A REFINED COUNTER-EXAMPLE TO THE SUPPORT CONJECTURE FOR ABELIAN VARIETIES

MICHAEL LARSEN AND RENÉ SCHOOF

Abstract. If $A/K$ is an abelian variety over a number field and $P$ and $Q$ are rational points, the original support conjecture asserted that if the order of $Q$ (mod $p$) divides the order of $P$ (mod $p$) for almost all primes $p$ of $K$, then $Q$ is obtained from $P$ by applying an endomorphism of $A$. This is now known to be untrue. In this note we prove that it is not even true modulo the torsion of $A$.

Let $A$ be an abelian variety over a number field $K$ and let $P$ and $Q$ be $K$-rational points of $A$. By inverting a suitable element in the ring of integers of $K$, one can always find a Dedekind domain $O$ with fraction field $K$ such that $A$ extends to an abelian scheme $\mathcal{A}$ over $O$ and $P$ and $Q$ extend to $O$-points of $\mathcal{A}$. Therefore, one can speak of reducing $P$ and $Q$ (mod $p$) for almost all (i.e., all but finitely many) primes $p$. In [1], C. Corrales-Rodríguez and R. Schoof proved that when $\text{dim } A = 1$, the condition

\begin{equation}
nP \equiv 0 \pmod{p} \implies nQ \equiv 0 \pmod{p}
\end{equation}

for all integers $n$ and almost all prime ideals $p$ implies

\begin{equation}
Q = fP, \quad \text{for some } f \in \text{End}_K(A).
\end{equation}

In [2], M. Larsen proved that (1) does not imply (2) for general abelian varieties but that it does imply

\begin{equation}
kQ = fP, \quad \text{for some } f \in \text{End}_K(A)
\end{equation}

and some positive integer $k$. The counter-example presented to (2) actually satisfies something stronger than (3), namely

\begin{equation}
Q = fP + T, \quad \text{for some } f \in \text{End}_K(A)
\end{equation}

and some torsion point $T \in A(K)$.

An early draft of [3] (version 2) claimed that (1) in fact implies (4). The proof given was incorrect, and the statement was removed from subsequent versions. (Version 3 is essentially the same as the published version [2], while version 4 corrects a series of misprints, in which $P$ was written for $Q$ and vice versa throughout several paragraphs of the proof of the main theorem.)

In this note we present an example to show that (1) does not imply (4).

Theorem 1. There exists an abelian variety $A$ over a number field $K$ and points $P$ and $Q$ which satisfy (1) but not (4).

The first named author was partially supported by NSF grant DMS-0100537.
Proof. Let $p$ be a prime. Let $K$ be a number field and let $E$ be an elliptic curve over $K$ without complex multiplication that possesses a point $R \in E(K)$ of infinite order. Suppose in addition that the $p$-torsion points of $E$ are rational over $K$ and let $R_1, R_2 \in E(K)$ be two independent points of order $p$. Consider the abelian surface $A$ obtained by dividing $E \times E$ by the subgroup generated by the point $(R_1, R_2)$. Then $A$ is defined over $K$.

We describe the ring of $K$-endomorphisms of $A$. Let $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, and let $\lambda_1, \lambda_2 \in p^{-1}\Lambda$ map to $R_1$ and $R_2$ respectively. Thus, if for certain integers $a$ and $b$ we have $a\lambda_1 + b\lambda_2 \in \Lambda$, then necessarily $a, b \in p\mathbb{Z}$. Let

$$M = \mathbb{Z}\begin{pmatrix} \lambda_1 \\ \lambda_2 \end{pmatrix} + \Lambda^2 \subset p^{-1}\Lambda^2.$$ 

The complex torus $A(\mathbb{C})$ is isomorphic to $\mathbb{C}^2/M$, and any endomorphism of $A(\mathbb{C})$ is given by a complex $2 \times 2$ matrix

$$(5) \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{C})$$

with

$$(6) \quad a\Lambda, b\Lambda, c\Lambda, d\Lambda \subset p^{-1}\Lambda$$

and

$$(7) \quad a\lambda_1 + b\lambda_2 \in k\lambda_1 + \Lambda, \; c\lambda_1 + d\lambda_2 \in k\lambda_2 + \Lambda$$

for some $k \in \mathbb{Z}$. As $E$ does not have complex multiplication, (6) implies $pa, pb, pc, pd \in \mathbb{Z}$. Multiplying (7) by $p$, we deduce that $a, b, c, d \in \mathbb{Z}$, and then (7) implies $a - k, b, c, d - k \in p\mathbb{Z}$. Conversely, any matrix (5) whose entries satisfy $a - k, b, c, d - k \in p\mathbb{Z}$ for some $k \in \mathbb{Z}$, lies in $\text{End}(A(\mathbb{C}))$ and therefore in $\text{End}_\mathbb{Z} A$. Since the curve $E$ and the points $R_1, R_2$ are defined over $K$, it lies therefore in $\text{End}_K A$.

Let $P$ and $Q$ denote the images of the points $(R, 0)$ and $(R, R)$ in $A(K)$ respectively. Suppose that $nP \equiv 0 \pmod{p}$ for some prime $p$ of good reduction and characteristic different from $p$. This means that $(nR, nR)$ is contained in the subgroup generated by $(R_1, R_2)$ in the group of points on $E \times E$ modulo $p$. Since the characteristic of $p$ is not $p$, the torsion points $R_1$ and $R_2$ are distinct modulo $p$. This implies that $nP \equiv 0 \pmod{p}$. It follows that $nP \equiv 0 \pmod{p}$. Therefore condition (11) is satisfied. And of course, so is the conclusion (3) of Larsen’s Theorem with $k = p$ and $f \in \text{End}_K(A)$ the endomorphism with matrix $\begin{pmatrix} 0 & p \\ 0 & 0 \end{pmatrix}$.

However, (4) does not hold because there is no endomorphism $g \in \text{End}_K(A)$ for which $P = gQ$ plus a torsion point. Indeed, this would imply

$$\begin{pmatrix} R \\ 0 \end{pmatrix} = \begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix} + p \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} R \\ R \end{pmatrix} + \begin{pmatrix} T_1 \\ T_2 \end{pmatrix}$$

for some $k \in \mathbb{Z}$ and some torsion points $T_1, T_2 \in E(K)$. Since $R$ has infinite order, inspection of the second coordinate shows that $k + pc + pd = 0$ so
that \( k \equiv 0 \pmod{p} \). On the other hand, looking at the first coordinate we see that \( 1 = pa + pb + k \), a contradiction.

\[ \square \]

**References**

[1] Corrales-Rodríguez, Capi; Schoof, René: The support problem and its elliptic analogue. *J. Number Theory* **64** (1997), no. 2, 276–290.

[2] Larsen, Michael: The support problem for abelian varieties. *J. Number Theory* **101** (2003), 398–403.

[3] Larsen, Michael: The support problem for abelian varieties, arXiv:math.NT/0211118.

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

Department of Mathematics, Indiana University, Bloomington, IN 47405, U.S.A.

*E-mail address*: schoof@science.uva.nl

Università di Roma “Tor Vergata”, Dipartimento di Matematica, Via della Ricerca Scientifica, I-00133 Roma, ITALY