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 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.

Introduction. Let G be a commutative algebraic group over a number field k, and let n and r be nonnegative integers. An element ξ in the Galois cohomology group $\mathrm{H}^r(k,G) := \mathrm{H}^r(\mathrm{Gal}(\overline{k}/k), G(\overline{k}))$ is divisible by n if there exists $\xi' \in \mathrm{H}^r(k,G)$ such that $n\xi' = \xi$. We say ξ is locally divisible by n if, for all primes v of k, there exists $\xi'_v \in \mathrm{H}^r(k_v, G)$ such that $n\xi'_v = \mathrm{res}_v(\xi)$. 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 p^n holds, except possibly when $p = 2$ and $n \geq 3$. A study of the problem for $r = 0$ and general G was initiated in [DZ01], with the case of elliptic curves studied in [DZ04, DZ07, PRV12]. For elliptic curves over $\mathbb{Q}$, their results show that the local-global principle holds for $n = 1$ or $p \geq 11$, and they have constructed counterexamples for $p^n = 4$.[1]

For $r \geq 2$ such questions are uninteresting, as nonarchimedean local fields have cohomological dimension 1. For $r = 1$ and G an elliptic curve, the question was in effect raised by Cassels [Cas62a, Problem 1.3]. In particular, he asked whether elements of $\mathrm{H}^1(k,G)$ that are everywhere locally trivial must be divisible. In response, Tate proved the local-global principle for divisibility by p, and while this did not fully answer the question it was sufficient for Cassels' immediate needs [Cas62b]. This and related questions also appear in Bašmakov [Baš72]. Çiperiani and Stix [ÇS13] recently considered the problem again showing 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 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 1. *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 defined over $\mathbb{Q}$ for which the local-global principle for divisibility by p^n fails in $\mathrm{H}^r(\mathbb{Q}, E)$.*

Notation. Throughout the paper p denotes a prime number, and n and r are nonnegative integers. As above, G is a 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 $\mathrm{Gal}(\overline{k}/k)$-module M, define

$$Ш^r(k,M) := \ker\left(\mathrm{H}^r(k,M) \xrightarrow{\prod \mathrm{res}_v} \prod_v \mathrm{H}^r(k_v, M)\right),$$

the product running over all primes of k.

Date: 17 May 2013.

[1] In a recent preprint Paladino et.al. give a proof of the local-global principle for powers of 5 and 7 as well [PRV].

The obstruction to the local-global principle for divisibility. The short exact sequence of $\mathrm{Gal}(\overline{K}/K)$-modules

$$0 \to G[n] \xrightarrow{\iota} G \xrightarrow{n} G \to 0$$

gives rise to a long exact sequence,

$$G(K) \xrightarrow{\delta_n} \mathrm{H}^1(K, G[n]) \xrightarrow{\iota_*} \mathrm{H}^1(K, G) \xrightarrow{n_*} \mathrm{H}^1(K, G) \xrightarrow{\delta_n} \mathrm{H}^2(K, G[n])\,. \tag{1}$$

Proposition 2. *Suppose G is an abelian variety, with dual $G^\vee$. If $Ш^1(k, G[n]) = 0$, then the local-global principle for divisibility by n holds in $G(k)$ and in $\mathrm{H}^1(k, G^\vee)$. Moreover, for every $\xi \in Ш^1(k, G[n])$, exactly one of the following hold:*

(1) $\xi = 0\,$;
(2) $\xi = \delta_n(\eta)$ *for some* $\eta \in G(k)$ *that is locally divisible by* n*, but is not divisible by* $n\,$; *or*
(3) $\iota_*(\xi) \neq 0$*, in which case* $\iota_*(\xi)$ *is divisible in* $Ш^1(k, G)$ *by all powers of* n*, or there exists* $\eta \in Ш^1(k, G^\vee)$ *such that* η *is not divisible by* n*.*

Remark 3. It is conjectured that $Ш^1(k, G)$ is always finite for abelian varieties, in which case there can be no nontrivial infinitely divisible elements as in case (3). Under this assumption the converse of the first statement in the proposition holds as well.

