curve without CM.*

Then A and A' are quadratic twists.

Proof By Corollary 2.6 there is a finite Galois extension L/k such that A_L and A'_L are isogenous. Hence A' also satisfies hypothesis ii). After possibly enlarging L/k, by Theorem 4.5, there are a number field F, Artin representations θ, θ' of $\mathrm{Gal}(L/k)$ realizable over F, and F-rational ℓ-adic representations ϱ, ϱ' of G_k of degree 2 such that $\varrho_{A, \ell} \simeq \theta \otimes_{\mathbb{Q}_\ell} \varrho$ and $\varrho_{A', \ell} \simeq \theta' \otimes_{\mathbb{Q}_\ell} \varrho'$, where ℓ is a prime totally split in F. Since $\varrho|_L \simeq \varrho'|_L$ and ϱ is strongly absolutely irreducible, there is a character χ of $\mathrm{Gal}(L/k)$ such that $\varrho' \simeq \chi \otimes \varrho$. If $\mathfrak{p} \in \Sigma_k$ is a prime of good reduction for A, let $\alpha_{\mathfrak{p}}$ and $\beta_{\mathfrak{p}}$ be the eigenvalues of $\varrho(\mathrm{Fr}_{\mathfrak{p}})$. By [20, Thm. 3] and Lemma 4.7, there exists a density 1 subset $\Sigma \subseteq \Sigma_k$ of primes of good reduction for A and A' such that for every $\mathfrak{p} \in \Sigma$ the quotient $\alpha_{\mathfrak{p}}/\beta_{\mathfrak{p}}$ is not a root of unity, and

$$\det(1 - (\theta' \otimes \chi \otimes \varrho)(\mathrm{Fr}_{\mathfrak{p}})T) = \det(1 - \epsilon_{\mathfrak{p}} \cdot (\theta \otimes \varrho)(\mathrm{Fr}_{\mathfrak{p}})T)$$

for some $\epsilon_{\mathfrak{p}} \in \{\pm 1\}$. Hence for every $\mathfrak{p} \in \Sigma$ we have

$$\det(1 - \alpha_{\mathfrak{p}} \cdot (\theta' \otimes \chi)(\mathrm{Fr}_{\mathfrak{p}})T) = \det(1 - \epsilon_{\mathfrak{p}} \alpha_{\mathfrak{p}} \cdot \theta(\mathrm{Fr}_{\mathfrak{p}})T).$$

Since Σ has density 1, for every $s \in \mathrm{Gal}(L/k)$ there must be $\epsilon_s \in \{\pm 1\}$ such that

$$\det(1 - (\theta' \otimes \chi)(s)T) = \det(1 - \epsilon_s \cdot \theta(s)T).$$

Since i) holds, by Corollary 4.3, there exists a quadratic character φ of $\mathrm{Gal}(L/k)$ such that $\theta' \otimes \chi \simeq \varphi \otimes \theta$. Therefore $\varrho_{A',\ell} \simeq \theta' \otimes \chi \otimes \varrho \simeq \varphi \otimes \theta \otimes \varrho \simeq \varphi \otimes \varrho_{A,\ell}$. $\qquad \square$

Remark 4.10 We note that the theorem above is not true for general even values of g. Let E be an elliptic curve defined over k without CM. Let A and A' be the 6-dimensional abelian varieties $E \otimes \theta$ and $E \otimes \theta'$, where θ and θ' are the Artin representations defined in Remark 4.4. Then A and A' are locally quadratic twists at almost all primes of Σ_k. However, if there were a quadratic character ε of G_k such that $\varrho_{A',\ell} \simeq \varepsilon \otimes \varrho_{A,\ell}$, then, arguing as in the proof of the above theorem, we would obtain that θ' is isomorphic to $\varepsilon \otimes \theta$, which contradicts Remark 4.4.

Theorem 4.11 *Suppose that* (1.1) *holds for A and A', and that:*

  (i) The dimension g of A is either odd or equal to 2.
  (ii) $A_{\overline{\mathbb{Q}}}$ is isogenous to the power of an elliptic curve with CM.

Then A and A' are quadratic twists.

Proof Let M denote the quadratic imaginary field associated with the elliptic factor of A. Suppose first that M is contained in k. By arguing as in the proof of Theorem 4.9, using Theorem 4.5 we can find a finite Galois extension L/k, a number field F, Artin representations $\theta, \theta' \colon \mathrm{Gal}(L/k) \to \mathrm{GL}_g(F)$, and continuous F-rational ℓ-adic characters $\chi, \chi', \overline{\chi}, \overline{\chi}'$ of G_k such that

$$\varrho_{A,\ell} \simeq (\theta \otimes \chi) \oplus (\overline{\theta} \oplus \overline{\chi}), \quad \text{and} \quad \varrho_{A',\ell} \simeq (\theta' \otimes \chi') \oplus (\overline{\theta}' \oplus \overline{\chi}'), \quad (4.4)$$

where ℓ is a prime totally split in F. After reordering χ and $\overline{\chi}$ if necessary, we may assume that $\chi|_L \simeq \chi'|_L$. Therefore there exists a character ψ of $\mathrm{Gal}(L/k)$ such that $\chi' \simeq \psi \chi$. By Lemma 4.7 there exists a density 1 subset $\Sigma \subseteq \Sigma_k$ of primes of good reduction for A and A' such that for every $\mathfrak{p} \in \Sigma$ the quotient $\chi(\mathrm{Fr}_\mathfrak{p})/\overline{\chi}(\mathrm{Fr}_\mathfrak{p})$ is not a root of unity, and

$$\det\left(1 - (\theta' \otimes \psi \chi \oplus \overline{\theta}' \otimes \overline{\psi \chi})(\mathrm{Fr}_\mathfrak{p})T\right) = \det\left(1 - \epsilon_\mathfrak{p} \cdot (\theta \otimes \chi \oplus \overline{\theta} \otimes \overline{\chi})(\mathrm{Fr}_\mathfrak{p})T\right)$$

for some $\epsilon_\mathfrak{p} \in \{\pm 1\}$. Hence for every $\mathfrak{p} \in \Sigma$ we have

$$\det\left(1 - (\theta' \otimes \psi \chi)(\mathrm{Fr}_\mathfrak{p})T\right) = \det\left(1 - \epsilon_\mathfrak{p} \cdot (\theta \otimes \chi)(\mathrm{Fr}_\mathfrak{p})T\right) .$$

