THE SUPPORT PROBLEM
FOR ABELIAN VARIETIES

BY

MICHAEL LARSEN*

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

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 $(\text{mod } p)$ reduction of $Q$ divides the order of the $(\text{mod } p)$ reduction of $P$ for almost all prime ideals $p$, then there exists a $K$-endomorphism $\phi$ of $A$ and a positive integer $k$ such that $\phi(P) = kQ$.

This note solves the support problem for abelian varieties over number fields, thus answering a question of C. Corrales-Rodríguez and R. Schoof [4]. Recently, G. Banaszak, W. Gajda, and P. Krasoń [2] and C. Khare and D. Prasad [6] have solved the problem for certain classes of abelian varieties for which the images of the $\ell$-adic Galois representations can be particularly well understood. A number of other authors have also made progress recently on closely related problems, including E. Kowalski [7], S. Wong [11], and N. Ailon and Z. Rudnick [1].

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

The main result is as follows:

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

$$nP \equiv 0 \pmod{p} \Rightarrow nQ \equiv 0 \pmod{p}. \quad (1)$$

Then there exist a positive integer $k$ and an endomorphism $\phi \in \text{End}_O(A)$ such that

$$\phi(P) = kQ. \quad (2)$$

* Partially supported by NSF Grant DMS-0100537
Note that as $\mathcal{A}$ is a Néron model of its generic fiber $A$ ([3] I 1.2/8), we have that $\text{End}_\mathcal{O}\mathcal{A} = \text{End}_K A$. We employ scheme notation only to make sense of the notion of the reduction of a point of $A \mod p$.

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 $\mathcal{O}$, $\mathcal{A}$, $P$, and $Q$ as above such that (1) holds but $Q \not\in (\text{End}_\mathcal{O}\mathcal{A})P$.

**Proof:** Let $\mathcal{O}$ be a ring containing $1/2$. Let $\mathcal{E}/\mathcal{O}$ be an elliptic curve with $\text{End}_\mathcal{O}\mathcal{E} = \mathbb{Z}$ whose 2-torsion is all $\mathcal{O}$-rational. Let $T_1$ and $T_2$ denote distinct 2-torsion points of $\mathcal{E}(\mathcal{O})$, and let $R$ denote a point of infinite order in $\mathcal{E}(\mathcal{O})$. Let $\mathcal{A} = \mathcal{E}^2$, $P = (R, R + T_1)$, 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 $\mod p$), so $P$ always has even order $\mod p$. Thus $nP \equiv 0 \mod p$ implies $2 \mid n$ and therefore $nQ = (nR, nR) = nP \equiv 0 \mod p$.

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

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

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

$$\phi(P) - Q \not\in m\mathcal{A}(\mathcal{O}).$$

**Proof:** The lemma follows from the Mordell-Weil theorem and the trivial fact that the image of $Q$ in the finitely generated abelian group $\mathcal{A}(\mathcal{O})/EP$ 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 $\alpha$ be an automorphism of $G$ such that $\alpha(G_i) \subseteq G_i$ for $i = 1, 2$. Suppose $\alpha$ 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, Ex.) to the $\alpha$-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 $\alpha$-stable) such that the image of $\psi$ is the pullback to $G/G_1 \times G/G_2$ of the graph of an $\alpha$-equivariant isomorphism $G/H_1 \to G/H_2$. By hypothesis, the two sides of this isomorphism must be trivial, so $\psi$ is surjective, which proves the lemma. \qed

Lemma 5: Let $M$ and $N$ be left modules of a ring $R$. Suppose that $N$ is semisimple. Let $\alpha, \beta \in \text{Hom}_R(M, N)$ be such that $\ker \alpha \subset \ker \beta$. Then there exists $\gamma \in \text{End}_R(N)$ 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 $\alpha$ and $\beta$. Thus, $N_\beta$ is isomorphic to a quotient of $N_\alpha$. 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 $\gamma$. \qed

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

We can now prove the main theorem. Let $\rho_\ell: G_K \to \text{GL}_2(\mathbb{Z}_\ell)$ denote the $\ell$-adic Galois representation given by the Tate module of $A$, and let $\bar{\rho}_\ell$ denote its (mod $\ell$) reduction. Let $G_n$ denote the Galois group of the field $K_n$ of $n$-torsion points on $A$. In particular, $G_\ell$ is the image of $\bar{\rho}_\ell$. Let $M_\ell = \text{End}_\mathbb{Z}(A[\ell](\bar{K})) \cong M_2(\mathbb{F}_\ell)$ denote the endomorphism ring of the additive group of $\ell$-torsion points of $A$ over $\bar{K}$. We choose $\ell$ 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 $E_\ell$ of $E$ in $M_\ell$ and the subring of $M_\ell$ generated by $G_\ell$ 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] §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 $H^1_{\text{sing}}(A, \mathbb{Z})$. Let $E^*$ be the centralizer of $E$ in $\text{End}_{\mathbb{Z}} H^1_{\text{sing}}(A, \mathbb{Z})$ and $E^{**}$ its double centralizer. As $E \otimes \mathbb{Q}$ is semisimple, $E^{**} \otimes \mathbb{Q} = E \otimes \mathbb{Q}$, so $E$ is of finite index in $E^{**}$. For $\ell$ sufficiently large, therefore, $E_\ell = E^{**}_\ell$. The commutator map gives a homomorphism of abelian groups $M_{2g}(\mathbb{Z}) \to \text{Hom}(E, M_{2g}(\mathbb{Z}))$ with kernel $E^*$. The sequence

