Vanishing of some Galois cohomology groups for elliptic curves

Tyler Lawson* Christian Wuthrich

September 23, 2015

Abstract

Let $E/\mathbb{Q}$ be an elliptic curve and p be a prime number, and let G be the Galois group of the extension of $\mathbb{Q}$ obtained by adjoining the coordinates of the p-torsion points on E. We determine all cases when the Galois cohomology group $H^1\big(G, E[p]\big)$ does not vanish, and investigate the analogous question for $E[p^i]$ when $i > 1$. We include an application to the verification of certain cases of the Birch and Swinnerton-Dyer conjecture, and another application to the Grunwald–Wang problem for elliptic curves.

1 Introduction

Let E be an elliptic curve over $\mathbb{Q}$ and p a prime number. Denote by K the Galois extension of $\mathbb{Q}$ obtained by adjoining the coordinates of the p-torsion points on E and let G be the Galois group of $K/\mathbb{Q}$. The Galois action on the p-torsion points $E[p]$ identifies G with a subgroup of $\mathrm{GL}\big(E[p]\big) \cong \mathrm{GL}_2(\mathbb{F}_p)$ via the representation $\rho\colon \mathrm{Gal}\big(\bar{\mathbb{Q}}/\mathbb{Q}\big) \to \mathrm{GL}\big(E[p]\big)$. A celebrated theorem of Serre [21] shows that G is equal to the full group $\mathrm{GL}_2(\mathbb{F}_p)$ for all but finitely many primes p when the curve is fixed.

We are interested in the vanishing of the Galois cohomology group $H^1\big(G, E[p]\big)$; see [22] or [19] for the basic definitions of Galois cohomology. This specific cohomology group appears as an obstruction in various contexts. For instance, Kolyvagin's work uses the vanishing of this group in the case G is equal to $\mathrm{GL}_2(\mathbb{F}_p)$ (see Proposition 9.1 in [14]). The following first theorem characterizes completely when this cohomology group does not vanish, answering a question at [15].

Theorem 1. *Fix a prime p. Let $E/\mathbb{Q}$ be an elliptic curve, $K = \mathbb{Q}(E[p])$, and G the Galois group of $K/\mathbb{Q}$. Then $H^1\big(G, E[p]\big)$ is trivial except in the following cases:*

- *$p = 3$, there is a rational point of order 3 on E, and there are no other isogenies of degree 3 from E that are defined over $\mathbb{Q}$.*
- *$p = 5$ and the quadratic twist of E by $D = 5$ has a rational point of order 5, but no other isogenies of degree 5 defined over $\mathbb{Q}$.*
- *$p = 11$ and E is the curve labeled as 121c2 in Cremona's tables [6], given by the global minimal equation $y^2 + x\,y = x^3 + x^2 - 3632\,x + 82757$.*

In each of these cases, $H^1\big(G, E[p]\big)$ has p elements.

Partial results on this question have appeared in various sources. For instance, Lemma 10 in [5] by Coates shows that $H^1\big(G, E[p]\big)$ vanishes when $E[p]$ is irreducible as a Galois module. Section 3 in [4] also treats related questions.

The above result extends to elliptic curves E over more general number fields F if we assume that $F \cap \mathbb{Q}(\mu_p) = \mathbb{Q}$, where $\mathbb{Q}(\mu_p)$ is the field generated by p-th roots of unity. Rather than a single elliptic curve for $p > 5$, one finds possibly infinitely many exceptions for $p = 11$ and $p = 17$, but only finitely

*Partially supported by NSF DMS-1206008.

many further exceptions for each $p > 17$ and none for all p such that $p \equiv 1 \pmod 3$. See Theorem 11 for a precise statement.

Next, we address the analogous question for $E[p^i]$ for $i > 1$, but assuming that $p > 3$.

