Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Antonella PERUCCA

The prime divisors of the number of points on abelian varieties

Tome 27, n[o] 3 (2015), p. 805-814.

<http://jtnb.cedram.org/item?id=JTNB_2015__27_3_805_0>

Journal de Théorie des Nombres
de Bordeaux **27** (2015), 805–814

The prime divisors of the number of points on abelian varieties

par Antonella PERUCCA

Résumé. Soient A, A' des courbes elliptiques ou variétés abéliennes pleinement de type GSp définies sur un corps de nombres. Cette classe contient les variétés abéliennes principalement polarisées avec anneau d'endomorphismes $\mathbb{Z}$ et de dimension 2 ou impaire. On compare le nombre de points des réductions des deux variétés. On montre que A et A' sont K-isogènes si la condition suivante est satisfaite pour un ensemble d'idéaux premiers $\mathfrak{p}$ de K de densité 1: les nombres premiers qui divisent $\#A(k_\mathfrak{p})$ divisent aussi $\#A'(k_\mathfrak{p})$. On généralise ce théorème dans une certaine mesure aux produits de telles variétés. On améliore des résultats de Hall et Perucca (2011) et de Ratazzi (2012).

Abstract. Let A, A' be elliptic curves or abelian varieties fully of type GSp defined over a number field K. This includes principally polarized abelian varieties with geometric endomorphism ring $\mathbb{Z}$ and dimension 2 or odd. We compare the number of points on the reductions of the two varieties. We prove that A and A' are K-isogenous if the following condition holds for a density-one set of primes $\mathfrak{p}$ of K: the prime numbers dividing $\#A(k_\mathfrak{p})$ also divide $\#A'(k_\mathfrak{p})$. We generalize this statement to some extent for products of such varieties. This refines results of Hall and Perucca (2011) and of Ratazzi (2012).

1. Introduction

Let A, A' be abelian varieties defined over a number field K. Let S be a density-one set of primes of K of good reduction for both A and A'. A well-known result of Faltings of 1983 [1, Cor. 2] implies that A, A' are K-isogenous if and only if for every $\mathfrak{p} \in S$ the following holds: the reductions of A and A' modulo $\mathfrak{p}$ are isogenous over the residue field $k_\mathfrak{p}$. For elliptic curves, this is equivalent to requiring that the number of points $\#A(k_\mathfrak{p})$

Manuscrit reçu le 8 décembre 2013, révisé le 30 juillet 2015, accepté le 2 octobre 2015.
Mathematics Subject Classification. 11G05, 11G10.
Mots-clefs. abelian variety of type GSp, product of elliptic curves, number of points, reduction, number field.
The author thanks Davide Lombardo for Theorem 3.3 and the anonymous referee for suggesting this possible improvement to the paper.

and $\#A'(k_\mathfrak{p})$ are equal. The aim of this paper is investigating analogous relations on the number of points that ensure that A, A' are isogenous.

In this paper we call an abelian variety *admissible* if it is either an elliptic curve or an abelian variety fully of type GSp. These are defined by considering the Galois action on the torsion points: a principally polarized abelian variety A of dimension g is said to be fully of type GSp if for all but finitely many prime numbers ℓ the image of the mod-ℓ representation of A is $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$. This condition holds in particular if the geometric endomorphism ring is $\mathbb{Z}$ and the dimension is 2 or odd.

We refine results by Hall and Perucca [3] and by Ratazzi [8]. We weaken the assumptions of respectively [3, Thm.] and [8, Thm. 1.6], obtaining the following:

Theorem 1.1. *Let A, A' be admissible abelian varieties defined over a number field K. Let S be a density-one set of primes of K over which A, A' have good reduction. If the condition*

$$\ell \mid \#A(k_\mathfrak{p}) \quad \Rightarrow \quad \ell \mid \#A'(k_\mathfrak{p})$$

holds for infinitely many prime numbers ℓ and for every $\mathfrak{p} \in S$ then A, A' are K-isogenous.

