Weil–Châtelet divisible elements in Tate–Shafarevich groups II: On a question of Cassels

MIRELA ÇIPERIANI AND JAKOB STIX

Abstract — For an abelian variety A over a number field k we discuss the divisibility in $\mathrm{H}^1(k, A)$ of elements of the subgroup $Ш(A/k)$. The results are most complete for elliptic curves over $\mathbb{Q}$.

Contents

1. Introduction

Let A be an abelian variety over an algebraic number field k with absolute Galois group Gal_k. We aim to determine whether elements of the Tate–Shafarevich group

$$Ш(A/k)$$

can become divisible in the Weil–Châtelet group $\mathrm{H}^1(k, A) = \mathrm{H}^1(k, A(k^{\mathrm{alg}}))$ with k^{alg} the algebraic closure of k, i.e., lie in the subgroup of divisible elements

$$\mathrm{div}(\mathrm{H}^1(k, A)) = \bigcap_{n\in\mathbb{N}} n\,\mathrm{H}^1(k, A).$$

This question was initially asked by Cassels in the case of elliptic curves (see [Ca62a] Problem 1.3) because an affirmative answer would imply that the kernel of the Cassels' pairing equals the maximal divisible subgroup of the Tate-Shafarevich group. This question appears again in [Ca62b] Problem (b) where Cassels completes his analysis of the kernel of Cassels' pairing but states that the question of the divisibility of $Ш(A/k)$ in $\mathrm{H}^1(k, A)$ remains open.

We will attempt to answer the above question one prime at a time. For a prime p we say that $Ш(A/k)$ is p-divisible in $\mathrm{H}^1(k, A)$ if

$$Ш(A/k) \subseteq p^n\,\mathrm{H}^1(k, A) \quad \text{for every } n \in \mathbb{N}.$$

In view of the conjectured finiteness of $Ш(A/k)$ which is known for elliptic curves over $\mathbb{Q}$ of analytic rank ≤ 1, the p-divisibility should be guaranteed for large p depending on A/k. Our aim therefore is to identify conditions that a prime number p must satisfy for the p-divisibility conclusion to hold, which are sufficient and as close as possible to being necessary.

For elliptic curves over $\mathbb{Q}$, Theorem 34 and Corollary 35 yield the following.

Theorem A. *Let $E/\mathbb{Q}$ be an elliptic curve defined over the rationals. Then the following holds.*

(1) *$Ш(E/\mathbb{Q})$ is p-divisible in $\mathrm{H}^1(\mathbb{Q}, E)$ for all primes $p > 7$.*
(2) *There is at most one odd prime number $p = 3, 5$ or 7, and then at most two quadratic twists $E^\tau/\mathbb{Q}$ of $E/\mathbb{Q}$, such that $Ш(E^\tau/\mathbb{Q})$ is not p-divisible in $\mathrm{H}^1(\mathbb{Q}, E^\tau)$.*
(3) *If $p = 5$ or 7 and $Ш(E/\mathbb{Q})$ is not p-divisible in $\mathrm{H}^1(\mathbb{Q}, E)$ then E has semistable reduction outside p.*

Date: February 19, 2013.
The authors acknowledge the hospitality and support provided by MATCH and the Newton Institute.
The first author was partially supported by NSF Grant DMS-07-58362 and by NSA Grant H98230-12-1-0208.

Note that our method can not handle the prime $p = 2$ and Brendan Creutz [Cr12] has now shown that for the elliptic curve $E : Y^2 = X(X + 80)(X + 205)$, labelled "1025b2" in Cremona's tables, $Ш(E/\mathbb{Q})$ is not divisible by 4 in $\mathrm{H}^1(\mathbb{Q}, E)$. More recently, Creutz found that divisibility by 9 fails for the elliptic curve $E : X^3 + Y^3 + 138Z^3 = 0$. The remaining cases $p = 5$ and $p = 7$ for elliptic curves over $\mathbb{Q}$ are open.

The essential content of Theorem 26 provides a uniform criterion for elliptic curves over an algebraic number field k that depends only on the degree of $k/\mathbb{Q}$. This is part (1) of Theorem B below, see Section §1.1.3 for the definition of $\pi(d)$; part (2) is proved as Corollary 30.

Theorem B. *Let E/k be an elliptic curve defined over an algebraic number field k of degree d over $\mathbb{Q}$. Then $Ш(E/k)$ is p-divisible in $\mathrm{H}^1(k, E)$ in the following two cases:*

(1) *For every prime number $p > \max\{(2^d + 2^{d/2})^2, \pi(d)\}$.*
(2) *If $p \geq 3$, the p-torsion subgroup $E_p \subseteq E$ is an irreducible Gal_k-representation, and $[k(\zeta_p) : k] \neq 2$ where ζ_p is a primitive p-th root of unity.*

Using the bound $\pi(d) < (1+3^{d/2})^2$ due to Oesterlé (unpublished), the bound in Theorem B (1) is simply $p > (2^d + 2^{d/2})^2$. For more on $\pi(d)$ we refer to Section §1.1.3.

Our method actually shows more. We define the **locally divisible** H^1 as the kernel

$$\mathrm{H}^1_{\mathrm{div}}(k, A) = \ker\Big(\mathrm{H}^1(k, A) \to \bigoplus_v \mathrm{H}^1(k_v, A)/\operatorname{div}\big(\mathrm{H}^1(k_v, A)\big)\Big)$$

containing the global cohomology classes which locally become divisible. Since the formation of $\operatorname{div}(-)$ is a functor, we find

$$\operatorname{div}(\mathrm{H}^1(k, A)) \subseteq \mathrm{H}^1_{\mathrm{div}}(k, A).$$

We now focus on the question of p-divisibility. Denote by M_{p^n} the p^n-torsion of an abelian group M and set $M_{p^\infty} = \cup_{n\in\mathbb{N}} M_{p^n}$. By local Tate duality we have that

$$\mathrm{H}^1(k_v, A) = \mathrm{Hom}(A^t(k_v), \mathbb{Q}/\mathbb{Z}),$$

where A^t denotes the dual abelian variety of A. Then Mattuck's theorem on the structure of $A^t(k_v)$ implies that $\operatorname{div}(\mathrm{H}^1(k_v, A)_{p^\infty}) = 0$ for $v \nmid p$. Hence, we have the following exact sequence

$$0 \to Ш(A/k)_{p^\infty} \to \mathrm{H}^1_{\mathrm{div}}(k, A)_{p^\infty} \to \bigoplus_{v|p} \operatorname{div}\big(\mathrm{H}^1(k_v, A)_{p^\infty}\big) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{\dim(A)\cdot[k:\mathbb{Q}]}. \tag{1.1}$$

The most general divisibility property that we prove can be viewed as a **local–to–global principle for p-divisibility** of elements in the Weil–Châtelet group with respect to certain p.

Theorem C. *Let A/k be an abelian variety over an algebraic number field, A^t its dual abelian variety, and p a prime number. If we assume that*

(i) *$\mathrm{H}^1(k(A^t_p)/k, A^t_p) = 0$, with the splitting field $k(A^t_p)$ of the p-torsion A^t_p of A^t, and*
(ii) *the Gal_k-modules A^t_p and $\mathrm{End}(A^t_p)$ have no common irreducible subquotient,*

in particular if $p \gg 0$, then $\operatorname{div}(\mathrm{H}^1(k, A))_{p^\infty} = \mathrm{H}^1_{\mathrm{div}}(k, A)_{p^\infty}$ holds and $Ш(A/k)$ is p-divisible in $\mathrm{H}^1(k, A)$.

In fact, Theorem A and Theorem B are, with the exception of two cases of elliptic curves $E/\mathbb{Q}$ with respect to $p = 11$, special cases of Theorem C. The proof of Theorem C and thus the answer to Cassels' divisibility question for almost all primes, actually follows immediately by Proposition 13 from Theorem D below (applied to A^t) and Theorem 23.

Theorem D is actually a local global principle, i.e., a vanishing result for $Ш^1(k, A_{p^n})$, see Section §2.1 for the definition, that might be of independent interest; for the proof see Theorem 19.

Theorem D. *Let A/k be an abelian variety over an algebraic number field, and let p be a prime number. Then*

$$Ш^1(k, A_{p^n}) = 0 \qquad \text{for all } n \geq 0,$$

if we assume that

(i) *$\mathrm{H}^1(k(A_p)/k, A_p) = 0$, with the splitting field $k(A_p)$ of the p-torsion A_p of A, and*
(ii) *the Gal_k-modules A_p and $\mathrm{End}(A_p)$ have no common irreducible subquotient.*

Our approach works also in the case when A/k is an abelian variety over the function field of a geometrically connected, smooth projective curve X over a finite field, at least with respect to divisibility questions for p distinct from the residue characteristic. However, since our current interest lies in the arithmetic case when k is an algebraic number field, we have not developed the geometric case in parallel.

Acknowledgments. The authors would like to thank Brian Conrad, Brendan Creutz, Wojciech Gajda, and Joseph Oesterlé for several useful discussions. The first author is also grateful to her advisor, Andrew Wiles, for introducing her to this method of thinking about the p-divisibility of the Tate-Shafarevich group.

1.1. **Notation.** We fix some notation which will be in use throughout the text.

1.1.1. Let k denote an algebraic number field with absolute Galois group Gal_k and ring of integers $\mathfrak{o}_k$. The completion of k at a place v is k_v. The finite places of k will be identified with the closed points of $X = \mathrm{Spec}(\mathfrak{o}_k)$.

1.1.2. Let M be an abelian group. The n-torsion subgroup is denoted by M_n, and M_{p^∞} denotes the p-primary torsion $\bigcup_n M_{p^n}$. The subgroup

$$\mathrm{div}(M) = \bigcap_{n\geq 1} nM$$

of divisible elements of M contains the maximal divisible subgroup of M

$$\mathrm{Div}(M) = \sum_{\varphi\in \mathrm{Hom}(\mathbb{Q},M)} \mathrm{im}(\varphi).$$

For matters of clarity we stress that **"a is p-divisible"** means that for every $n \geq 1$ there is a'_n with $a = p^n a'_n$. Observe that $\mathrm{div}(M)$ can be strictly larger than $\mathrm{Div}(M)$, as for example with $d \in \mathbb{N}$ in:

$$M = \big(\bigoplus_n \frac{1}{dn}\mathbb{Z}/\mathbb{Z}\big)/\ker\big(\mathrm{sum} : \bigoplus_n \frac{1}{d}\mathbb{Z}/\mathbb{Z} \to \frac{1}{d}\mathbb{Z}/\mathbb{Z}\big)$$

where $\mathrm{div}(M) = \frac{1}{d}\mathbb{Z}/\mathbb{Z}$ and $\mathrm{Div}(M) = 0$.

1.1.3. For every positive $d \in \mathbb{N}$, we define $\pi(d)$ to be the maximal prime number p such that there exists an elliptic curve E defined over a number field k of degree $d = [k : \mathbb{Q}]$, which admits a non-trivial k-rational p-torsion point.

Merel [Me94] showed that $\pi(d)$ is finite and gave the upper bound ($d > 1$)

$$\pi(d) < d^{3d^2}. \tag{1.2}$$

The best result in the literature to our knowledge is the bound by Parent [Pa99]

$$\pi(d) < 65 \cdot (3^d - 1) \cdot (2d)^6, \tag{1.3}$$

while an unpublished result of Oesterlé[1] yields the estimate

$$\pi(d) < (1 + 3^{d/2})^2. \tag{1.4}$$

For small values of d the following values of $\pi(d)$ are known precisely: Mazur in [Ma78] Theorem 2 shows $\pi(1) = 7$, Kamienny [Ka92] building on work of Kenku and Momose proves $\pi(2) = 13$, and Parent shows $\pi(3) = 13$ in [Pa00] with the prime 17 dealt with in [Pa03]. Unpublished work by Kamienny, Stein and Stoll (resp. together with Derickx) shows $\pi(4) = 17$ (resp. $\pi(5) = 19$).

[1]The improved bound for $\pi(d)$ due to Oesterlé from 1995 is unpublished. Moreover, Parent found a gap for $d = 3$ and $p = 43$, but was later able to repair the gap in [Pa00] under an arithmetic assumption which was a consequence of the Birch and Swinnerton-Dyer conjecture. Fortunately, this assumption was later proved by Kato. We thank J. Oesterlé for first hand information on his bound.

2. Reminder on global Galois cohomology

2.1. **Tate–Shafarevich groups and Poitou–Tate duality.** Let k be an algebraic number field and M a discrete Gal_k-module. We set

$$Ш^i(k, M) = \ker\Big(\mathrm{H}^i(k, M) \xrightarrow{\prod_v \mathrm{res}_v} \prod_v \mathrm{H}^i(k_v, M)\Big)$$

with the restriction maps res_v induced by the embedding $k \hookrightarrow k_v$, and the product ranges over all places v of k.

Let M be a finite Gal_k-module and $M^D := \mathrm{Hom}(M, \mu_\infty)$ its Cartier dual, here μ_∞ denotes the group of roots of unity in k^{alg}. Poitou–Tate duality yields a perfect pairing of finite groups

$$Ш^1(k, M) \times Ш^2(k, M^D) \to \mathbb{Q}/\mathbb{Z},$$

see [NSW08] VIII Theorem (8.6.7).

The Tate–Shafarevich group $Ш(A/k)$ for an abelian variety A over k is defined[2] as

$$Ш(A/k) = Ш^1(k, A(k^{\mathrm{alg}})),$$

and in particular is a torsion group. It follows that Cassels' question decomposes into p-primary parts. We will now concentrate on the p-primary part for a fixed prime number p.

2.2. **The Selmer group and generalized Selmer groups.** Let A/k be an abelian variety. The p^n-torsion Selmer group of A is defined as

$$\mathrm{H}^1_{\mathrm{Sel}}(k, A_{p^n}) = \ker\Big(\mathrm{H}^1(k, A_{p^n}) \to \prod_v \mathrm{H}^1(k_v, A)\Big)$$

with v ranging over all places of k. A diagram chase with the cohomology sequence of the Kummer sequence $0 \to A_{p^n} \to A \xrightarrow{p^n \cdot} A \to 0$ over k and all the localisations k_v yields the fundamental short exact sequence

$$0 \to A(k)/p^n A(k) \xrightarrow{\delta_{\mathrm{kum}}} \mathrm{H}^1_{\mathrm{Sel}}(k, A_{p^n}) \to Ш(A/k)_{p^n} \to 0. \tag{2.1}$$

It is known that $\mathrm{H}^1_{\mathrm{Sel}}(k, A_{p^n})$ is a finite group.