Proof. Exactness of (1) implies that an element $\eta \in \mathrm{H}^r(k, G)$ is locally divisible by n if and only if $\delta_n(\eta) \in Ш^{r+1}(k, G[n])$, and is divisible by n if and only if $\delta_n(\eta) = 0$. The same is obviously true if one replaces G by its dual. The first statement in the Proposition then follows from Tate's local duality theorems [Tat63, §2] which imply that $Ш^1(k, G[n]) \simeq Ш^2(k, G^\vee[n])$.

Exactness of (1) also implies that the cases in the second statement of the proposition are exhaustive and mutually exclusive. Moreover, if $\xi = \delta_n(\eta)$ as in case (2), then η is locally divisible by n, but not globally. For the claim in case (3) see [Cre13, Thm 3]. $\square$

The following proposition formalizes our method of constructing nontrivial classes in $Ш^1(k, G[p^n])$.

Lemma 4. *Let $\iota : G[p] \subset G[p^n]$ be the inclusion map. If $\xi \in \mathrm{H}^1(k, G[p])$ is such that $\mathrm{res}_v(\xi) \in \delta_p(G(k_v)[p])$ for all primes v, then*

(1) $\iota_*(\xi) \in Ш^1(k, G[p^n])$;
(2) $\iota_*(\xi) = 0$ *if and only* $\xi \in \delta_p(G(k)[p^{n-1}])$;
(3) if $\xi = \delta_p(\eta)$ *for some* $\eta \in G(k)$*, then* $p^{n-1}\eta$ *is locally divisible by* p^n*; and*
(4) if $\xi = \delta_p(\eta)$ *for some* $\eta \in G(k)$ *and* $\iota_*(\xi) \neq 0$*, then* $p^{n-1}\eta$ *is not divisible by* p^n*.*

Proof. The exact sequence $0 \to G[p] \xrightarrow{\iota} G[p^n] \xrightarrow{p} G[p^{n-1}] \to 0$ gives rise to a commutative diagram with exact rows:

$$\begin{array}{ccccc}
G(K)[p^{n-1}] & \xrightarrow{\delta_p} & \mathrm{H}^1(K, G[p]) & \xrightarrow{\iota_*} & \mathrm{H}^1(K, G[p^n]) \\
\downarrow{\scriptstyle \iota} & & \| & & \\
G(K) & \xrightarrow{\delta_p} & \mathrm{H}^1(K, G[p])\,. & &
\end{array}$$

This shows that, for $\xi \in \mathrm{H}^1(K, G[p])$, $\iota_*(\xi) = 0$ if and only if $\xi \in \delta_p(G(K)[p^{n-1}])$. The first two statements in the proposition follow easily. The last two statements are easily deduced from exactness and commutativity of the following diagram.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & G(K)[p] & \longrightarrow & G(K) & \xrightarrow{p} & G(K) & \xrightarrow{\delta_p} & \mathrm{H}^1(K, G[p]) \\
 & & \downarrow{\scriptstyle \iota} & & \| & & \downarrow{\scriptstyle p^{n-1}} & & \downarrow{\scriptstyle \iota_*} \\
0 & \longrightarrow & G(K)[p^n] & \longrightarrow & G(K) & \xrightarrow{p^n} & G(K) & \xrightarrow{\delta_{p^n}} & \mathrm{H}^1(K, G[p^n])
\end{array}$$

$\square$

The examples for $p = 2$.

Proposition 5. *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 $n \geq 2$, 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 6. This example was constructed by Dvornicich and Zannier who proved the proposition in the case $n = 2$ [DZ04, §4]. Using Lemma 4 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 δ_2 with isomorphism $\mathrm{H}^1(K, E[2]) \simeq \left(K^\times/K^{\times 2}\right)^2$ is given explicitly by

$$P = (x_0, y_0) \longmapsto \begin{cases} (x_0 - 1365, x_0 - 1430) & \text{if } P \neq P_1, P_2 \\ (-1, -65) & \text{if } P = P_1 \\ (65, 65) & \text{if } P = P_2 \\ (1, 1) & \text{if } P = 0 \end{cases} .$$

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. On the other hand, none are squares in $\mathbb{Q}$ and $E(\mathbb{Q})[2^\infty] = E(\mathbb{Q})[2]$. So the result follows from Lemma 4 $\square$