The proof is based on the following theorem, which is an application of results for elliptic curves by Serre and by Frey and Jarden ([9, Lem. 9 and Thm. 7], [2, Thm. A]) and the corresponding results for abelian varieties fully of type GSp by Hindry and Ratazzi ([5, Thm. 1.6], [8, Thm. 1.5]). These kind of statements also relate to a problem considered by Kowalski [6, Problem 1.2].

Theorem 1.2 (Horizontal isogeny theorem)**.** *Let A, A' be admissible abelian varieties defined over a number field K. If the condition $K(A[\ell]) \subseteq K(A'[\ell])$ holds for infinitely many prime numbers ℓ then A, A' are K-isogenous.*

Note, the condition $K(A[\ell]) = K(A'[\ell])$ for every prime number ℓ does not in general imply that A and A' are K-isomorphic because of an example by Zarhin, see [11, §12]: there are elliptic curves that are not K-isomorphic but such that for every prime number ℓ there exists a K-isogeny between them of degree coprime to ℓ.

We also consider products:

Theorem 1.3. *Let A and A' be abelian varieties defined over a number field K. Suppose that the geometrically simple $\bar{K}$-quotients of A and of A' are admissible. Let S be a density-one set of primes of K over which A, A' have good reduction.*

(1) *If the condition*

$$\#A(k_\mathfrak{p}) = \#A'(k_\mathfrak{p})$$

holds for every $\mathfrak{p} \in S$ then A and A' are $\bar{K}$-isogenous.

(2) *If the condition*

$$\ell \mid \#A(k_{\mathfrak{p}}) \quad \Rightarrow \quad \ell \mid \#A'(k_{\mathfrak{p}})$$

holds for infinitely many prime numbers ℓ and for every $\mathfrak{p} \in S$ then every geometrically simple $\bar{K}$-quotient of A is also a $\bar{K}$-quotient of A'.

In other words, knowing which prime numbers divide $\#A(k_{\mathfrak{p}})$ for a density-one set of primes $\mathfrak{p}$ is sufficient to characterize the simple factors of the Poincaré Reducibility Theorem decomposition of $A \otimes_K \bar{K}$ up to isogeny.

Note, in our results we cannot consider only finitely many prime numbers ℓ: for example if the Mordell-Weil groups $A(K)$ and $A'(K)$ respectively contain all points of order ℓ for every prime number under consideration, then our assumptions provide no further information.

We conclude with an open problem, namely investigating to which extent the following property fails: for an abelian variety A defined over a number field K, and for $\mathfrak{p}$ varying in a density-one set of primes of K, the function $\mathfrak{p} \mapsto \#A(k_{\mathfrak{p}})$ characterizes the isogeny class of A.

2. Preliminaries

Let K be a number field, and fix a Galois closure $\bar{K}$ of K. Let A be an abelian variety of dimension g defined over K. If ℓ is a prime number, we denote by $A[\ell]$ the group of ℓ-torsion points and by $K_\ell := K(A[\ell])$ the smallest extension of K over which these points are defined. We call G_ℓ the Galois group of K_ℓ/K, which we consider embedded in $\mathrm{GL}_{2g}(\mathbb{F}_\ell)$ via the mod-ℓ representation, after having fixed a basis for $A[\ell]$.

We fix a polarization of A and suppose ℓ does not divide its degree so that one can define the Weil pairing on $A[\ell]$. The pairing takes its values in μ_ℓ, the group of ℓ-th roots of unity, so its existence implies $\mu_\ell \subseteq K_\ell$. We write $H_\ell \subseteq G_\ell$ for the Galois group of $K_\ell/K(\mu_\ell)$. There is a natural embedding $G_\ell/H_\ell \to \mathrm{Aut}(\mu_\ell) = \mathbb{F}_\ell^\times$, and we write $\chi_\ell : G_\ell \to \mathbb{F}_\ell^\times$ for the composition of this embedding with the quotient map $G_\ell \to G_\ell/H_\ell$. The induced homomorphism $\chi_\ell : G_K \to \mathbb{F}_\ell^\times$ is the cyclotomic character.