Theorem 2. *Fix a prime $p > 3$. Let $E/\mathbb{Q}$ be an elliptic curve, $K_i = \mathbb{Q}(E[p^i])$ the extension of $\mathbb{Q}$ obtained by adjoining the coordinates of all p^i-torsion points, and G_i the Galois group of $K_i/\mathbb{Q}$. Then $H^1\big(G_2, E[p^2]\big)$ is trivial if and only if $H^1\big(G_i, E[p^i]\big)$ is trivial for all $i \geqslant 2$. This vanishing holds if and only if (E, p) is not among the following cases:*

- *$p = 5$ or $p = 7$ and E contains a rational p-torsion point.*
- *$p = 5$ and there is an isogeny $\varphi\colon E \to E'$ of degree 5 defined over $\mathbb{Q}$ and the quadratic twist by $D = 5$ of E contains a rational 5-torsion point.*
- *$p = 5$ and there is an isogeny $\varphi\colon E \to E'$ of degree 5 defined over $\mathbb{Q}$ but none of degree 25 and the quadratic twist by $D = 5$ of E' contains a rational 5-torsion point.*
- *$p = 5$ and E admits an isogeny $E \to E' \to E''$ of degree 25 defined over $\mathbb{Q}$ and E' contains a rational 5-torsion point.*
- *$p = 11$ and E is 121c1 or 121c2.*

Again, we will also obtain some results that are valid over more general base fields F with $F \cap \mathbb{Q}(\mu_p) = \mathbb{Q}$, and some that are valid for $p = 3$. See Section 6.

This more general question has also been investigated before, and Cha has obtained results in this direction in [3]. He proved the vanishing of $H^1\big(G_i, E[p^i]\big)$ when $p > 3$, the curve has semi-stable reduction at an unramified place above p, and E does not have a rational p-torsion point. He also describes when this cohomology group vanishes for $p = 3$ under his assumptions. The method of proof is similar.

The results in Theorem 2 can be applied to the Grunwald–Wang problem for elliptic curves as formulated by Dvornicich and Zannier in [9]. In Proposition 25, we give an example of an elliptic curve $E/\mathbb{Q}$ with a point $P \in E(\mathbb{Q})$ divisible by $m = 9$ in $E(\mathbb{Q}_\ell)$ for almost all primes ℓ but not divisible by 9 in $E(\mathbb{Q})$. Previously, the only known examples [10] were with $m = 4$. In Theorem 24, we also give a simplified proof of the result in [20] that it is impossible to find such a point P when $m = p^2$ and $p > 3$.

The paper is structured as follows. We begin with some background in Section 2, both establishing notation and reducing to cases where the Galois group G does not contain a nontrivial homothety. In Section 3 we prove a general form of Theorem 1. Section 4 establishes a vanishing result for H^2. In Section 5 we give an application to verifying cases of the Birch and Swinnerton-Dyer conjecture, correcting an oversight in [13]. Our main results classifying the vanishing of $H^1(G_i, E[p^i])$ are then discussed in Section 6, and some supplementary numerical computations for $H^1(G_2, E[p^2])$ are included in Section 7. Finally, in Section 8 we give the application to the Grunwald–Wang problem for elliptic curves.

Acknowledgments

It is our pleasure to thank Jean Gillibert and John Coates for interesting comments and suggestions. We are also grateful to Brendan Creutz for pointing us to [7].

2 Preliminaries and notation

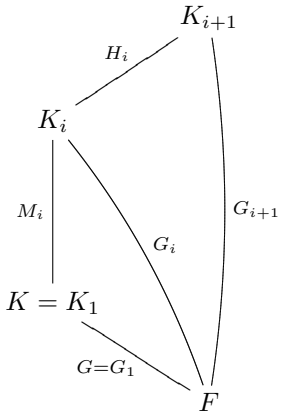
Throughout this paper E will be an elliptic curve defined over a number field F and p will be a prime number. We will denote by $K = F\big(E[p]\big)$ the number field obtained by adjoining the coordinates of the p-torsion points to F. Let G be the Galois group of K/F. More generally, for $i \geqslant 1$ we let $K_i = F\big(E[p^i]\big)$ and $G_i = \mathrm{Gal}(K_i/F)$. The faithful actions of G_i on $E[p^i]$ give embeddings $G_i \hookrightarrow \mathrm{Aut}(E[p^i]) \cong \mathrm{GL}_2(\mathbb{Z}/p^i)$, and so we may regard them as subgroups.