Since Σ has density 1, for every $s \in \mathrm{Gal}(L/k)$ there must be $\epsilon_s \in \{\pm 1\}$ such that

$$\det(1 - (\theta' \otimes \psi)(s)T) = \det(1 - \epsilon_s \cdot \theta(s)T).$$

Corollary 4.3 yields a quadratic character φ of G_k such that $\theta' \otimes \psi \simeq \varphi \otimes \theta$. Thus

$$\varrho_{A',\ell} \simeq (\theta' \otimes \psi \chi) \oplus (\overline{\theta}' \otimes \overline{\psi \chi}) \simeq \varphi \otimes (\theta \otimes \chi \oplus \overline{\theta} \otimes \overline{\chi}) \simeq \varphi \otimes \varrho_{A,\ell} .$$

Suppose now that M is not contained in k. Arguing as in the previous case, we see that there are a continuous character $\chi: G_{kM} \to \overline{\mathbb{Q}}_\ell^\times$, a quadratic character φ of $\mathrm{Gal}(L/kM)$, and an Artin representation θ of $\mathrm{Gal}(L/kM)$ such that

$$\varrho_{A,\ell} \simeq \mathrm{Ind}_{kM}^k(\theta \otimes \chi), \quad \varrho_{A',\ell} \simeq \mathrm{Ind}_{kM}^k(\varphi \otimes \theta \otimes \chi), \quad \varphi^\sigma \otimes \theta^\sigma \simeq \varphi \otimes \theta^\sigma.$$

The third of the above isomorphisms follows from

$$\varphi^\sigma \otimes \theta^\sigma \otimes \chi^\sigma \simeq \overline{\varphi} \otimes \overline{\theta} \otimes \overline{\chi} \simeq \varphi \otimes \overline{\theta} \otimes \overline{\chi} \simeq \varphi \otimes \theta^\sigma \otimes \chi^\sigma,$$

where we have used (4.3). Suppose that g is odd. Taking determinants of $\varphi^\sigma \otimes \theta^\sigma \simeq \varphi \otimes \theta^\sigma$, we get $(\varphi^\sigma)^g = \varphi^g$, that is, φ^σ and φ coincide as characters of $\mathrm{Gal}(L/kM)$. Hence φ extends to a character $\tilde{\varphi}$ of $\mathrm{Gal}(L/k)$, and

$$\varrho_{A',\ell} \simeq \tilde{\varphi} \otimes \mathrm{Ind}_{kM}^k(\theta \otimes \chi) \simeq \tilde{\varphi} \otimes \varrho_{A,\ell}.$$

Taking determinants of the above isomorphism, we see that $\tilde{\varphi}^{2g} = 1$. Since trivially we also have $\tilde{\varphi}^4 = 1$, the fact that g is odd implies that $\tilde{\varphi}$ is quadratic. If $g = 2$, then apply Lemma 4.12 below taking $N = kM$.   □

The next lemma is applied in the proof of the above theorem in the case $g = 2$. We state and prove it also in the case $g = 3$ for future reference.

Lemma 4.12 *Suppose that* (1.1) *holds for A and A', and that:*

  (i) A and A' have dimension ≤ 3.
  (ii) There exist a quadratic extension N/k contained in the endomorphism field K/k and a quadratic character $\chi: G_N \to \{\pm 1\}$ such that $A_{N,\chi} \sim A'_N$.
 (iii) A has Frobenius traces concentrated in N.

Then A and A' are quadratic twists.

Proof Let E/N denote the field extension cut out by χ. Let E^{Gal}/k denote the Galois closure of E/k. Since E/k contains the quadratic subextension N/k, the possibilities for $\mathrm{Gal}(E^{\mathrm{Gal}}/k)$ are $C_2 \times C_2, C_4$, or D_4. In the first two cases, the character χ extends to a character $\tilde{\chi}$ of $\mathrm{Gal}(E^{\mathrm{Gal}}/k)$ such that $\tilde{\chi}^4 = 1$. By iii), we have that $\varrho_{A',\ell} \simeq \tilde{\chi} \otimes \varrho_{A,\ell}$. If $g = 3$, then $\tilde{\chi}^6 = 1$, and hence $\tilde{\chi}$ must be quadratic. If $g = 2$, the lemma follows from Proposition 2.11 and Lemma 2.12 (note that $\tilde{\chi}|_K$ is indeed quadratic). Suppose finally that $\mathrm{Gal}(E^{\mathrm{Gal}}/k) \simeq D_4$. Then there exists a biquadratic extension F/k such that $FN = E^{\mathrm{Gal}}$. Therefore, there exists a (quadratic) character ψ of $\mathrm{Gal}(F/k)$ such that $\psi|_N = \chi|_N$. By iii), we have that $\varrho_{A',\ell} \simeq \psi \otimes \varrho_{A,\ell}$, which completes the proof of the lemma.   □

4.3 Products of pairwise geometrically nonisogenous elliptic curves

In this section we prove that the local-global QT principle holds for products of pairwise geometrically nonisogenous elliptic curves. We resume the notations from the previous section. The following lemma will be used in this and later sections.

Lemma 4.13 *Let A be an abelian variety defined over k. Suppose that $A_{\overline{\mathbb{Q}}}$ is isogenous to the product $B \times C$ of abelian varieties B, C defined over $\overline{\mathbb{Q}}$ such that*

$$\mathrm{Hom}(B, C^s) = 0 \tag{4.5}$$

for all $s \in G_k$. Then there exist abelian varieties B', C' defined over k such that A is isogenous to $B' \times C'$.

