ON THE LOCAL-GLOBAL PRINCIPLE FOR DIVISIBILITY IN THE
COHOMOLOGY OF ELLIPTIC CURVES

BRENDAN CREUTZ

Abstract. For every prime power $p^n$ with $p = 2$ or 3 and $n \geq 2$ we give an example of an elliptic curve over $\mathbb{Q}$ containing a rational point which is locally divisible by $p^n$ but is not divisible by $p^n$. For these same prime powers we construct examples showing that the analogous local-global principle for divisibility in the Weil-Châtelet group can also fail.

1. Introduction

Let $G$ be a connected commutative algebraic group over a number field $k$, and let $n$ and $r$ be nonnegative integers. An element $\rho$ in the Galois cohomology group $H^r(k, G) := H^r(\text{Gal}(\overline{k}/k), G(\overline{k}))$ is divisible by $n$ if there exists $\rho' \in H^r(k, G)$ such that $n\rho' = \rho$. We say $\rho$ is locally divisible by $n$ if, for all primes $v$ of $k$, there exists $\rho'_v \in H^r(k_v, G)$ such that $n\rho'_v = \text{res}_v(\rho)$. It is natural to ask whether every element locally divisible by $n$ is necessarily divisible by $n$. When the answer is yes, we say the local-global principle for divisibility by $n$ holds.

For $r = 0$ and $G = \mathbb{G}_m$, the answer is given by the Grunwald-Wang theorem (see [NSW08, IX.1]); the local-global principle for divisibility by $n$ holds, except possibly when 8 divides $n$. The case $r = 1$ and $G = \mathbb{G}_m$ is trivial in light of Hilbert’s theorem 90. For $r \geq 2$ and general $G$, a result of Tate implies that the local-global principle for divisibility by $n$ always holds (see Theorem 2.1 below).

A study of the problem for $r = 0$ and general $G$ was initiated by Dvornicich and Zannier in [DZ01], with particular focus on elliptic curves in [DZ04, DZ07, PRV12]. For elliptic curves over $\mathbb{Q}$, their results show that the local-global principle for divisibility by a prime power $p^n$ holds for $n = 1$ or $p \geq 11$, and they have constructed counterexamples for $p^n = 4$ [1]. For $r = 1$ and $G$ an elliptic curve, the question was in effect raised by Cassels [Cas62, Problem 1.3]. In particular, he asked whether elements of $H^1(k, G)$ that are everywhere locally trivial must be divisible. In response, Tate proved the local-global principle for divisibility by a prime $p$ [Cas62b]. Cassels’ question is considered again in [Bas72], and recently by Çiperian and Stix [CS13] who showed that, for elliptic curves over $\mathbb{Q}$, the local-global principle for divisibility by $p^n$ holds for all prime powers with $p \geq 11$. An example showing that it does not hold in general over $\mathbb{Q}$ for any $p^n = 2^n$ with $n \geq 2$ was constructed in [Cre13].

In this note we produce examples settling these questions for the remaining undecided powers of the primes 2 and 3. We prove the following.

Theorem. Let $n \geq 2$ be an integer, let $p \in \{2, 3\}$ and let $r \in \{0, 1\}$. Then there exists an elliptic curve $E$ over $\mathbb{Q}$ for which the local-global principle for divisibility by $p^n$ fails in $H^r(\mathbb{Q}, E)$.

[1] Paladino et al. have recently announced a proof of the local-global principle for powers of 5 and 7 [PRV].
Acknowledgements. It is a pleasure to thank Jakob Stix for a number of helpful comments, including pointing out case (3) in Theorem 2.1.

Notation. Throughout the paper \( p \) denotes a prime number, \( m \) and \( n \) are a positive integers, and \( r \) is a nonnegative integer. As above, \( G \) is a connected commutative algebraic group defined over a number field \( k \) with a fixed algebraic closure \( \overline{k} \). We will use \( K \) to denote a field containing \( k \) and use \( \overline{K} \) to denote a fixed algebraic closure of \( K \) containing \( \overline{k} \). For a \( \text{Gal}(\overline{k}/k) \)-module \( M \), let \( M^\vee \) denote its Cartier dual and define
\[
\bigwedge^r(k, M) := \ker \left( H^r(k, M) \xrightarrow{\prod \text{res}_v} \prod_v H^r(k_v, M) \right),
\]
the product running over all primes of \( k \).

