LOCAL-GLOBAL PRINCIPLES FOR WEIL-CHÂTELET DIVISIBILITY IN POSITIVE CHARACTERISTIC

BRENDAN CREUTZ AND JOSÉ FELIPE VOLOCH

Abstract. We extend existing results characterizing Weil-Châtelet divisibility of locally trivial torsors over number fields to global fields of positive characteristic. Building on work of González-Avilés and Tan, we characterize when local-global divisibility holds in such contexts, providing examples showing that these results are optimal. We give an example of an elliptic curve over a global field of characteristic 2 containing a rational point which is locally divisible by 8, but is not divisible by 8 as well as examples showing that the analogous local-global principle for divisibility in the Weil-Châtelet group can also fail.

1. Introduction

Let k be a global field and A/k an abelian variety. The flat cohomology group $\mathrm{H}^1(k, A)$ is called the Weil-Châtelet group. It parameterizes k-torsors under A and contains the Shafarevich-Tate group,

$$Ш(k, A) := \ker\left(\mathrm{H}^1(k, A) \to \prod \mathrm{H}^1(k_v, A)\right) ,$$

where the product runs over all completions k_v of k. It is conjectured that $Ш(k, A)$ is finite, and in particular that it contains no nontrivial divisible elements. Cassels asked whether the elements of $Ш(k, A)$ are divisible in the larger group $\mathrm{H}^1(k, A)$ [Cas62a, Problem 1.3]. Closely related to this is the question of whether, for given integers $r \geq 0$ and m, the map

$$\mathrm{H}^r(k, A)/m\,\mathrm{H}^r(k, A) \to \prod \mathrm{H}^r(k_v, A)/m\,\mathrm{H}^r(k_v, A) \tag{1.1}$$

is injective. Indeed, a positive answer to Cassels' question follows from the injectivity of these maps for $r = 1$ and $m \geq 1$. In the case that the characteristic p of k does not divide m this has been investigated in [Baš72, Cas62b, ÇS15, Cre13, Cre16, DZ01, DZ04, DZ07, LW, PRV12, PRV14]. In particular, when $p \nmid m$ it is known that the local-global principle for divisibility by m in $\mathrm{H}^r(k, A)$ holds (i.e., that the map in (1.1) is injective) in all of the following cases:

(1) $r \geq 2$ ([Cre16, Theorem 2.1]);
(2) A is an elliptic curve, and m is prime ([Cas62b, Lemma 6.1]);
(3) A is an elliptic curve over $\mathbb{Q}$ and $m = \ell^n$ is a power of a prime $\ell \geq 5$ [ÇS15] [PRV14, Corollary 4] and [LW, Theorem 24];
(4) A is an elliptic curve over a number field k and $m = \ell^n$ is a power of a sufficiently large prime, depending only on the degree of k [ÇS15, PRV12].

On the other hand, there are examples showing that that the local-global principle for divisibility by m in $\mathrm{H}^r(k, A)$ can fail in the following situations:

(5) $r = 0$, A is an abelian surface over $\mathbb{Q}$ and $m = 2$ [CF96, p. 61];
(6) $r = 0$, A is an elliptic curve over $\mathbb{Q}$ and $m = 2^n$ with $n \geq 2$ [DZ07];
(7) $r \in \{0, 1\}$, A is an abelian variety over $\mathbb{Q}$ and m is any prime number [Cre13];

(8) $r \in \{0,1\}$, A is an elliptic curve over $\mathbb{Q}$ and $m = 3^n$ with $n \geq 2$ [Cre16].

Moreover, in (7) and (8) the examples given for $r = 1$ satisfy $Ш(k, A) \not\subset m\,\mathrm{H}^1(k, A)$ showing that the answer to Cassels' original question is also no.

In this paper we are interested in these questions when $m = p^n$ is a power of the characteristic of k. In this case [GAT12, Proposition 3.5] shows that for an elliptic curve A/k, the local-global principle for divisibility by p^n in $\mathrm{H}^r(k, A)$ holds except possibly if $r \in \{0, 1\}$, $p = 2$ and $n \geq 3$ (for $r \geq 2$ see Lemma 4). Their results imply that the only possible counterexamples must be non-constant elliptic curves with j-invariant in k^8 (see Corollary 8 below). We show that this is sharp and, moreover, that Cassels' question has a negative answer over global fields of positive characteristic. Specifically we prove the following.

Theorem 1 (Proposition 15)**.** *There exists a non-isotrivial elliptic curve E over $k = \mathbb{F}_2(t)$ with $j(E) \in k^8$ such that $Ш(k, E) \not\subset 8\,\mathrm{H}^1(k, E)$.*

Theorem 2 (Proposition 16)**.** *There exists a non-isotrivial elliptic curve E over $k = \mathbb{F}_2(t)$ with $j(E) \in k^8$ such that the local-global principle for divisibility by 2^n in $E(k)$ fails for every $n \geq 3$.*

In Propositions 18 and 19 we give examples of isotrivial elliptic curves over global fields of characteristic 2 for which the local-global principle for divisibility by 8 can fail. Interestingly, such examples do not occur over $\mathbb{F}_2(t)$ (see Proposition 17).

