ACADEMIC PRESS

Available at WWW.MATHEMATICSWEB.ORG POWERED BY SCIENCE @ DIRECT•

Journal of Number Theory 101 (2003) 398–403

JOURNAL OF Number Theory

http://www.elsevier.com/locate/jnt

The support problem for abelian varieties

Michael Larsen[1]

Department of Mathematics, Indiana University, Bloomington, IN 47405, USA

Received 19 December 2002; revised 6 January 2003

Communicated by D. Goss

Abstract

Let A be an abelian variety over a number field K. If P and Q are K-rational points of A such that the order of the (mod $\mathfrak{p}$) reduction of Q divides the order of the (mod $\mathfrak{p}$) reduction of P for almost all prime ideals $\mathfrak{p}$, then there exists a K-endomorphism ϕ of A and a positive integer k such that $\phi(P) = kQ$.

MSC: 11G10; 11R34

Keywords: Support problem; Abelian variety; Galois representation

This note solves the support problem for abelian varieties over number fields, thus answering a question of Corrales-Rodrigáñez and Schoof [4]. Recently, Banaszak et al. [2] and Khare and Prasad [6] have solved the problem for certain classes of abelian varieties for which the images of the ℓ-adic Galois representations can be particularly well understood. A number of other authors have also made progress recently on closely related problems, including Kowalski [7], Wong [11], and Ailon and Rudnick [1].

The main result is as follows:

Theorem 1. *Let K be a number field, $\mathcal{O}_K$ its ring of integers, and $\mathcal{O}$ the coordinate ring of an open subscheme of* Spec $\mathcal{O}_K$. *Let $\mathcal{A}$ be an abelian scheme over $\mathcal{O}$ and $P, Q \in \mathcal{A}(\mathcal{O})$ arbitrary sections. Suppose that for all $n \in \mathbb{Z}$ and all prime ideals $\mathfrak{p}$ of $\mathcal{O}$, we have*

E-mail address: larsen@math.indiana.edu.

[1] Partially supported by NSF Grant DMS-0100537.

0022-314X/03/$ - see front matter
doi:10.1016/S0022-314X(03)00040-4

the implication

$$nP \equiv 0 \pmod{\mathfrak{p}} \Rightarrow nQ \equiv 0 \pmod{\mathfrak{p}}. \tag{1}$$

Then there exist a positive integer k and an endomorphism $\phi \in \mathrm{End}_{\mathcal{O}}(\mathscr{A})$ *such that*

$$\phi(P) = kQ. \tag{2}$$

Note that as $\mathscr{A}$ is a Néron model of its generic fiber A [3, I 1.2/8], we have that $\mathrm{End}_{\mathcal{O}}\, \mathscr{A} = \mathrm{End}_K\, A$. We employ scheme notation only to make sense of the notion of the reduction of a point of $A \pmod{\mathfrak{p}}$.

It is clear that if $Q = \phi(P)$, the order of any reduction of Q divides that of the corresponding reduction of P. One might ask whether the converse is true or, in other words, whether one can strengthen (2) to ask that $k = 1$. The following proposition shows that in general the answer is negative:

Proposition 2. *There exist* $\mathcal{O}$, $\mathscr{A}$, P, *and* Q *as above such that* (1) *holds but* $Q \notin (\mathrm{End}_{\mathcal{O}}\, \mathscr{A})P$.

Proof. Let $\mathcal{O}$ be a ring containing $1/2$. Let $\mathscr{E}/\mathcal{O}$ be an elliptic curve with $\mathrm{End}_{\mathcal{O}}\, \mathscr{E} = \mathbb{Z}$ whose 2-torsion is all $\mathcal{O}$-rational. Let T_1 and T_2 denote distinct 2-torsion points of $\mathscr{E}(\mathcal{O})$, and let R denote a point of infinite order in $\mathscr{E}(\mathcal{O})$. Let $\mathscr{A} = \mathscr{E}^2$, $P = (R, R + T_1)$, and $Q = (R, R + T_2)$. Then the reductions of R and $R + T_1$ cannot both have odd order (since T_1 has order exactly 2 in any reduction $\pmod{\mathfrak{p}}$), so P always has even order $\pmod{\mathfrak{p}}$. Thus $nP \equiv 0 \pmod{\mathfrak{p}}$ implies $2 \mid n$ and therefore

$$nQ = (nR, nR) = nP \equiv 0 \pmod{\mathfrak{p}}.$$

On the other hand, $\mathrm{End}_{\mathcal{O}}\, \mathscr{A} = M_2(\mathbb{Z})$, so no endomorphism of $\mathscr{A}$ sends P to Q. □