Proof Choose an isogeny $\varphi \colon B \times C \to A_{\overline{\mathbb{Q}}}$. Let B' denote the abelian subvariety of $A_{\overline{\mathbb{Q}}}$ generated by $\varphi(B)$ and its Galois conjugates $\varphi(B)^s$ for $s \in G_k$. Define C' analogously. Note that B' and C' are defined over k. By (4.5), we have $\mathrm{Hom}(B', C') = 0$, and hence the addition map $\psi \colon B' \times C' \to A$ has finite kernel. Therefore

$$\dim(A) \geq \dim(B') + \dim(C') \geq \dim(B) + \dim(C) = \dim(A) \,.$$

Hence A and $B' \times C'$ have the same dimension, and thus ψ is an isogeny. $\square$

By the above lemma and Theorem 3.1, the local-global QT principle holds for products of pairwise geometrically nonisogenous elliptic curves one of whose factors does not have CM. From now on, we focus on the case that all factors have CM.

Lemma 4.14 *Suppose that A is isogenous to the product of g elliptic curves E_i with CM, say by M_i, and pairwise not $\overline{\mathbb{Q}}$-isogenous. Then there is a subset $\Sigma \subseteq \Sigma_k$ of density 1 consisting of primes of absolute residue degree 1 and of good reduction for A such that for every $\mathfrak{p} \in \Sigma$, of norm p, we have*

$$L_{\mathfrak{p}}(A, T) = \prod_{i=1}^{g}(1 - \alpha_i T)(1 - p\alpha_i^{-1}T) \,, \tag{4.6}$$

where the reciprocal roots $\alpha_i \in \overline{\mathbb{Q}}$ satisfy:

  (i) *If $\mathfrak{p}$ splits in M_i, then $\alpha_i \in M_i - \mathbb{Q}$ and $\alpha_i/\sqrt{p}$ is not a root of unity.*
  (ii) *If $\mathfrak{p}$ is inert in M_i, then $\alpha_i = \sqrt{-p}$ and $\alpha_i \notin M_j$ for any j.*

Proof If $\mathfrak{p}$ splits in kM_i, consider the decomposition $\varrho_{E_i,\ell}|_{kM} \simeq \chi \oplus \overline{\chi}$ from Theorem 4.5 noting that χ is an M_i-rational Hecke character in this case; if $\mathfrak{p}$ is inert in kM_i, then use the description of ϱ_{E_i} as the induction of χ from kM_i down to k. We spare the details to the reader. $\square$

Proposition 4.15 *Suppose that (1.1) holds for A and A', and that $A_{\overline{\mathbb{Q}}}$ is isogenous to the product of g nonisogenous elliptic curves with CM. Then A and A' are quadratic twists.*

Proof By Corollary 2.6 and Lemma 4.13, there exist elliptic curves E_i, E'_i defined over k such that $E_{i,\overline{\mathbb{Q}}}$ and $E'_{i,\overline{\mathbb{Q}}}$ are isogenous, and $A \sim \prod_i E_i$ and $A' \sim \prod_i E'_i$. Suppose first that $g = 2$. Lemma 4.13 also implies that if M_i denotes the CM field of E_i, then the endomorphism field K of A is kM_1M_2. From the description of $L_{\mathfrak{p}}(A, T)$

from Lemma 4.14, we see that E_i and E'_i satisfy (1.1). Then, by Corollary 3.2, there are quadratic characters φ_i of G_k such that $\varrho_{E'_i,\ell} \simeq \varphi_i \otimes \varrho_{E_i,\ell}$. By Theorem 3.3, we must have $\varphi_1|_K = \varphi_2|_K$. Let now χ_i denote the nontrivial character of $\mathrm{Gal}(kM_i/k)$ if this group is nontrivial, and the trivial character otherwise. There exist integers $\delta_1, \delta_2 \in \{0, 1\}$ such that $\varphi_2 = \chi_1^{\delta_1}\chi_2^{\delta_2}\varphi_1$. Then

$$\varrho_{A',\ell} \simeq (\varphi_1 \otimes \varrho_{E_1,\ell}) \oplus (\chi_1^{\delta_1}\chi_2^{\delta_2}\varphi_1 \otimes \varrho_{E_2,\ell}) \simeq \chi_1^{\delta_1}\varphi_1 \otimes (\varrho_{E_1,\ell} \oplus \varrho_{E_2,\ell}) \simeq \chi_1^{\delta_1}\varphi_1 \\ \otimes \varrho_{A,\ell},$$

where we have used that $\chi_i \otimes \varrho_{E_i,\ell} \simeq \varrho_{E_i,\ell}$.

Suppose now that $g \geq 3$. By hypothesis, there exists a density 1 subset $\Sigma \subseteq \Sigma_k$ such that for every $\mathfrak{p} \in \Sigma$ there exists $\epsilon_\mathfrak{p} \in \{\pm 1\}$ such that $L_\mathfrak{p}(A', T) = L_\mathfrak{p}(A, \epsilon_\mathfrak{p}T)$. Let $A_i := E_1 \times E_i$ and $A'_i := E'_1 \times E'_i$ for every $i \geq 2$. From the description of $L_\mathfrak{p}(A, T)$ from Lemma 4.14, by shrinking Σ if necessary, we may assume that $L_\mathfrak{p}(A'_i, T) = L_\mathfrak{p}(A_i, \epsilon_\mathfrak{p}T)$ for every $\mathfrak{p} \in \Sigma$. By the $g = 2$ case, there exists a quadratic character φ_i of G_k such that $A'_i \sim A_{i,\varphi_i}$. Hence