2. The obstruction to the local-global principle for divisibility.

Because \( K \) has characteristic 0, multiplication by \( n \) is a finite étale endomorphism of \( G \). Hence, for any \( r \geq 0 \), the short exact sequence of \( \text{Gal}(\overline{K}/K) \)-modules
\[
0 \to G[n] \xrightarrow{\iota} G \xrightarrow{n} G \to 0
\]
gives rise to an exact sequence,
\[
H^r(K, G[n]) \xrightarrow{\iota^*} H^r(K, G) \xrightarrow{n^*} H^r(K, G)[n] \xrightarrow{\delta_n} H^{r+1}(K, G[n]) \xrightarrow{\iota^*} H^{r+1}(K, G).
\]

From this one easily sees that an element \( \rho \in H^r(k, G) \) is locally divisible by \( n \) if and only if \( \delta_n(\rho) \in \bigwedge^{r+1}(k, G[n]) \), and that \( \rho \) is divisible by \( n \) if and only if \( \delta_n(\rho) = 0 \). In particular, the local-global principle for divisibility by \( n \) in \( H^r(k, G) \) holds whenever \( \bigwedge^{r+1}(k, G[n]) = 0 \). Combining this observation with Tate’s duality theorems yields the following.

Theorem 2.1. Assume any of the following:

(1) \( r = 0 \) and \( \bigwedge^1(k, G[n]) = 0 \);
(2) \( r = 1 \) and \( \bigwedge^1(k, G[n]^\vee) = 0 \); or
(3) \( r \geq 2 \).

Then the local-global principle for divisibility by \( n \) in \( H^r(k, G) \) holds.

Proof. As noted above, in each case it suffices to show that \( \bigwedge^{r+1}(k, G[n]) = 0 \). Case (1) is trivial, and cases (2) and (3) follow immediately from [Tat63, Theorem 3.1]. \( \square \)

The following proposition shows that when \( G \) is a principally polarized abelian variety, the conditions in the theorem are necessary, at least conjecturally.

Proposition 2.2. Suppose \( G \) is an abelian variety with dual \( G^\vee \). Then for every \( \xi \in \bigwedge^1(k, G[n]) \), exactly one of the following hold:

(1) \( \xi = 0 \);
(2) \( \xi = \delta_n(\rho) \) for some \( \rho \in G(k) \) that is locally divisible by \( n \), but is not divisible by \( n \); or
(3) \( \iota_n(\xi) \neq 0 \), in which case there either exists \( \rho \in \bigwedge^1(k, G^\vee) \) such that \( \rho \) is not divisible by \( n \), or \( \iota_n(\xi) \) is divisible in \( \bigwedge^1(k, G) \) by all powers of \( n \).

If \( G \) is a principally polarized abelian variety and \( \bigwedge^1(k, G) \) is finite, then the local-global principle for divisibility by \( n \) holds in \( H^r(k, G) \) for every \( r \geq 0 \) if and only if \( \bigwedge^1(k, G[n]) = 0 \).
Proof. Exactness of (2.1) implies that the cases in the first statement of the proposition are exhaustive and mutually exclusive. For the claim in case (3) we may apply [Cre13] Thm 3, which states that \( \text{III}^1(k, G') \subset n \text{H}^1(k, G') \) if and only if the image of \( \iota_* : \text{III}^1(k, G[n]) \to \text{III}^1(k, G) \) is contained in the maximal divisible subgroup of \( \text{III}^1(k, G) \).

Now suppose \( G \) is a principally polarized and that \( \text{III}^1(k, G) \) is finite. We must prove the equivalence in the second statement. One direction follows from Theorem 2.1 since \( G[n] = G[n]' \). The other direction follows from the first statement in the proposition, since finiteness of \( \text{III}^1(k, G) \) implies that it contains no nontrivial divisible elements as in case (3). \( \square \)

The next lemma formalizes a method for constructing elements of \( \text{III}^1(k, G[mn]) \), for some \( m \geq 1 \).