The Selmer group $\mathrm{H}^1_{\mathrm{Sel}}(k, A_{p^n})$ is a global H^1 with local Selmer-conditions determined by the image of the boundary map δ_{kum} of the Kummer sequence

$$\mathrm{Sel}_v = \delta_{\mathrm{kum}}\big(A(k_v)/p^n A(k_v)\big) \subset \mathrm{H}^1(k_v, A_{p^n})$$

at every place. We shall be working with the following generalized Selmer groups. Let Q be a finite set of finite places. The **Selmer group free at** Q is defined as

$$\mathrm{H}^1_{\mathrm{Sel}_Q}(k, A_{p^n}) = \ker\Big(\mathrm{H}^1(k, A_{p^n}) \to \prod_{v \notin Q} \mathrm{H}^1(k_v, A_{p^n})/\mathrm{Sel}_v\Big)$$

and the **Selmer group trivial at** Q is defined as

$$\mathrm{H}^1_{\mathrm{Sel}^Q}(k, A_{p^n}) = \ker\Big(\mathrm{H}^1(k, A_{p^n}) \to \prod_{v \notin Q} \mathrm{H}^1(k_v, A_{p^n})/\mathrm{Sel}_v \times \prod_{v \in Q} \mathrm{H}^1(k_v, A_{p^n})\Big).$$

Consequently, we have the following inclusions

$$\mathrm{H}^1_{\mathrm{Sel}^Q}(k, A_{p^n}) \subseteq \mathrm{H}^1_{\mathrm{Sel}}(k, A_{p^n}) \subseteq \mathrm{H}^1_{\mathrm{Sel}_Q}(k, A_{p^n}).$$

In the case when Q is the set of primes of k dividing p, we use $\mathrm{H}^1_{\mathrm{Sel}^p}(k, A_{p^n})$ (resp. $\mathrm{H}^1_{\mathrm{Sel}_p}(k, A_{p^n})$) to denote the Selmer groups $\mathrm{H}^1_{\mathrm{Sel}^Q}(k, A_{p^n})$ (resp. $\mathrm{H}^1_{\mathrm{Sel}_Q}(k, A_{p^n})$).

[2]Indeed, the traditional definition of $Ш(A/k)$ is equivalent due to the subtle equality

$$\mathrm{H}^1(k_v, A) = \mathrm{H}^1(k_v, A(k_v^{\mathrm{alg}})) = \mathrm{H}^1(k_v, A(k^{\mathrm{alg}})).$$

3. Subgroups of GL_2 over finite prime fields

The purpose of this section is to provide the following classification statement.

Theorem 1. *Let V be a vector space over $\mathbb{F}_p$ of dimension 2. For a subgroup $G \subseteq \mathrm{GL}(V)$ the following are equivalent.*

(1) (i) *V and $\mathrm{End}(V)$ have no common irreducible factor as G-modules, and*
(ii) $\mathrm{H}^1(G, V) = 0$.

(2) (i) *The group G is not contained in a subgroup of $\mathrm{GL}(V)$ that is isomorphic to the symmetric group S_3, in particular $p > 2$, and*
(ii) *If V is a reducible G-module, namely an extension*

$$0 \to \chi_1 \to V \to \chi_2 \to 0 \tag{3.1}$$

for characters $\chi_i : G \to \mathbb{F}_p^*$, then we require that $\chi_1 \neq \mathbf{1}, \chi_2^2$ and $\chi_2 \neq \mathbf{1}, \chi_1^2$.

The proof of Theorem 1 requires some preparation. We first recall the well known classification of subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$, see §2 of [Se72].

Proposition 2. *Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ and let $\overline{G}$ be the image under the natural map $\mathrm{GL}_2(\mathbb{F}_p) \to \mathrm{PGL}_2(\mathbb{F}_p)$. Then one of the following holds.*

(1) *$p \mid \#G$ and G is contained in a Borel $B \subset \mathrm{GL}_2(\mathbb{F}_p)$.*
(2) *$p \mid \#G$ and G contains $\mathrm{SL}_2(\mathbb{F}_p)$.*
(3) *$p \nmid \#G$ and G is contained in a normalizer of a split torus.*
(4) *$p \nmid \#G$ and G is contained in a normalizer of a non-split torus.*
(5) *$p \nmid \#G$ and $\overline{G}$ is isomorphic to A_4, S_4, or A_5.* □

3.1. **Computation of cohomology.** A p-Sylow subgroup P of $\mathrm{GL}(V)$ is mapped under a suitable isomorphism $\mathrm{GL}(V) \cong \mathrm{GL}_2(\mathbb{F}_p)$ induced by a choice of basis for V to the standard p-Sylow subgroup

$$U = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \ ; \ b \in \mathbb{F}_p \right\} \subset \mathrm{GL}_2(\mathbb{F}_p).$$

The normalizer N of P in $\mathrm{GL}(V)$ is mapped to the standard Borel subgroup

$$B = \left\{ \begin{pmatrix} a_1 & b \\ 0 & a_2 \end{pmatrix} \ ; \ a_1, a_2 \in \mathbb{F}_p^*, \ b \in \mathbb{F}_p \right\} \subseteq \mathrm{GL}_2(\mathbb{F}_p).$$

The two characters $\chi_i : N \to \mathbb{F}_p^*$ defined by the isomorphism $N \cong B$ and

$$\chi_i(\begin{pmatrix} a_1 & b \\ 0 & a_2 \end{pmatrix}) = a_i,$$

for $i = 1, 2$, occur in an exact sequence of N-modules

$$0 \to \chi_1 \to V \to \chi_2 \to 0. \tag{3.2}$$

The diagonal torus $T \subset B$ corresponds to a subgroup $S \subset N$ such that $N = P \rtimes S$ with S acting on P through the character

$$\chi_1/\chi_2 : S \subset N \to \mathbb{F}_p^* = \mathrm{Aut}(P).$$

For a subgroup $G \subset \mathrm{GL}(V)$ with $p \mid \#G$, up to conjugation, we may assume that $P \subset G$ and determine the normalizer $N_G(P)$ of P in G as $N \cap G$. The extension (3.2) restricts to an exact sequence as $N_G(P)$-modules in which by abuse of notation we write $\chi_i = \chi_i|_{N_G(P)}$. As before, the semi-direct product structure $N_G(P) = P \rtimes (S \cap G)$ has $S \cap G \cong N_G(P)/P$ acting on P via the character χ_1/χ_2.

Lemma 3. *(1) If $p \nmid \#G$, then $\mathrm{H}^1(G, V) = 0$.*
(2) If $p \mid \#G$, then the $N_G(P)$-equivariant quotient map $\varphi : V \twoheadrightarrow \chi_2$ induces an injection

$$\mathrm{H}^1(G, V) \hookrightarrow \mathrm{Hom}_{N_G(P)}(P, \chi_2).$$

In particular, then $\mathrm{H}^1(G, V) = 0$ except possibly if $\chi_1 = \chi_2^2$.

Proof: (1) is clear and only recalled for completeness. For (2), as the index of $N_G(P)$ in G is prime to p we have $\mathrm{H}^1(G,V) \hookrightarrow \mathrm{H}^1(N_G(P),V)$ so that we may assume $G = N_G(P)$. Since the index of P in G is prime to p, we find

$$\mathrm{H}^1(G,V) = \mathrm{H}^1(P,V)^{G/P}$$

and it remains to show that the map $\mathrm{H}^1(P,V) \to \mathrm{H}^1(P,\chi_2) = \mathrm{Hom}(P,\chi_2)$ is injective. We consider the long exact cohomology sequence for the extension (3.2). Since $\mathrm{H}^0(P,\chi_1) = \mathrm{H}^0(P,V)$, the connecting map

$$\delta : \mathbb{F}_p = \mathrm{H}^0(P,\chi_2) \to \mathrm{H}^1(P,\chi_1) = \mathrm{Hom}(P,\chi_1) \cong \mathbb{F}_p$$

is an isomorphism, and the map $\mathrm{H}^1(P,V) \to \mathrm{H}^1(P,\chi_2)$ is indeed injective. □

3.2. **When there are homotheties.** The center of $\mathrm{GL}(V)$ is the group $Z \cong \mathbb{F}_p^*$ of scalar automorphisms. We formulate a more general lemma, because later our proof of Theorem 23 depends on it.

Lemma 4. *Let W be a finite dimensional $\mathbb{F}_p$-vector space, and let $G \subset \mathrm{GL}(W)$ be a subgroup which intersects the center $\mathbb{F}_p^* \cong Z \subset \mathrm{GL}(W)$ non-trivially. Then the following holds.*

(1) *W and the adjoint representation $\mathrm{End}(W)$ have no common irreducible factor.*
(2) $\mathrm{H}^1(G,W) = 0$.

Proof: (1) The group $H = G \cap Z$ of homotheties in G acts trivially on every irreducible factor of $\mathrm{End}(W)$ and faithfully on every irreducible factor of W. Hence none of them can occur in both W and $\mathrm{End}(W)$.

(2) The inflation/restriction sequence for $H \lhd G$ reads

$$0 \to \mathrm{H}^1(G/H, W^H) \to \mathrm{H}^1(G,W) \to \mathrm{H}^1(H,W)^{G/H}.$$

Since H was assumed to be non-trivial and is necessarily of order prime to p, both W^H and $\mathrm{H}^1(H,W)$ vanish, and consequently also $\mathrm{H}^1(G,W) = 0$. □

Lemma 5. *Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ such that (5) of Proposition 2 holds. Then G meets the center Z of $\mathrm{GL}_2(\mathbb{F}_p)$ non-trivially.*

Proof: It suffices to discuss the case $\overline{G} = A_4$. If $G \cap Z = 1$, then we have a copy

$$A_4 \subseteq \mathrm{GL}_2(\mathbb{F}_p),$$

in particular $p > 2$. The 2-Sylow subgroup of A_4, the Klein 4-group $V_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, has a completely reducible representation theory already rationally over $\mathbb{F}_p$ as we may produce enough projectors already rationally over $\mathbb{F}_p$. Hence V_4 is contained in a split torus $C = \mathbb{F}_p^* \times \mathbb{F}_p^*$ and must agree with the 2-torsion of C. Thus V_4 already contains the central element

$$-1 \in \mathbb{F}_p^* \cong Z,$$

a contradiction. □

3.3. **The adjoint representation.** The action of the normalizer of a torus is best understood by identifying $V = A = \mathbb{F}_p[\alpha]$ with a separable quadratic $\mathbb{F}_p$-algebra. Then

$$\mathrm{Aut}(A/\mathbb{F}_p) = \mathbb{Z}/2\mathbb{Z},$$

of which we denote the generator by F (since it is the Frobenius if A is a field). Let us consider the associated normalizer of a torus $G = A^* \rtimes \langle F \rangle \subset \mathrm{GL}(V)$. We introduce two new G-module structures on V denoted

- A_0 with action factoring through $G \twoheadrightarrow \langle F \rangle$ followed by the F-action on $V = A_0$, and
- A_1 with action factoring through

$$G = A^* \rtimes \langle F \rangle \to A^* \rtimes \langle F \rangle = G$$

which maps F to F and $\lambda \in A^*$ to $\lambda/F(\lambda)$, followed by the defining action on $V = A_1$.

Lemma 6. *In the above notation,* $\mathrm{End}(V)$ *decomposes as a* $G = \mathbb{F}_p[\alpha]^* \rtimes \langle F \rangle$*-module as*

$$A_0 \oplus A_1 \xrightarrow{\sim} \mathrm{End}(V)$$
$$(a_0, a_1) \mapsto \big(v \mapsto a_0 v + a_1 F(v)\big).$$

Proof: We compute compatibility with F

$$(F(a_0), F(a_1)) \mapsto \big(v \mapsto F(a_0)v + F(a_1)F(v)\big) = F \circ \big(v \mapsto a_0 v + a_1 F(v)\big) \circ F^{-1}$$

and compatibility wtih $\lambda \in A^*$

$$(a_0, \frac{\lambda}{F(\lambda)} \cdot a_1) \mapsto \big(v \mapsto a_0 v + \frac{\lambda}{F(\lambda)} a_1 F(v)\big) = \big(v \mapsto \lambda \cdot (a_0(\lambda^{-1}v) + a_1 F(\lambda^{-1} \cdot v))\big).$$

Clearly, the map restricted to either A_i is injective. Since A^* acts trivially on A_0 but non-trivially on A_1 (except for the case $A = \mathbb{F}_2 \times \mathbb{F}_2$ were a direct computation confirms the lemma) this implies that the sum of the map still is injective. By comparing dimensions we deduce that it is an isomorphism. □

Lemma 7. *Let* V *be a reducible representation with characters* $\chi_i : G \to \mathbb{F}_p^*$ *for* $i = 1, 2$ *as irreducible factors. Then the irreducible factors of* $\mathrm{End}(V)$ *are* $\chi_1 \otimes \chi_2^{-1}, \mathbf{1}, \mathbf{1}$*, and* $\chi_2 \otimes \chi_1^{-1}$*.*

Proof: Choosing the right ordering we have a short exact sequence $0 \to \chi_1 \to V \to \chi_2 \to 0$. The dual $V^\vee$ then sits in the short exact sequence $0 \to \chi_2^{-1} \to V^\vee \to \chi_1^{-1} \to 0$, and tensoring the two sequences yields the desired decomposition of $\mathrm{End}(V) = V^\vee \otimes V$. □

We next address the special case where $G \cong S_3$.

Lemma 8. *If* $G \cong S_3$*, then* V *and* $\mathrm{End}(V)$ *have a common irreducible factor.*

Proof: We discuss the cases $p = 2$, $p = 3$ and $p \nmid \#G$ separately.

The case $p = 2$. Here a good model is $V = \mathbb{F}_4$ and $G = \mathrm{GL}_2(\mathbb{F}_2)$ acts as $\mathbb{F}_4^* \rtimes \mathrm{Gal}(\mathbb{F}_4/\mathbb{F}_2)$. As in Lemma 6 we denote the generator of $\mathrm{Gal}(\mathbb{F}_4/\mathbb{F}_2)$ in $\mathrm{GL}(V)$ by F. By Lemma 6 the map $V \to A_1$ which maps $v \mapsto F(v)$ is an isomorphism of V onto a direct summand of $\mathrm{End}(V)$. Indeed, for $\lambda \in \mathbb{F}_4^*$ we find

$$F(\lambda v) = \lambda^2 F(v) = \lambda^{-1} F(v) = \frac{\lambda}{F(\lambda)} F(v)$$

while the compatibility with F is obvious.

The case $p = 3$. Here the 3-cycle of $G = S_3$ must act after choosing a suitable basis as

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Therefore G is contained in the standard Borel. As S_3 is not abelian, the two characters $\chi : G \to \mathbb{F}_3^*$ by projecting to a diagonal entry must be distinct. Hence one is trivial and the other one is the sign character. By Lemma 7 the trivial character also occurs in $\mathrm{End}(V)$.

The case $p \nmid \#G$. By representation theory prime to p there is a unique faithful representation of dimension 2 of $G = S_3$ over $\mathbb{F}_p$. Namely, the 3-cycle lies in a torus C, either as

$$\begin{pmatrix} \zeta_3 & 0 \\ 0 & \zeta_3^{-1} \end{pmatrix}$$

in the split torus if $3 \mid p - 1$ (here ζ_3 denotes a primitive cubic root of unity), or as the 3-torsion of a nonsplit torus if $3 \mid p + 1$. With the notation of Lemma 6, a transposition agrees with the generator F of a spliting $N/C \to N$ for the normalizer N of the torus. The action on $A_1 \subset \mathrm{End}(V)$ is also faithful by the formula from Lemma 6 as otherwise F would fix the 3-cycle and $G = S_3$ would be commutative, a contradiction. The uniqueness of a faithful 2-dimensional representation for S_3 thus shows that $V \cong A_1 \subset \mathrm{End}(V)$ as G-representations. □

Corollary 9. *The determinant of the unique faithful* 2*-dimensional* S_3 *representation* V *over* $\mathbb{F}_p$ *is the mod* p *sign character* $\mathrm{sign} : S_3 \to \{\pm 1\} \subseteq \mathbb{F}_p^*$*.*

Proof: This follows from the discussion of this representation in the proof or Lemma 8. Alternatively, we can remark that the representation V is already defined over $\mathbb{Z}$ as the kernel $V_{\mathbb{Z}}$ of the natural map

$$\text{sum} \ : \ \text{ind}_{(2,3)}^{S_3}(\mathbf{1}) \to \mathbf{1}$$

which sums up the components in the natural basis of the tautological permutation representation. Then

$$\det(V_{\mathbb{Z}}) = \det(\text{ind}_{(2,3)}^{S_3}(\mathbf{1})) = \text{sign},$$

according to one of the definitions of the sign character. □

3.4. **Proof of Theorem 1.** By Lemma 8, both properties (1) and (2) fail if G is contained in a subgroup of $\mathrm{GL}(V)$ that is isomorphic to S_3. We thus may assume (i) of (2), and in particular that $p \geq 3$, since $\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$.