$$\epsilon_\mathfrak{p} \cdot \mathrm{Tr}(\varrho_{A_i,\ell}(\mathrm{Fr}_\mathfrak{p})) = \mathrm{Tr}(\varrho_{A'_i,\ell}(\mathrm{Fr}_\mathfrak{p})) = \varphi_i(\mathrm{Fr}_\mathfrak{p}) \cdot \mathrm{Tr}(\varrho_{A_i,\ell}(\mathrm{Fr}_\mathfrak{p})) \qquad (4.7)$$

for every $\mathfrak{p} \in \Sigma$. Moreover, by Hecke's equidistribution theorem, there is a density 1 subset $\Sigma' \subseteq \Sigma$ such that for every $\mathfrak{p} \in \Sigma'$, we have $\mathrm{Tr}(\varrho_{A_i,\ell}(\mathrm{Fr}_\mathfrak{p})) \neq 0$ unless $\mathfrak{p}$ is both inert in M_1 and M_i. Let $\Sigma_i \subseteq \Sigma'$ be the subset of those $\mathfrak{p}$ which are split in M_1 or split in M_i. Note that $\Sigma_2 \cap \Sigma_i$ has density equal to 5/8. From (4.7), for every $\mathfrak{p} \in \Sigma_2 \cap \Sigma_i$, we have $\varphi_i(\mathrm{Fr}_\mathfrak{p}) = \epsilon_\mathfrak{p} = \varphi_2(\mathrm{Fr}_\mathfrak{p})$. Since φ_i and φ_2 are quadratic and coincide on a set of Frobenius elements of density $> 1/2$, they must coincide. Hence $A' \sim \prod_i E'_i \sim \prod_i E_{i,\varphi_2} \sim A_{\varphi_2}$. $\qquad \square$

5 Proof of the main theorem

We borrow from [6, §4.1] the labels $\mathbf{A}, \ldots, \mathbf{F}$ for the absolute type of an abelian surface. See [7, §3.2.1] or [8, §3.5] for the description of the absolute types $\mathbf{A}, \ldots, \mathbf{N}$ of an abelian threefold. Note that if (1.1) holds for A and A', then they have the same absolute type by Corollary 2.6. Recall that they also have the same endomorphism field by Lemma 2.2. To complete the proof of Theorem 1.1 we will distinguish the cases $g = 2$ and $g = 3$. Before, we recall a construction that will be used in several proofs (in fact, it has already appeared implicitly via Theorem 4.5). We refer to [19, Chap. II] for further details.

Remark 5.1 Let B be an abelian variety defined over k of dimension g, and let M be a number field. Suppose that there is a $\mathbb{Q}$-algebra embedding $M \hookrightarrow \mathrm{End}^0(B)$. Choose a prime ℓ totally split in M, so that the $[M : \mathbb{Q}]$ embeddings $\lambda_i : M \hookrightarrow \overline{\mathbb{Q}}_\ell$, take values in $\mathbb{Q}_\ell$. Define

$$V_{\lambda_i}(B) := V_\ell(B) \otimes_{M \otimes \mathbb{Q}_\ell, \lambda_i} \mathbb{Q}_\ell, \qquad (5.1)$$

where $\mathbb{Q}_\ell$ is being regarded as an $M \otimes \mathbb{Q}_\ell$-module via λ_i. It has dimension $2g/[M : \mathbb{Q}]$ as a vector space over $\mathbb{Q}_\ell$. We let G_k act naturally on $V_\ell(B)$ and trivially on $\mathbb{Q}_\ell$. With this action, there is an isomorphism $V_\ell(B) \simeq \bigoplus_i V_{\lambda_i}(B)$.

5.1 Abelian surfaces

Throughout this section assume $g = 2$. Theorem 1.1 follows from Theorem 3.1 or Corollary 2.7 if the absolute type of A and A' is **A**, from Theorem 3.1 if it is **C**, from Theorem 4.9 if it is **E**, and from Theorem 4.11 if it is **F**. We will complete the proof of Theorem 1.1 in the remaining cases.

5.1.1 Absolute type D

The case that $A_{\overline{\mathbb{Q}}}$ is the product of two elliptic curves is covered by Proposition 4.15. Assume from now on that the geometric endomorphism algebra of A is a quartic CM field, which we will call M. By [24, p. 515, Proposition 3] and [25, p.64], one of the following three cases occurs:

  (i) $K = k$ and $\operatorname{End}^0(A) \simeq M$.
 (ii) K/k is quadratic and $\operatorname{End}^0(A)$ is a real quadratic field.
(iii) K/k is cyclic of degree 4 and $\operatorname{End}^0(A) \simeq \mathbb{Q}$.

Let ℓ be a prime totally split in M, and let $\lambda_1, \ldots, \lambda_4$ be the embeddings of M into $\mathbb{Q}_\ell$. The following lemma is an easy consequence of Faltings isogeny theorem.

Lemma 5.2 *We have* $\operatorname{Hom}_{G_K}(V_{\lambda_i}, V_{\lambda_j}) = 0$ *for* $i \neq j$, *and* $\operatorname{End}_{G_K}(V_{\lambda_i}) \simeq \mathbb{Q}_\ell$.

Set $n = 4/[K : k] = [\operatorname{End}^0(A) : \mathbb{Q}]$. By [15, Thm. 3, Rem. 2, p. 186] (see also the first part of the proof of [5, Thm. 2.9]), there is an isomorphism

$$V_\ell(A) \simeq \bigoplus_{i=1}^{n} \operatorname{Ind}_K^k(V_{\lambda_i}) \tag{5.2}$$

of G_k-modules, where we assume that $\lambda_1, \ldots, \lambda_n$ have been ordered so that their restrictions to $\operatorname{End}^0(A)$ are all distinct. Note that A falls in case (i) (resp. ii, iii) if and only if so does A'.