**Lemma 2.3.** Let \( m \geq 1 \) and let \( j : G[n] \subset G[mn] \) be the inclusion map. Suppose \( \xi \in \text{H}^1(k, G[n]) \) is such that \( \text{res}_v(\xi) \in \delta_n(G(k_v)[m]) \), for all primes \( v \) of \( k \). Then

1. \( j_* (\xi) \in \text{III}^1(k, G[mn]) \);
2. \( j_* (\xi) = 0 \) if and only if \( \xi \in \delta_n(G(k)[m]) \);
3. if \( \xi = \delta_n(\rho) \) for some \( \rho \in G(k) \), then \( mn \rho \) is locally divisible by \( mn \); and
4. if \( \xi = \delta_n(\rho) \) for some \( \rho \in G(k) \) and \( j_* (\xi) \neq 0 \), then \( mn \rho \) is not divisible by \( mn \).

**Proof.** The connecting homomorphism \( G(K)[m] \to \text{H}^1(k, G[n]) \) arising from the short exact sequence

\[
0 \to G[n] \xrightarrow{j} G[mn] \xrightarrow{n} G[m] \to 0
\]

is the restriction of the \( \delta_n \) to \( G(K)[m] \). This implies that

\[
\ker (j_* : \text{H}^1(K, G[n]) \to \text{H}^1(K, G[mn])) = \delta_n(G(K)[m]),
\]

from which the first two statements in the proposition easily follow.

The inclusion \( j : G[n] \subset G[mn] \) also induces a commutative diagram

\[
\begin{array}{ccc}
G(K)[n] & \xrightarrow{j} & G(K) \\
\downarrow & & \downarrow \\
G(K)[mn] & \xrightarrow{mn} & G(K)
\end{array}
\]

\[
\begin{array}{ccc}
\text{H}^1(K, G[n]) & \xrightarrow{\delta_n} & \text{H}^1(K, G[n]) \\
\downarrow & & \downarrow \\
\text{H}^1(K, G[mn]) & \xrightarrow{\delta_{mn}} & \text{H}^1(K, G[mn])
\end{array}
\]

where the rows are the exact sequence (2.1) with \( r = 0 \), and the same sequence with \( mn \) in place of \( n \). From this the last two statements can be deduced easily. \( \square \)

3. The examples for \( p = 2 \)

**Proposition 3.1.** Let \( E \) be the elliptic curve defined by \( y^2 = (x + 2795)(x - 1365)(x - 1430) \) and let \( P = (341 : 59136 : 1) \in E(\mathbb{Q}) \). For every \( n \geq 1 \), the point \( 2^{n-1} P \) is locally divisible by \( 2^n \), but not divisible by \( 2^n \). In particular, the local-global principle for divisibility by \( 2^n \) in \( E(\mathbb{Q}) \) fails for every \( n \geq 2 \).

**Remark 3.2.** This example was constructed by Dvornicich and Zannier who proved the proposition in the case \( n = 2 \) [DZ04 §4]. Using Lemma 2.3 their arguments apply to all \( n \geq 2 \). We include our own proof here since our examples for \( p = 3 \) will be obtained using a similar, though more involved argument.
Proof. Fix the basis \( P_1 = (1365 : 0 : 1), P_2 = (1430 : 0 : 1) \) for \( E[2] \). By [Sil86, Proposition X.1.4] the composition of \( \delta_2 \) with isomorphism \( H^1(K, E[2]) \cong (K^\times/K^{\times 2})^2 \) is given explicitly by

\[
Q = (x_0, y_0) \mapsto \begin{cases} 
(x_0 - 1365, x_0 - 1430) & \text{if } Q \neq P_1, P_2 \\
(-1, -65) & \text{if } Q = P_1 \\
(65, 65) & \text{if } Q = P_2 \\
(1, 1) & \text{if } Q = 0
\end{cases}
\]

In particular, \( \delta_2(P) = (-1, -1) \) and \( \delta_2(E(K)[2]) \) is generated by \( \{(-1, -65), (65, 65)\} \). It follows that \( \delta_2(P) \in \delta_2(E(K)[2]) \) if and only if at least one of \( 65, -65 \) or \(-1 \) is a square in \( K \). If \( K = \mathbb{Q}_v \) for some \( v \leq \infty \), then one of these is a square. Indeed, \( 65 \) is a square in \( \mathbb{R} \) and in \( \mathbb{Q}_2, -1 \) is a square \( \mathbb{Q}_5 \) and for all other primes \( v \) the Legendre symbols satisfy the identity \( \left( \frac{-1}{v} \right) = \left( \frac{65}{v} \right) \). Hence \( \xi := \delta_2(P) \) satisfies the hypothesis of Lemma 2.3 with \( (m, n) \) replaced by \( (2^{n-1}, 2) \).