We will also use the groups $H_i = \mathrm{Gal}(K_{i+1}/K_i)$ and $M_i = \mathrm{Gal}(K_i/K)$. We note that, as H_i is the kernel of the map $G_{i+1} \to G_i$, it is identified with a subgroup of

$$\ker\Big(\mathrm{GL}_2(\mathbb{Z}/p^{i+1}) \to \mathrm{GL}_2(\mathbb{Z}/p^i)\Big) \cong \mathrm{Mat}_2(\mathbb{F}_p),$$

where the conjugation action of $G_{i+1} \subset \mathrm{GL}_2(\mathbb{Z}/p^{i+1})$ is by the adjoint representation. Therefore, all elements in H_i have order p and commute with the elements of M_{i+1} inside G_{i+1}.

In summary, we have the following situation:



We will later use the inflation-restriction sequence

$$0 \longrightarrow H^1\big(G_i, E[p^j]\big) \xrightarrow{\inf} H^1\big(G_{i+1}, E[p^j]\big) \xrightarrow{\mathrm{res}} H^1\big(H_i, E[p^j]\big)^{G_i} \longrightarrow H^2\big(G_i, E[p^j]\big) \tag{1}$$

which is valid for all $1 \leqslant j \leqslant i$. In inductive arguments, we will also use that the short exact sequence

$$0 \longrightarrow E[p] \longrightarrow E[p^j] \longrightarrow E[p^{j-1}] \longrightarrow 0$$

gives a long exact sequence

$$E(F)[p^{j-1}] \longrightarrow H^1\big(G_i, E[p]\big) \longrightarrow H^1\big(G_i, E[p^j]\big) \longrightarrow H^1\big(G_i, E[p^{j-1}]\big). \tag{2}$$

As mentioned in the introduction, these cohomology groups only start to be interesting when $E[p]$ is reducible. The following argument for this is given in [3] as Theorem 7.

Lemma 3. *If G contains a non-trivial homothety, then $H^1\big(G_i, E[p^i]\big) = 0$.*

Proof. Let g be a non-trivial homothety. Since g is central, $\langle g \rangle$ is a normal subgroup in G. Consider the inflation-restriction sequence

$$0 \longrightarrow H^1\big(G/\langle g \rangle, E[p]^{g=1}\big) \longrightarrow H^1\big(G, E[p]\big) \longrightarrow H^1\big(\langle g \rangle, E[p]\big)$$

The homothety g cannot have fixed points in $E[p]$; in particular $E(F)[p] = 0$. The left-hand side cohomology group in the above sequence is therefore trivial. The right-hand side is also trivial because $\langle g \rangle$ is of order coprime to p.

We assume by induction that $H^1\big(G_i, E[p^i]\big)$ and $H^1\big(G_i, E[p]\big)$ are both trivial. By assumption, the restriction maps

$$H^1\big(G_{i+1}, E[p^i]\big) \longrightarrow H^1\big(H_i, E[p^i]\big)^{G_i} \cong \mathrm{Hom}\big(H_i, E[p^i]\big)^{G_i}$$

$$H^1\big(G_{i+1}, E[p]\big) \longrightarrow H^1\big(H_i, E[p]\big)^{G_i} \cong \mathrm{Hom}\big(H_i, E[p]\big)^{G_i}$$

from (1) are both injective. Note that the target groups are actually equal because all elements in H_i have order p. Since M_{i+1} and H_i commute, the action of G_i on H_i factors through G, so the target in both cases is $\mathrm{Hom}\big(H_i, E[p]\big)^G$.