Proposition 5.3 *If* $\operatorname{End}^0(A_{\overline{\mathbb{Q}}})$ *is a quartic CM field, then Theorem 1.1 holds.*

Proof In case (i), the proposition follows from Theorem 3.1. Note that $\varrho_{A,\ell}$ satisfies the hypotheses of this theorem by Lemma 5.2. In case (ii) (resp. iii), the proposition follows from case (i) (resp. ii) and Lemma 4.12. Note that we can apply this lemma since A has Frobenius traces concentrated in K as it follows from (5.2). □

Remark 5.4 An alternative way to prove Proposition 5.3 in case i) consists in choosing a prime ℓ inert in M. Then $V_\ell(A)$ is an M_λ-module of dimension 1, and hence strongly absolutely irreducible. Therefore there exists a character φ of G_k such that $\varrho_{A',\ell} \simeq \varphi \otimes \varrho_{A,\ell}$, and then the proposition follows from Proposition 2.11.

5.1.2 Absolute type B

Suppose that A has absolute type **B**, that is, $A_{\overline{\mathbb{Q}}}$ is either:

(i) isogenous to the product of two nonisogenous non CM elliptic curves, or
(ii) simple and $M := \mathrm{End}^0(A_{\overline{\mathbb{Q}}})$ is a real quadratic field.

The endomorphism field K/k is at most quadratic. If $K = k$, then Theorem 1.1 follows from Theorem 3.1. Assume that K/k is quadratic. Let ℓ be a prime, which we assume split in M if we are in case i). Then, there are strongly absolutely irreducible ℓ-adic representations $\varrho, \varrho' : G_K \to \mathrm{GL}_2(\mathbb{Q}_\ell)$ such that $\varrho_{A,\ell} \simeq \mathrm{Ind}_K^k(\varrho)$ and $\varrho_{A',\ell} \simeq \mathrm{Ind}_K^k(\varrho')$. In case i), we have that A_K is isogenous to the product of two elliptic curves E_1, E_2 defined over K, and we may take $\varrho = \varrho_{E_i,\ell}$; in case ii), let ϱ be the representation afforded by $V_\lambda(A)$, where λ is an embedding of M into $\mathbb{Q}_\ell$. Theorem 1.1 then follows from the case $K = k$ and Lemma 4.12.

5.2 Abelian threefolds

In this section we assume that $g = 3$. If the absolute type of A is **A**, then Theorem 1.1 follows from Corollary 2.7 or Theorem 3.1; if it is **M**, it follows from Theorem 4.9; if it is **N**, it follows from Theorem 4.11.

Lemma 5.5 *If A has absolute type **C**, **D**, **G**, **I**, or **K**, then Theorem 1.1 holds.*

Proof By Lemma 4.13, there exist abelian varieties B, B' defined over k such that A is isogenous to $B \times B'$ and $\mathrm{End}(B_{\overline{\mathbb{Q}}}) \simeq \mathbb{Z}$. By Faltings isogeny theorem, there exist $\mathbb{Q}_\ell[G_k]$-modules V, V' such that $V_\ell(A) \simeq V \oplus V'$ and $\mathrm{End}_{G_F}(V) \simeq \mathbb{Q}_\ell$ for every finite extension F/k. Then the lemma follows from Theorem 3.1. □

The next two results consider abelian threefolds that contain an elliptic factor E with CM by M that is not geometrically isogenous to any other factor.

Proposition 5.6 *Let B be an abelian surface defined over k, and χ and ψ be quadratic characters. Suppose that $\mathrm{Hom}(E_{\overline{\mathbb{Q}}}, B_{\overline{\mathbb{Q}}}) = 0$ and that (1.1) holds for $A := E \times B$ and $A' := E_\chi \times B_\psi$. Then A and A' are quadratic twists.*

Proof We may reduce to the case that $\chi = 1$. Indeed, this particular case of the proposition applies to the pair A and A'_χ, and A and A'_χ are quadratic twists if and only if so are A and A'. Assume henceforth that $\chi = 1$.

We will assume that $k \neq kM$, as otherwise the proposition follows from Theorem 3.1. Also by Theorem 3.1, there is a quadratic character ε of G_{kM} such that $A_{kM,\varepsilon} \sim A'_{kM}$. In fact, the proof of the theorem shows that ε satisfies $E_{kM} \sim E_{kM,\varepsilon}$, which implies that ε must be trivial. Let φ denote the nontrivial character of $\mathrm{Gal}(kM/k)$. We will assume that $\psi \neq 1$, as otherwise there is nothing to show. We will also assume that $\varphi \neq \psi$, as otherwise the result follows from $A' \sim E \times B_\varphi \sim E_\varphi \times B_\varphi \sim A_\varphi$. By taking the restriction of scalars of $A_{kM} \sim A'_{kM}$ from kM to k, we obtain

$$B \times B_\varphi \sim B_\psi \times B_{\psi\varphi}. \tag{5.3}$$

We will distinguish three cases: a) B is simple (over k); b) $B \sim C \times D$, where C and D are elliptic curves over k which are not quadratic twists. c) $B \sim C \times C_\xi$, where C is an elliptic curve over k and ξ is a quadratic character.

Suppose that a) holds. From (5.3) we see that either $B \sim B_\psi$ or $B_\varphi \sim B_\psi$. In the first case, we obtain that $A \sim A'$, and in the latter case we have

$$A' \sim E \times B_\psi \sim E_\varphi \times B_\varphi \sim A_\varphi \,.$$

Suppose that b) holds. Then (5.3) implies that $C \sim C_\psi$ or $C \sim C_{\psi\varphi}$ and $D \sim D_\psi$ or $D \sim D_{\psi\varphi}$. We claim that there exists $i \in \{0, 1\}$ such that $C \sim C_{\psi\varphi^i}$ and $D \sim D_{\psi\varphi^i}$. Indeed, otherwise A would be the product of three elliptic curves with CM by the quadratic fields attached to the characters $\varphi, \psi, \varphi\psi \neq 1$. But this is absurd, for the quadratic fields attached to these characters cannot all be simultaneously imaginary. By the claim, we have

$$A' \sim E \times C_\psi \times D_\psi \sim E \times C_{\varphi^i} \times D_{\varphi^i} \sim A_{\varphi^i} \,.$$