The case V reducible. Let V as a G-module be an extension of the character χ_2 by the character χ_1. By Lemma 7, the irreducible factors of $\mathrm{End}(V)$ as a G-module are $\chi_1 \otimes \chi_2^{-1}, \mathbf{1}$, and $\chi_2 \otimes \chi_1^{-1}$. So (i) of (1) holds if and only if $\chi_1 \neq \mathbf{1}, \chi_2^2$ and $\chi_2 \neq \mathbf{1}, \chi_1^2$, which is exactly what (ii) of (2) asks for. Moreover, Lemma 3 shows that (ii) of (1) follows from (ii) of (2).

The case V irreducible. Let $p \mid \#G$. As G is not contained in a Borel, we conclude by Proposition 2 that G contains $\mathrm{SL}_2(\mathbb{F}_p)$. Now as $p \geq 3$ the group G necessarily meets the center of $\mathrm{GL}(V)$ non-trivially, so that (1) holds by Lemma 4.

If $p \nmid \#G$ and the image of G in $\mathrm{PGL}_2(\mathbb{F}_p)$ is one of the exceptional cases A_4, S_4 or A_5, namely in case (5) of Proposition 2, then Lemma 5 and Lemma 4 show that (1) holds.

It remains to show (1) in the case that $p \nmid \#G$ and G is contained in the normalizer $N = C \rtimes \mathbb{Z}/2\mathbb{Z}$ of a torus $C \subset \mathrm{GL}_2(\mathbb{F}_p)$ and V is an irreducible G-module. Part (ii) of (1) holds trivially. Lemma 6 now tells us about the action of G on $\mathrm{End}(V)$. Let $H = G \cap C$ be the intersection with the torus, hence a subgroup in G of index ≤ 2. Because V is not a reducible G-module and $p \geq 3$ we have $\#G \geq 3$ and therefore $H \neq 1$.

If (1) part (i) fails, then in the decomposition $\mathrm{End}(V) = A_0 \oplus A_1$ of Lemma 6 we must have $V \cong A_1$, because H acts trivially on the first summand $A_0 \subset \mathrm{End}(V)$. The representation $V \otimes \mathbb{F}_{p^2}$ regarded as an H-module decomposes as a sum of characters $\chi_1 \oplus \chi_2$ of H. The representation $A_1 \subset \mathrm{End}(V)$ decomposes after scalar extension to $\mathbb{F}_{p^2}$ as H-module as $\chi_1\chi_2^{-1} \oplus \chi_2\chi_1^{-1}$. Comparing the two, we find either $\chi_1 = \mathbf{1} = \chi_2$, whence $H = 1$ contradicting the irreduciblity of V as a G-module. Or, $\chi_1 = \chi_2^2 \neq 1$ and $\chi_2 = \chi_1^2 \neq 1$ which means χ_1 and χ_2 are of order 3 and determine each other. In this case $H \cong \mathbb{Z}/3\mathbb{Z}$ and acts on V non-centrally and without a common fixed vector. In any case, split or non-split, the subgroup $H \subset C$ is normal but not central in N. Hence either $H = G$ and G can be embedded in a subgroup S_3 of $\mathrm{GL}(V)$, or $H \lhd G$ of index 2 and $G \cong S_3$ itself. In any case, this violates (i) of (2) and was excluded in the beginning of the proof. This completes the proof of Theorem 1. □

3.5. **Families of exceptional cases in GL_n.** In Theorem 1, the family of subgroups

$$S_3 \subseteq \mathrm{GL}_2(\mathbb{F}_p)$$

provides a family of exceptions, which according to the theorem is the only family (varying p) acting irreducibly in dimension $n = 2$ such that condition (2) fails. We would like to illustrate that this is only the tip of the iceberg when the dimension n grows.

Example 10. Let $G/\mathbb{Q}$ be a not necessarily connected linear algebraic group. By [GP03] Theorem 1, there is a simple finite dimensional algebra $A/\mathbb{Q}$, in general non-associative and non-commutative. Hence, we have a non-trivial bilinear map

$$m : A \otimes_{\mathbb{Q}} A \to A,$$

such that the $\mathbb{Q}$-algebraic group $\underline{\mathrm{Aut}}(A)$ is isomorphic over $\mathbb{Q}$ to G. We regard A as a (faithful) algebraic G-representation

$$G = \underline{\mathrm{Aut}}(A) \hookrightarrow \mathrm{GL}(A). \tag{3.3}$$

The adjoint to m with respect to the adjoint pair of functors $-\otimes_{\mathbb{Q}} A$ and $\mathrm{Hom}_{\mathbb{Q}}(A,-)$ on G-representations

$$m^{\#} : A \to \mathrm{Hom}_{\mathbb{Q}}(A,A) = \mathrm{End}(A)$$

is a non-trivial map of G-representations.

If we choose integral models for all structures involved, we can reduce mod p for almost all p and find another exceptional family of subgroups

$$G(\mathbb{F}_p) \subseteq \mathrm{GL}_n(\mathbb{F}_p)$$

with $n = \dim_{\mathbb{Q}}(A)$ such that Theorem 1 (2) fails.

It is not clear to us, whether the representations (3.3) in Example 10 are necessarily irreducible. However, also when we assume the representation to be irreducible, we are not spared of more exceptional cases.

Example 11. The monster finite simple group M is the largest sporadic simple group of order

$$|M| = 2^{46}\cdot 3^{20}\cdot 5^9\cdot 7^6\cdot 11^2\cdot 13^3\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 41\cdot 47\cdot 59\cdot 71 \approx 8\cdot 10^{53}.$$

It was predicted by Fischer and independently Griess in 1973 and later constructed by Griess [Gr82] as an automorphism group of the (real) Griess algebra

$$A = \mathbf{1}\oplus V$$

of dimension $1+196883$. The action on the 196883-dimensional piece V yields the smallest irreducible representation of M. The M-action on V preserves the non-trivial product

$$\mu : V\otimes V \subset A\otimes A \to A \to V$$

that is the V-component of the product of the Griess algebra $A\otimes A\to A$ projected to V. This product is defined over a ring R of finite type over $\mathbb{Z}$ and thus admits non-trivial specialisations to fields $\mathbb{F}_p$ for a positive Dirichlet density of primes p. In fact, by [Gr82] page 2, the irreducible character χ of V takes rational values, and therefore by the Brauer–Speiser Theorem [CR87] (74.27) has Schur index equal to 1. It can thus be defined over $\mathbb{Q}$ by [CR87] Theorem (74.5) (iii), and consequently, a non-trivial multiplication

$$\mu : V\otimes V \to V$$

can even be defined over $R=\mathbb{Q}$. Thus all but finitely many primes are ok. This shows that for dimension $n = 196883$ there is a series of exceptional subgroups

$$M \subset \mathrm{GL}_n(\mathbb{F}_p)$$

isomorphic to the monster group, where Theorem 1 (2) fails.

4. Vanishing of the Selmer group trivial at Q

We recall that k will always be an algebraic number field with ring of integers $\mathfrak{o}_k$.

4.1. **The obstruction for a local–global principle for divisibility.** Divisibility by p^n is controlled by an obstruction class as follows.

Lemma 12. *Let A/k be an abelian variety and let p be a prime number. For $n\in\mathbb{N}$ there is a short exact sequence*

$$0 \to \mathrm{H}^1_{\mathrm{div}}(k,A)_{p^\infty} \cap p^n\cdot \mathrm{H}^1(k,A) \to \mathrm{H}^1_{\mathrm{div}}(k,A)_{p^\infty} \xrightarrow{\delta_n} Ш^2(k,A_{p^n}). \tag{4.1}$$

Proof: The short exact sequence $0\to A_{p^n}\to A \xrightarrow{p^n\cdot} A\to 0$ of Gal_k-modules together with restriction to Gal_{k_v} yields a commutative diagram

$$\begin{array}{ccccc}
\mathrm{H}^1(k,A) & \xrightarrow{p^n\cdot} & \mathrm{H}^1(k,A) & \xrightarrow{\delta_n} & \mathrm{H}^2(k,A_{p^n}) \\
\downarrow & & \downarrow & & \downarrow \\
\mathrm{H}^1(k_v,A) & \xrightarrow{p^n\cdot} & \mathrm{H}^1(k_v,A) & \xrightarrow{\delta_n} & \mathrm{H}^2(k_v,A_{p^n}).
\end{array}$$

As classes in $\mathrm{H}^1_{\mathrm{div}}(k, A)$ are locally divisible, a diagram chase shows that $\delta_n(\mathrm{H}^1_{\mathrm{div}}(k, A))$ takes values in $Ш^2(k, A_{p^n})$. This proves the lemma. □

Proposition 13. *Let A/k be an abelian variety and let p be a prime number. If for $n \in \mathbb{N}$ with the dual abelian varity A^t we have $Ш^1(k, A^t_{p^n}) = 0$, then $\mathrm{H}^1_{\mathrm{div}}(k, A)_{p^\infty} \subseteq p^n \cdot \mathrm{H}^1(k, A)$.*

Proof: By Lemma 12 and Poitou–Tate duality, see [NSW08] VIII Theorem (8.6.7), the obstruction for divisibility by p^n lies in

$$Ш^2(k, A_{p^n}) = \mathrm{Hom}(Ш^1(k, A^t_{p^n}), \mathbb{Q}/\mathbb{Z}) = 0.$$

Now the proposition follows immediately from the exact sequence (4.1) of Lemma 12. □

Let Q be a finite set of primes. Then obviously

$$Ш^1(k, A^t_{p^n}) \subseteq \mathrm{H}^1_{\mathrm{Sel}^Q}(k, A^t_{p^n})$$

so that in view of Proposition 13 we can deduce divisibility by p^n from vanishing theorems for Selmer groups trivial at Q.

4.2. **The obstruction for divisibility in Cassels' question.** As far as Cassels' original question is concerned, namely the divisibility by p^n of only $Ш(A/k)$ instead of $\mathrm{H}^1_{\mathrm{div}}(k, A)$ in $\mathrm{H}^1(k, A)$, we can formulate a necessary and sufficient condition[3] as follows.

Proposition 14. *Let A/k be an abelian variety and let p be a prime number. For $n \in \mathbb{N}$ the following are equivalent.*

(i) $Ш(A/k) \subseteq p^n \cdot \mathrm{H}^1(k, A)$.
(ii) *The natural map $i_* : Ш^1(k, A^t_{p^n}) \to Ш(A^t/k)$ factors over* $\mathrm{Div}\big(Ш(A^t/k)\big)$.

Proof: By Lemma 12 assertion (i) is equivalent to the vanishing of the Kummer boundary map restricted to $Ш(A/k)$ which factors as

$$\delta : Ш(A/k)/\mathrm{Div}(Ш(A/k)) \to Ш^2(k, A_{p^n}). \tag{4.2}$$

Assertion (ii) is clearly equivalent to the vanishing of

$$Ш^1(k, A^t_{p^n}) \to Ш(A^t/k)/\mathrm{Div}(Ш(A^t/k)), \tag{4.3}$$

so that it remains to argue that (4.3) is the adjoint of (4.2) under the Poitou–Tate pairing $\langle -, - \rangle_{\mathrm{PT}}$ recalled in Section §2.1 and the Cassels–Tate pairing $\langle -, - \rangle_{\mathrm{CT}}$, since the latter is non-degenerate modulo the maximal divisible subgroup.

For $\alpha' \in Ш^1(k, A^t_{p^n})$ and $\alpha \in Ш(A/k)$ we compute the Cassels–Tate pairing of $i_*(\alpha')$ with α following basically the Weil-pairing definition of the Cassels–Tate pairing as in [PS99] §12.2. Instead of computing the boundary of α after choosing p^n large enough and lifting α to $\mathrm{H}^1(k, A_{p^n})$ with respect to

$$0 \to A_{p^n} \to A_{p^{2n}} \xrightarrow{p^n} A_{p^n} \to 0,$$

we can similarly compute the boundary directly with respect to

$$0 \to A_{p^n} \to A \xrightarrow{p^n} A \to 0.$$

Therefore $\langle i_*(\alpha'), \alpha \rangle_{\mathrm{CT}}$ depends only on α' and $\delta(\alpha)$, and the further formulae in [PS99] §12.2 translate immediately into the description of the Poitou–Tate pairing $\langle \alpha', \delta(\alpha) \rangle_{\mathrm{PT}}$ as is explicitly described in the paragraph above Theorem 4.20 in [Mi86]. This finishes the proof. □

Remark 15. (1) In this paper, assertion (ii) of Proposition 14 will always follow from the vanishing of $Ш^1(k, A_{p^n})$. Therefore, in all cases the more general assertion on divisibility properties of $\mathrm{H}^1_{\mathrm{div}}(k, A)$ will follow.

(2) It follows from (2.1) that we have a short exact sequence

$$0 \to \{a \in A(k); a \in p^n \cdot A(k_v) \text{ for all } v \}/p^n \cdot A(k) \to Ш^1(k, A_{p^n}) \to Ш(A/k)_{p^n} \tag{4.4}$$

[3]The statement of Proposition 14 was suggested to us by Brendan Creutz.

Cases where $\{a \in A(k); a \in p^n \cdot A(k_v) \text{ for all } v\ \} \neq p^n \cdot A(k)$ are known, even when $k = \mathbb{Q}$ and $A = E$ is an elliptic curve: see [DZ04] for $p^n = 4$, and more generally in [Pa10]. These examples yield in particular cases where

$$Ш^1(k, A_{p^n}) \neq 0,$$

but in view of Proposition 14 and (4.4) this does not imply that Cassels' question has a negative answer for A^t/k.

(3) Brendan Creutz in [Cr12] also proves Proposition 14 and uses it to show that for every prime p there exists an abelian variety $A/\mathbb{Q}$ such that $Ш(A/\mathbb{Q})$ is not divisible by p in $\mathrm{H}^1(\mathbb{Q}, A)$. Furthermore, he also finds an elliptic curve $E/\mathbb{Q}$ such that $Ш(E/\mathbb{Q})_2$ is not divisible by 4 in $\mathrm{H}^1(\mathbb{Q}, E)$.