Let $E = \mathrm{End}_{\mathcal{O}}\, \mathscr{A}$. We begin by showing that (2) is implied by its $\pmod{m}$ analogue for sufficiently large m.

Lemma 3. *Given* $\mathcal{O}$, $\mathscr{A}$, *and* E *as above and* $\mathcal{O}$*-points* P *and* Q *of* $\mathscr{A}$, *either* P *and* Q *satisfy* (2) *or there exists* n *such that for all* $\phi \in E$ *and all* $m \geqslant n$,

$$\phi(P) - Q \notin m\mathscr{A}(\mathcal{O}).$$

Proof. The lemma follows from the Mordell–Weil theorem and the trivial fact that the image of Q in the finitely generated abelian group $\mathscr{A}(\mathcal{O})/EP$ is of finite order if it is m-divisible for infinitely many values of m. □

Next, we prove two simple algebraic lemmas.

Lemma 4. *Let G be a group with normal subgroups G_1 and G_2 such that G/G_i is finite and abelian for $i = 1, 2$. Let α be an automorphism of G such that $\alpha(G_i) \subset G_i$ for $i = 1, 2$. Suppose α acts trivially on G/G_1 and as a scalar m on G/G_2, where $m - 1$ is prime to G/G_2. Then every coset of G_1 meets every coset of G_2.*

Proof. Applying Goursat's lemma [8, I, Example] to the α-equivariant map

$$\psi : G/(G_1 \cap G_2) \to G/G_1 \times G/G_2,$$

we find normal subgroups $H_1 \supset G_1$ and $H_2 \supset G_2$ of G (automatically α-stable) such that the image of ψ is the pullback to $G/G_1 \times G/G_2$ of the graph of an α-equivariant isomorphism $G/H_1 \tilde{\to} G/H_2$. By hypothesis, the two sides of this isomorphism must be trivial, so ψ is surjective, which proves the lemma. □

Lemma 5. *Let M and N be left modules of a ring R. Suppose that N is semisimple. Let $\alpha, \beta \in \mathrm{Hom}_R(M, N)$ be such that $\ker \alpha \subset \ker \beta$. Then there exists $\gamma \in \mathrm{End}_R(N)$ such that $\beta = \gamma \circ \alpha$.*

Let $M_\alpha = \ker \alpha$ and $M_\beta = \ker \beta$, so $M_\alpha \subset M_\beta$. Let $N_\alpha \cong M/M_\alpha$ and $N_\beta \cong M/M_\beta$ denote the images of α and β. Thus, N_β is isomorphic to a quotient of N_α. As N is semisimple, there is a projection map $N \to N_\alpha$. Composing this with the quotient map $N_\alpha \to N_\beta$ and the inclusion $N_\beta \subset N$ we obtain the desired map γ.

We remark that Lemma 5 holds more generally for any abelian category.

We can now prove the main theorem. Let $\rho_\ell : G_K \to \mathrm{GL}_{2g}(\mathbb{Z}_\ell)$ denote the ℓ-adic Galois representation given by the Tate module of A, and let $\bar{\rho}_\ell$ denote its $(\mathrm{mod}\ \ell)$ reduction. Let G_n denote the Galois group of the field K_n of n-torsion points on A. In particular, G_ℓ is the image of $\bar{\rho}_\ell$. Let $M_\ell = \mathrm{End}_{\mathbb{Z}}(A[\ell](\bar{K})) \cong M_{2g}(\mathbb{F}_\ell)$ denote the endomorphism ring of the additive group of ℓ-torsion points of A over $\bar{K}$. We choose ℓ sufficiently large that it enjoys the following properties:

(a) The group of homotheties in $\rho_\ell(G_K)$ is of index $< \ell - 1$ in $\mathbb{Z}_\ell^*$.
(b) The image E_ℓ of E in M_ℓ and the subring of M_ℓ generated by G_ℓ are mutual centralizers. In particular, both are semisimple algebras.
(c) If for some $\phi \in E$, one has $\phi(P) - Q \in \ell A(K)$, then P and Q satisfy (2).