On the other hand, \( 65, -65 \) and \(-1 \) are not squares in \( \mathbb{Q}_2 \), and \( E(\mathbb{Q})[2^\infty] = E(\mathbb{Q})[2] \) (the reduction mod 3 is nonsingular, so the 2-primary torsion must inject into the group of \( \mathbb{F}_3 \)-points on the reduced curve. This group has order less than 8 by Hasse’s theorem). So the result follows from Lemma 2.3. \( \square \)

Proposition 3.3. Let \( E \) be the elliptic curve defined by \( y^2 = x(x + 80)(x + 205) \). Then \( \text{III}^1(\mathbb{Q}, E) \nsubseteq 4 \text{H}^1(\mathbb{Q}, E) \). In particular, the local-global principle for divisibility by \( 2^n \) in \( \text{H}^1(\mathbb{Q}, E) \) fails for every \( n \geq 2 \).

Proof. This is [Cre13, Theorem 5]; we are content to sketch the proof. Much like the previous proof, one uses the explicit description of the map \( \delta_2 : E(K) \to \text{H}^2(K, E[2]) \cong (K^\times/K^{\times 2})^2 \) to show that there is an element \( \xi \in \text{H}^1(\mathbb{Q}, E[2]) \setminus \delta_2(E(\mathbb{Q})) \) which maps into \( \delta_2(E(\mathbb{Q}_v)) \) everywhere locally. Lemma 2.3 then shows that the image of \( \xi \) in \( \text{H}^1(k, E[4]) \) falls under case 3 of Proposition 2.2. This gives the result, since \( \text{III}^1(\mathbb{Q}, E)[2^\infty] \) is finite (as one can check in multiple ways, with or without the assistance of a computer). \( \square \)

4. DIAGONAL CUBIC CURVES AND 3-COVERINGS

The examples for \( p = 2 \) were constructed using an explicit description of the map

\[
E(K) \xrightarrow{\delta_2} \text{H}^1(K, E[2]) \cong (K^\times/K^{\times 2})^2.
\]

Another way to describe the connecting homomorphism is in the language of \( n \)-coverings. An \( n \)-covering of an elliptic curve \( E \) over \( K \) is a \( K \)-form of the multiplication by \( n \) map on \( E \). In other words, an \( n \)-covering of \( E \) is a morphism \( \pi : C \to E \) such that there exists an isomorphism \( \psi : E_K \to C_K \) of the curves base changed to the algebraic closure \( K \) which satisfies \( \pi \circ \psi = n \). We now summarize how this notion can be used to give an interpretation of the group \( \text{H}^1(K, E[n]) \). Details may be found in [CFO08, §1].

An isomorphism of \( n \)-coverings of \( E \) is, by definition, an isomorphism in the category of \( E \)-schemes. The automorphism group of the \( n \)-covering \( n : E \to E \) can be identified with \( E[n] \) acting by translations. By a standard result in Galois cohomology (the twisting principle) the \( K \)-forms of \( n : E \to E \) are parameterized, up to isomorphism by \( \text{H}^1(K, E[n]) \). Under this identification the connecting homomorphism \( \delta_n \) sends a point \( P \in E(K) \) to the
isomorphism class of the $n$-covering,

$$\pi_P : E \to E, \quad Q \mapsto nQ + P.$$ 

In particular, the isomorphism class of an $n$-covering $\pi : C \to E$ is equal to $\delta_n(P)$ if and only if $P \in \pi(C(K))$.

Our examples for $p = 3$ will come from elliptic curves of the form $E : x^3 + y^3 + dz^3 = 0$ with distinguished point $(1 : −1 : 0)$, where $d \in \mathbb{Q}^\times$. For these curves we can write down some of the 3-coverings quite explicitly. According to Selmer, the following lemma goes back to Euler (see [Sel51, Theorem 1]).