The group G_ℓ is contained in the general symplectic group $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ so we can consider the multiplier map

$$\nu : \mathrm{GSp}_{2g}(\mathbb{F}_\ell) \to \mathbb{F}_\ell^\times \,.$$

The g-th power ν^g equals the determinant and restricting to G_ℓ the multiplier map ν gives the cyclotomic character χ_ℓ. Consequently H_ℓ is contained in the symplectic group $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$.

Let S be a density-one set of primes of K of good reduction for A. If v_ℓ denotes the ℓ-adic valuation, we define Φ_ℓ to be the following map:

$$\Phi_\ell : S \to \{0,1\} \qquad \mathfrak{p} \mapsto \min\{1, v_\ell(\#A(k_{\mathfrak{p}}))\}\,.$$

Note, this map distinguishes for each $\mathfrak{p} \in S$ whether ℓ divides or not the positive integer $\#A(k_\mathfrak{p})$. We also write $\mathcal{E} := \mathrm{End}_{\bar{K}}(A) \otimes \mathbb{Q}$.

We repeatedly make use of the following: If A is an elliptic curve without CM then for all but finitely many ℓ we have $G_\ell = \mathrm{GL}_2(\mathbb{F}_\ell)$, see [9, Thm. 2]. If A is an elliptic curve with CM defined over K then for all but finitely many ℓ we have that G_ℓ is a Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$, see [9, §4.5, Cor.]. Recall that the cardinality of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ is either $(\ell-1)^2$ or ℓ^2-1 according to whether it is split or non split. Moreover, all elements of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ are semi simple because they are diagonalizable over $\bar{\mathbb{F}}_\ell$.

As a reference for abelian varieties (fully) of type GSp we suggest [10, 5, 8]. A principally polarized abelian variety A of dimension g is said to be fully of type GSp if for all but finitely many prime numbers ℓ the image of the mod-ℓ representation is the group $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$. A necessary condition for A to be fully of type GSp is $\mathrm{End}_{\bar{K}} A = \mathbb{Z}$, and this condition is also sufficient in dimension 2 or odd by [10, Thm. 3]. In particular, abelian varieties fully of type GSp are geometrically simple. Abelian varieties fully of type GSp are also of type GSp (i.e. the Mumford-Tate group is GSp_{2g}) by a result of Deligne and others, see [4, Thm. 2.7]. In particular the Hodge group is Sp_{2g}, see [5, Def. 5.1].

We make use of the following two lemmas about the mod-ℓ representation of abelian varieties:

Lemma 2.1. *Let A be an abelian variety defined over a number field K. Suppose $\mathfrak{p} \in S$ is not over ℓ and does not ramify in K_ℓ and $\mathfrak{q}$ is a prime of K_ℓ over $\mathfrak{p}$. If $\phi_\mathfrak{q} \in G_\ell$ is the Frobenius $\mathfrak{q} \mid \mathfrak{p}$, then $\Phi_\ell(\mathfrak{p}) = 1$ if and only if* $\det(\phi_\mathfrak{q} - 1) = 0$.

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

We also consider an abelian variety A' over K and analogously define K'_ℓ, G'_ℓ, H'_ℓ, Φ'_ℓ, $\mathcal{E}'$. We then suppose that the primes in S are also of good reduction for A'. We write $\Gamma_\ell \subseteq G_\ell \times G'_\ell$ for the Galois group of the compositum $K_\ell K'_\ell / K$.

Lemma 2.2. *Let A, A' be abelian varieties defined over a number field K. If $\Phi_\ell \leq \Phi'_\ell$, then* $\det(\gamma - 1) = 0$ *implies* $\det(\gamma' - 1) = 0$ *for every* $(\gamma, \gamma') \in \Gamma_\ell$.