Part (a) follows from a result of Serre [10, Section 2]. Part (b) is a well-known folklore corollary of Faltings' proof of the Tate conjecture. See [9, p. 24] for a statement. We sketch a proof. The endomorphism ring E acts on $H^1_{\mathrm{sing}}(A, \mathbb{Z})$. Let E^* be the commutant of E in $\mathrm{End}_{\mathbb{Z}} H^1_{\mathrm{sing}}(A, \mathbb{Z})$ and E^{**} its double commutant. As $E \otimes \mathbb{Q}$ is semisimple, $E^{**} \otimes \mathbb{Q} = E \otimes \mathbb{Q}$, so E is of finite index in E^{**}. For ℓ sufficiently large, therefore, $E_\ell = E_\ell^{**}$. The commutator map gives a homomorphism of abelian groups $M_{2g}(\mathbb{Z}) \to \mathrm{Hom}(E, M_{2g}(\mathbb{Z}))$ with kernel E^*. The sequence

$$0 \to E^* \to M_{2g}(\mathbb{Z}) \to \mathrm{Hom}(E, M_{2g}(\mathbb{Z}))$$

remain exact after tensoring with $\mathbb{F}_\ell$ for $\ell \gg 0$. Therefore, the commutant of E_ℓ in M_ℓ is E_ℓ^* for $\ell \gg 0$, and likewise the commutant of E_ℓ^* in M_ℓ is $E_\ell^{**} = E_\ell$ for $\ell \gg 0$. By the double commutant theorem, E_ℓ and E_ℓ^* are semisimple. Now, Deligne [5, 2.7] asserts that for all $\ell \gg 0$, the commutant of $E \otimes \mathbb{Z}_\ell$ in the endomorphism ring of the ℓ-adic Tate module $T_\ell A = H^1_{\text{sing}}(A, \mathbb{Z}) \otimes \mathbb{Z}_\ell$, is the image of $\mathbb{Z}_\ell[G_K]$, or in other words, $\text{im}(\mathbb{Z}_\ell[G_K] \to \text{End}(T_\ell A)) = E^* \otimes \mathbb{Z}_\ell$, which implies (b). Part (c) follows from Lemma 3.

The Kummer sequence for A/K gives a natural E_ℓ-equivariant embedding

$$A(K)/\ell A(K) \hookrightarrow H^1(G_K, A[\ell](\bar{K})) = H^1(G_K, A[\ell](K_\ell)).$$

By (a), the group G_ℓ contains a non-trivial subgroup S_ℓ which acts by scalar multiplication on $A[\ell](K_\ell)$. Since

$$A[\ell](K_\ell)^{S_\ell} = H^1(S_\ell, A[\ell](K_\ell)) = 0,$$

the inflation-restriction sequence

$$0 \to H^1(G_\ell/S_\ell, A[\ell](K_\ell)^{S_\ell}) \to H^1(G_\ell, A[\ell](K_\ell)) \to H^1(S_\ell, A[\ell](K_\ell))^{G_\ell/S_\ell}$$

implies $H^1(G_\ell, A[\ell](K_\ell)) = 0$. The inflation-restriction sequence

$$0 \to H^1(G_\ell, A[\ell](K_\ell)) \to H^1(G_K, A[\ell](K_\ell)) \to H^1(G_{K_\ell}, A[\ell](K_\ell))^{G_\ell}$$

implies

$$A(K)/\ell A(K) \hookrightarrow \text{Hom}(G_{K_\ell}, A[\ell](K_\ell))^{G_\ell} = \text{Hom}_{\mathbb{F}_\ell[G_\ell]}(G_{K_\ell}^{\text{ab}} \otimes \mathbb{F}_\ell, A[\ell](K_\ell)) \qquad (3)$$

is injective. For any $X \in A(K)$, we write $[X]$ for the class of the image of $X + \ell A(X)$ in the right-hand side of (3).