Suppose finally that c) holds. In this case, (5.3) amounts to

$$(1 + \xi)(1 + \varphi)\operatorname{Tr}(\varrho_{C,\ell}) = \psi(1 + \xi)(1 + \varphi)\operatorname{Tr}(\varrho_{C,\ell}) \,.$$

Since there exists a density 1 subset Σ' of Σ_{kM} such that for every $\mathfrak{p} \in \Sigma'$ the trace of $\varrho_{C,\ell}(\operatorname{Fr}_\mathfrak{p})$ is nonzero, the above equality implies

$$1 + \xi|_{kM} = \psi|_{kM}(1 + \xi|_{kM}) \,.$$

Hence, either $\psi|_{kM} = 1$ or $\psi|_{kM} = \xi|_{kM}$. We deduce that there exist $i, j \in \{0, 1\}$ such that $\psi = \varphi^i \xi^j$, and then $A' \sim E \times C_\psi \times C_{\xi\psi} \sim E \times C_{\varphi^i} \times C_{\xi\varphi^i} \sim A_{\varphi^i}$. $\qquad\square$

Corollary 5.7 *Let B and B' be abelian surfaces defined over k, and E and E' be elliptic curves defined over k with CM. If $\operatorname{Hom}(E_{\overline{\mathbb{Q}}}, B_{\overline{\mathbb{Q}}}) = 0$ and (1.1) holds for $A := E \times B$ and $A' := E' \times B'$, then A and A' are quadratic twists.*

Proof By Theorem 3.1, there exists a quadratic character φ of G_{kM} such that

$$E'_{kM} \times B'_{kM} \sim E_{kM,\varphi} \times B_{kM,\varphi} \,.$$

Since $\operatorname{Hom}(E_{\overline{\mathbb{Q}}}, B_{\overline{\mathbb{Q}}}) = 0$, it follows that $E'_{kM} \sim E_{kM,\varphi}$ and $B'_{kM} \sim B_{kM,\varphi}$. In particular, for every prime $\mathfrak{p} \in \Sigma_k$ split in kM, except for a density 0 set, E and E' (resp. B and B') are locally quadratic twists at $\mathfrak{p}$. Similarly, for every $\mathfrak{p} \in \Sigma_k$ inert in kM, except for a density 0 set, the facts that $L_\mathfrak{p}(E, T) = 1 + \operatorname{Nm}(\mathfrak{p})T^2$ and that A and A' are locally quadratic twists at $\mathfrak{p}$ imply that E and E' (resp. B and B') are locally quadratic twists at $\mathfrak{p}$. Hence, by Corollary 3.2 and the case $g = 2$ of Theorem 1.1, there exist quadratic characters χ, ψ of G_k such that $E' \sim E_\chi$ and $B' \sim B_\psi$, and then the corollary follows from Proposition 5.6. $\qquad\square$

Corollary 5.8 *If A has absolute type F, J, or L, then Theorem 1.1 holds.*

Proof It suffices to note that by Lemma 4.13 we can apply Corollary 5.7. $\qquad\square$

5.2.1 Absolute type B

In this case $\text{End}^0(A_{\overline{\mathbb{Q}}})$ is a quadratic imaginary field. If $K = k$, then Theorem 1.1 follows from Theorem 3.1. Otherwise, K/k is quadratic and A and A' have Sato–Tate group $N(\mathrm{U}(3))$. Then, for a prime ℓ totally split in M, we have that $V_\ell(A) \simeq \text{Ind}_K^k(V_\lambda(A))$, where λ is an embedding of M into $\overline{\mathbb{Q}}_\ell$. Theorem 1.1 then follows from the case $K = k$ and Lemma 4.12.

5.2.2 Absolute type E

We will need the following lemma.

Lemma 5.9 *Suppose that* (1.1) *holds for A and A', and that:*

(i) *The endomorphism field K/k of A is a degree 3 cyclic extension.*
(ii) *A has Frobenius traces concentrated in K.*

Then A and A' are quadratic twists.

Proof By Theorem 3.3, there is a quadratic character χ of G_K such that $A'_K \sim A_{K,\chi}$ cutting out an extension L/K such that L/k is Galois. If $L = K$, the lemma is clear. Otherwise $\text{Gal}(L/k) \simeq S_3$ of C_6. In any case, there is a quadratic extension F/k such that $L = FK$. Let ψ be the nontrivial quadratic character of F/k, so that $\psi|_K = \chi$. By $ii)$, we have $\varrho_{A,\ell} \otimes \psi = \varrho_{A,\ell} \otimes \chi$, and the lemma follows. □

Let us return to the case that A has absolute type **E**. We can choose a prime ℓ such that $\varrho_{A,\ell}|_K \simeq \varrho_1 \oplus \varrho_2 \oplus \varrho_3$, where the $\varrho_i : G_K \to \text{GL}_2(\overline{\mathbb{Q}}_\ell)$ are strongly absolutely irreducible pairwise nonisomorphic representations. If $\varrho_{A,\ell}$ is reducible, then one of the ϱ_i descends to G_k and the Zariski closure of its image is connected. Theorem 1.1 then follows from Theorem 3.1. Suppose that $\varrho_{A,\ell}$ is irreducible. Then, K/k has degree 3 or 6, depending on whether the Sato–Tate group of A is E_s or $E_{s,t}$. In the first case, Theorem 1.1 follows from Lemma 5.9. In the second case, let N/k be the quadratic subextension of K/k. By the previous case, A_N and A'_N are quadratic twists, and then Theorem 1.1 follows from Lemma 4.12.

5.2.3 Absolute type H

We may assume that A is absolutely simple and that $\text{End}^0(A_{\overline{\mathbb{Q}}})$ is a sextic CM field M, as otherwise Theorem 1.1 follows from Corollary 5.7. From [8, §4.3], we see that one of the following cases occurs:

(i) $K = k$ and $\text{End}^0(A) \simeq M$.
(ii) K/k is quadratic and $\text{End}^0(A)$ is a real cubic field.
(iii) K/k is cyclic of order 3 and $\text{End}^0(A)$ is an imaginary quadratic field.
(iv) K/k is cyclic of order 6 and $\text{End}^0(A) \simeq \mathbb{Q}$.