Proof. By the Cebotarev Density Theorem there is some prime $\mathfrak{p} \in S$ not over ℓ, unramified in $K_\ell K'_\ell$ and whose Frobenius conjugacy class in Γ_ℓ contains (γ, γ'). Lemma 2.1 implies the values $\Phi_\ell(\mathfrak{p})$, $\Phi'_\ell(\mathfrak{p})$ respectively identify whether or not $\det(\gamma - 1), \det(\gamma' - 1)$ are non-zero, and thus the hypothesis $\Phi_\ell(\mathfrak{p}) \leq \Phi'_\ell(\mathfrak{p})$ implies the statement. □

We will apply the following lemma to assume that for elliptic curves the CM is defined over the base field:

Lemma 2.3. *If two elliptic curves A, A' defined over a number field K are $K\mathcal{E}\mathcal{E}'$-isogenous, then they are K-isogenous.*

Proof. This assertion is proven for example in [3, Lem. 4]. □

3. Independence properties of torsion fields

In this section, we consider finitely many abelian varieties and investigate the fields obtaining by adding the respective torsion points of prime order.

Proposition 3.1. *Let A be an abelian variety defined over a number field K. Suppose that A is fully of type* GSp *or that A is an elliptic curve with CM defined over K. If L is a finite extension of K then for all but finitely many prime numbers ℓ we have $L \cap K_\ell = K$.*

Proof. For elliptic curves, we refer to [3, Prop. 1]. The proof for abelian varieties fully of type GSp is analogous, see [8, Lem. 5.7]. □

The following theorem is an easy application of results of Hindry, Ratazzi and Lombardo:

Theorem 3.2. *Let $A_1, \ldots, A_N$ be admissible abelian varieties defined over a number field K, in pairs not $\bar{K}$-isogenous. Then there is some integer $c > 0$ such that the following holds: for every prime number ℓ the extensions $K(A_i[\ell])$ for $i = 1, \ldots, N$ are linearly disjoint over some Galois extension of $K(\mu_\ell)$ of degree dividing c.*

Proof. Up to increasing c, it suffices to find an extension of $K(\mu_\ell)$ of degree at most c, rather than dividing c. Since the Galois closure of an extension of degree d has degree at most $d!$, it is also not a problem to require that the extension is Galois, again up to increasing c. For N elliptic curves, we may apply [4, Prop. 6.2] $N-1$ times, where the assumptions are satisfied by [4, Lem. 2.4 and Thm. 2.10]. Note, the finite index in [4, Prop. 6.2] is independent of ℓ because the same is true for the cokernel in [4, Thm. 2.10]. If the abelian varieties are all fully of type GSp then the assertion is proven in [5, Thm. 1.4 (2) and (3)].

Recall that elliptic curves without CM are fully of type GSp. Then the mixed case consists of one product of abelian varieties fully of type GSp times one product of elliptic curves with CM. Up to multiplying c by a finite constant, we may suppose that the CM of each elliptic curve is defined over K. We apply Theorem 3.3 to conclude. □

The following statement relates to results in [5] and [7]:

Theorem 3.3 (Lombardo 2015)**.** *Let $A = \prod_{i=1}^n A_i$ and $B = \prod_{j=1}^m B_j$ be abelian varieties defined over K. Suppose that $A_1, \dots, A_n$ are fully of type* GSp*, in pairs not $\bar{K}$-isogenous. Suppose that $B_1, \dots, B_m$ are elliptic curves with CM defined over K, in pairs not $\bar{K}$-isogenous. Then for every prime number $\ell \gg 0$ the torsion fields $K(A[\ell])$ and $K(B[\ell])$ are linearly disjoint over $K(\mu_\ell)$.*

Proof. Since we are assuming that the CM of the elliptic curves is defined over K, the extension $K(B[\ell])/K(\mu_\ell)$ is abelian. By Lemma 3.4 we know that for $\ell \gg 0$ the group $K(A[\ell])/K(\mu_\ell)$ does not have any non-trivial abelian quotients. By a straight-forward application of the Goursat's Lemma we deduce that $K(A[\ell])$ and $K(B[\ell])$ are linearly disjoint over $K(\mu_\ell)$. □

If g is a positive integer, we denote by $\nu : \mathrm{GSp}_{2g}(\mathbb{F}_\ell) \to \mathbb{F}_\ell^\times$ the multiplier map. The kernel of ν is $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$.