4.3. **The Selmer splitting field.** Let A/k be an abelian variety. We denote by

$$\mathrm{H}^1_{\mathrm{Sel}}(k(A_p)/k, A_p)$$

the intersection of $\mathrm{H}^1_{\mathrm{Sel}}(k, A_p)$ with the image under inflation of $\mathrm{H}^1(k(A_p)/k, A_p)$ in $\mathrm{H}^1(k, A_p)$. Then we have the following commutative diagram with exact rows

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{H}^1_{\mathrm{Sel}}(k(A_p)/k, A_p) & \xrightarrow{\inf} & \mathrm{H}^1_{\mathrm{Sel}}(k, A_p) & \xrightarrow{\mathrm{res}} & \mathrm{Hom}_{\mathrm{Gal}(k(A_p)/k)}(\mathrm{Gal}^{\mathrm{ab}}_{k(A_p)} \otimes \mathbb{F}_p, A_p) \\
 & & \cap\mathrel{|} & & \cap\mathrel{|} & & \| \\
0 & \longrightarrow & \mathrm{H}^1(k(A_p)/k, A_p) & \xrightarrow{\inf} & \mathrm{H}^1(k, A_p) & \xrightarrow{\mathrm{res}} & \mathrm{H}^1(k(A_p), A_p)^{\mathrm{Gal}(k(A_p)/k)}
\end{array}$$

The restriction map defines a canonical continuous Gal_k-equivariant pairing

$$\mathrm{H}^1_{\mathrm{Sel}}(k, A_p) \times \left(\mathrm{Gal}^{\mathrm{ab}}_{k(A_p)} \otimes \mathbb{F}_p\right) \to A_p. \tag{4.5}$$

Let M denote the quotient of $\mathrm{Gal}^{\mathrm{ab}}_{k(A_p)} \otimes \mathbb{F}_p$ by the right kernel of the above pairing. The restriction map factors as follows

$$\mathrm{H}^1_{\mathrm{Sel}}(k, A_p) \to \mathrm{Hom}_{\mathrm{Gal}(k(A_p)/k)}(M, A_p) \subset \mathrm{Hom}_{\mathrm{Gal}(k(A_p)/k)}(\mathrm{Gal}^{\mathrm{ab}}_{k(A_p)} \otimes \mathbb{F}_p, A_p).$$

Observe that the finiteness of the Selmer group $\mathrm{H}^1_{\mathrm{Sel}}(k, A_p)$ implies that M is finite. Hence the quotient M corresponds to a finite Galois extension $L/k(A_p)$, that we call the **Selmer splitting field** of A with respect to the prime p, more precisely $M = \mathrm{Gal}(L/k(A_p))$. Since M is a quotient as $\mathrm{Gal}(k(A_p)/k)$-module, the field L is in fact Galois over k and $\mathrm{Gal}(k(A_p)/k)$ acts on M by conjugation after lifting under the quotient map $\mathrm{Gal}(L/k) \twoheadrightarrow \mathrm{Gal}(k(A_p)/k)$.

Lemma 16. *Let A/k be an abelian variety, and let L be the Selmer splitting field with respect to p. Then the following holds.*

(1) *The following sequence is exact:*

$$0 \to \mathrm{H}^1_{\mathrm{Sel}}(k(A_p)/k, A_p) \to \mathrm{H}^1_{\mathrm{Sel}}(k, A_p) \to \mathrm{Hom}_{\mathrm{Gal}(k(A_p)/k)}(\mathrm{Gal}(L/k(A_p)), A_p) \tag{4.6}$$

(2) *Every irreducible $\mathrm{Gal}(k(A_p)/k)$-module subquotient of $\mathrm{Gal}(L/k(A_p))$ is isomorphic to an irreducible subquotient of A_p.*

Proof: (1) follows from the definition of L. For (2) we note that pairing 4.5 yields an injective map

$$\mathrm{Gal}(L/k(A_p)) = M \hookrightarrow \mathrm{Hom}(\mathrm{H}^1_{\mathrm{Sel}}(k, A_p), A_p) \cong A_p \oplus \ldots \oplus A_p \tag{4.7}$$

of $\mathrm{Gal}(k(A_p)/k)$-modules, where $\mathrm{H}^1_{\mathrm{Sel}}(k, A_p)$ carries the trivial action. □

4.4. **The vanishing of some generalized Selmer groups.**

Proposition 17. *Let A/k be an abelian variety, and let p be a prime number, such that*

(i) $\mathrm{H}^1(k(A_p)/k, A_p) = 0$.

Let Q be a finite set of finite primes of k not dividing p, and fix $n \in \mathbb{N}$ such that

(ii) *A has good reduction at v for all $v \in Q$;*

(iii) *the set of Frobenius elements* $\mathrm{Frob}_w \in \mathrm{Gal}(L/k(A_p))$ *where* L *is the Selmer splitting field of* A/k *with respect to* p *and* w *denotes a prime of* $k(A_p)$ *dividing* v*, when* v *ranges over* Q*, generates* $\mathrm{Gal}(L/k(A_p))$ *as a* $\mathrm{Gal}(k(A_p)/k)$*-module;*

(iv) $A_{p^n}(k_v)$ *is a free* $\mathbb{Z}/p^n\mathbb{Z}$*-module for all* $v \in Q$*.*

Then for all $m \leq n$ *we have that*

$$\mathrm{H}^1_{\mathrm{Sel}^Q}(k, A_{p^m}) = 0.$$

Proof: Step 1: We first treat $m = 1$. We set $k_1 = k(A_p)$, and $k_{1,w}$ for the completion of $k(A_p)$ in w. Localization at v yields a commutative diagram

$$\begin{array}{ccc} \mathrm{H}^1_{\mathrm{Sel}}(k, A_p) & \xrightarrow{\mathrm{res}_{k_1/k}} & \mathrm{Hom}_{\mathrm{Gal}(k_1/k)}(\mathrm{Gal}(L/k_1), A_p) \\ \downarrow & & \downarrow{\scriptstyle \mathrm{ev}_w} \\ \mathrm{H}^1_{\mathrm{nr}}(k_v, A_p) & \xrightarrow{\mathrm{res}_{k_{1,w}/k_v}} & \mathrm{H}^1_{\mathrm{nr}}(k_{1,w}, A_p) = A_p \end{array}$$

with the evaluation map ev_w mapping a morphism $\varphi : \mathrm{Gal}(L/k_1) \to A_p$ to its value $\varphi(\mathrm{Frob}_w)$ at the Frobenius element of w. Assumption (iii), the sequence (4.6), and assumption (i) imply

$$\mathrm{H}^1_{\mathrm{Sel}^Q}(k, A_p) \subseteq \mathrm{H}^1_{\mathrm{Sel}}(k(A_p)/k, A_p) \subseteq \mathrm{H}^1(k(A_p)/k, A_p) = 0.$$

Step 2: We now show the general case by induction on m terminating in n. As an abbreviation we set

$$\mathbb{L}_{m,v} = \mathrm{Sel}^Q_v \subseteq \mathrm{H}^1(k_v, A_{p^m})$$

for the Selmer condition trivial at Q for A_{p^m}-coefficients. Then the following diagram is commutative and the rows are exact

$$\begin{array}{ccccccccc} & & \mathbb{L}_{m-1,v} & \longrightarrow & \mathbb{L}_{m,v} & \longrightarrow & \mathbb{L}_{1,v} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{H}^1(k_v, A_{p^{m-1}})/\delta_{\mathrm{kum}}\big(A_p(k_v)\big) & \longrightarrow & \mathrm{H}^1(k_v, A_{p^m}) & \xrightarrow{p^{m-1}\cdot} & \mathrm{H}^1(k_v, A_p) & & \end{array} \tag{4.8}$$

The snake lemma applied to (4.8) yields that in the commutative diagram

$$\begin{array}{ccccccc} A_p(k) & \xrightarrow{\delta_{\mathrm{kum}}} & \mathrm{H}^1(k, A_{p^{m-1}}) & \longrightarrow & \mathrm{H}^1(k, A_{p^m}) & \longrightarrow & \mathrm{H}^1(k, A_p) \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ \prod_v A_p(k_v) & \xrightarrow{\delta_{\mathrm{kum}}} & \prod_v \frac{\mathrm{H}^1(k_v, A_{p^{m-1}})}{\mathbb{L}_{m-1,v}} & \longrightarrow & \prod_v \frac{\mathrm{H}^1(k_v, A_{p^m})}{\mathbb{L}_{m,v}} & \longrightarrow & \prod_v \frac{\mathrm{H}^1(k_v, A_p)}{\mathbb{L}_{1,v}} \end{array} \tag{4.9}$$

the bottom row is exact. The map δ_{kum} in the bottom row is the zero map: by assumption (iv) when $v \in Q$, then $A_{p^m}(k_v)/A_{p^{m-1}}(k_v) \to A_p(k_v)$ is surjective for $m \leq n$, or, in general for $v \notin Q$, by comparing the boundary maps for the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_{p^{m-1}} & \longrightarrow & A_{p^m} & \xrightarrow{p^{m-1}\cdot} & A_p & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A_{p^{m-1}} & \longrightarrow & A & \xrightarrow{p^{m-1}\cdot} & A & \longrightarrow & 0 \end{array}$$

(It is the limitation of assumption (iv) that forces the induction to terminate at n). Again the snake lemma applied to (4.9), more precisely a diagram chase, yields exactness of

$$\mathrm{H}^1_{\mathrm{Sel}^Q}(k, A_{p^{m-1}}) \to \mathrm{H}^1_{\mathrm{Sel}^Q}(k, A_{p^m}) \to \mathrm{H}^1_{\mathrm{Sel}^Q}(k, A_p)$$

so that with Step 1 we deduce the theorem by induction on m. □

Remark 18. It seems difficult to set up an inductive argument to prove $Ш^1(k, A_{p^m}) = 0$ for all $m \leq n$ directly.

We are now ready to give a proof of Theorem D from the introduction.

Theorem 19. *Let A/k be an abelian variety over an algebraic number field, and let p be a prime number. Then*

$$Ш^1(k, A_{p^n}) = 0$$

for all $n \geq 0$, if we assume that

(i) $\mathrm{H}^1(k(A_p)/k, A_p) = 0$, *with the splitting field $k(A_p)$ of the p-torsion A_p of A, and*
(ii) *the Gal_k-modules A_p and $\mathrm{End}(A_p)$ have no common irreducible subquotient.*

Proof: We are going to show that an auxiliary finite set of finite primes Q exists (depending on n) such that conditions (ii)–(iv) of Proposition 17 hold. Then

$$Ш^1(k, A_{p^n}) \subseteq \mathrm{H}^1_{\mathrm{Sel}^Q}(k, A_{p^n}) = 0$$

by Proposition 17 proves the theorem.

First we prove that the Selmer splitting field L of A/k and $k(A_{p^n})$ are linearly disjoint over $k(A_p)$. Indeed, let $K = L \cap k(A_{p^n})$ be their intersection and set $\overline{M} = \mathrm{Gal}(K/k(A_p))$ for the abelian Galois group over $k(A_p)$. Then, since K/k is Galois, the projection

$$\mathrm{Gal}(L/k(A_p)) \twoheadrightarrow \overline{M}$$

is a surjection of $\mathrm{Gal}(k(A_p)/k)$-modules. It follows from Lemma 16 that $\overline{M}$ has a composition series as $\mathrm{Gal}(k(A_p)/k)$-module consisting of irreducible subquotients of A_p. On the other hand, the group $\mathrm{Gal}(k(A_{p^n})/k(A_p))$ is a subgroup of

$$N = \ker\big(\mathrm{GL}(A_{p^n}) \to \mathrm{GL}(A_p)\big).$$

The group N is solvable with abelian subquotients

$$N_m = \ker\big(\mathrm{GL}(A_{p^m}) \to \mathrm{GL}(A_{p^{m-1}})\big)$$

that are canonically $\mathrm{Gal}(k(A_p)/k)$-modules and isomorphic to the adjoint representation of $\mathrm{Gal}(k(A_p)/k)$ on $\mathrm{End}(A_p)$. Since, by assumption, A_p and $\mathrm{End}(A_p)$ share no irreducible subquotient, we deduce that $\overline{M} = 0$ and $K = k(A_p)$, which means that L and $k(A_{p^n})$ are linearly disjoint over $k(A_p)$.

The Chebotarev density theorem enables us to choose a finite set Q of finite places $v \nmid p$ in the locus of good reduction of A/k, so that the Frobenius elements Frob_v for $v \in Q$ satisfy

(a) the image of Frob_v in $\mathrm{Gal}(k(A_{p^n})/k)$ is trivial,
(b) the images of Frob_v for $v \in Q$ generate $\mathrm{Gal}(L/k(A_p))$.

The linear disjointness of L and $k(A_{p^n})$ over $k(A_p)$ implies that (a) and (b) do not contradict each other. This shows (ii)–(iv) of Proposition 17 for the set Q and concludes the proof. □

Remark 20. Let A/k be an abelian variety over a number field k, and let $n \in \mathbb{N}$. In [DZ01] Dvornicich and Zannier started the investigation, actually for general commutative algebraic groups, of whether an element $a \in A(k)$ that is locally divisible by n in $A(k_v)$ for (almost) all places v of k must necessarily be globally divisible by n, i.e, $a \in nA(k)$. The vanishing criterion of Theorem 19 above together with the exact sequence (4.4) gives a criterion for the equality

$$\{a \in A(k);\ a \in p^n \cdot A(k_v) \text{ for all } v\ \} = p^n \cdot A(k) \tag{4.10}$$

to hold for a prime number p and all $n \geq 1$. Below in Section §5 we will verify this criterion in various cases for elliptic curves and thus reprove results obtained on cases where (4.10) holds, namely [PRV12] Corollary 2.

4.5. **The criterion in the case of elliptic curves.** Based on the group theory of GL_2 in Section §3 we can show the following criterion for a p-primary local–to–global principle for divisibility in the special case of elliptic curves.

Theorem 21. *Let E/k be an elliptic curve and let p be a prime number. We assume that the following holds for $G = \mathrm{Gal}(k(E_p)/k) \subseteq \mathrm{GL}(E_p)$.*

(i) *The group G is not contained in a subgroup of $\mathrm{GL}(E_p)$ that is isomorphic to the symmetric group S_3, in particular $p > 2$; and*
(ii) *If E_p is a reducible G-module, then its semisimplification E_p^{ss} is not of the form*
  (a) *$\mathbf{1} \oplus \epsilon_p$ with the mod p cyclotomic character ϵ_p, or*
  (b) *$\chi \oplus \chi^2$ for a character $\chi : \mathrm{Gal}_k \to \mathbb{F}_p^*$ such that $\chi^3 = \epsilon_p$.*

Then the elements of $\mathrm{H}^1_{\mathrm{div}}(k, E)$ and in particular of $Ш(E/k)$ are p-divisible in $\mathrm{H}^1(k, E)$.

Proof: Since the determinant of the mod p representation $\overline{\rho}_E : \mathrm{Gal}_k \to \mathrm{GL}(E_p)$ is the cyclotomic character ϵ_p, conditions (i) and (ii) guarantee by Theorem 1 that

- E_p and $\mathrm{End}(E_p)$ have no common irreducible factor as Gal_k-modules,
- and $\mathrm{H}^1(G, E_p) = 0$.

We deduce by Theorem 19 that $Ш^1(k, E_{p^n}) = 0$ for all $n \geq 0$, and thus

$$\mathrm{H}^1_{\mathrm{div}}(k, E)_{p^\infty} \subseteq p^n \cdot \mathrm{H}^1(k, E)$$

for all $n \geq 0$ by Proposition 13. This concludes the proof. □

4.6. **Divisibility by almost all primes — review of Bashmakov's results.** Bashmakov gives a partial answer to Cassels' question, at least when p is large. In [Ba72] §5, the treatment is said to be restricted to CM-abelian varieties, but is only carried out for elliptic curves.

Proposition 22 (Bashmakov [Ba72] Proposition 22)**.** *Let k be an algebraic number field and let E/k be an elliptic curve. Then for almost all p we have $Ш(E/k)_{p^\infty} \subseteq \mathrm{div}(\mathrm{H}^1(k, E))$. In particular, for such p, every class in $Ш(E/k)$ is p-divisible in $\mathrm{H}^1(k, E)$.*

Bashmakov's main tool in the proof of Proposition 22 is provided by a result of Serre [Se79] that the image of Gal_k acting on the full Tate module $\mathrm{T}\, E = \prod_\ell \mathrm{T}_\ell\, E$ contains an open subgroup of the diagonal torus. For an abelian variety instead of an elliptic curve but restricted to the ℓ-component this is due to Bogomolov. The bound for p, such that Proposition 22 holds, provided by Bashmakov's method depends on the index of this open subgroup in the diagonal torus. In the meantime, Serre has improved his result so that this approach now shows the following.