Let ℓ be a prime totally split in M. If we set $n = 6/[K : k] = [\text{End}^0(A) : \mathbb{Q}]$, then $V_\ell(A)$ admits a decomposition analogous to (5.2), and hence A has Frobenius traces concentrated in K. In case (i), Theorem 1.1 follows from Theorem 3.1. In case (ii) (resp. iii, iv), it follows from case i) and Lemma 4.12 (resp. case i) and Lemma 5.9, case (iii) and Lemma 4.12.

6 Examples

In this final section, we provide two examples. Let A be an abelian variety defined over the number field k, and let ℓ be a prime. For a prime $\mathfrak{p}$ of Σ_k coprime to ℓ, we let $a_{\mathfrak{p}}(A)$ denote $\mathrm{Tr}(\varrho_{A,\ell}(\mathrm{Fr}_{\mathfrak{p}}))$.

6.1 First example

We will exhibit two abelian surfaces A and A' defined over $\mathbb{Q}$ which, despite not being quadratic twists, satisfy $a_p(A) = \pm a_p(A')$ for all rational odd primes p. Let C and C' denote the genus 2 curves defined over $\mathbb{Q}$ given by

$$y^2 = x^5 - x \quad \text{and} \quad y^2 = x^5 + 4x .$$

Let A and A' denote the Jacobians of C and C'. Note that C and C' have good reduction outside 2 and thus so do A and A'.

Proposition 6.1 *For every odd prime p, we have $a_p(A) = \pm a_p(A')$. Nonetheless, A and A' are not quadratic twists.*

Proof By computing $L_3(A, T)$ and $L_3(A', T)$, one sees that A_3 and A'_3 are not quadratic twists, and hence neither are A and A'. Let p be an odd prime. We will rely on the results of [9] in order to show that $a_p(A) = \pm a_p(A')$. Accordingly to [9, Table 5], define $K = \mathbb{Q}(\sqrt{2}, i)$, $L = K(2^{1/4})$, and $L' = K(\sqrt{2 + \sqrt{2}})$. Let r (resp. s, s') denote the residue degree of p in K (resp. L, L'). Since $L \cap L' = K$ and $\mathrm{Gal}(L/\mathbb{Q}) \simeq C_2 \times C_4$ and $\mathrm{Gal}(L/\mathbb{Q}) \simeq D_4$, we have three cases: i) if $r = 1$, then $s, s' = 1$ or 2; if $r = 2$, then $s, s' = 2$ or 4; if $r = 4$, then $s = s' = 4$. Then [9, Prop. 4.9], implies that $a_p(A) = a_p(A') = 0$ in cases ii) and iii), and that $a_p(A) = \pm a_p(A')$ in case i). $\qquad\square$

6.2 Second example

We will exhibit two abelian fourfolds A and A' defined over $\mathbb{Q}$ which, despite not being quadratic twists, are locally quadratic twists at all rational odd primes. This example was obtained by means of a computer exploration of the family of curves $y^2 = x^9 + ax$, with $a \in \mathbb{Q}$, carried by Edgar Costa, to whom I express my deepest gratitude. Let C and C' denote the genus 4 curves defined over $\mathbb{Q}$ and given by the affine models

$$y^2 = x^9 + x \quad \text{and} \quad y^2 = x^9 + 16x .$$

Let A and A' denote the Jacobians of C and C'. Note that C and C' have good reduction outside 2 and thus so do A and A'.

Proposition 6.2 *For every odd prime p, the reductions A_p and A'_p are quadratic twists. Nonetheless, A and A' are not.*

Proof Let $L/\mathbb{Q}$ denote the minimal extension over which all homomorphisms from $A_{\overline{\mathbb{Q}}}$ to $A'_{\overline{\mathbb{Q}}}$ are defined. By [26, Thm. 4.2], the extension $L/\mathbb{Q}$ is finite, Galois, and unramified outside 2. We first show that A and A' are not quadratic twists. Suppose the contrary, that is, that there exists a quadratic character $\chi \colon G_{\mathbb{Q}} \to \{\pm 1\}$ such that $A' \sim A_{\chi}$. Note that χ necessarily factors through an at most quadratic subextension $N/\mathbb{Q}$ of $L/\mathbb{Q}$. Hence, $N/\mathbb{Q}$ is unramified outside 2, which means that N is either $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$, or $\mathbb{Q}(\sqrt{-2})$. One easily computes

$$\operatorname{Tr} \varrho_{A,\ell}(\operatorname{Fr}_{17}) = -8\,, \qquad \operatorname{Tr} \varrho_{A',\ell}(\operatorname{Fr}_{17}) = 8\,,$$

which implies that 17 is inert in N. This is however a contradiction with the possibilities determined for N.

Let p be an odd prime. We will next show that A_p and A'_p are quadratic twists. Let F denote $\mathbb{Q}(2^{1/4})$. Note that the map

$$\phi \colon C_F \to C'_F\,, \qquad \phi(x, y) = (\sqrt{2}x, 2^{9/4}y) \tag{6.1}$$

defines an isomorphism. If $p \equiv 1, 7 \pmod 8$, then $a := 2^{1/2} \in \mathbb{F}_p$. The isomorphism shows that A_p and A'_p are quadratic twists. Suppose from now on that $p \equiv 3, 5 \pmod 8$. We claim that A_p and A'_p are in fact isogenous. By Lemma 6.3 below, there exist integers s and s' such that

$$L_p(A, T) = 1 + sT^4 + p^4 T^8\,, \quad L_p(A', T) = 1 + s'T^4 + p^4 T^8\,. \tag{6.2}$$