Lemma 3.4. *Let $A = \prod_{i=1}^n A_i$, where $A_1, \dots, A_n$ are abelian varieties defined over K, fully of type* GSp *and in pairs not $\bar{K}$-isogenous. For every $\ell \gg 0$ the group* $\mathrm{Gal}(K(A[\ell])/K)$ *equals*

$$\{(\sigma_1, \dots, \sigma_n) \in \prod_{i=1}^n \mathrm{GSp}_{2\dim(A_i)}(\mathbb{F}_\ell) \mid \nu(\sigma_i) = \nu(\sigma_{i'}) \; \forall i, i' = 1, \dots, n\}$$

so in particular we have $\mathrm{Gal}(K(A[\ell])/K(\mu_\ell)) = \prod_{i=1}^n \mathrm{Sp}_{2\dim(A_i)}(\mathbb{F}_\ell)$ *and this group does not have any non-trivial abelian quotients.*

Proof. We write

$$G_\ell := \mathrm{Gal}(K(A[\ell])/K) \quad \text{and} \quad H_\ell := \mathrm{Gal}(K(A[\ell])/K(\mu_\ell))\,.$$

By assumption we can identify $\mathrm{Gal}(K(A_i[\ell])/K)$ with $\mathrm{GSp}_{2\dim(A_i)}(\mathbb{F}_\ell)$ and $\mathrm{Gal}(K(A_i[\ell])/K(\mu_\ell))$ with $\mathrm{Sp}_{2\dim(A_i)}(\mathbb{F}_\ell)$ for every $\ell \gg 0$.

Let $\sigma \in G_\ell$ and for $i = 1, \dots, n$ denote by σ_i the restriction of σ to $K(A_i[\ell])$. Since the restriction of σ_i to $K(\mu_\ell)$ is independent of i and is determined by the multiplier $\nu(\sigma_i)$, we deduce that the condition $\nu(\sigma_i) = \nu(\sigma_{i'})$ for every $i, i' = 1, \dots, n$ must hold. We have thus shown that G_ℓ is contained in the set as in the statement.

For every $\ell \gg 0$ the cyclotomic character $\chi_\ell : G_K \to \mathbb{F}_\ell^\times$ is surjective: since automorphisms of $K(\mu_\ell)$ can be extended to $K(A[\ell])$ we deduce that $\nu(\sigma_i)$ takes all values in $\mathbb{F}_\ell^\times$ by varying σ. Thus we are left to show that

$$H_\ell = \prod_{i=1}^n \mathrm{Sp}_{2\dim(A_i)}(\mathbb{F}_\ell)$$

holds for every $\ell \gg 0$. By assumption the Hodge group of A_i equals $\mathrm{Sp}_{2\cdot\dim A_i}$ and the strong Mumford Tate conjecture [5, Conj. 1.2] holds for A_i. Then by [5, Thm. 1.4] the Hodge group of A is $\prod_i \mathrm{Sp}_{2\dim(A_i)}$ and the strong Mumford Tate conjecture holds for A. Consequently the index of H_ℓ inside $\prod_i \mathrm{Sp}_{2\dim(A_i)}(\mathbb{F}_\ell)$ is bounded by a constant that is independent of ℓ. For $\ell \gg 0$ the index must be 1 because the index m of a proper subgroup of $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ satisfies $m! \geq \frac{1}{2} \cdot \# \mathrm{Sp}_{2g}(\mathbb{F}_\ell) \geq \ell$, see for example [5, Lem. 2.5 and 2.13].