Let $V_\ell = G_{K_\ell}^{\text{ab}} \otimes \mathbb{F}_\ell$. Suppose that for all $\sigma \in V_\ell$, the condition $[Q](\sigma) = 0$ implies $[P](\sigma) = 0$. Applying Lemma 5 to the $\mathbb{F}_\ell[G_\ell]$-modules $M = V_\ell$ and $N = A[\ell](K_\ell)$, we obtain an $\mathbb{F}_\ell[G_\ell]$-module endomorphism γ of N such that $\gamma \circ [P] = [Q]$. By (b), the endomorphism γ lies in the image of E_ℓ, and lifting it to an endomorphism $\phi \in E$, we conclude $[\phi(P) - Q] = 0$. By (3), this means $\phi(P) - Q \in \ell A(K)$, and by (c), this implies (2).

Therefore, we may assume that there exists $\sigma \in V_\ell$ with $[Q](\sigma) = 0$ and $[P](\sigma) \neq 0$. The pair (P, Q) defines a G_ℓ-equivariant map $V_\ell \to A[\ell](K_\ell) \times A[\ell](K_\ell)$. The Galois action on $A[\ell^2](\bar{K})$ defines a G_ℓ-equivariant map $V_\ell \to M_\ell$ since we have

$$\text{Gal}(K_{\ell^2}/K_\ell) = \ker(G_{\ell^2} \to G_\ell) \overset{\log}{\hookrightarrow} \ker(\text{End}(A[\ell^2](\bar{K}))) \to \text{End}(A[\ell](\bar{K})) = M_\ell.$$

By (a), there exists a non-trivial homothety in G_ℓ. It acts trivially on M_ℓ since the action of G_ℓ on M_ℓ is by conjugation, and by definition, it acts as a non-trivial scalar on $A[\ell](K_\ell) \times A[\ell](K_\ell)$. By Lemma 4, the image of V_ℓ in $A[\ell](K_\ell) \times A[\ell](K_\ell) \times M_\ell$ is the product of its images in $A[\ell](K_\ell) \times A[\ell](K_\ell)$ and in M_ℓ. Applying (a) again, there exists $\sigma \in V_\ell$ such that $[P](\sigma) \neq 0$, $[Q](\sigma) = 0$, and σ maps to a non-zero homothety in M_ℓ.

Let $K_{\ell^2}(\ell^{-1}P, \ell^{-1}Q)$ denote the extension of K_ℓ associated to

$$\ker V_\ell \to A[\ell](K_\ell) \times A[\ell](K_\ell) \times M_\ell;$$

thus $K_{\ell^2}(\ell^{-1}P, \ell^{-1}Q)$ is the extension of K generated by the coordinates of all points $R \in A(\bar{K})$ such that $\ell R \in \mathbb{Z}P + \mathbb{Z}Q + A[\ell](K_\ell)$. By Cebotarev, we can fix a prime $\mathfrak{p}$ of $\mathcal{O}$ which is unramified in $K_{\ell^2}(\ell^{-1}P, \ell^{-1}Q)$ and whose Frobenius conjugacy class in $\mathrm{Gal}(K_{\ell^2}(\ell^{-1}P, \ell^{-1}Q)/K)$ contains the image of σ in $\mathrm{Gal}(K_{\ell^2}(\ell^{-1}P, \ell^{-1}Q)/K_\ell)$. Reducing $(\mathrm{mod}\ \mathfrak{p})$ we obtain a finite field $\mathbb{F}_\mathfrak{p}$ such that the ℓ-primary part of $\mathscr{A}(\mathbb{F}_\mathfrak{p})$ contains $(\mathbb{Z}/\ell\mathbb{Z})^{2g}$ (since the Frobenius at $\mathfrak{p}$ fixes K_ℓ) but has no element of order ℓ^2 (since the Frobenius at $\mathfrak{p}$ acts as a non-trivial homothety on $A[\ell^2](K_{\ell^2}(\ell^{-1}P, \ell^{-1}Q)) = A[\ell^2](\bar{K})$). Moreover, the image of P in $\mathscr{A}(\mathbb{F}_\mathfrak{p})$ is not divisible by ℓ, but the image of Q is. This means that the order of P is divisible by ℓ but the order of Q is prime to ℓ, contrary to (1). □