Theorem 23. *Let k be an algebraic number field and let A/k be an abelian variety. Then for almost all p we have $\mathrm{H}^1_{\mathrm{div}}(k, A)_{p^\infty} = \mathrm{div}(\mathrm{H}^1(k, A))_{p^\infty}$. In particular, for such p, every class in $Ш(A/k)$ is p-divisible in $\mathrm{H}^1(k, A)$.*

Proof: Let $\rho_{A^t,p} : \mathrm{Gal}_k \to \mathrm{GL}(\mathrm{T}_p(A^t))$ be the Galois representation on the p-adic Tate module of the dual abelian variety A^t. Then Serre, [Se86] §2, has shown that there is an integer $N \geq 1$ independent of p such that $\rho_{A^t,p}(\mathrm{Gal}_k)$ contains the diagonal $(\mathbb{Z}_p^*)^N$. Thus, for $p > N + 1$, the image $G = G_{1,p}(A^t)$ of the mod p representation $\overline{\rho}_{A^t,p} : \mathrm{Gal}_k \to \mathrm{GL}(A^t_p)$ meets the center of $\mathrm{GL}(A^t_p)$ non-trivially. By Lemma 4 we find that for $p > N + 1$ the modules A^t_p and $\mathrm{End}(A^t_p)$ have no common irreducible factor and also $\mathrm{H}^1(G, A^t_p) = 0$. We conclude by Theorem 19 that

$$Ш^1(k, A^t_{p^n}) = 0$$

for all $n \geq 0$. By Proposition 13 this completes the proof. □

Remark 24. It is tempting to ask, whether the bound for p in Theorem 23 depends only on k and maybe $\dim(A)$ but not on the particular abelian variety A/k. Theorem 26 (2) provides such a uniform bound on p in terms of only the degree of $k/\mathbb{Q}$ in the case of elliptic curves.

5. The case of elliptic curves

5.1. **Applications to elliptic curves over number fields.** We first analyze the conditions asked by Theorem 21 in the case of elliptic curves over arbitrary number fields.

Corollary 25. *Let k be a number field. Then for 'most' elliptic curves E/k, in particular for infinitely many of them, the group $\mathrm{H}^1_{\mathrm{div}}(k,E)$ and in particular $Ш(E/k)$ is p-divisible in $\mathrm{H}^1(k,E)$ for all odd primes p.*

Proof: Jones [Jo10] (for $k=\mathbb{Q}$) and Zywina [Zy10] consider the set of elliptic curves

$$Y^2 = X^3 + aX + b$$

such that a and b are integers of k and $h(a,b) < x$ (where h denotes a height on such pairs). They show ([Zy10] Theorem 1.3 and Theorem 1.6) that the ratio of the cardinality of the subset of elliptic curves such that

$$\frac{|\operatorname{SL}_2(\mathbb{F}_p)|}{|\operatorname{Gal}(k(E_p)/k) \cap \operatorname{SL}_2(\mathbb{F}_p)|} \leq 2 \tag{5.1}$$

for every prime p by the total number of curves in the box $h(a,b) < x$ approaches 1 as x goes to infinity. When (5.1) holds and $p > 2$, then $\operatorname{Gal}(k(E_p)/k)$ can neither be contained in an S_3 nor in a Borel subgroup of $\operatorname{GL}(E_p)$. Hence in this sense for 'most' elliptic curves E/k the conditions of Theorem 21 hold for every prime $p > 2$. □

Recall from Section §1.1.3 that $\pi(d)$ is the maximal prime number such that an elliptic curve E over a number field $k/\mathbb{Q}$ of degree d admits a non-trivial k-rational p-torsion point.

Theorem 26. *Let E/k be an elliptic curve defined over an algebraic number field k of degree d over $\mathbb{Q}$. Then the following holds.*

1. *The group $\mathrm{H}^1_{\mathrm{div}}(k,E)$ and therefore $Ш(E/k)$ is p-divisible in $\mathrm{H}^1(k,E)$ for a prime number $p \geq 5$ under the following conditions:*
   - (i) *The extension $k(\zeta_p)/k$ has degree ≥ 3, and*
   - (ii) *no elliptic curve E' which is k-isogenous to E has a k-rational p-torsion point, in particular if $p > \pi(d)$, and*
   - (iii) *$p > (Nv + \sqrt{Nv})^2$ where $Nv = |\mathbb{F}_v|$ is the size of the residue class field $\mathbb{F}_v$ for a place $v \nmid 3p$ of k.*
2. *If $p > \max\{(2^d + 2^{d/2})^2, \pi(d)\}$, then $\mathrm{H}^1_{\mathrm{div}}(k,E)$ and therefore $Ш(E/k)$ is p-divisible in $\mathrm{H}^1(k,E)$.*

Proof: (1) Since the determinant of the mod p representation $\overline{\rho}_E : \mathrm{Gal}_k \to \operatorname{GL}(E_p)$ is the cyclotomic character ϵ_p, property (i) shows that $\det(\operatorname{Gal}(k(E_p)/k))$ has order ≥ 3. This implies $\operatorname{Gal}(k(E_p)/k)$ is not contained in a subgroup of $\operatorname{GL}(E_p)$ that is isomorphic to the symmetric group S_3 (see Corollary 9). Hence, we are only concerned by the second condition of Theorem 21. Since (ii) implies that $E_p^{\mathrm{ss}} \ncong \mathbf{1} \oplus \epsilon_p$, it remains to verify that E_p^{ss} is not of the form $\chi \oplus \chi^2$ for some character $\chi : \mathrm{Gal}_k \to \mathbb{F}_p^*$ such that $\chi^3 = \epsilon_p$.

We argue by contradiction. Note that the ramification at $v \nmid 3p$ of a character χ that solves $\chi^3 = \epsilon_p$ is at most tame and of degree $e_v \mid 3$. Let k'/k be an extension of degree e_v depending on v with a place $w \mid v$ of k' such that k'_w/k_v is totally tamely ramified of degree e_v. In particular, the size Nw of the residue field $\mathbb{F}_w$ at w agrees with Nv. It follows then from Abhyankar's Lemma and $E_p^{\mathrm{ss}} = \chi \oplus \chi^2$ that the inertia group $\mathrm{I}_w \subset \mathrm{Gal}_{k'}$ acts unipotently on $E_p = \mathrm{T}_p(E)/p\,\mathrm{T}_p(E)$. Since a priori the action of inertia on $\mathrm{T}_p(E)$ is quasi-unipotent, Lemma 27 below applies, and I_w must even act unipotently. The criterion of semistable reduction [SGA7$_I$] IX §3 Proposition 3.5 then shows that E/k has semistable reduction at w after scalar extension to k'.

If E/k has multiplicative reduction in w, then there is an unramified quadratic character $\delta : \mathrm{Gal}_{k'_w} \to \{\pm 1\}$ such that as a $\mathrm{Gal}_{k'_w}$-representation

$$E_p^{\mathrm{ss}}|_{\mathrm{Gal}_{k'_w}} \cong \delta \oplus \delta\epsilon_p \cong \chi \oplus \chi^2.$$

If $\delta = \chi$ and $\delta\epsilon_p = \chi^2$, then $\delta = \chi = \epsilon_p$ and thus $\epsilon_p(\mathrm{Frob}_w) = \pm 1 \in \mathbb{F}_p^*$, which means

$$p \mid Nw \pm 1 = Nv \pm 1.$$

If on the other hand $\delta = \chi^2$ and $\delta\epsilon_p = \chi$, then $\delta = \chi^2 = \epsilon_p^2$ and thus $\epsilon_p(\mathrm{Frob}_w^2) = \pm 1 \in \mathbb{F}_p^*$, which means

$$p \mid (Nw)^2 \pm 1 = (Nv)^2 \pm 1.$$

Finally, if E/k has good reduction in w, then E_p is an unramified $\mathrm{Gal}_{k'_w}$-module and

$$a = a_w = 1 + Nw - |\overline{E}(\mathbb{F}_w)| \equiv \mathrm{tr}(\mathrm{Frob}_w \,|E_p^{\mathrm{ss}}) \mod p$$

Since $E_p^{\mathrm{ss}}|_{\mathrm{Gal}_{k'_w}} \cong \chi \oplus \chi^2$ where $\chi^3 = \epsilon_p$ (as in Mazur's argument presented in [Se79]) we deduce that

$$p \mid \big(\chi(\mathrm{Frob}_w)^2 + \chi(\mathrm{Frob}_w)\big)^3 - a^3 \equiv Nv + (Nv)^2 + 3Nv \cdot a - a^3 \mod p$$

with $a \in \mathbb{Z}$ and $|a| \leq 2\sqrt{Nv}$ due to the Hasse–Weil bound. An analysis of the function $f(x) = 3Nx - x^3$ on the interval $-2\sqrt{N} \leq x \leq 2\sqrt{N}$ shows that

$$|3Nv \cdot a - a^3| \leq 2\sqrt{(Nv)^3}.$$

Consequently, we find

$$0 < (Nv - \sqrt{Nv})^2 \leq Nv + (Nv)^2 + 3Nv \cdot a - a^3 \leq (Nv + \sqrt{Nv})^2$$

which leads in the case of good reduction at w to

$$p \leq (Nv + \sqrt{Nv})^2.$$

Consequently, if $p > (Nv + \sqrt{Nv})^2$ then $E_p^{\mathrm{ss}} \ncong \chi \oplus \chi^2$ as claimed.

(2) Observe that if $p > \max\{(2^d + 2^{d/2})^2, \pi(d)\}$, then p must be odd and hence condition (iii) holds with respect to any place $v \mid 2$. Moreover, since $p > \pi(d)$, condition (ii) holds by definition of $\pi(d)$. Finally, for (i) we use the crude estimate

$$[k(\zeta_p) : k] \geq \frac{[\mathbb{Q}(\zeta_p) : \mathbb{Q}]}{[k : \mathbb{Q}]} = \frac{p-1}{d} > \frac{(2^d + 2^{d/2})^2 - 1}{d} > \frac{4^d}{d} \geq \frac{1 + d \cdot 3}{d} > 3.$$

Therefore, (2) holds as a special case of (1). □

Lemma 27. *Let p be an odd prime number. Let $\rho : G \to \mathrm{GL}_2(\mathbb{Z}_p)$ be a quasi-unipotent continuous representation of a pro-finite group G such that the mod p representation $\overline{\rho} : G \to \mathrm{GL}_2(\mathbb{F}_p)$ is unipotent. If ρ is not unipotent, then $p = 3$ and $\rho(G) \cong \mathbb{Z}/3\mathbb{Z}$.*

Proof: Since we assume that G acts quasi-unipotently, there is an open normal subgroup $G^0 \subset G$ such that $\rho|_{G^0}$ is unipotent. If G^0 acts non-trivially, then it fixes a unique $\mathbb{Z}_p$-line, and $\rho(G)$ lies in a Borel subgroup, namely the normalizer of the stabilizer of the line. Due to ρ being quasi-unipotent and $\overline{\rho}$ being unipotent, the corresponding diagonal characters map to a finite group of 1-units in $\mathbb{Z}_p^*$ and therefore are trivial. Hence the representation ρ is unipotent.

If on the other hand $\rho(G^0) = 1$, then $\rho(G)$ is a torsion subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ and therefore isomorphic to its image in $\mathrm{GL}_2(\mathbb{F}_p)$ (see Lemma 9 in [So07]). Since we may assume that ρ is non-trivial we conclude that $\rho(G) \cong \mathbb{Z}/p\mathbb{Z}$, and that we have a non-trivial $M \in \mathrm{GL}_2(\mathbb{Q}_p)$ with $M^p = 1$. The characteristic polynomial of M is quadratic over $\mathbb{Q}_p$ and its roots are non-trivial pth roots of unity. Hence the pth cyclotomic extension $\mathbb{Q}_p(\zeta_p)$ is at most quadratic over $\mathbb{Q}_p$, whence $p \leq 3$. □

Corollary 28. *Let E/k be an elliptic curve defined over an algebraic number field k, and let p be a prime number. Then $\mathrm{H}^1_{\mathrm{div}}(k, E)$ is p-divisible in $\mathrm{H}^1(k, E)$ under the following conditions:*

1. *The extension $k(\zeta_p)/k$ has degree ≥ 3, and*
2. *one of the following holds:*
   - (a) *E has good reduction above a place v of k with norm $Nv = 3$ and $p > 11$.*
   - (b) *no elliptic curve E' which is k-isogenous to E has a k-rational p-torsion point and $3 \mid p - 1$ but the degree of $\mathbb{Q}(\zeta_p) \cap k$ over $\mathbb{Q}$ is prime to 3.*
   - (c) *$3 \mid p - 1$, the prime p is unramified in $k/\mathbb{Q}$, and $p > \pi(d)$ where d is the degree of $k/\mathbb{Q}$.*

Remark 29. The conditions (b) and (c) in Corollary 28 both already imply condition (1).

Proof of Corollary 28: As in the proof of Theorem 26 we deduce from (1) that the first condition of Theorem 21 holds. Hence, we are only concerned by the second condition of Theorem 21. We therefore assume that E_p is a reducible Gal_k-representation with semi-simplification $E_p^{\mathrm{ss}} = \chi_1 \oplus \chi_2$. In order to satisfy the second condition of Theorem 21 we have to exclude the following two cases:

(A) $E_p^{\mathrm{ss}} = \mathbf{1} \oplus \epsilon_p$,
(B) $E_p^{\mathrm{ss}} = \chi \oplus \chi^2$ with $\chi^3 = \epsilon_p$.

Under the assumption (c) we have $\mathbb{Q}(\zeta_p) \cap k = \mathbb{Q}$ and the assumption in (b) on k-rational torsion points holds again by definition of $\pi(d)$. So (c) in fact implies (b). Under the assumption (b) the option (A) is excluded and the equation $\chi^3 = \epsilon_p$ has no solution, which excludes option (B).

It remains to discuss assumptions (a). Let v be a place of k with residue field $\mathbb{F}_v$ of cardinality Nv and where E has good reduction $\overline{E}/\mathbb{F}_v$, then as in the proof of Theorem 26 we have $a \in \mathbb{Z}$ with $|a| \leq 2\sqrt{Nv}$ and

$$a = \mathrm{tr}(\mathrm{Frob}_v \,|\, \mathrm{T}_p(E)) \equiv \chi_1(\mathrm{Frob}_v) + \chi_2(\mathrm{Frob}_v) \mod p.$$

We distinguish the two cases and argue similarly to the proof of Theorem 26.

(A) If $E_p^{\mathrm{ss}} = \mathbf{1} \oplus \epsilon_p$, then
$$1 + Nv - a \equiv 0 \mod p.$$
(B) If $E_p^{\mathrm{ss}} = \chi \oplus \chi^2$ with $\chi^3 = \epsilon_p$, then
$$(Nv + (Nv)^2) + 3a \cdot Nv - a^3 \equiv \big(\chi(\mathrm{Frob}_v)^2 + \chi(\mathrm{Frob}_v)\big)^3 - a^3 \equiv 0 \mod p.$$

We finally exploit assumption (a), so that $Nv = 3$ and $|a| \leq 3$. The constraints in the two cases now are

(A) p divides one of $4 - a \in \{1, 2, 3, 4, 5, 6, 7\}$,
(B) p divides one of $12 + 9a - a^3 \in \{12, 2, 4, 12, 20, 22, 12\}$.