Proposition 7. *Let E be the elliptic curve defined by $y^2 = x(x+80)(x+205)$. Then $Ш^1(\mathbb{Q}, E) \not\subset 4\,\mathrm{H}^1(\mathbb{Q}, E)$. In particular, the local-global principle for divisibility by 2^n in $\mathrm{H}^1(\mathbb{Q}, E)$ fails for every $n \geq 2$.*

Proof. This is [Cre13, Theorem 5]. $\square$

n-coverings. The examples for $p = 2$ were constructed using an explicit description of the map

$$E(K) \xrightarrow{\delta_2} \mathrm{H}^1(K, E[2]) \simeq \left(K^\times/K^{\times 2}\right)^2 .$$

Another way to describe the connecting homomorphism is in the language of n-coverings. An n-covering of E is a morphism of curves, $\pi : C \to E$ defined over K such that there exists an isomorphism $\psi : E \to C$ defined over $\overline{K}$ such that $\pi \circ \psi = n$. Two n-coverings are isomorphic if there is an isomorphism of the covering curves which is compatible with the maps to E.

Theorem 8. *The set of isomorphism classes of n-coverings defined over K can be identified with the group $\mathrm{H}^1(K, E[n])$. Under this identification the connecting homomorphism δ_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 an n-covering $\pi : C \to E$ is equal to $\delta_n(P)$ if and only if $P \in \pi(C(K))$.

Proof. See [CFO$^+$08, §1]. $\square$

Diagonal cubic curves as 3-coverings. 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.

Lemma 9. *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*

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

is a 3-covering of E.

Proof. See [Sel51, Theorem 1] □

Lemma 10. *Suppose $d = 3d'$ and let $\xi \in \mathrm{H}^1(K, E[3])$ be the class corresponding to the 3-covering as in Lemma 9 with $C : x^3 + 3y^3 + d'z^3 = 0$. Then $\xi \in \delta_3(E(K)[3])$ if any of the following hold:*

(1) $3 \in K^{\times 3}$;
(2) $d' \in K^{\times 3}$;
(3) $3d \in K^{\times 3}$;
(4) $d \in K^{\times 3}$ *and K contains the 9th roots of unity; or*
(5) $d \in K^{\times 3}$, *K contains a cube root of unity ζ_3 such that $3\zeta_3 \in K^{\times 3}$.*

Corollary 11. *Suppose $d = 3d'$ and let $\xi \in \mathrm{H}^1(\mathbb{Q}, E[3])$ be the class of the 3-covering in Lemma 10. Then $\mathrm{res}_v(\xi) \in \delta_3(E(\mathbb{Q}_v)[3])$, for every prime $v \nmid d$.*

Proof. Suppose $v \nmid d$ and set $K = \mathbb{Q}_v$. By assumption $d, d', 3$, and $3d$ are units and, since $\mathbb{Z}_v^\times/\mathbb{Z}_v^{\times 3}$ 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 $\mathbb{Z}_v^\times/\mathbb{Z}_v^{\times 3}$ is trivial in this case). In light of this, and the first three cases in the lemma, we may assume $d \in \mathbb{Q}_v^{\times 3}$ and that $\mathbb{Z}_v$ contains a primitive cube root of unity ζ_3. If ζ_3 is a cube, then case (4) of the lemma applies. If ζ_3 is not a cube, then the class of 3 is contained in the subgroup of $\mathbb{Q}_v^\times/\mathbb{Q}_v^{\times 3}$ generated by ζ_3, in which case (5) of the lemma applies. This establishes the corollary. □

Proof of Lemma 10. By Theorem 8 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. The 3-torsion points are the intersections of E with the hyperplanes defined by $x = 0$, $y = 0$ and $z = 0$. In the first three cases (resp.) the points

$$(-\sqrt[3]{3} : 1 : 0)\,, \quad (-\sqrt[3]{d'} : 0 : 1)\,, \text{ and } \quad (0 : -\sqrt[3]{3d} : 3)$$

are defined over K, and the explicit formula for π given in Lemma 9 shows that they map to $(1 : -1 : 0) \in E(K)[3]$.