All of the results above establishing the local-global principle for divisibility by m in $\mathrm{H}^0(k, A)$ and $\mathrm{H}^1(k, A)$ are obtained by showing that the group $Ш^1(k, A[m])$ (or its dual) of locally trivial classes in $\mathrm{H}^1(k, A[m])$ vanishes. Building on [GAT12], we give a necessary and sufficient criterion for the vanishing of $Ш^1(k, A[m])$ in the case that A is an elliptic curve (see Theorem 5). This allows to construct the examples in Theorems 1 and 2 demonstrating the failure of the local-global principle for divisibility in $\mathrm{H}^r(k, A)$. To obtain the stronger result of Theorem 1 that $Ш(k, A) \not\subset 8\,\mathrm{H}^1(k, A))$ we establish the following characterization of the divisibility of $Ш(k, A)$ in the Weil-Châtelet group.

Theorem 3. *Let A be an abelian variety over a global field k with dual abelian variety A^* and let m be an integer. An element $T \in Ш(k, A)$ lies in $m\,\mathrm{H}^1(k, A)$ if and only if the image of the map*

$$Ш^1(k, A^*[m]) \to Ш(k, A^*)$$

induced by the inclusion of group schemes $A^*[m] \subset A^*$ is orthogonal to T with respect to the Cassels-Tate pairing. In particular, $Ш(k, A) \subset m\,\mathrm{H}^1(k, A)$ if and only if the image of $Ш^1(k, A^*[m])$ lies in the divisible subgroup of $Ш(k, A^*)$.

The proof of this theorem is given in Section 4. It was first proved in [Cre13, Theorem 4] under the hypothesis that the characteristic of k does not divide m using the "Weil pairing definition" of the Cassels-Tate pairing from [PS99]. To handle the case that n is divisible by the characteristic we make use of duality theorems in flat cohomology developed in [Mil86, Chapter 3] and [GA09].

2. Locally trivial torsors and divisibility

The orthogonality condition in Theorem 3 holds trivially if $Ш^1(k, A^*[m]) = 0$. When this is the case more is true.

Lemma 4. *Maintain the notation from Theorem 3. Assume any of the following:*

(1) $r = 0$ *and* $\text{Ш}^1(k, A[m]) = 0$,
(2) $r = 1$ *and* $\text{Ш}^1(k, A^*[m]) = 0$, *or*
(3) $r \geq 2$.

Then the local-global principle for divisibility by m *holds in* $\mathrm{H}^r(k, A)$.

Proof. It suffices to prove this assuming $m = p^n$ is a prime power. When p does not divide the characteristic of k this is proven in [Cre16, Theorem 2.1]. So let us assume $\mathrm{char}(k) = p$. The sequence

$$0 \to A[p^n] \to A \xrightarrow{p^n} A \to 0 \tag{2.1}$$

is exact on the flat site and gives rise to an exact sequence in flat cohomology,

$$\mathrm{H}^r(k, A) \xrightarrow{(p^n)_*} \mathrm{H}^r(k, A) \to \mathrm{H}^{r+1}(k, A[p^n]) \,.$$

From this we see that the obstruction to an element of $\mathrm{H}^r(k, A)$ being divisible by p^n is a class in $\mathrm{H}^{r+1}(k, A[p^n])$. Therefore an element of $\mathrm{H}^r(k, A)$ that is locally, but not globally, divisible by p^n must give a nontrivial element of $\text{Ш}^{r+1}(k, A[p^n])$. In case (1) the conclusion follows immediately from this observation.

In case (2) the conclusion follows from this observation once one takes into account that there is a perfect pairing

$$\text{Ш}^1(k, A^*[p^n]) \times \text{Ш}^2(k, A[p^n]) \to \mathbb{Q}_p/\mathbb{Z}_p$$

[GA09, Theorem 1.1].

In case (3) the statement holds trivially because $\mathrm{H}^r(k, A)(p) = 0$. Indeed for $r = 2$ this is [GAT12, Lemma 3.3] and for $r \geq 3$ this follows from the fact that k has strict p-cohomological dimension 2 ([GS06, Prop. 6.1.9 and Prop. 6.1.2]) and the fact that $\mathrm{H}^r(k, A) = \mathrm{H}^r(\mathrm{Gal}(k), A(k_s))$ since A is smooth. □

In light of Theorem 3 and Lemma 4 we are interested in determining the group $\text{Ш}^1(k, A[p^n])$. The following theorem achieves this in the case that A is an elliptic curve. The proof uses results of [GAT12] cited in the introduction as well as a classical computation in the cohomology of finite groups used in the proof of the Grunwald-Wang Theorem.

Theorem 5. *Suppose* A *is an abelian variety over a global field* k *of characteristic* p *sith separable closure* k_s *such that* $A(k_s)[p^n]$ *is cyclic. Set* $K = k(A(k_s)[p^n])$ *and* $G = \mathrm{Gal}(K/k)$. *Then* $\text{Ш}^1(k, A[p^n]) = 0$, *unless* G *is noncyclic and not isomorphic to any of its decomposition groups, in which case* $\text{Ш}^1(k, A[p^n]) = \mathbb{Z}/2\mathbb{Z}$.