For the last assertion it suffices to consider the projections of some abelian quotient of H_ℓ: these are trivial because for $\ell \gg 0$ the group $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ has no non-trivial abelian quotients. $\square$

We will use the following application of the above theorem:

Lemma 3.5. *Let $A_1, \ldots, A_n, A'_1, \ldots, A'_m$ be admissible abelian varieties defined over a number field K, in pairs not $\bar{K}$-isogenous. Then for every prime number $\ell \gg 0$ we may find $\sigma \in \mathrm{Gal}(\bar{K}/K)$ such that σ acts as the identity on $A_i[\ell]$ for every $i = 1, \ldots, n$ and does not fix any point in $A'_i[\ell] \setminus \{0\}$ for every $i = 1, \ldots, m$.*

Proof. We may suppose for elliptic curves with CM that this is defined over K because if the requested property holds over a finite Galois extension of K then it also holds over K. Let c be as in Theorem 3.2 for the varieties $A_1, \ldots, A_n, A'_1, \ldots, A'_m$. Without loss of generality it suffices to show that the following holds for every prime number $\ell \gg 0$: any normal subgroup of index dividing c of the Galois group of $K(A_1[\ell])/K(\mu_\ell)$ contains an automorphism that does not fix any point in $A_1[\ell] \setminus \{0\}$. If A_1 is an elliptic curve that has CM over K and $\ell \gg 0$ then all elements of $K(A_1[\ell])/K(\mu_\ell)$ correspond to semi simple matrices of determinant 1 thus every such matrix that is not the identity does not fix any point in $A_1[\ell] \setminus \{0\}$. Now suppose that A_1 is fully of type GSp, and let $g = \dim A_1$. Consider the diagonal matrices of the form

$$\begin{pmatrix} \lambda \mathrm{Id}_g & \\ & \lambda^{-1} \mathrm{Id}_g \end{pmatrix}$$

where λ is in the multiplicative group $\mathbb{F}_\ell^\times$ and λ^{-1} is the inverse of λ. These matrices belong to $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ and have multiplier 1 hence they are in the Galois group of $K(A_1[\ell])/K(\mu_\ell)$, see also [8, Lem. 2.2]. By taking ℓ sufficiently large we have $\ell - 1 > 2c$ so any normal subgroup of index dividing c of this Galois group contains a matrix of the above type with $\lambda \neq 1$ hence not fixing any point in $A_1[\ell] \setminus \{0\}$. $\square$

4. Proof of the theorems

Proof of Theorem 1.2. We first exclude the possibility that one of the two abelian varieties is an elliptic curve with CM and the other is fully of type GSp. Since these two abelian varieties are not $\bar{K}$-isogenous then the assumption on the torsion fields does not hold by Theorem 3.2. We may now assume that A, A' are both elliptic curves or are both fully of type GSp.

For two elliptic curves, we first reduce to the case where the CM is defined over K. Indeed, if $L := K\mathcal{E}\mathcal{E}'$ then we have $LK_\ell \subseteq LK'_\ell$ for every $\ell \in \Lambda$ so the assumptions of the theorem also hold over L. We may then apply the theorem over L and use Lemma 2.3 to show that since A and A' are L-isogenous then they are also K-isogenous.

We now prove that A and A' are $\bar{K}$-isogenous. For elliptic curves we have: by [2, Thm. 3.5 and Prop. 2.8] (applied with $E_1 = A'$ and $E_2 = A$ and $c = 1$) then either A, A' both have CM or they both do not have CM and moreover the two elliptic curves are $\bar{K}$-isogenous. If A and A' are fully of type GSp then the assumptions of [8, Thm. 1.5] are satisfied (setting $c = 1$) hence we deduce that A and A' are $\bar{K}$-isogenous.