The relations between elementary symmetric polynomials and power sums show that (6.2) implies that $\#C(\mathbb{F}_{p^i}) = \#C'(\mathbb{F}_{p^i}) = p^i + 1$ for $i = 1, \dots, 3$. But (6.1) immediately implies that $\#C(\mathbb{F}_{p^4}) = \#C'(\mathbb{F}_{p^4})$. Thus $L_p(A, T) = L_p(A', T)$, and A_p and A'_p are isogenous. $\qquad\square$

Lemma 6.3 *Let A denote the Jacobian of a curve defined by an affine model $y^2 = x^9 + cx$ for $c \in \mathbb{Q}^{\times}$. For every prime $p \equiv 3, 5 \pmod 8$ of good reduction for A, there exists an integer s such that the L-polynomial of A at p is of the form*

$$L_p(A, T) = 1 + sT^4 + p^4 T^8\,.$$

Proof We will apply [16, Thm. 1.1] with $m_1 = 9$, $n_1 = 0$, $m = 1$, $n = 2$, $k_1 = c$, $k_2 = -1$, $\xi_1 = 7/16$, and $\xi_2 = 1/2$. In light of part (2) of loc. cit., it suffices to show that the integer $\mu(\xi)$ appearing in that formula is 4. Here ξ denotes the pair of rational numbers (ξ_1, ξ_2). By the discussion preceding [16, Thm. 1.1], $\mu(\xi)$ is the order of p in $(\mathbb{Z}/16\mathbb{Z})^{\times}$. If $p \equiv 3, 5 \pmod 8$, then this order is 4. $\qquad\square$

Data Availability The manuscript has no associated data.

Declarations

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

1. Banaszak, G., Kedlaya, K.S.: An algebraic Sato-Tate group and Sato-Tate conjecture. Indiana Univ. Math. J. **64**, 245–274 (2015)
2. Faltings, G.: Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. Invent. Math. **73**, 349–366 (1983)
3. Fité, F.: Artin representations attached to pairs of isogenous abelian varieties. J. Number. Theory. **133**(4), 1331–1345 (2013)
4. Fité, F., Guitart, X.: Fields of definition of elliptic k-curves and the realizability of all genus 2 Sato-Tate groups over a number field. Trans. Amer. Math. Soc. **370**(7), 4623–4659 (2018)
5. Fité, F., Guitart, X.: Tate module tensor decompositions and the Sato-Tate conjecture for certain abelian varieties potentially of GL_2-type. Mathematische. Zeitschrift. **300**, 2975–2995 (2022)
6. Fité, F., Kedlaya, K.S., Rotger, V., Sutherland, A.V.: Sato-Tate distributions and Galois endomorphism modules in genus 2. Compositio. Mathematica. **148**(5), 1390–1442 (2012)
7. Fité, F., Kedlaya, K.S., Sutherland, A.V.: Sato-Tate groups of abelian threefolds: a preview of the classification. Contemp. Math. **770**, 103–129 (2021)
8. Fité, F., Kedlaya, K.S., Sutherland, A.V.: *Sato–Tate groups of abelian threefolds*, arXiv:2106.13759 (2021)
9. Fité, F., Sutherland, A.V.: Sato-Tate distributions of twists of $y^2 = x^5 - x$ and $y^2 = x^6 + 1$. Algebra. Number. Theory. **8**, 543–585 (2014)
10. Hecke, E.: Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen. Math. Z. **6**(1–2), 11–51 (1920)
11. Katz, N.M.: Galois properties of torsion points on abelian varieties. Invent. Math. **62**, 481–502 (1981)
12. Khare, C.B., Larsen, M.: Abelian varieties with isogenous reductions. C. R. Math. Acad. Sci. Paris **358**(9–10), 1085–1089 (2020)
13. Kings, G.: Higher regulators, hilbert modular surfaces, and special values of L-functions. Duke Math. J. **92**(1), 61–127 (1998)
14. The LMFDB Collaboration, *The L-functions and modular forms database*, release 1.2.1, https://www.lmfdb.org, 2021 Accessed Jul 2021
15. Milne, J.: On the arithmetic of abelian varieties. Invent. Math. **17**, 177–190 (1972)
16. Nie, M.: Zeta functions of trinomial curves and maximal curves. Finite. Fields. Their Appl. **39**, 52–82 (2016)
17. Rajan, C.S.: On strong multiplicity one for ℓ-adic representations. Internat. Math. Res. Notices. (3), 161–172 (1998)
18. Ramakrishnan, D.: *Recovering modular forms from squares*, appendix to "A problem of Linnik for elliptic curves and mean-value estimates for automorphic representations" by W. Duke and E. Kowalski, Invent. Math. **139**, 1–39 (2000)

19. Ribet, K.A.: Galois action on division points on abelian varieties with many real multiplications. Am. J. Math. **98**, 751–804 (1976)
20. Sawin, W.: Ordinary primes for Abelian surfaces. C. R. Math. Acad. Sci. Paris **354**(6), 566–568 (2016)
21. Serre, J.-P.: Proprietés galoisennes des points d'ordre fini des courbes elliptiques. Invent. Math. **15**, 259–331 (1972)
22. Serre, J.-P.: Quelques applications du théorème de densité de Chebotarev. Inst. Hautes Études Sci. Publ. Math. No. **54**, 323–401 (1981)
23. Serre, J.-P.: Lectures on $N_X(p)$. CRC Press, Boca Raton, FL (2012)
24. Shimura, G.: On the zeta-function of an abelian variety with complex multiplication. Ann. Math. **94**(2), 504–533 (1971)
25. Shimura, G.: Abelian varieties with complex multiplication and modular forms. Princeton University Press, Princeton, NJ (1998)
26. Silverberg, A.: Fields of definition for homomorphisms of abelian varieties. J. Pure Appl. Algebra. **77**, 253–262 (1992)
27. Wong, S.: Twists of Galois representations and projective automorphisms. J. Number. Theory. **74**, 1–18 (1999)