Remark 6. *When* E/k *is an ordinary elliptic curve with* $j(E) \notin k^p$, *a stronger statement is true: the restriction map* $\mathrm{H}^1(k, E[p^n]) \to \mathrm{H}^1(k_v, E[p^n])$ *is injective for any prime* v *of* k. *In the case* $n = 1$ *this follows from the existence of an injective map* $\mathrm{H}^1(k, E[p]) \hookrightarrow k$ *(functorial in* k*) (see [Ulm91, Vol90]). The result for general* n *follows by an induction argument suggested to us by Ulmer.*

Proof of Theorem 5. To ease notation, set $M = A[p^n]$. Then $K = k(M(k_s))$ and $G = \mathrm{Gal}(K/k)$. By the Main Theorem of [GAT12], $\text{Ш}^1(k, M) \simeq \text{Ш}^1(\mathrm{Gal}(k), M(k_s))$. The inflation map gives an exact sequence

$$0 \to \mathrm{H}^1(G, M(k_s)) \to \mathrm{H}^1(\mathrm{Gal}(k), M(k_s)) \to \mathrm{H}^1(\mathrm{Gal}(K), M(k_s)) \,.$$

The action of $\mathrm{Gal}(K)$ on $M(k_s)$ is trivial, so $Ш^1(\mathrm{Gal}(K), M(k_s)) = 0$ by Chebotarev's theorem. It follows that $Ш^1(\mathrm{Gal}(k), M(k_s))$ is isomorphic to

$$Ш^1(G, M) := \ker\left(\mathrm{H}^1(G, M(k_s)) \xrightarrow{\mathrm{res}_v} \prod_v \mathrm{H}^1(G_v, M(k_s))\right),$$

where $G_v \subset G$ denotes the decomposition group at the prime v and the product runs over all primes. Since every cyclic subgroup of G occurs as a decomposition group, Theorem 5 follows from the next lemma. □

Lemma 7. *Let $G \subset (\mathbb{Z}/p^n\mathbb{Z})^\times = \mathrm{Aut}(\mathbb{Z}/p^n\mathbb{Z})$ and let M be the G-module isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$ on which G acts in the canonical way.*

(1) If G is not cyclic, then $p = 2$, $n \geq 3$ and $-1 \in G$.
(2) $\mathrm{H}^1(G, M) = 0$ unless $p = 2$, $n \geq 3$ and $-1 \in G$, in which case $\mathrm{H}^1(G, M) \simeq \mathbb{Z}/2\mathbb{Z}$.
(3) If $G' \subsetneq G$ is a proper subgroup, then the restriction map $\mathrm{H}^1(G, M) \to \mathrm{H}^1(G', M)$ is the zero map.

Proof. (1) is easy and (2) is a well known computation (c.f. [NSW08, Lemma 9.1.4]). To prove (3) we may assume that $-1 \in G'$. Then we can write $G = \mu_2 \times \langle\alpha\rangle$, and $G' = \mu_2 \times \langle\alpha^k\rangle$, where $k = [G : G'] \geq 2$ and $\alpha \in 1 + 2^s u$ with $s \geq 2$ and u odd. Consider cohomology of the short exact of μ_2-modules,

$$0 \to M^{\langle\alpha\rangle} \xrightarrow{i} M^{\langle\alpha^k\rangle} \to Q \to 0,$$

where Q is the quotient. Since $M^G = M^{G'} = M^{\mu_2}$, this gives an exact sequence

$$0 \to Q^{\mu_2} \hookrightarrow \mathrm{H}^1(\mu_2, M^{\langle\alpha\rangle}) \xrightarrow{i_*} \mathrm{H}^1(\mu_2, M^{\langle\alpha^k\rangle})$$

We claim that all terms in this sequence have order 2, so $i_* = 0$. Indeed, $Q^{\mu_2} \simeq \mathbb{Z}/2\mathbb{Z}$, as Q is cyclic and contains an element of order 2 (since $2 \mid k$). The proof of (2) shows that the inflation map gives an isomorphism $\mathbb{Z}/2\mathbb{Z} \simeq \mathrm{H}^1(\mu_2, M^{\langle\alpha\rangle}) \simeq \mathrm{H}^1(G, M)$, and similarly for G'. Under these isomorphisms, the restriction map $\mathrm{H}^1(G, M) \to \mathrm{H}^1(G', M)$ is given by i_* which is the zero map. □

Corollary 8. *Suppose E is an elliptic curve over a global field k of characteristic p. Then the local-global principle for divisibility by p^n holds in $\mathrm{H}^r(k, E)$ except possibly if $r \in \{0, 1\}$, $p = 2$, $n \geq 3$, E is a non-constant ordinary elliptic curve and the j-invariant of E is an 8-th power.*

Proof. By Lemma 4, the local-global principle for divisibility by p^n can only fail for $r \in \{0, 1\}$ and then only when $Ш^1(k, E[p^n]) \neq 0$. Let $K = k(E[p^n](k_s))$, $G = \mathrm{Gal}(K/k)$ and suppose $Ш^1(k, E[p^n]) \neq 0$. By Theorem 5 G is not cyclic. By Lemma 7 we must have that the exponent of $E[p^n](k_s)$ is divisible by 8. This implies that $p = 2$, $n \geq 3$, $j(E) \in k^8$ and E is ordinary. Finally, if E is constant, then the p^n-torsion points are defined over a finite field and G is cyclic, a contradiction. □

For supersingular elliptic curves we have the following.