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

remain exact after tensoring with $\mathbb{F}_\ell$ for $\ell \gg 0$. Therefore, the commutator of $E_\ell$ in $M_\ell$ is $E^*_\ell$ for $\ell \gg 0$, and likewise the commutator of $E^{**}_\ell$ in $M_\ell$ is $E^{**}_\ell = E_\ell$ for $\ell \gg 0$. By the double commutant theorem, $E_\ell$ and $E^{**}_\ell$ are semisimple. Now, [5] 2.7 asserts that for all $\ell \gg 0$, the centralizer of $E_\ell \otimes \mathbb{Z}_\ell$ in the endomorphism ring of the $\ell$-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 $E_\ell$-equivariant embedding

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

By (a), the group $G_\ell$ contains a non-trivial subgroup $S_\ell$ 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

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

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 $V_\ell = G_{K_\ell}^{ab} \otimes \mathbb{F}_\ell$. 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 $\gamma$ of $N$ such that $\gamma \circ [P] = [Q]$. By (b), the endomorphism $\gamma$ lies in the image of $E_\ell$, 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 $G_\ell$-equivariant map $V_\ell \to A[\ell](K_\ell) \times A[\ell](K_\ell)$. The Galois action on $A[\ell^2](\overline{K})$ defines a $G_\ell$-equivariant map $V_\ell \to M_\ell$ since we have

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

By (a), there exists a non-trivial homothety in $G_\ell$. It acts trivially on $M_\ell$ since the action of $G_\ell$ on $M_\ell$ 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 $V_\ell$ 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 $M_\ell$. Applying (a) again, there exists $\sigma \in V_\ell$ such that $[P](\sigma) \neq 0$, $[Q](\sigma) = 0$, and $\sigma$ maps to a non-zero homothety in $M_\ell$.

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

**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 $\text{Spec} \mathcal{O}_K$. Let $A_1, A_2$ be abelian schemes
over \( \mathcal{O} \) and \( P_i \in \mathcal{A}_i(\mathcal{O}) \) arbitrary sections. Suppose that for all \( n \in \mathbb{Z} \) and all prime ideals \( \mathfrak{p} \) of \( \mathcal{O} \), we have the implication

\[
nP_1 \equiv 0 \pmod{\mathfrak{p}} \Rightarrow nP_2 \equiv 0 \pmod{\mathfrak{p}}.
\]

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

\[
\psi(P_1) = kP_2.
\]

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

\[
\phi \in \text{End}_\mathcal{O} \mathcal{A} = \text{End}_\mathcal{O} \mathcal{A}_1 \times \text{End}_\mathcal{O} \mathcal{A}_2 \times \text{Hom}_\mathcal{O}(\mathcal{A}_1, \mathcal{A}_2) \times \text{Hom}_\mathcal{O}(\mathcal{A}_2, \mathcal{A}_1)
\]

such that \( \phi(P) = kQ \). Letting \( \psi \) denote the image of \( \phi \) under projection to \( \text{Hom}_\mathcal{O}(\mathcal{A}_1, \mathcal{A}_2) \), we obtain the corollary. \( \square \)

REFERENCES

[1] Ailon, N.; Runick, Z.: Torsion points on curves and common divisors of \( a^k - 1 \) and \( b^k - 1 \), arXiv: math.NT/0202102 v2, preprint, Feb. 28, 2002.
[2] Banaszak, G.; Gajda, W.; Krasoń, P.: A support problem for the intermediate Jacobians of \( \ell \)-adic representations, http://www.math.uiuc.edu/Algebraic-Number-Theory/0332, preprint, Jan. 29, 2002.
[3] Bosch, S.; Lütkebohmert, W.; Raynaud, M.: Néron models, Ergebnisse der Mathematik und ihrer Grenzgebiete, 21. Springer-Verlag, Berlin, 1990.
[4] Corrales-Rodríguez, C.; Schoof, R.: The support problem and its elliptic analogue. J. Number Theory 64 (1997), no. 2, 276–290.
[5] Deligne, P.: Conjectures de Tate et Shafarevitch, Séminaire Bourbaki 1983/84, n° 616, Astérisque 121/122.
[6] Khare, C.; Prasad, D.: Reduction of homomorphisms mod \( p \) and algebraicity, arXiv: math.NT/0211004v1, preprint, Nov. 1, 2002.
[7] Kowalski, E.: Some local-global applications of Kummer theory, preprint.
[8] Lang, S.: Algebra, second edition, Addison-Wesley, Menlo Park, CA, 1984.
[9] Serre, J-P.: Lettre à Daniel Bertrand du 8/6/1984, Collected Papers Vol. IV.
[10] Serre, J-P.: Lettre à Ken Ribet du 7/3/1986, *Collected Papers Vol. IV*.

[11] Wong, S.: Power residues on abelian varieties. *Manuscripta Math.* **102** (2000), 129–138.