We conclude the proof by showing that any $\bar{K}$-isogeny is defined over K. Let $f : A \to A'$ be a $\bar{K}$-isogeny of degree d defined over some finite Galois extension F of K. Let σ be in $\mathrm{Gal}(F/K)$. We want to prove $f - {}^\sigma f = 0$ and we accomplish this by showing that the kernel of $f - {}^\sigma f$ contains $A[\ell]$ for infinitely many prime numbers ℓ. Indeed, if $\ell \gg 0$ and if $K_\ell \subseteq K'_\ell$ then we have

$$F \cap K_\ell K'_\ell = F \cap K'_\ell = K$$

by applying to A' Proposition 3.1. In particular, we may extend σ to $FK_\ell K'_\ell$ and suppose that σ acts as the identity on $K_\ell K'_\ell$. Then for every $R \in A[\ell]$ we have ${}^\sigma R = R$ and ${}^\sigma(f(R)) = f(R) \in A'[\ell]$. So we have

$${}^\sigma f(R) = {}^\sigma f({}^\sigma R) = {}^\sigma(f(R)) = f(R)$$

hence $(f - {}^\sigma f)(R) = f(R) - {}^\sigma f(R) = 0$ for every $R \in A[\ell]$. □

Proof of Theorem 1.1. For two elliptic curves, we first reduce to the case where the CM is defined over K. Consider the field $L := K\mathcal{E}\mathcal{E}'$. For a density-one set of primes $\mathfrak{q}$ of L we have: $\mathfrak{q}$ is of good reduction for A and A'; the prime $\mathfrak{p} := \mathfrak{q} \cap K$ is in S; $\mathfrak{q}$ has degree one hence $k_\mathfrak{q} = k_\mathfrak{p}$. We deduce that the assumptions of the theorem hold for L if they hold for K. Then it suffices to apply Lemma 2.3 to conclude.

By Theorem 1.2, it suffices to show that for all prime numbers $\ell \gg 0$ as in the statement we have $K_\ell \subseteq K'_\ell$. The proof goes as in [3, Lem. 5] and [8, §5.1]: we apply Lemma 2.2 and under the assumption $\Phi_\ell \leq \Phi'_\ell$ we get $K_\ell \subseteq K'_\ell$. □

Proof of Theorem 1.3. Both conditions also hold over a finite extension of K because every number field has a density-one set of primes of degree one (the corresponding residue fields are unchanged). Since we are only interested in a $\bar{K}$-isogeny we may then replace K by a finite Galois extension and assume that all homomorphisms are defined over K. In particular, the simple factors of the Poincaré Reducibility Theorem decomposition of A and A' are geometrically simple and every geometrically simple $\bar{K}$-quotient of A (respectively, of A') is $\bar{K}$-isogenous to a factor of A (respectively, of A'). The assumptions are also invariant under a K-isogeny so we may suppose that the factors of A and A' are in pairs either equal or not $\bar{K}$-isogenous.

Proof of (1): We first reduce to the case where A and A' have no common factor. Let B be a common factor of A and A'. If $A/B = A'/B = 0$ then $A = A' = B$ and the statement is proven. If without loss of generality $A/B = 0$ and $A'/B \neq 0$ then we find a contradiction. Indeed, there is a positive density of primes $\mathfrak{p}$ splitting completely in the field $K(A'/B[2])$ and in particular such that $\#A'/B(k_\mathfrak{p})$ is even. Since S is a set of density-one, there are primes as such in S and they satisfy

$$\#(A/B)(k_\mathfrak{p}) = 1 \quad \text{and} \quad \#(A'/B)(k_\mathfrak{p}) \neq 1 \quad \text{hence} \quad \#A(k_\mathfrak{p}) \neq \#A'(k_\mathfrak{p})$$

against the assumptions. Now suppose that A/B and A'/B are both non-zero. Then these varieties again satisfy the assumptions in the statement. Moreover, having a $\bar{K}$-isogeny between A/B and A'/B implies that A and A' are $\bar{K}$-isogenous. We may then iterate the above process and reduce to the case where the given abelian varieties have no common factor.