Lemma 9. *Suppose E is a supersingular elliptic curve over a global field k of characteristic p. Then $\mathrm{H}^1(k, E)$ is p-divisible.*

Proof. The p-torsion subgroup-scheme of E sits in an exact sequence

$$0 \to \alpha_p \to E[p] \to \alpha_p \to 0\,, \tag{2.2}$$

where α_p is the kernel of $F : \mathbb{G}_a \to \mathbb{G}_a$, defined by $F(x) = x^p$. Since $\mathrm{H}^i(k, \mathbb{G}_a) = 0$ for $i > 0$, we see that $\mathrm{H}^i(k, \alpha_p) = 0$ for $i \neq 1$. The long exact sequence associated to (2.1) then shows that $\mathrm{H}^2(k, E[p]) = 0$. So multiplication by p on $\mathrm{H}^1(k, E)$ is surjective. □

In the remainder of this section we collect various results that will be used to construct the examples in the following section.

Lemma 10. *Suppose E is an elliptic curve over a global field k of characteristic p and that $P \in E(k)$ is locally divisible by m, but not globally divisible by m. Then the image of P in $E(k)/mE(k)$ does not lie in the image of $E(k)_{tors}$.*

Proof. The assumption on P implies that its image under the connecting homomorphism $\delta : E(k)/mE(k) \to \mathrm{H}^1(k, E[m])$ is a nontrivial element of $\text{Ш}^1(k, E[m])$. By Theorem 5 we may assume that $m = 2^n$ and that there is some completion of k such that $E(k_v)$ contains no point of exact order 2^n. Now by way of contradiction suppose $P = 2^n Q + T$ with $Q \in E(k)$ and $T \in E(k)_{tors}$. The only nontrivial element of $\text{Ш}^1(k, E[m])$ has order 2, so $T \in E[2]$. Since P is locally divisible by 2^n, we can find $R \in E(k_v)$ such that $P = 2^n R$. But then $T = 2^n(R - Q)$ which shows that $R - Q$ is a point of order 2^{n+1} in $E(k_v)$ □

Proposition 11. *Let k be a global field of characteristic p and suppose $\text{Ш}^1(k, A[p^n]) \neq 0$. Then there exists a separable extension L/k and a point $P \in A(L)$ that is locally divisible by p^n, but not globally divisible by p^n.*

Remark 12. *Our proof is based on that of* [DZ07, Theorem 3] *which proves the result when p does not divide the characteristic of k.*

Proof. To ease notation, set $M = A[p^n]$. Let $\xi \in \text{Ш}^1(k, M)$ be a nonzero element. By the Main Theorem of [GAT12], ξ is in the image of the inflation map $\mathrm{H}^1(\mathrm{Gal}(k), M(k_s))$. In particular, a separable extension L/k kills ξ if and only if $M(L) \neq \emptyset$. The class $\xi \in \mathrm{H}^1(k, M)$ may be represented by an A-torsor $\pi : T \to A$ under M, (also called an M-covering of A). For any separable extension L/k, consider the exact sequence,

$$A(L)/p^n \overset{\delta}{\hookrightarrow} \mathrm{H}^1(L, A[p^n]) \to \mathrm{H}^1(L, A) = \mathrm{H}^1(\mathrm{Gal}(L), A(k_s))\,,$$

where the equality follows from the fact that A is smooth. The image of ξ in $\mathrm{H}^1(L, A)$ is trivial if and only if $T(L) \neq \emptyset$. When this is the case, $\mathrm{res}_L(\xi) = \delta(P)$ for some $P \in A(L)$. Therefore, to prove the proposition it suffices to find a separable extension L/k linearly disjoint from $K := k(M(k_s))$ such that $T(L) \neq \emptyset$.

Note that T is geometrically irreducible, since T_{k_s} is isomorphic to A_{k_s}. Therefore, T is k-birational to a hypersurface $H : f(x_1, \dots, x_s, y) = 0$, where $f \in k[x_1, \dots, x_s, y]$ is irreducible in $k_s[x_1, \dots, x_s, y]$ and separable in y. This follows from the fact that there is a separating basis for the function field of T over k [FJ86, Lemma 2.6.1]. Since global fields are Hilbertian [FJ86, Thm 13.4.2], there exist a Zariski dense set of $\mathbf{a} = (a_1, \dots, a_s) \in \mathbb{A}^s(k)$ such that $f(\mathbf{a}, y)$ is irreducible over K [FJ86, Corollary 12.2.3]. Adjoining a root of $f(\mathbf{a}, y)$ to k gives rise to a separable extension L/k such that $H(L) \neq \emptyset$ and $M(L) = \emptyset$. Since the set of such $\mathbf{a}$ is Zariski dense, we conclude that the same is true with T in place of H. □