Hence, if $p > 11$ none of the cases (A) or (B) can occur, and thus E/k satisfies the assumptions of Theorem 21 for p. □

Corollary 30. *Let E/k be an elliptic curve defined over an algebraic number field k, and let p be an odd prime number. Then $\mathrm{H}^1_{\mathrm{div}}(k, E)$ is p-divisible in $\mathrm{H}^1(k, E)$ if E_p is an irreducible Gal_k-representation and $[k(\zeta_p) : k] \neq 2$.*

Proof: We have to verify the conditions of Theorem 21. Since E_p is assumed irreducible, condition (ii) is automatic. In order to satisfy also condition (i) of Theorem 21 we argue by contradiction. If $\mathrm{Gal}(k(E_p)/k) \subseteq \mathrm{GL}(E_p)$ lies in a copy of S_3, then for E_p to be irreducible we must have $p \geq 5$ and $\mathrm{Gal}(k(E_p)/k) \cong S_3 \subseteq \mathrm{GL}_2(\mathbb{F}_p)$. But then

$$[k(\zeta_p) : k] = |\det(\mathrm{Gal}(k(E_p)/k)| = |\det(S_3)| = 2$$

by Corollary 9 and this was excluded. □

5.2. **Quadratic twists.** For an elliptic curve E/k and a character

$$\tau : \mathrm{Gal}_k \to \{\pm 1\} \subseteq \mathrm{Aut}(E)$$

we denote by E^τ the quadratic twist of E by τ. The p-torsion of the twist E^τ is given by $(E^\tau)_p = E_p \otimes \tau$ as a Gal_k-module.

Corollary 31. *Let k be a number field and let E/k be an elliptic curve.*

(1) *Let $p \geq 3$ be a fixed prime number. Then among the quadratic twists of E there are at most 3 twists E^τ such that $\mathrm{H}^1_{\mathrm{div}}(k, E^\tau)$ is not p-divisible in $\mathrm{H}^1(k, E^\tau)$.*
(2) *For all but a finite number of quadratic twists E^τ of E the group $\mathrm{H}^1_{\mathrm{div}}(k, E^\tau)$ is p-divisible in $\mathrm{H}^1(k, E^\tau)$ for all $p \geq 3$.*

Proof: (1) We verify the conditions of Theorem 21 for almost all quadratic twists. Since twisting is transitive, we may first assume that $G = \mathrm{Gal}(k(E_p)/k) \subseteq \mathrm{GL}(E_p)$ is isomorphic to one of the groups

(a) the trivial group,

(b) $\mathbb{Z}/2\mathbb{Z}$, non-centrally in $\mathrm{GL}(E_p)$ (see Corollary 9),
(c) $\mathbb{Z}/3\mathbb{Z}$,
(d) S_3.

For a non-trivial $\tau : \mathrm{Gal}_k \to \{\pm 1\}$ we find $G^\tau = \mathrm{Gal}(k(E_p^\tau)/k) \subseteq \mathrm{GL}(E_p^\tau)$ equal to respectively

(a) $\mathbb{Z}/2\mathbb{Z}$, centrally in $\mathrm{GL}(E_p^\tau)$,
(b) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$,
(c) $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$,
(d) $S_3 \times \mathbb{Z}/2\mathbb{Z}$, since a transposition in S_3 cannot be central in $\mathrm{GL}(E_p^\tau)$.

Consequently, every non-trivial twist E^τ satisfies condition (1) of Theorem 21, which means that in general, at most one of the twists of E/k can fail condition (1) of Theorem 21.

Secondly, we assume that E_p is reducible and that condition (2) of Theorem 21 fails. If a non-trivial twist E^τ also fails condition (2), then twisting by τ either preserves $\mathbf{1} \oplus \epsilon_p$ or $\chi \oplus \chi^2$ with $\chi^3 = \epsilon_p$, or it transforms one to the other. In any case, the character $\tau \neq \mathbf{1}$ is one of the following list

(a) $(\mathbf{1} \oplus \epsilon_p) \otimes \tau \cong \mathbf{1} \oplus \epsilon_p$: then $\tau = \epsilon_p$,
(b) $(\chi \oplus \chi^2) \otimes \tau \cong \chi \oplus \chi^2$: then $\tau = \chi = \epsilon_p$,
(c) $(\mathbf{1} \oplus \epsilon_p) \otimes \tau \cong \chi \oplus \chi^2$: then $\tau = \chi = \epsilon_p$ or $\tau = \chi^2 = \epsilon_p^2$,
(d) $(\chi \oplus \chi^2) \otimes \tau \cong \mathbf{1} \oplus \epsilon_p$: then $\tau = \chi = \epsilon_p$ or $\tau = \chi^2 = \epsilon_p^2$.

In any case $\tau = \epsilon_p$ or ϵ_p^2 which cannot both be non-trivial quadratic characters. Hence, condition (2) of Theorem 21 can in general only fail for at most 2 twists of E/k.

(2) Due to (1) it suffices to show that for $p \gg 3$ and all quadratic twists E^τ/k the group $\mathrm{H}^1_{\mathrm{div}}(k, E^\tau)$ is p-divisible in $\mathrm{H}^1(k, E^\tau)$. If E/k has no CM, then by [Se72] §4.4 we have

$$\mathrm{Gal}(k(E_p)/k) = \mathrm{GL}(E_p)$$

for $p \gg 3$. If E/k has CM, then by [Se72] §4.5 the image $\mathrm{Gal}(k(E_p)/k) \subseteq \mathrm{GL}(E_p)$ contains a full (split or non-split) torus $C \subset \mathrm{GL}(E_p)$ for $p \gg 3$. In both cases $\mathrm{Gal}(k(E_p)/k)$ contains the group of diagonal matrices $\cong \mathbb{F}_p^*$ and continues to contain at least the squares $\cong (\mathbb{F}_p^*)^2 \neq 1$ after twisting. Lemma 4 then provides that the conditions of Theorem 21 are satisfied for all quadratic twists of E. □

Corollary 32. *Let k be a number field. For every $j \in k$ there is an elliptic curve E/k with j-invariant j such that $\mathrm{H}^1_{\mathrm{div}}(k, E)$ and therefore $Ш(E/k)$ is p-divisible in $\mathrm{H}^1(k, E)$ for all odd primes p.*

Proof: Quadratic twists share the same j-invariant, and Corollary 31. □

Remark 33. Corollary 32 would be automatic if among the quadratic twists of a given E/k we could find a curve E^τ with $Ш(E^\tau/k) = 0$ or at least of order a power of 2.

5.3. **Applications to elliptic curves over $\mathbb{Q}$.** Now we attempt to find optimal results in the case of $k = \mathbb{Q}$.

Theorem 34. *Let $E/\mathbb{Q}$ be an elliptic curve defined over the rationals. Then the following holds.*

(1) *$\mathrm{H}^1_{\mathrm{div}}(\mathbb{Q}, E)$ and therefore $Ш(E/\mathbb{Q})$ is p-divisible in $\mathrm{H}^1(\mathbb{Q}, E)$ for all primes $p > 7$.*
(2) *Let p be an odd prime number such that $\mathrm{H}^1_{\mathrm{div}}(\mathbb{Q}, E)$ is not p-divisible in $\mathrm{H}^1(\mathbb{Q}, E)$. Then we have one of the following cases.*
   (a) *$p = 3$ and $E_3^{\mathrm{ss}} = \mathbf{1} \oplus \epsilon_3$,*
   (b) *$p = 5$ and $E_5^{\mathrm{ss}} = \mathbf{1} \oplus \epsilon_5$, or $E_5^{\mathrm{ss}} = \epsilon_5^3 \oplus \epsilon_5^2$,*
   (c) *$p = 7$ and $E_7^{\mathrm{ss}} = \mathbf{1} \oplus \epsilon_7$.*

   In particular, in all the above cases the inertia group $\mathrm{I}_v \subset \mathrm{Gal}_{\mathbb{Q}}$ for a place $v \nmid p$ acts through a p-group on $\mathrm{T}_p(E)$. Moreover, in case (b) and (c) the curve E has semistable reduction outside of p.
(3) *$\mathrm{H}^1_{\mathrm{div}}(\mathbb{Q}, E)$ and therefore $Ш(E/\mathbb{Q})$ is p-divisible in $\mathrm{H}^1(\mathbb{Q}, E)$ for all odd primes p where E has supersingular or non-split multiplicative reduction at p.*

Proof: (1) Observe that by Theorem 26 (2) we know that $\mathrm{H}^1_{\mathrm{div}}(\mathbb{Q}, E)$ and hence $Ш(E/\mathbb{Q})$ are p-divisible in $\mathrm{H}^1(\mathbb{Q}, E)$ for all primes $p > \max\{(2+\sqrt{2})^2, \pi(1)\}$. Since $11 < (2+\sqrt{2})^2 < 12$ and $\pi(1) = 7$ by Mazur [Ma78] Theorem 2, it follows that we can now restrict our attention to the case $p = 11$.

Again by work of Mazur (see Theorem 2 in [Ma78]) we know that $E(\mathbb{Q})_{11}$ is trivial and hence all we need is to identify (and deal differently with) all $E/\mathbb{Q}$ such that E_{11}^{ss} is of the form $\chi \oplus \chi^2$ for a character $\chi : \mathrm{Gal}_k \to \mathbb{F}_{11}^*$ such that $\chi^3 = \epsilon_{11}$. Observe that $\chi^3 = \epsilon_{11}$ implies that $\chi = \epsilon_{11}^{\otimes 7}$. We know that elliptic curves such that E_{11} is reducible correspond up to quadratic twist to non-cuspidal rational points[4] of $X_0(11)$ of which there are three (see [BK75] page 79). These three rational points correspond up to quadratic twist to the following three elliptic curves $E/\mathbb{Q}$ of conductor 121 (the code is as in Cremona's list [Cr]):

elliptic curve	$[a_1, a_2, a_3, a_4, a_6]$	j-invariant	$\mathrm{tr}(\mathrm{Frob}_2 \mid \mathrm{T}_{11}(E))$	E_{11}^{ss}
121b1	$[0, -1, 1, -7, 10]$	-2^{15}	0	$\epsilon_{11}^{\otimes 3} \oplus \epsilon_{11}^{\otimes 8}$
121c1	$[1, 1, 0, -2, -7]$	-11^2	1	$\epsilon_{11}^{\otimes 4} \oplus \epsilon_{11}^{\otimes 7}$
121c2	$[1, 1, 0, -3632, 82757]$	$-11 \cdot 131^3$	1	$\epsilon_{11}^{\otimes 4} \oplus \epsilon_{11}^{\otimes 7}$

These elliptic curves $E/\mathbb{Q}$ have good reduction outside 11. By reducing the affine equation of the respective elliptic curve modulo 2 and counting $|\overline{E}(\mathbb{F}_2)|$ we compute

$$\mathrm{tr}(\mathrm{Frob}_2 \mid \mathrm{T}_{11}(E)) = 2 + 1 - |\overline{E}(\mathbb{F}_2)|$$

recorded in the table above. On the other hand, since for these curves E_{11} is reducible and unramified away from 11 class field theory tells us that $E_{11}^{\mathrm{ss}} \cong \epsilon_{11}^a \oplus \epsilon_{11}^b$ for some $a, b \in \mathbb{Z}/10\mathbb{Z}$ with $a + b \equiv 1 \mod 10$. To complete the above table we determine the pair (a, b) by comparing $\mathrm{tr}(\mathrm{Frob}_2 \mid \mathrm{T}_{11}(E))$ with $2^a + 2^b \mod 11$ as follows.

(a, b)	$(0, 11)$	$(1, 10)$	$(2, 9)$	$(3, 8)$	$(4, 7)$	$(5, 6)$
$2^a + 2^b \mod 11$	3	3	-1	0	1	-3

If a quadratic twist $E^\tau/\mathbb{Q}$ has $E_{11}^{\tau,\mathrm{ss}} = \epsilon_{11}^{\otimes 7} \oplus \epsilon_{11}^{\otimes 4} \cong E_{11}^{\mathrm{ss}} \otimes \tau$, then τ must be a power of ϵ_{11}, namely $\tau = \mathbf{1}$ or $\tau = \epsilon_{11}^{\otimes 5}$, and so this does not occur for $\tau = \epsilon_{11}^{\otimes 5}$ in view of the above determined structure of E_{11}^{ss} in the three cases.

Consequently, in the case of $p = 11$ we are left with exactly two potential exceptions, the two 11-isogenous non-CM curves labeled "121c1" and "121c2". For these two curves only, the criterion of Theorem 21 does not apply. Let E be one of the elliptic curves labeled "121c1" or "121c2". Since E has good reduction outside the regular prime $p = 11$, and since the Galois action on E_{11}^{ss} factors over ϵ_{11} we deduce from [ÇS12] Proposition 5 with $k = \mathbb{Q}$ that our potential exceptions obey the theorem as well.

(2) The list follows immediately from Theorem 21 and the analysis of its conditions in the proof of part (1). Note that $\chi^3 = \epsilon_7$ has no solution.

We concude that for $v \nmid p$ the inertia group I_v acts unipotently on $E_p = \mathrm{T}_p(E)/p\,\mathrm{T}_p(E)$. The action of I_v on $\mathrm{T}_p(E)$ is a priori quasi-unipotent, so that Lemma 27 applies and the action is in fact unipotent for $p = 5$ or $p = 7$. We conclude by the criterion for semistable reduction, see [SGA7$_I$] IX §3 Proposition 3.5.

(3) We now consider the case when E has either supersingular or non-split multiplicative reduction at p. In this case the second condition of Theorem 21 holds because

(i) if E has supersingular reduction at p then $\rho_{E,1}$ is irreducible (see Proposition 2.11 in [DDT97]); and

(ii) if E has non-split multiplicative reduction at p, we have that $E_p^{\mathrm{ss}}|_{\mathrm{Gal}_{\mathbb{Q}_p}} = \delta \oplus \delta\epsilon_p$ where δ is the unique unramified quadratic character of $\mathrm{Gal}_{\mathbb{Q}_p}$ (see Proposition 2.12 in [DDT97]).

[4] We thank Brian Conrad for suggesting this way of dealing with the prime 11.

It remains to verify the first condition of Theorem 21 for $p = 3$. We argue by contradiction and assume that the image of $\mathrm{Gal}_{\mathbb{Q}}$ in $\mathrm{GL}(E_3)$ is contained in a subgroup isomorphic to S_3. Then the proof of Lemma 8 shows that E_3 is reducible with semisimplification $E_3^{\mathrm{ss}} = \mathbf{1} \oplus \epsilon_3$ and we are back in the case of the second condition of Theorem 21 that we already dealt with. □

Corollary 35. *Among the quadratic twists $E^\tau/\mathbb{Q}$ of an elliptic curve $E/\mathbb{Q}$ we find at most one odd prime number $p = 3, 5$ or 7 and at most*

(a) *2 twists for $p = 3$,*
(b) *2 twists for $p = 5$,*
(c) *1 twist for $p = 7$,*

such that $\mathrm{H}^1_{\mathrm{div}}(\mathbb{Q}, E^\tau)$ is not p-divisible in $\mathrm{H}^1(\mathbb{Q}, E^\tau)$. In case (b) and (c) such a twist has semistable reduction at all $\ell \neq p$. In particular, for all but at most 2 of the quadratic twists of $E/\mathbb{Q}$ we have that $\mathrm{H}^1_{\mathrm{div}}(\mathbb{Q}, E^\tau)$ and therefore $Ш(E^\tau/\mathbb{Q})$ is p-divisible in $\mathrm{H}^1(\mathbb{Q}, E^\tau)$ for all odd prime numbers p.