**Lemma 4.1.** Let $E : x^3 + y^3 + dz^3 = 0$ and suppose $a, b, c \in \mathbb{Q}^\times$ are such that $abc = d$. Then the curve $C : aX^3 + bY^3 + cZ^3 = 0$ together with the map $\pi : C \to E$ defined by

\[
\begin{align*}
    x + y &= 9abcX^3Y^3Z^3, \\
    x - y &= (aX^3 - bY^3)(bY^3 - cZ^3)(cZ^3 - aX^3), \\
    z &= 3(abX^3Y^3 + bcY^3Z^3 + caZ^3X^3)XYZ
\end{align*}
\]

is a 3-covering of $E$.

**Proof.** A direct computation verifies that these equations define a nonconstant morphism $\pi : C \to E$, which, by virtue of the fact that $E$ and $C$ are smooth genus 1 curves, implies that it is finite and étale. The map $\psi : E_K \to C_K$ defined by

$$x = \sqrt[3]{a}X, \quad y = \sqrt[3]{b}Y, \quad z = \sqrt[3]{c}dZ$$

is clearly an isomorphism. It is quite evident that $E[3]$, which is cut out by $xyz = 0$, is mapped by $\pi \circ \psi$ to the identity $(1 : −1 : 0) \in E_K$. Therefore $\pi \circ \psi$ is an isogeny which factors through multiplication by 3. Since it has degree 9 it must in fact be multiplication by 3, and so $\pi$ is a 3-covering. $\square$

**Lemma 4.2.** Suppose $d = 3d'$ and let $\xi \in H^1(K, E[3])$ be the class corresponding to the 3-covering as in Lemma 4.1 with $C : X^3 + 3Y^3 + dZ^3 = 0$. Then $\xi \in \delta_3(E(K)[3])$ if any of the following hold:

1. $3 \in K^\times$;
2. $d' \in K^\times$;
3. $3d \in K^\times$;
4. $d \in K^\times$ and $K$ contains the 9th roots of unity; or
5. $d \in K^\times$ and $K$ contains a cube root of unity $\zeta_3$ such that $3\zeta_3 \in K^\times$.

**Corollary 4.3.** Suppose $d = 3d'$ and let $\xi \in H^1(\mathbb{Q}, E[3])$ be the class of the 3-covering in Lemma 4.2. Then $\text{res}_v(\xi) \in \delta_3(E(\mathbb{Q}_v)[3])$, for every prime $v \mid d$.

**Proof.** Suppose $v \nmid d$ and set $K = \mathbb{Q}_v$. By assumption, $d, d', 3,$ and $3d$ are units and, since $\mathbb{Z}_v^\times/\zeta_3^\times$ is cyclic, one of them must be a cube. Moreover, if $\mathbb{Q}_v$ does not contain a primitive cube root of unity, then they are all cubes (since $\mathbb{Z}_v^\times/\zeta_3^\times$ is trivial in this case). In light of this, and the first three cases in the lemma, we may assume $d \in \mathbb{Q}_v^\times$ and that $\mathbb{Z}_v$ contains a primitive cube root of unity $\zeta_3$. If $\zeta_3$ is a cube, then case 4 of the lemma applies. If $\zeta_3$ is not a cube, then the class of 3 is contained in the subgroup of $\mathbb{Q}_v^\times/\zeta_3^\times$ generated by $\zeta_3$, in which case 5 of the lemma applies. This establishes the corollary. $\square$
Proof of Lemma 4.2. By the discussion at the beginning of this section, it suffices to show that in each of these cases there is a $K$-rational point on $C$ which maps to a 3-torsion point on $E$.

Let $\xi$ be a primitive 9th root of unity and $d$ be a cube root of $d$. Then
\[(\sqrt[3]{d} : 1 : 0), (-\sqrt[3]{d} : 0 : 1), \text{ and } (0 : -\sqrt[3]{3d} : 3)\]
are defined over $K$, and the explicit formula for $\pi$ given in Lemma 4.1 shows that they map to $(1 : -1 : 0) \in E(K)[3]$.