Corollary 6. *Let K be a number field, $\mathcal{O}_K$ its ring of integers, and $\mathcal{O}$ the coordinate ring of an open subscheme of* $\mathrm{Spec}\,\mathcal{O}_K$. *Let $\mathscr{A}_1, \mathscr{A}_2$ be abelian schemes over $\mathcal{O}$ and $P_i \in \mathscr{A}_i(\mathcal{O})$ arbitrary sections. Suppose that for all $n \in \mathbb{Z}$ and all prime ideals $\mathfrak{p}$ of $\mathcal{O}$, we have the implication*

$$nP_1 \equiv 0 \pmod{\mathfrak{p}} \quad \Rightarrow \quad nP_2 \equiv 0 \pmod{\mathfrak{p}}.$$

Then there exist a positive integer k and an endomorphism $\psi \in \mathrm{Hom}_\mathcal{O}(\mathscr{A}_1, \mathscr{A}_2)$ such that

$$\psi(P_1) = kP_2.$$

Proof. Let $\mathscr{A} = \mathscr{A}_1 \times \mathscr{A}_2$, $P = (P_1, 0)$, $Q = (0, P_2)$. Applying Theorem 1, we conclude that there exist a positive integer k and an endomorphism

$$\phi \in \mathrm{End}_\mathcal{O}\,\mathscr{A} = \mathrm{End}_\mathcal{O}\,\mathscr{A}_1 \times \mathrm{End}_\mathcal{O}\,\mathscr{A}_2 \times \mathrm{Hom}_\mathcal{O}(\mathscr{A}_1, \mathscr{A}_2) \times \mathrm{Hom}_\mathcal{O}(\mathscr{A}_2, \mathscr{A}_1)$$

such that $\phi(P) = kQ$. Letting ψ denote the image of ϕ under projection to $\mathrm{Hom}_\mathcal{O}(\mathscr{A}_1, \mathscr{A}_2)$, we obtain the corollary. □

Acknowledgments

I would like to thank R. Schoof for his helpful comments on earlier versions of this paper.

References

[1] N. Ailon, Z. Runick, Torsion points on curves and common divisors of $a^k - 1$ and $b^k - 1$, preprint, February 28, 2002, arXiv: math.NT/0202102 v2.
[2] G. Banaszak, W. Gajda, P. Krasoń, A support problem for the intermediate Jacobians of ℓ-adic representations, preprint, January 29, 2002, http://www.math.uiuc.edu/Algebraic-Number-Theory/0332.
[3] S. Bosch, W. Lütkebohmert, M. Raynaud, Néron Models, Ergebnisse der Mathematik und ihrer Grenzgebiete, Vol. 21, Springer, Berlin, 1990.
[4] C. Corrales-Rodrigáñez, R. Schoof, The support problem and its elliptic analogue, J. Number Theory 64 (2) (1997) 276–290.
[5] P. Deligne, Conjectures de Tate et Shafarevitch, Séminaire Bourbaki 1983/84, No. 616, Astérisque 121/122 (1985) 25–41.
[6] C. Khare, D. Prasad, Reduction of homomorphisms mod p and algebraicity, preprint, November 1, 2002, arXiv: math.NT/0211004v1.
[7] E. Kowalski, Some local–global applications of Kummer theory, preprint.
[8] S. Lang, Algebra, 2nd Edition, Addison–Wesley, Menlo Park, CA, 1984.
[9] J-P. Serre, Lettre à Daniel Bertrand du 8/6/1984, Œuvres, Collected Papers, Vol. IV, Springer-Verlag, Berlin, 2000.
[10] J-P. Serre, Lettre à Ken Ribet du 7/3/1986, Œuvres, Collected Papers, Vol. IV, Springer-Verlag, Berlin, 2000.
[11] S. Wong, Power residues on abelian varieties, Manuscripta Math. 102 (2000) 129–138.