Proof: The proof is straight forward following the proof of part (1) of Corollary 31 together with the knowledge of the precise structure of bad pairs (E, p) for $k = \mathbb{Q}$ from Theorem 34 (2). It remains to exclude that among the twists of a given $E/\mathbb{Q}$ more than one of the cases (a)–(c) can occur. Cases (b) and (c) cannot both among the twists for a fixed $E/\mathbb{Q}$ since no elliptic curve has rational isogeny of degree 35 by [Ke82] Theorem 1.

We argue by contradiction. Let us assume that the primes 3 and $p \in \{5, 7\}$ occur as bad primes among the twists of $E/\mathbb{Q}$. Note that for the prime $p = 5$ the two possible bad semisimplifications are twists of each other by ϵ_5^2. Therefore, after twisting, we may assume that $E_p^{\mathrm{ss}} = \mathbf{1} \oplus \epsilon_p$ and that there is a quadratic character τ with $E_3^{\tau,\mathrm{ss}} = \mathbf{1} \oplus \epsilon_3$.

It follows from Lemma 27 that an inertia group $\mathrm{I}_\ell \subset \mathrm{Gal}_{\mathbb{Q}}$ for $\ell \neq 3$ acts on $\mathrm{T}_3(E^\tau)$

(1) either unipotently and E^τ has semistable reduction at ℓ,
(2) or via a finite 3-group and E^τ has potentially good reduction at ℓ, more precisely with the image of inertia $\Phi_\ell \cong \mathbb{Z}/3\mathbb{Z}$.

In the potentially good reduction case and for $\ell \neq p$ we find the same image Φ_ℓ in $\mathrm{GL}(E_p^\tau)$, namely as the image of inertia in the geometric automorphism group of the special fibre of the potential good reduction of E^τ. From $E_p^{\tau,\mathrm{ss}} = \tau \oplus \tau\epsilon_p$ we conclude that the mod p representation E_p^τ does not allow I_ℓ to act via a 3-group. Thus $E^\tau/\mathbb{Q}$ is in fact semistable at ℓ. Consequently, the Galois module structure of $E_p^{\tau,\mathrm{ss}}$ now implies that τ must be unramified outside $3p$.

If τ ramifies at p, then $E_p^{\tau,\mathrm{ss}} = \tau \oplus \tau\epsilon_p$ forbids semistable reduction at p for E^τ, whence $E_3^{\tau,\mathrm{ss}} = \mathbf{1} \oplus \epsilon_3$ shows that E^τ has potentially good reduction at p. More precisely, good reduction at p occurs after a Galois extension $k/\mathbb{Q}$ with ramification degree 3 above p (for example the extension $k = \mathbb{Q}(E_3^\tau)$ works). But then $E_p^{\tau,\mathrm{ss}} = \tau \oplus \tau\epsilon_p$ still forbids good ordinary reduction. In case of supersingular reduction, the image of inertia $\mathrm{I}_{k,p} = \mathrm{I}_p \cap \mathrm{Gal}_k$ at p (after the extension) is contained in the intersection of a non-split torus in $\mathrm{GL}(E_p)$ with the split torus associated to the decomposition $E_p^{\tau,\mathrm{ss}} = \tau \oplus \tau\epsilon_p$. This intersection is contained in the central diagonal torus, and therefore τ and $\tau\epsilon_p$ agree on $\mathrm{I}_{k,p}$. This leads to $\epsilon_p(\mathrm{I}_{k,p}) = 1$ in contradiction to $\epsilon_p(\mathrm{I}_p) = \mathbb{F}_p^*$ and $|\,\mathrm{I}_p\,/\,\mathrm{I}_{k,p}\,| = 3$.

It follows that τ must be unramified outside 3, and then $\tau = \epsilon_3$ or $\tau = \mathbf{1}$ so that in any case $E_3^{\mathrm{ss}} = (\mathbf{1} \oplus \epsilon_3) \otimes \tau = \epsilon_3 \oplus \mathbf{1}$. Hence, there is an elliptic curve $E'/\mathbb{Q}$ with a $\mathbb{Q}$-rational point of order $3p$ that is $\mathbb{Q}$-isogenous to E. This contradicts Mazur's list [Ma77] Theorem 8 of possible orders of rational torsion points. □

Remark 36. (1) It is interesting to note that the difficult odd prime numbers with respect to showing p-divisibility for elliptic curves E over $\mathbb{Q}$ are exactly the odd *Mazur prime numbers*, i.e., those prime numbers for which E may contain $\mathbb{Q}$-rational p-torsion elements. To some extent this is a consequence of our method, but it is tempting to look for a deeper connection.

(2) In this respect it is amusing that in order to produce p-torsion in $Ш(E^\tau/\mathbb{Q})$ for quadratic twists of $E/\mathbb{Q}$, a frequent assumption requires E to have a $\mathbb{Q}$-rational p-torsion point. For example, in [BO03] Theorem 2 Balog and Ono show that if $p = 3, 5$ or 7 such that E is good[5]

[5]Apparently a mild constraint, see [BO03].

with respect to p and has a $\mathbb{Q}$-rational p-torsion point, then with τ_d ranging over quadratic characters of fundamental discriminant d, and $E^d = E^{\tau_d}$, we have an asymptotic lower bound

$$\left|\{0 < -d < x \ ; \ E^d \text{ has analytic rank 0, and } Ш(E^d/\mathbb{Q})_p \neq 0\}\right| \gg \frac{x^{1/2+1/(2p)}}{\log^2 x}$$

as x goes to infinity. In particular, an assumption that we like to avoid, namely having rational p-torsion, actually helps us to show that our p-divisibility result Corollary 35 is non-trivial because the Tate–Shafarevich group in question actually sometimes has non-trivial p-torsion.

(3) Matsuno in [Ma07] Theorem 5.1 shows that $\dim_{\mathbb{F}_p} Ш(E/\mathbb{Q})_p$ is unbounded for $p = 2, 3, 5, 7$ or 13 among all elliptic curves $E/\mathbb{Q}$. More precisely, this result also searches for p-torsion elements in the Tate–Shafarevich group among quadratic twists of a given elliptic curve with a reducible mod p representation. The list of primes is exactly the list of primes p such that the modular curve $X_0(p)$ is rational.

Corollary 37. *Let $E/\mathbb{Q}$ be an elliptic curve which does not have a rational 4-cyclic subgroup. Then among the quadratic twists of E there are infinitely many $E'/\mathbb{Q}$ with $Ш(E'/\mathbb{Q})$ divisible in $\mathrm{H}^1(\mathbb{Q}, E')$.*

Proof: Observe that if E has a 4-cyclic subgroup defined over $\mathbb{Q}$ then it has a 2-cyclic subgroup defined over $\mathbb{Q}$, and thus a non-trivial $\mathbb{Q}$-rational 2-torsion point and $\#E_2(\mathbb{Q}) \geq 2$. Hence we have to consider the following three cases.

(1) $E_2(\mathbb{Q}) = 0$: by Theorem 1.4 of Mazur and Rubin [MR10] we know that E has infinitely many twists E' such that $\mathrm{H}^1_{\mathrm{Sel}}(\mathbb{Q}, E'_2)$ is trivial and consequently so is $Ш(E'/\mathbb{Q})_2$.
(2) $E_2(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$ and E has no 4-cyclic subgroup defined over $\mathbb{Q}$:
   (a) if E has no 4-cyclic subgroup defined over $\mathbb{Q}(E_2)$ then E has infinitely many twists E' such that the $\mathbb{Z}/2\mathbb{Z}$-rank of $\mathrm{H}^1_{\mathrm{Sel}}(\mathbb{Q}, E'_2)$ equals 1 (see Theorem 1.3 of Klagsbrun [Kl11]);
   (b) if E has a 4-cyclic subgroup defined over $\mathbb{Q}(E_2)$ then since elliptic curves over $\mathbb{Q}$ do not have constant 2-Selmer parity [MR10], by Theorem 1.5 of Klagsbrun [Kl11] we have that E has infinitely many twists E' such that the $\mathbb{Z}/2\mathbb{Z}$-rank of $\mathrm{H}^1_{\mathrm{Sel}}(\mathbb{Q}, E'_2)$ equals 1.

   Consequently, E has infinitely many quadratic twists E' such that $Ш(E'/\mathbb{Q})_2$ is trivial.
(3) $E_2(\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$ and E has no 4-cyclic subgroup defined over $\mathbb{Q}$: by work of Heath-Brown [HB94], Swinnerton-Dyer [SD08] and Kane [Ka10] (see Theorem 2), we know that E has infinitely many twists E' such that the $\mathbb{Z}/2\mathbb{Z}$-rank of $\mathrm{H}^1_{\mathrm{Sel}}(\mathbb{Q}, E'_2)$ equals 2 and hence $Ш(E'/\mathbb{Q})_2$ is trivial.

Then by Corollary 35 for an infinite subset of these twists E', in fact all but at most 2, we have that $Ш(E'/\mathbb{Q})$ is p-divisible in $\mathrm{H}^1(\mathbb{Q}, E')$ for all primes p. □

Corollary 38. *Let $E/\mathbb{Q}$ be an elliptic curve with $\mathbb{Q}$-rational 2-torsion, i.e., an elliptic curve in twisted Legendre form $aY^2 = X(X-1)(X-\lambda)$. Then $\mathrm{H}^1_{\mathrm{div}}(\mathbb{Q}, E)$ and therefore $Ш(E/\mathbb{Q})$ is p-divisible in $\mathrm{H}^1(\mathbb{Q}, E)$ for all $p \geq 5$.*

Proof: A quadratic twist of $E/\mathbb{Q}$ still has $\mathbb{Q}$-rational 2-torsion. By Mazur [Ma77] Theorem 8, the only $\mathbb{Q}$-rational torsion of odd order that can occur for E is of order 3. Hence the cases (b) and (c) of Theorem 34 (2) cannot occur. Note that upon twisting by the quadratic ϵ_5^2 we interchange the two cases in (b). □

5.4. **An example: the Jacobian of the Selmer curve.** The plane cubic

$$S = \{3X^3 + 4Y^3 + 5Z^3 = 0\}$$

describes Selmer's curve of genus 1 violating the Hasse principle. Its Jacobian $E = \mathrm{Pic}^0_S$ is an elliptic curve over $\mathbb{Q}$ of analytic rank 0 given by the homogeneous equation

$$X^3 + Y^3 + 60Z^3 = 0 \tag{5.2}$$

with $[1:-1:0]$ as its origin. The curve E has Mordell-Weil group $E(\mathbb{Q}) = 0$, see [Ca91] §18 Lemma 2, and 3-torsion in an exact sequence

$$0 \to \mu_3 \to E_3 \to \mathbb{Z}/3\mathbb{Z} \to 0, \tag{5.3}$$

which splits over a field $k/\mathbb{Q}$ if and only if 60 is a cube in k. Moreover, E has complex multiplication by $\mathfrak{o} = \mathbb{Z}[\zeta_3]$, and the complex multiplication is defined over $\mathbb{Q}(\zeta_3)$. The curve S and E have good reduction over $U = \operatorname{Spec}(\mathbb{Z}[1/30])$.

The curve S, as a principal homogeneous space under E describes a non-trivial 3-torsion element $[S] \in Ш(E/\mathbb{Q})$, see [Ma93] I §4 and §9. Mazur and Rubin determine

$$Ш(E/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

unconditionally, see [Ma93] Theorem 1 and §9. The Selmer curve S served in [ÇS12] Theorem B and §8 as an example generating a non-trivial intersection

$$\langle [S] \rangle = Ш(E/\mathbb{Q}) \cap \operatorname{Div}(\mathrm{H}^1(\mathbb{Q}, E)).$$

Here we answer the divisibility question of Cassels for E and thus justify [ÇS12] Remark 25.

Proposition 39. *For the Jacobian $E/\mathbb{Q}$ of the Selmer curve we have*

$$Ш(E/\mathbb{Q}) + \operatorname{Div}(\mathrm{H}^1(\mathbb{Q}, E))_{3^\infty} = \operatorname{div}(\mathrm{H}^1(\mathbb{Q}, E))_{3^\infty} = \mathrm{H}^1_{\mathrm{div}}(\mathbb{Q}, E)_{3^\infty}.$$

The proof of Proposition 39 requires some preparation. On E_{3^∞}, the 3-primary torsion, $\mathrm{Gal}_{\mathbb{Q}(\zeta_3)}$ acts via $\mathfrak{o}$-linear automorphisms, more precisely R-linear automorphisms for

$$R = \mathfrak{o} \otimes \mathbb{Z}_3 = \mathbb{Z}_3[\zeta_3].$$

The ring R is a discrete valuation ring, and as an R-module $\mathrm{T}_3(E)$ is a free module of rank 1. Therefore we obtain a character

$$\chi_E : \mathrm{Gal}_{\mathbb{Q}(\zeta_3)} \to R^*$$

describing the action on $\mathrm{T}_3(E)$, and a posteriori also the action on E_{3^n}. Since $E/\mathbb{Q}$ has good reduction outside $v \mid 30$, the character χ_E is unramified outside $2, 3, 5$.

Lemma 40. *The character χ_E is surjective onto the 1-units $U^1_R = 1 + (\zeta_3 - 1)R \subset R^*$.*

Proof: First, the action is via a 3-group since E_{3^n} has a filtration with quotients

$$E_{3^{m+1}}/E_{3^m} \cong E_3,$$

which over $\mathbb{Q}(\zeta_3)$ is further filtered with trivial quotients by (5.3). So the action is unipotent and therefore through a 3-group. Hence χ_E takes values in U^1_R. The group of 1-units has the structure

$$U^1_R \cong \mu_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3.$$

By Nakayama's Lemma it suffices to check the surjectivity of

$$\operatorname{im}(\chi_E) \twoheadrightarrow U^1_R/(U^1_R)^3.$$

A computation reveals that the image of U^1_R in $(R/9R)^*$ is killed by 3: we compute modulo 9 and use $3 = (\zeta_3 + 1)(\zeta_3 - 1)^2$ to see

$$\begin{aligned}\big(1 + (\zeta_3 - 1)a\big)^3 &= 1 + 3(\zeta_3 - 1)a(1 + (\zeta_3 - 1)a) + (\zeta_3 - 1)^3 a^3 \\ &= 1 + (\zeta_3 - 1)^3\big((\zeta_3 + 1)a(1 + (\zeta_3 - 1)a) + a^3\big) \\ &\equiv 1 + (\zeta_3 - 1)^3(2a + a) \equiv 1.\end{aligned}$$

The induced map

$$U^1_R/(U^1_R)^3 \to (R/9R)^*$$

is surjective and both sides have 27 elements, hence an isomorphism. It therefore remains to show that $\mathrm{Gal}_{\mathbb{Q}(\zeta_3)}$ acts via a group of order 27 on E_9. A computation with SAGE [S+10] shows

$$\begin{aligned}\mathbb{Q}(E_3) &= \mathbb{Q}(\zeta_3, \sqrt[3]{60}), \\ \mathbb{Q}(E_9) &= \mathbb{Q}(\zeta_9, \sqrt[3]{60}, \sqrt[3]{3}).\end{aligned} \tag{5.4}$$

and this completes the proof. □

Lemma 41. *Any non-trivial R-submodule of E_{3^n} contains the μ_3-part of E_3.*

Proof: As an R-module E_{3^n} is cyclic, hence every submodule contains the (ζ_3-1)-torsion, which is a module of 3-elements contained in the 3-torsion E_3. By the Lemma 1 above, an R-submodule is also a $\mathrm{Gal}_{\mathbb{Q}(\zeta_3)}$-submodule, and there is only $\mu_3 \subset E_3$, becasue 60 is not a cube in $\mathbb{Q}(\zeta_3)$. □

Corollary 42. *Let v be a place different from $2,3,5$ that splits in $\mathbb{Q}(\zeta_3)$. If $\mu_3 \subseteq E_3$ is not in the kernel of the map*

$$E_3/(\mathrm{Frob}_v - 1)E_3 \to E_{3^n}/(\mathrm{Frob}_v - 1)E_{3^n},$$

induced by inclusion $E_3 \subset E_{3^n}$, then $\mathrm{Frob}_v = 1$ in $\mathrm{Gal}(\mathbb{Q}(E_{3^n})/\mathbb{Q})$.