In case (4) K Contains a primitive 9th root of unity ζ_9 and a cube root $\sqrt[3]{d}$ of d. Then

$$\Big((2\zeta_9^5 + \zeta_9^4 + \zeta_9^2 + 2\zeta_9)\sqrt[3]{d} : (-\zeta_9^3 + \zeta_9^2 + \zeta_9 - 1)\sqrt[3]{d} : -3\Big) \in C(K)\,,$$

and one can check[2] that it maps under π 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 ζ_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 π to the point $(\zeta^2 : -1 : 0)$. □

[2]A `Magma` [BCP97] script verifying these claims can be found in the source file of the `arXiv` distribution of this article.

The examples for $p = 3$.

Proposition 12. *Let $E : x^3 + y^3 + 30z^3 = 0$ 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 9, and let $\xi \in \mathrm{H}^1(\mathbb{Q}, E[3])$ 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 11, $\mathrm{res}_v(\xi) \in \delta_3(E(\mathbb{Q}_v)[3])$ for all primes $v \nmid 30$. Also, since $10 \in \mathbb{Q}_3^{\times 3}$ and 3 is a cube in both $\mathbb{Q}_2$ and $\mathbb{Q}_5$ the first two cases of Lemma 10 show that $\mathrm{res}_v(\xi) \in \delta_3(E(\mathbb{Q}_v)[3])$ also for $v \mid 30$. On the other hand, $\xi \neq 0$ (one can check that $P \notin 3E(\mathbb{Q})$), and since $E(\mathbb{Q})[3] = 0$ the result follows from Lemma 4. $\square$

Remark 13. 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 divisibilitiy by 3^n in $E(\mathbb{Q})$ fails for all $n \geq 2$.

Proposition 14. *Let $d \in \{138, 165, 300, 354\}$ and let $E : x^3 + y^3 + dz^3 = 0$ be the elliptic curve over $\mathbb{Q}$ with distinguished point $P_0 = (1 : -1 : 0)$. Then $\text{Ш}^1(\mathbb{Q}, E) \not\subset 9\,\mathrm{H}^1(\mathbb{Q}, E)$. In particular, the local-global principle for divisibility by 3^n in $\mathrm{H}^1(\mathbb{Q}, E)$ 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 9, and let $\xi \in \mathrm{H}^1(\mathbb{Q}, E[3])$ be the corresponding cohomology class. In all cases one easily checks that $d' \in \mathbb{Q}_3^{\times 3}$ and that $3 \in \mathbb{Q}_v^{\times 3}$ for all $v \mid d'$. So using the first two cases of Lemma 10 and Corollary 11 we see that $\mathrm{res}_v(\xi) \in \delta_3(E(\mathbb{Q}_v)[3])$ for every prime v. Then, by Lemma 4, the image of ξ in $\mathrm{H}^1(\mathbb{Q}, E[9])$ lies in $\text{Ш}^1(\mathbb{Q}, E[9])$.

For these values of d, Selmer showed that $E(\mathbb{Q}) = \{(1 : -1 : 0)\}$ and $C(\mathbb{Q}) = \emptyset$ [Sel51, Theorem IX and Table 4b]. The latter implies that the image of ξ in $\text{Ш}^1(\mathbb{Q}, E[3^n])$ is nontrivial for every $n \geq 2$. Moreover, Selmer's proof shows that $3\text{Ш}^1(\mathbb{Q}, E)[3^\infty] = 0$. In particular $\text{Ш}^1(\mathbb{Q}, E)[3^\infty]$ contains no nontrivial infinitely divisible elements. Thus we are in case (3) of Proposition 2, and conclude that there exists some element of $\text{Ш}^1(\mathbb{Q}, E)$ which is not divisible by 9 in $\mathrm{H}^1(\mathbb{Q}, E)$. $\square$

Remark 15. The argument in the proof above shows that $C \in \text{Ш}^1(\mathbb{Q}, E)$, but does not show that $C \notin 9\,\mathrm{H}^1(\mathbb{Q}, E)$. Rather, the elements of $\text{Ш}^1(\mathbb{Q}, E)$ which are proven not to be divisible by 9 in $\mathrm{H}^1(\mathbb{Q}, E)$ are those that are not orthogonal to C with respect to the Cassels-Tate pairing.

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)

[ÇS13] Mirela Çiperiani 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., Grundlehren 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 (13,13i)

[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)

School of Mathematics and Statistics, The University of Sydney, NSW 2006, Australia
E-mail address: `brendan.creutz@maths.usyd.edu.au`
URL: `http://magma.maths.usyd.edu.au/~bcreutz`