Lemma 13. *Suppose k is a field of characteristic 2 and $E/k : y^2 + xy = x^3 + ax^2 + b$. Then $k(E[8]) = k(a^{1/8}, b^{1/8}, u, v)$, where $u^2 + u = a, v^2 + v = b$.*

Proof. It is clear that $k(b^{1/8}) \subset k(E[8])$, we just need to verify the separable part. First, the non-trivial 2-torsion point is $(0, b^{1/2})$. The 4-torsion is generated by $(b^{1/4}, b^{1/2} + ub^{1/4})$. So $k(E[4]) = k(b^{1/4}, u)$. Finally, to get the 8-torsion one needs to solve $w^2 + w = b^{1/4} + a$ in $k(b^{1/4}, u)$ by the formulas in e.g. [Vol90], which is equivalent to solving $v^2 + v = b$. □

Theorem 14 (Tate, Milne)**.** *Let E be an elliptic curve over a global field k of positive characteristic. Then*

- *(1) The rank of $E(k)$ is at most the analytic rank of E.*
- *(2) If E is isotrivial or if the analytic and algebraic ranks of E coincide, then*
  - *(a) $Ш(k, E)$ is finite and has the order predicted by the Birch and Swinnerton-Dyer conjectural formula.*
  - *(b) The Cassels-Tate pairing on $Ш(k, E)$ is nondegenerate.*

This theorem was proved by Tate [Tat64] except for the statements about the p-part of $Ш(k, E)$ above. Milne proved the corresponding results for the p-part in [Mil75] with the assumption that $p > 2$ as the necessary results in crystalline cohomology had this restriction at the time. The restriction was later lifted by Illusie [Ill79], allowing Milne's proof to extend to $p = 2$ as well.

3. Examples

In this section we give examples of elliptic curve over global fields of characteristic 2 for which the local-global principle for divisibility by powers of 2 fails.

Proposition 15. *For the elliptic curve $E : y^2 + xy = x^3 + t^8x^2 + (t^{16} + 1)/t^8$ over $k = \mathbb{F}_2(t)$ we have $Ш(k, E) \not\subset 8\,\mathrm{H}^1(k, E)$.*

Proof. By Lemma 13 we have $K := k(E[8]) = k(u, v)$, where $u^2 + u = t$, $v^2 + v = (t^2 + 1)/t$. Then $\mathrm{Gal}(K/k) \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$ and all decomposition groups are cyclic, so $Ш^1(k, E[8]) \neq 0$ by Theorem 5. This curve has analytic rank 0 so, by Theorem 14, $E(k)$ has rank 0, $Ш(k, E)$ is finite and the Cassels-Tate pairing is nondegenerate. By Lemma 10 we see that the map $Ш^1(k, E[8]) \to Ш(k, E)$ is injective, hence nonzero. The result then follows from Theorem 3. □

Proposition 16. *The elliptic curve $E : y^2 + xy = x^3 + t^8x^2 + 1/t^8$ over $k = \mathbb{F}_2(t)$ has Mordell-Weil group $E(k) \simeq \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ generated by the point $T = (0, 1/t^4)$ of order 2 and the point*

$$P = \left(\frac{t^4 + 1}{t^2}, \frac{t^{10} + t^8 + 1}{t^4}\right)$$

of infinite order. For every $n \geq 3$, the point $2^{n-1}P$ is locally divisible by 2^n, but is not globally divisible by 2^n.

Proof. The 8-division field is $k(E[8]) = k(u, v), u^2 + u = t, v^2 + v = 1/t$ by Lemma 13. All decomposition groups are cyclic, so $Ш^1(k, E[8]) \simeq \mathbb{Z}/2\mathbb{Z}$ by Theorem 5. The j-invariant of E is t^8, which is not a 16-th power. So $E[2^n](k_s) = E[8](k_s)$ and, hence, $Ш^1(k, E[2^n]) \simeq Ш^1(\mathrm{Gal}(k), E[2^n]) \simeq \mathbb{Z}/2\mathbb{Z}$, for all $n \geq 3$. A 2-descent on E shows that $Ш(k, E)[2] = 0$

(alternatively, the analytic rank and algebraic rank are both 1, so the order of $Ш(k,E)$ can be computed by the Birch and Swinnerton-Dyer conjectural formula by Theorem 14). It follows that the nontrivial element of $Ш^1(k,E[2^n])$ lies in the image of the injective map $\delta_{2^n}: E(k)/2^nE(k) \to \mathrm{H}^1(k,E[2^n])$. The point $2^{n-1}P$ represents the unique class of order 2 in $E(k)/2^nE(k)$ that is disjoint from the image of $E(k)_{tors}$. Hence $\delta_{2^n}(2^{n-1}P)$ is the nontrivial element of $Ш^1(k,E[2^n])$. ☐

The curves appearing in Propositions 15 and 16 are not isotrivial. The next proposition shows that the local-global principle for 2-divisibility holds for isotrivial elliptic curves over $\mathbb{F}_2(t)$.