Proof: As we assume that v splits in $\mathbb{Q}(\zeta_3)$, we know that Frob_v acts via R-linear automorphisms. In particular the subgroup

$$(\mathrm{Frob}_v - 1)E_{3^n} \subset E_{3^n}$$

is an R-submodule. Lemma 41 shows that either $\mu_3 \subseteq (\mathrm{Frob}_v - 1)E_{3^n}$, or $(\mathrm{Frob}_v - 1)E_{3^n} = 0$. □

We recall from [ÇS12] §8 the result of the computation of the following étale cohomology groups (see loc. cit. for the definition of $\mathrm{H}^i_!(U, E_3)$)

$$\mathrm{H}^1(U, E_3) = \mathrm{H}^1_{\mathrm{Sel}_3}(\mathbb{Q}, E_3) = \mathrm{H}^1_{\mathrm{Sel}}(\mathbb{Q}, E_3) = Ш(E/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z},$$

$$\mathrm{H}^1_c(U, E_3) = \mathrm{H}^1_!(U, E_3) = \mathrm{H}^1_{\mathrm{Sel}^3}(\mathbb{Q}, E_3) = \langle [S] \rangle \cong \mathbb{Z}/3\mathbb{Z},$$

and

$$\mathrm{H}^1(U, E_{3^n}) = \mathrm{H}^1_{\mathrm{Sel}_3}(\mathbb{Q}, E_{3^n}) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3^n\mathbb{Z},$$

$$\mathrm{H}^1_c(U, E_{3^n}) = \mathrm{H}^1_!(U, E_{3^n}) = \mathrm{H}^1_{\mathrm{Sel}^3}(\mathbb{Q}, E_{3^n}) = \langle [S] \rangle \cong \mathbb{Z}/3\mathbb{Z}.$$

and

$$\mathrm{H}^1_{\mathrm{div}}(\mathbb{Q}, E)_{3^\infty} = \mathrm{H}^1_{\mathrm{Sel}_3}(\mathbb{Q}, E_{3^\infty}) = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Q}_3/\mathbb{Z}_3.$$

We now compute the obstruction to divisibility by 3^n as classes over U by exploiting the cohomology sequence of étale cohomology associated to

$$0 \to E_{3^n} \to E_{3^{n+1}} \to E_3 \to 0$$

namely

$$0 \to \mathrm{H}^1(U, E_{3^n}) \to \mathrm{H}^1(U, E_{3^{n+1}}) \to \mathrm{H}^1(U, E_3) \xrightarrow{\delta} \mathrm{H}^2_!(U, E_{3^n}) \to 0.$$

A priori the map on the right lands in $\mathrm{H}^2(U, E_{3^n})$. But as we start with $\mathrm{H}^1(U, E_3)$ that contains by coincidence only locally divisible classes, we obtain a map into $\mathrm{H}^2_!(U, E_{3^n})$. Then we count and find that the image of δ is of order 3, while Artin–Verdier duality says

$$\#\,\mathrm{H}^2_!(U, E_{3^n}) = \#\,\mathrm{H}^1_!(U, E_{3^n}) = 3.$$

Proof of Proposition 39: We only have to deal with "the" $\mathbb{Z}/3Z$-factor of $\mathrm{H}^1_{\mathrm{div}}(\mathbb{Q}, E)_{3^\infty}$ and show that it becomes 3^n divisible in $\mathrm{H}^1(V, E)$ for small enough $V \subset U$. This factor is generated by an element in $\mathrm{H}^1(U, E_3)$ and as such has an obstruction in $\mathrm{H}^2_!(U, E_{3^n})$ which by the above is non-zero. Well, as an obstruction against being 3^n-divisible in $\mathrm{H}^1(U, E)$. So we have to shrink now U to V. Then the obstruction lies in the dual of the subgroup defined by

$$0 \to \mathrm{H}^1_!(V, E_{3^n}) \to \mathrm{H}^1_!(U, E_{3^n}) \to \bigoplus_{v \in U \setminus V} \mathrm{H}^1_{\mathrm{nr}}(k_v, E_{3^n}).$$

So we have to find a $V \subset U$ such that the Selmer curve that generates $\mathrm{H}^1_!(U, E_{3^n})$ does not die in

$$\mathrm{H}^1_{\mathrm{nr}}(k_v, E_{3^n}) = E_{3^n}/(\mathrm{Frob}_v - 1)E_{3^n}$$

upon evaluating a representing cocycle in the Frobenius Frob_v.

Here we have to recall, where the cocycles take their values: we have a surjection

$$\langle 2, 3, 5 \rangle = \mathbb{Z}[1/30]^*/(\mathbb{Z}[1/30]^*)^3 = \mathrm{H}^1(U, \mu_3) \twoheadrightarrow \mathrm{H}^1(U, E_3)$$

and the Selmer curve is represented by the class of 6, it means that evaluation in Frobenius takes values in the $\mu_3 \subset E_3 \subset E_{3^n}$. Now, a first conditon for non-trivial value is that μ_3 does survive in

$$E_3/(\mathrm{Frob}_v - 1)E_3.$$

But if Frob_v acts non-trivially on E_3, then the coinvariants are a proper quotient, namely the $\mathbb{Z}/3\mathbb{Z}$-quotient, and therefore μ_3 dies. Thus we must have that v is chosen in such a way that v splits completely in $\mathbb{Q}(E_3)/\mathbb{Q}$. Then the Selmer curve localises to

$$\text{Selmer curve cocycle}(\mathrm{Frob}_v) = \mathrm{Frob}_v(\sqrt[3]{6})/\sqrt[3]{6} \in \mu_3 \subset E_3.$$

We further want that this survives under mapping to $E_{3^n}/(\mathrm{Frob}_v - 1)E_{3^n}$ and by Lemma 42 this means that we need $\mathrm{Frob}_v = 1$ in $\mathrm{Gal}(\mathbb{Q}(E_{3^n})/\mathbb{Q})$.

We see that we can find $V = U \setminus \{v\}$ with $\mathrm{H}^1_!(V, E_{3^n}) = 0$ if and only if

$$\mathbb{Q}(E_{3^n}) \text{ and } \mathbb{Q}(\sqrt[3]{6}, \zeta_3)$$

are linearly disjoint over $\mathbb{Q}(\zeta_3)$. Now over $\mathbb{Q}(\zeta_3)$ both fields are abelian and it therefore suffices to check linear disjointness with the field extension in $\mathbb{Q}(E_{3^n})/\mathbb{Q}(\zeta_3)$ that correspoinds to the mod 3 quotient of the Galois group, that is $\mathbb{Q}(E_9)/\mathbb{Q}(\zeta_3)$ as follows from the proof of Lemma 40. But in (5.4) we have computed $\mathbb{Q}(E_9)$ explicitly, and it is not difficult to see that

$$\sqrt[3]{6} \notin \mathbb{Q}(E_9).$$

This concludes the proof of Proposition 39. □

References

[Ba72] Bashmakov, M. I., The cohomology of abelian varieties over a number field, (English translation) *Russian Math. Surveys* **27** (1972), no. 6, 25–70.

[BK75] Birch, B. J., Kuyk, W., editors, *Modular functions of one variable IV*, Proceedings of the International Summer School on Modular Functions of One Variable and Arithmetical Applications, Antwerp 1972, Lecture Notes in Mathematics **476**, Springer, 1975, iv+151pp.

[BO03] Balog, A., Ono, K., Elements of class groups and Shafarevich-Tate groups of elliptic curves, *Duke Math. J.* **120** (2003), no. 1, 35–63.

[Ca62a] Cassels, J. W. S., Arithmetic on curves of genus 1. III. The Tate-Shafarevic and Selmer groups, *Proc. London Math. Soc.* (3) **12** 1962, 259–296.

[Ca62b] Cassels, J. W. S., Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung, *Journal für die reine und angewandte Mathematik* **211** (1962), 95–112.

[Ca91] Cassels, J. W. S., *Lectures on elliptic curves*, London Mathematical Society Student Texts **24**, Cambridge University Press, 1991, vi+137pp.

[Cr] Cremona, J. E., *Elliptic Curve Data*, http://www.warwick.ac.uk/ masgaj/ftp/data/.

[Cr12] Creutz, B., Locally trivial torsors that are not Weil-Châtelet divisible, to appear in *Bull. Lond. Math. Soc.*, arXiv:1206.2420v2[mathNT], 2012.

[ÇS12] Çiperiani, M., Stix, J., Weil–Châtelet divisible elements in Tate–Shafarevich groups I: The Bashmakov problem for elliptic curves over $\mathbb{Q}$, to appear in Compos. Math.

[CR87] Curtis, Ch., Reiner, I., *Methods of representation theory, Vol. II, with applications to finite groups and orders*, Pure and Applied Mathematics, Wiley, New York, 1987, xviii+951.

[DDT97] Darmon, H., Diamond, F., Taylor, R., Fermat's last theorem, in: *Elliptic curves, modular forms & Fermat's last theorem* (Hong Kong, 1993), Int. Press, Cambridge, MA, 1997, 2–140.

[DZ01] Dvornicich, R., Zannier, U., Local-global divisibility of rational points in some commutative algebraic groups, *Bull. Soc. Math. France* **129** (2001), no. 3, 317–338.

[DZ04] Dvornicich, R., Zannier, U., An analogue for elliptic curves of the Grunwald-Wang example, *C. R. Math. Acad. Sci. Paris* **338** (2004), no. 1, 47–50.

[GP03] Gordeev, N. L., Popov, V. L., Automorphism groups of finite dimensional simple algebras, *Ann. of Math.* (2) **158** (2003), no. 3, 1041–1065.

[Gr82] Griess, R. L., Jr., The friendly giant, *Invent. Math.* **69** (1982), no. 1, 1–102.

[SGA7$_I$] Grothendieck, A., *Groupes de Monodromie en Géometrie Algébrique I*, Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I), directed by A. Grothendieck, with collaboration of M. Raynaud and D. S. Rim, Lecture Notes in Mathematics **288**, Springer, 1972, viii+523pp.

[HB94] Heath-Brown, D. R., The size of Selmer groups for the congruent number problem. II. *Invent. Math.* **118** (1994), no. 2, 331–370.

[Jo10] Jones, N., Almost all elliptic curves are Serre curves, *Trans. Amer. Math. Soc.* **362** (2010), no. 3, 1547–1570.

[Ka92] Kamienny, S., Torsion points on elliptic curves and q-coefficients of modular forms, *Invent. Math.* **109** (1992), no. 2, 221–229.
[Ka10] Kane, D.M., On the ranks of the 2-Selmer groups of twists of a given elliptic curve, to appear in *Algebra & Number Theory*, arXiv:1009.1365v2[math.NT], 2010.
[Ke82] Kenku, M. A., On the number of **Q**-isomorphism classes of elliptic curves in each **Q**-isogeny class, *J. Number Theory* **15** (1982), no. 2, 199–202.
[Kl11] Klagsbrun, Z., Selmer ranks of quadratic twists of elliptic curves, Ph.D Thesis, University of California, Irvine, 2011.
[Ma77] Mazur, B., Modular curves and the Eisenstein ideal, *IHES Publ. Math.* **47**, (1977), 33–186.
[Ma78] Mazur, B., Rational isogenies of prime degree (with an appendix by D. Goldfeld), *Invent. Math.* **44** (1978), no. 2, 129–162.
[Ma93] Mazur, B., On the passage from local to global in number theory, *Bull. Amer. Math. Soc.* **29** (1993), no. 1, 14–50.
[Ma07] Matsuno, K., Construction of elliptic curves with large Iwasawa λ-invariants and large Tate-Shafarevich groups, *Manuscripta Math.* **122** (2007), no. 3, 289–304.
[Me94] Merel, L., Bornes pour la torsion des courbes elliptiques sur les corps de nombres, *Invent. Math.* **124** (1996), no. 1-3, 437–449.
[Mi86] Milne, J.S., *Arithmetic duality theorems*, Perspectives in Mathematics, 1. Academic Press, Inc., Boston, MA, 1986.
[MR10] Mazur, B., Rubin, K., Ranks of twists of elliptic curves and Hilbert's Tenth Problem, *Invent. Math.* **181** (2010), 541–575.
[NSW08] Neukirch, J., Schmidt, A., Wingberg, K., *Cohomology of number fields*, second edition, Grundlehren der Mathematischen Wissenschaften **323**, Springer, 2008, xvi+825pp.
[Pa99] Parent, P., Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres, *Journal für die reine und angewandte Mathematik* **506** (1999), 85–116.
[Pa00] Parent, P., Torsion des courbes elliptiques sur les corps cubiques, *Ann. Inst. Fourier (Grenoble)* **50** (2000), no. 3, 723–749.
[Pa03] Parent, P., No 17-torsion on elliptic curves over cubic number fields, *J. Théor. Nombres Bordeaux* **15** (2003), no. 3, 831–838.
[Pa10] Paladino, L., On counterexamples to local-global divisibility in commutative algebraic groups, *Acta Arith.* **148** (2011), no. 1, 21–29.
[PRV12] Paladino, L., Ranieri, G., Viada, E., On local-global divisibility by p^n in elliptic curves, *Bull. Lond. Math. Soc.* **44**(2012), no. 4, 789–802.
[PS99] Poonen, B., Stoll, M., The Cassels-Tate pairing on polarized abelian varieties, *Ann. of Math. (2)* **150** (1999), no. 3, 1109–1149.
[S$^+$10] Stein, W. A., et al., *Sage Mathematics Software (Version 4.6)*, The Sage Development Team, 2010, http://www.sagemath.org.
[Se72] Serre, J.-P., Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), no. 4, 259–331.
[Se79] Serre, J.-P., Points rationnels des courbes modulaires $X_0(N)$ [d'après Barry Mazur], *Séminaire Bourbaki* (1977/78), exposé **511**, Lecture Notes in Math. **710** (1979), 89–100.
[Se86] Serre, J.-P., Lettre à Ken Ribet du 7/3/1986, no. 138 in: J.-P. Serre, Œuvres, Vol. 4, Springer Verlag, 2003.
[So07] Soulé, C., An introduction to arithmetic groups, *Frontiers in number theory, physics, and geometry. II*, 247–276, Springer, Berlin, 2007.
[SD08] Swinnerton-Dyer, P., The effect of twisting on the 2-Selmer group. *Math. Proc. Cambridge Philos. Soc.* **145** (2008), no. 3, 513–526.
[Zy10] Zywina, D., Elliptic curves with maximal Galois action on their torsion points, *Bull. Lond. Math. Soc.* **42** (2010), no. 5, 811–826.

Mirela Çiperiani, Department of Mathematics, the University of Texas at Austin, 1 University Station, C1200 Austin, Texas 78712, USA
E-mail address: mirela@math.utexas.edu
URL: http://www.ma.utexas.edu/users/mirela/

Jakob Stix, Mathematisches Institut, Universität Heidelberg, Im Neuenheimer Feld 288, 69120 Heidelberg, Germany
E-mail address: stix@mathi.uni-heidelberg.de
URL: http://www.mathi.uni-heidelberg.de/~stix/