In case (1) $K$ contains a primitive 9th root of unity $\zeta_9$ and a cube root $\sqrt[3]{d}$ of $d$. Then
\[\left((2\zeta_9^3 + \zeta_9^4 + \zeta_9^2 + 2\zeta_9)\sqrt[3]{d} : (-\zeta_9^3 + \zeta_9^2 + \zeta_9 - 1)\sqrt[3]{d} : -3\right) \in C(K),\]
and one can check that it maps under $\pi$ to the point $(0 : -\sqrt[3]{d} : 1)$. In case (5) $K$ contains cube roots $\sqrt[3]{d}$ and $\beta = \sqrt[3]{3\zeta_3}$, where $\zeta_3$ is a cube root of unity. One may check that $(\beta^2 \sqrt[3]{d} : \beta \sqrt[3]{d} : -3) \in C(K)$, and that this point maps under $\pi$ to the point $(\zeta^2 : -1 : 0)$. \[\square\]

5. The Examples for $p = 3$

Proposition 5.1. Let $E : x^3 + y^3 + 3z^3 = 0$ be the elliptic curve over $\mathbb{Q}$ with distinguished point $P_0 = (1 : -1 : 0)$, and let $P = (1523698559 : -2736572309 : 826803945) \in E(\mathbb{Q})$.

For every $n \geq 2$, $3^{n-1}P$ is locally divisible by $3^n$, but not divisible by $3^n$. In particular, the local-global principle for divisibility by $3^n$ in $E(\mathbb{Q})$ fails for every $n \geq 2$.

Proof. Let $C : X^3 + 3Y^3 + 10Z^3$ be the 3-covering of $E$ as in Lemma 4.1 and let $\xi \in \text{H}^1(\mathbb{Q}, E[3])$ be the corresponding cohomology class. One may check that the point $Q = (−11 : 3 : 5) \in C(\mathbb{Q})$ maps to $P$. Thus $\xi = \delta_3(P)$. By Corollary 4.3 $\text{res}_v(\xi) \in \delta_3(E(\mathbb{Q}_v)[3])$ for all primes $v \nmid 30$. Also, since $10 \in \mathbb{Q}_3^\times$ and 3 is a cube in both $\mathbb{Q}_2$ and $\mathbb{Q}_3$ the first two cases of Lemma 4.2 show that $\text{res}_v(\xi) \in \delta_3(E(\mathbb{Q}_v)[3])$ also for $v \mid 30$. On the other hand, $\xi \neq 0$ because $C(\mathbb{Q})$ does not contain a point lying on the subscheme defined by $XYZ = 0$. Since, $E(\mathbb{Q})[3] = 0$ the result follows by applying Lemma 2.3. \[\square\]

Remark 5.2. For any $d \in \{51, 132, 159, 213, 219, 246, 267, 321, 348, 402, 435\}$ the same argument applies, giving more examples where the local-global principle for divisibility by $3^n$ in $E(\mathbb{Q})$ fails for all $n \geq 2$.

Proposition 5.3. Let $d \in \{138, 165, 300, 354\}$ and let $E : x^3 + y^3 + 3z^3 = 0$ be the elliptic curve over $\mathbb{Q}$ with distinguished point $P_0 = (1 : -1 : 0)$. Then $\text{III}^1(\mathbb{Q}, E) \not\subset 9 \text{H}^1(\mathbb{Q}, E)$. In particular, the local-global principle for divisibility by $3^n$ in $\text{H}^1(\mathbb{Q}, E)$ fails for every $n \geq 2$.

Proof. Set $d' = d/3$. Let $C : X^3 + 3Y^3 + d'Z^3$ be the 3-covering of $E$ as in Lemma 4.1 and let $\xi \in \text{H}^1(\mathbb{Q}, E'[3])$ be the corresponding cohomology class. In all cases one easily checks that $d' \in \mathbb{Q}_3^\times$ and that $3 \in \mathbb{Q}_v^\times$ for all $v \mid d'$. So using the first two cases of Lemma 4.2 and Corollary 4.3 we see that $\text{res}_v(\xi) \in \delta_3(E(\mathbb{Q}_v)[3])$ for every prime $v$. Then, by Lemma 2.3 the image of $\xi$ in $\text{H}^1(\mathbb{Q}, E[9])$ lies in $\text{III}^1(\mathbb{Q}, E[9])$.