Proposition 17. *If E is an isotrivial elliptic curve over $k = \mathbb{F}_2(t)$, then $Ш^1(k,E[2^n]) = 0$ for all $n \geq 1$.*

Proof. We can assume E is ordinary and not constant. Then E becomes constant after a nonconstant quadratic extension K/k and $K(E[2^n])$ is a constant extension of K. Since k has genus 0, there is some prime of k that ramified in K. Since $K(E[2^n])$ is a constant extension, there is a unique prime of $K(E[2^n])$ above v. Since $k(E[2^n]) \subset K(E[2^n])$, there is a unique prime above v in $k(E[2^n])$. Therefore the decomposition group of this prime in $k(E[2^n])$ is isomorphic to $\mathrm{Gal}(k(E[2^n])/k)$. Hence $Ш^1(k(E[2^n])) = 0$ by Theorem 5. ☐

There are, however, isotrivial curves over positive genus global fields of characteristic 2 for which the local-global principle for divisibility by powers of 2 can fail.

Proposition 18. *For the isotrivial elliptic curve $E: y^2 + xy = x^3 + t^8x^2 + \omega$ over the field $k = \mathbb{F}_4(t,s)$, where $s^2 + st = t^3 + 1, \omega^2 + \omega + 1 = 0$ we have $Ш(k,E) \not\subset 8\,\mathrm{H}^1(k,E)$.*

Proof. If $c^2 + c = t^8$, the change of variables $y = y + cx$ changes the curve to $y^2 + xy = x^3 + \omega$. The 8-torsion of the latter curve is defined over $\mathbb{F}_{16}$. So $k(E[8]) = k(u,v), u^2 + u = t, v^2 + v = \omega$, which is unramified over k and has no inert primes, so Theorem 5 applies, showing that $Ш^1(k,E[8]) \neq 0$. We show below that $E(k)$ is finite. Then by Lemma 10 the map $Ш^1(k,E[8]) \to Ш(k,E)$ is injective and nonzero. By Theorem 14, $Ш(k,E)$ is finite and the Cassels-Tate pairing on it is nondegenerate. We conclude that $Ш(k,E) \not\subset 8\,\mathrm{H}^1(k,E)$ by Theorem 3.

It remains to show that $E(k)$ is finite. Both k and $k(u,v)$ are function fields of isogenous elliptic curves and k is the function field of an elliptic curve over $\mathbf{F}_2$ with 4 points, so its eigenvalues of Frobenius are $(-1 \pm \sqrt{-7})/2$. On the other hand, E is a twist of $y^2 + xy = x^3 + \omega$ which is an elliptic curve over $\mathbf{F}_4$ with 6 points, so its eigenvalues of Frobenius are $(-1 \pm \sqrt{-15})/2$. The eigenvalues of the two curves live in different quadratic fields so they are not isogenous. Therefore $E(k)$ and $E(k(E[8]))$ are torsion. ☐

Proposition 19. *Let E/k be the isotrivial elliptic curve in Proposition 18. There is a finite extension L/k for which the local-global principle for divisibility by 8 fails in $E(L)$.*

Proof. This follows from Proposition 11. ☐

4. The proof of Theorem 3

First note that the second statement of the theorem follows from the first since it is known that the Cassels-Tate pairing annihilates only the divisible subgroups [Mil86, III.9.5] or [GA09, Theorem 1.2]. By [Cre13, Theorem 4] it suffices to prove the first statement in the case that $m = p^n$ is a power of the characteristic of k.

The sequence

$$0 \to A[p^n] \to A \xrightarrow{p^n} A \to 0$$

is exact on the flat site and gives rise to an exact sequence in flat cohomology. Let $\delta : \mathrm{H}^1(k, A) \to \mathrm{H}^2(k, A[p^n])$ be the boundary map arising from (2.1), and let $\iota : \text{Ш}^1(k, A^*[p^n]) \to \text{Ш}(k, A^*)$ be the map induced by the inclusion $A^*[p^n] \hookrightarrow A^*$. One has the Cassels-Tate pairing,

$$\langle\, ,\, \rangle_1 : \text{Ш}(k, A^*) \times \text{Ш}(k, A) \to \mathbb{Q}/\mathbb{Z}$$

(see [GA09, Theorem 1.2] and [Mil86, Theorem II.5.6 & Corollary III.9.5]) as well as a perfect pairing of finite groups

$$\langle\, ,\, \rangle_2 : \text{Ш}^1(k, A^*[p^n]) \times \text{Ш}^2(k, A[p^n]) \to \mathbb{Q}/\mathbb{Z}$$

(see [GA09, Theorem 1.1] and [Mil86, Theorem III.8.2 & Proposition II.4.13]). We claim that these pairings are compatible with δ and ι in the sense that for any $x \in \text{Ш}^1(k, A^*[p^n])$ and $y \in \text{Ш}(k, A)$,

$$\langle \iota(x), y\rangle_1 = \langle x, \delta(y)\rangle_2 \,.$$

The theorem follows from this claim, because $\langle\, ,\rangle_2$ is perfect, and x is divisible by p^n in $\mathrm{H}^1(k, A)$ if and only if $\delta(x) = 0$.