Let $A_1, \ldots, A_n$ be the different factors of A and let $A'_1, \ldots, A'_m$ be the different factors of A'. By Lemma 3.5 we can find a prime number ℓ and σ in $\mathrm{Gal}(\bar{K}/K)$ such that σ acts as the identity on $A_i[\ell]$ for every $i = 1, \ldots, n$ and does not fix any point in $A'_j[\ell] \setminus \{0\}$ for every $j = 1, \ldots, m$. By applying the Cebotarev Density Theorem with respect to the compositum of the extensions $K(A_i[\ell])$ and $K(A'_j[\ell])$ for every i, j we find a positive density of primes $\mathfrak{p}$ of K such that $\ell \mid \#A(k_\mathfrak{p})$ and $\ell \nmid \#A'(k_\mathfrak{p})$, contradicting the assumptions.

Proof of (2): We may suppose that A (respectively A') does not have repeated factors because neither the assumptions nor the conclusions would be affected. We have already reduced to the case where every geometrically simple $\bar{K}$-quotient of A (respectively, of A') is $\bar{K}$-isogenous to a factor of A (respectively, of A'), and where the factors of A and A' are in pairs either equal or not $\bar{K}$-isogenous. Then it suffices to prove that every factor of A is also a factor of A'. Let $A'_1, \ldots, A'_m$ with $m \geq 1$ be the different factors of A' and suppose that A_1 is a factor of A which is not one of $A'_1, \ldots, A'_m$. Analogously to the proof of the first assertion, we may apply Lemma 3.5 to find a prime number ℓ satisfying the condition in the statement and a positive density of primes $\mathfrak{p}$ of K such that $\ell \mid \#A(k_\mathfrak{p})$ and $\ell \nmid \#A'(k_\mathfrak{p})$, contradiction. $\square$

References

[1] G. Faltings, "Finiteness theorems for abelian varieties over number fields", in *Arithmetic geometry (Storrs, Conn., 1984)*, Springer, New York, 1986, p. 9-27.

[2] G. Frey & M. Jarden, "Horizontal isogeny theorems", *Forum Math.* **14** (2002), no. 6, p. 931-952.
[3] C. Hall & A. Perucca, "On the prime divisors of the number of points on an elliptic curve", *C. R. Math. Acad. Sci. Paris* **351** (2013), no. 1-2, p. 1-3.
[4] M. Hindry & N. Ratazzi, "Torsion dans un produit de courbes elliptiques", *J. Ramanujan Math. Soc.* **25** (2010), no. 1, p. 81-111.
[5] ———, "Points de torsion sur les variétés abéliennes de type GSp", *J. Inst. Math. Jussieu* **11** (2012), no. 1, p. 27-65.
[6] E. Kowalski, "Some local-global applications of Kummer theory", *Manuscripta Math.* **111** (2003), no. 1, p. 105-139.
[7] D. Lombardo, "On the ℓ-adic Galois representations attached to nonsimple abelian varieties", http://arxiv.org/abs/1402.1478.
[8] N. Ratazzi, "Classe d'isogénie de variétés abéliennes pleinement de type GSp", *J. Number Theory* **147** (2015), p. 156-171.
[9] J.-P. Serre, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques", *Invent. Math.* **15** (1972), no. 4, p. 259-331.
[10] ———, *Œuvres. Collected papers. IV*, Springer-Verlag, Berlin, 2000, 1985–1998, viii+657 pages.
[11] Y. G. Zarhin, "Homomorphisms of abelian varieties over finite fields", in *Higher-dimensional geometry over finite fields*, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., vol. 16, IOS, Amsterdam, 2008, p. 315-343.

Antonella Perucca
Fakultät Mathematik Universität Regensburg
Universitätsstrasse 31
93053 Regensburg
GERMANY
E-mail: antonella.perucca@mathematik.uni-regensburg.de
URL: http://www.uni-regensburg.de/Fakultaeten/nat_Fak_I/perucca/index.html