For these values of $d$, Selmer showed that $E(\mathbb{Q}) = \{(1 : -1 : 0)\}$ and $C(\mathbb{Q}) = \emptyset$. \[\square\]

The points given below were found with the assistance of the Magma computer algebra system described in [BGP97]. A Magma script verifying the claims here can be found in the source file of the arXiv distribution of this article.
nontrivial for every \( n \geq 2 \). Moreover, Selmer’s proof shows that \( 3\text{III}^1(\mathbb{Q}, E)[3^{\infty}] = 0 \). In particular \( \text{III}^1(\mathbb{Q}, E)[3^{\infty}] \) contains no nontrivial infinitely divisible elements. Thus we are in case (3) of Proposition 2.2 and conclude that there exists some element of \( \text{III}^1(\mathbb{Q}, E) \) which is not divisible by 9 in \( H^1(\mathbb{Q}, E) \).

\[
\square
\]

Remark 5.4. The argument in the proof above shows that \( C \in \text{III}^1(\mathbb{Q}, E) \), but does not show that \( C \notin 9H^1(\mathbb{Q}, E) \). Rather, the elements of \( \text{III}^1(\mathbb{Q}, E) \) which are proven not to be divisible by 9 in \( H^1(\mathbb{Q}, E) \) are those that are not orthogonal to \( C \) with respect to the Cassels-Tate pairing. See [Cre13, Theorem 4].

References

[Baš72] M. I. Bašmakov, Cohomology of Abelian varieties over a number field, Uspehi Mat. Nauk 27 (1972), no. 6(168), 25–66 (Russian). MR0399110 (53 #2961)

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput. 24 (1997), no. 3-4, 235–265, DOI 10.1006/jsco.1996.0125. Computational algebra and number theory (London, 1993). MR1484478

[Cas62a] J. W. S. Cassels, Arithmetic on curves of genus 1. III. The Tate-Šafarevič and Selmer groups, Proc. London Math. Soc. (3) 12 (1962), 259–296. MR0163913 (29 #1212)

[Cas62b] ______, Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung, J. Reine Angew. Math. 211 (1962), 95–112. MR0163915 (29 #1214)

[ČS13] Mirela Ciperiani and Jakob Stix, Weil–Châtelet divisible elements in Tate–Shafarevich groups II: On a question of Cassels, J. Reine Angew. Math. (2013). (to appear).

[CFO+08] J. E. Cremona, T. A. Fisher, C. O’Neil, D. Simon, and M. Stoll, Explicit \( n \)-descent on elliptic curves. I. Algebra, J. Reine Angew. Math. 615 (2008), 121–155, DOI 10.1515/CRELLE.2008.012. MR2384334 (2009g:11067)

[Cre13] Brendan Creutz, Locally trivial torsors that are not Weil-Châtelet divisible, Bull. Lond. Math. Soc., posted on 2013, DOI 10.1112/blms/bdt019, (to appear in print).

[DZ01] Roberto Dvornicich and Umberto Zannier, Local-global divisibility of rational points in some commutative algebraic groups, Bull. Soc. Math. France 129 (2001), no. 3, 317–338 (English, with English and French summaries). MR1881198 (2002k:14031)

[DZ04] ______, An analogue for elliptic curves of the Grunwald-Wang example, C. R. Math. Acad. Sci. Paris 338 (2004), no. 1, 47–50, DOI 10.1016/j.crma.2003.10.034 (English, with English and French summaries). MR2038083 (2004k:11088)

[DZ07] ______, On a local-global principle for the divisibility of a rational point by a positive integer, Bull. Lond. Math. Soc. 39 (2007), no. 1, 27–34, DOI 10.1112/blms/bdl002. MR2303515 (2007k:14030)

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, Cohomology of number fields, 2nd ed., Grundlehen der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008. MR2392026 (2008m:11223)

[PRV12] Laura Paladino, Gabriele Ranieri, and Evelina Viada, On local-global divisibility by \( p^n \) in elliptic curves, Bull. Lond. Math. Soc. 44 (2012), no. 4, 789–802, DOI 10.1112/blms/bds012. MR2967246

[PRV] ______, On the minimal set for counterexamples to the local-global principle, available at arXiv:1107.3431v1.

[Sel51] Ernst S. Selmer, The Diophantine equation \( ax^3 + by^3 + cz^3 = 0 \), Acta Math. 85 (1951), 203–362 (1 plate). MR0041871 (13,13c)

[Sil86] Joseph H. Silverman, The arithmetic of elliptic curves, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986. MR817210 (87g:11070)

[Tat63] John Tate, Duality theorems in Galois cohomology over number fields, Proc. Internat. Congr. Mathematicians (Stockholm, 1962), Inst. Mittag-Leffler, Djursholm, 1963, pp. 288–295. MR0175892 (31 #168)