Let X be the unique smooth complete curve over the field of constants of k having function field k. For a sufficiently small open affine subscheme $U \subset X$, we may extend A and A^* to dual abelian schemes $\mathcal{A}$ and $\mathcal{A}^*$ over U. For $0 \le i \le 2$, there are pairings as in the following diagram.

$$\text{(4.1)}\qquad \begin{array}{llcccccc}
(24) & \{\, ,\, \}: & D^i(U, \mathcal{A}^*)(p) & \times & D^{2-i}(U, \mathcal{A})(p) & \to & \mathbb{Q}/\mathbb{Z} \\
 & & \downarrow & & \uparrow & & \| \\
(13) & \langle\, ,\, \rangle: & \mathrm{H}^i(U, \mathcal{A}^*)(p) & \times & \mathrm{H}_c^{2-i}(U, \mathcal{A})(p) & \to & \mathbb{Q}/\mathbb{Z} \\
 & & \uparrow\theta & & \downarrow\partial_c & & \downarrow \\
(12) & [\, ,\,]: & \mathrm{H}^i(U, \mathcal{A}^*[p^n]) & \times & \mathrm{H}_c^{3-i}(U, \mathcal{A}[p^n]) & \to & \mathbb{Q}_p/\mathbb{Z}_p \\
 & & \uparrow & & \downarrow & & \| \\
\text{Lemma 4.7} & (\, ,\,): & D^i(U, \mathcal{A}^*[p^n]) & \times & D^{3-i}(U, \mathcal{A}[p^n]) & \to & \mathbb{Q}_p/\mathbb{Z}_p
\end{array}$$

(The labels in the left column indicate where the pairing is defined in [GA09])

The injective (resp. surjective) maps from (resp. to) the $D^\bullet$ terms are the canonical maps given by the definition of these groups (op. cit. pages 211 and 221). The pairings $\{\, ,\}$ and $(\, ,\,)$ are induced by the other pairings via these maps. The maps θ and ∂_c are as in op. cit. Remark 5.3, which shows that they are compatible with the pairings. Therefore (4.1) is a commutative diagram of pairings. To prove the claim we use this in the case $i = 1$.

When U is sufficiently small the canonical map $\mathrm{H}^1(U, \mathcal{A}^*) \to \mathrm{H}^1(k, A^*)$ is injective (op. cit. Lemma 6.2), and $D^1(U, \mathcal{A}^*[p^n]) = \text{Ш}^1(k, A^*[p^n])$ (op. cit. Proposition 4.6). The map θ is induced by the inclusion $\mathcal{A}^*[p^n] \hookrightarrow \mathcal{A}^*$, so the image of $x \in \text{Ш}^1(k, A^*[p^n]) = D^1(U, \mathcal{A}^*[p^n])$ under the composition

$$D^1(U, \mathcal{A}^*[p^n]) \to \mathrm{H}^1(U, \mathcal{A}^*[p^n]) \xrightarrow{\theta} \mathrm{H}^1(U, \mathcal{A}^*) \hookrightarrow \mathrm{H}^1(k, \mathcal{A}^*)$$

is $\iota(x)$.

The map ∂_c sits in a commutative diagram with exact rows

$$
\begin{array}{ccccccc}
\mathrm{H}^1_c(U,\mathcal{A}) & \xrightarrow{p^n} & \mathrm{H}^1_c(U,\mathcal{A}) & \xrightarrow{\partial_c} & \mathrm{H}^2_c(U,\mathcal{A}[p^n]) & & \\
 & & \downarrow & & \downarrow & & \\
\mathrm{H}^1(U,\mathcal{A}) & \xrightarrow{p^n} & \mathrm{H}^1(U,\mathcal{A}) & \xrightarrow{\partial} & \mathrm{H}^2(U,\mathcal{A}[p^n]) & & \\
 & & & \searrow & & \searrow & \\
 & & \mathrm{H}^1(k,A) & \xrightarrow{p^n} & \mathrm{H}^1(k,A) & \xrightarrow{\delta} & \mathrm{H}^2(k,A[p^n])
\end{array}
\tag{4.2}
$$

(op. cit. proof of Lemma 5.6). The vertical maps in this diagram are the composition of the surjective maps in (4.1) with the canonical inclusions $D^\bullet(U,\star) \subset \mathrm{H}^\bullet(U,\star)$. For any U, the image of $D^2(U,\mathcal{A}[p^n])$ in $\mathrm{H}^2(k,\mathcal{A}[p^n])$ is equal to $\text{Ш}^2(k,A[p^n])$ (proof of op. cit. Proposition 4.5). Lemma 6.5 of op. cit. shows that, provided U is sufficiently small, $D^1(U,\mathcal{A}) = \text{Ш}(k,A)$. Taken together, this implies that if U is sufficiently small and $y' \in \mathrm{H}^1_c(U,\mathcal{A})$ is a lift of $y \in D^1(U,\mathcal{A}) = \text{Ш}^1(k,\mathcal{A})$, then the image of y' under the composition

$$\mathrm{H}^1_c(U,\mathcal{A}) \xrightarrow{\partial_c} \mathrm{H}^2_c(U,\mathcal{A}[p^n]) \to D^2(U,\mathcal{A}[p^n]) \to \text{Ш}^2(k,A[p^n])$$

is equal to $\delta(y)$.

Theorems 4.8 and 6.6 of op. cit. show that $\langle\, ,\,\rangle_1$ and $\langle\, ,\,\rangle_2$ are given by $\{\, ,\}$ and $(\, ,\,)$, respectively, provided U is taken to be sufficiently small. Thus we have $\langle \iota(x), y\rangle_1 = \langle x, \delta(y)\rangle_2$ as required. This completes the proof of Theorem 3.

Acknowledgements

We would like to thank D. Ulmer for the argument mentioned in remark 6. The second author would like to also thank the Simons Foundation (grant # 234591) for financial support.

References

[Baš72] M. I. Bašmakov, *Cohomology of Abelian varieties over a number field*, Uspehi Mat. Nauk **27** (1972), no. 6(168), 25–66 (Russian). ↑1

[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. ↑1

[Cas62b] ———, *Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung*, J. Reine Angew. Math. **211** (1962), 95–112. ↑1

[CF96] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus 2*, London Mathematical Society Lecture Note Series, vol. 230, Cambridge University Press, Cambridge, 1996. ↑1

[ÇS15] Mirela Çiperiani and Jakob Stix, *Weil-Châtelet divisible elements in Tate-Shafarevich groups II: On a question of Cassels*, J. Reine Angew. Math. **700** (2015), 175–207. ↑1

[Cre13] Brendan Creutz, *Locally trivial torsors that are not Weil-Châtelet divisible*, Bull. Lond. Math. Soc. **45** (2013), no. 5, 935–942. ↑1, 2, 8

[Cre16] ———, *On the local-global principle for divisibility in the cohomology of elliptic curves*, Math. Res. Lett. **23** (2016), no. 2, 377–387. ↑1, 2, 3

[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). ↑1

[DZ04] ———, *An analogue for elliptic curves of the Grunwald-Wang example*, C. R. Math. Acad. Sci. Paris **338** (2004), no. 1, 47–50 (English, with English and French summaries). ↑1

[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. ↑1, 5

[FJ86] Michael D. Fried and Moshe Jarden, *Field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 11, Springer-Verlag, Berlin, 1986. ↑5

[GS06] Philippe Gille and Tamás Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Studies in Advanced Mathematics, vol. 101, Cambridge University Press, Cambridge, 2006. ↑3

[GAT12] Cristian D. González-Avilés and Ki-Seng Tan, *On the Hasse principle for finite group schemes over global function fields*, Math. Res. Lett. **19** (2012), no. 2, 453–460. ↑2, 3, 5

[GA09] Cristian D. González-Avilés, *Arithmetic duality theorems for 1-motives over function fields*, J. Reine Angew. Math. **632** (2009), 203–231. MR2544149 ↑2, 3, 8

[Ill79] Luc Illusie, *Complexe de de Rham-Witt et cohomologie cristalline*, Ann. Sci. École Norm. Sup. (4) **12** (1979), no. 4, 501–661. ↑6

[LW] Tyler Lawson and Christian Wuthrich, *Vanishing of some cohomology groups for elliptic curves*, available at arXiv:1505.02940v2. ↑1

[Mil86] J. S. Milne, *Arithmetic duality theorems*, Perspectives in Mathematics, vol. 1, Academic Press, Inc., Boston, MA, 1986. ↑2, 7, 8

[Mil75] ———, *On a conjecture of Artin and Tate*, Annals of Mathematics. Second Series **102** (1975), no. 3, 517–533. ↑6

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, 2nd ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008. ↑4

[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. ↑1

[PRV14] ———, *On the minimal set for counterexamples to the local-global principle*, J. Algebra **415** (2014), 290–304. ↑1

[PS99] Bjorn Poonen and Michael Stoll, *The Cassels-Tate pairing on polarized abelian varieties*, Ann. of Math. (2) **150** (1999), no. 3, 1109–1149. ↑2

[Ser92] Jean-Pierre Serre, *Topics in Galois theory*, Research Notes in Mathematics, vol. 1, Jones and Bartlett Publishers, Boston, MA, 1992. Lecture notes prepared by Henri Damon [Henri Darmon]; With a foreword by Darmon and the author. ↑

[Sko01] Alexei Skorobogatov, *Torsors and rational points*, Cambridge Tracts in Mathematics, vol. 144, Cambridge University Press, Cambridge, 2001. ↑

[Tat64] John Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog* (1964), 415–440. Séminaire Bourbaki. Vol. 9, Exp. No. 306. ↑6

[Ulm91] Douglas L. Ulmer, *p-descent in characteristic p*, Duke Math. J. **62** (1991), no. 2, 237–265. ↑3

[Vol90] J. F. Voloch, *Explicit p-descent for elliptic curves in characteristic p*, Compositio Math. **74** (1990), no. 3, 247–258. ↑3, 6

School of Mathematics and Statistics, University of Canterbury, Private Bag 4800, Christchurch 8140, New Zealand

E-mail address: brendan.creutz@canterbury.ac.nz

URL: http://www.math.canterbury.ac.nz/~bcreutz

School of Mathematics and Statistics, University of Canterbury, Private Bag 4800, Christchurch 8140, New Zealand and Department of Mathematics, University of Texas, Austin, TX 78712, USA

E-mail address: felipe.voloch@canterbury.ac.nz

URL: http://www.math.canterbury.ac.nz/~f.voloch