The homothety g acts trivially on H_i and non-trivially on any non-zero point in $E[p]$. Therefore, there are no homomorphisms from H_i to $E[p]$ which are fixed by g. It follows that $H^1\big(G_{i+1}, E[p^i]\big)$ and $H^1\big(G_{i+1}, E[p]\big)$ are both trivial. The exact sequence (2) now implies that $H^1\big(G_{i+1}, E[p^{i+1}]\big)$ is also trivial. □

Lemma 4. *Suppose $p > 2$. Assume that G does not contain a non-trivial homothety and $F \cap \mathbb{Q}(\mu_p) = \mathbb{Q}$. Then G is contained in a Borel subgroup.*

Proof. By the Weil pairing, the determinant of ρ is the Teichmüller character ω describing the action of Galois on the p-th roots of unity μ_p. The assumption $F \cap \mathbb{Q}(\mu_p) = \mathbb{Q}$ implies that $\det\colon G \to \mathbb{F}_p^\times$ must be surjective.

Assume first that $p > 3$. We fix a basis of $E[p]$ and view G as a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. By the classification of maximal subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$, we have to show that the following cases can not occur: G is a subgroup of the normalizer of a split Cartan group, G is a subgroup of the normalizer of a non-split Cartan group, or G maps to an exceptional group A_4, A_5 or S_4 in $\mathrm{PGL}_2(\mathbb{F}_p)$.

Suppose G is a subgroup of the group of diagonal and anti-diagonal matrices, which is the normalizer of a split Cartan subgroup. Suppose moreover that G is not a subgroup of the diagonal matrices. The square of $\left(\begin{smallmatrix} 0 & b \\ c & 0 \end{smallmatrix}\right) \in G$ is the homothety by bc. Therefore, all anti-diagonal elements in G must be of the form $\left(\begin{smallmatrix} 0 & c^{-1} \\ c & 0 \end{smallmatrix}\right)$. Multiplying this with a diagonal element $\left(\begin{smallmatrix} u & 0 \\ 0 & v \end{smallmatrix}\right)$ in G then shows that all diagonal elements must have determinant 1. Hence the determinant would not be surjective for $p > 3$.

Next, suppose that G is a subgroup of the normalizer of a non-split Cartan group. Since G contains no non-trivial homothety, the image of G in $\mathrm{PGL}_2(\mathbb{F}_p)$ is isomorphic to G. In other words, G must be a subgroup of a dihedral group of order $2(p+1)$. No such group could have a surjective map onto $\mathbb{F}_p^\times$ if $p > 3$.

Finally, assume that G is exceptional. As before, our hypothesis implies that G is isomorphic to a subgroup of A_4, A_5 or S_4. However the only case in which we could have a surjective map onto $\mathbb{F}_p^\times$ with $p > 3$ is when $p = 5$ and G is a cyclic group of order 4 in S_4. However, as $\mathbb{F}_5$ contains the fourth roots of unity μ_4, all such subgroups are diagonalizable in $\mathrm{GL}_2(\mathbb{F}_5)$.

We now return to the case $p = 3$. By assumption, G is isomorphic to its image in $\mathrm{PGL}_2(\mathbb{F}_p)$, which is the full symmetric group on the four elements $\mathbb{P}^1(\mathbb{F}_3)$. Since the determinant is surjective, the image of G cannot be contained in the alternating group. Therefore it is not transitive on $\mathbb{P}^1(\mathbb{F}_3)$, and G is contained in a Borel subgroup. □

From now on we will suppose that $\varphi\colon E \to E'$ is an isogeny of degree p defined over F, and write $E[\varphi]$ for its kernel. The dual isogeny is denoted by $\hat{\varphi}\colon E' \to E$. We will now also fix a basis of $E[p]$ with the property that the first point belongs to $E[\varphi]$. In this basis, the Galois representation $\rho\colon \mathrm{Gal}\big(\bar{F}/F\big) \to \mathrm{GL}\big(E[p]\big) \cong \mathrm{GL}_2(\mathbb{F}_p)$ now takes values in the Borel subgroup of upper triangular matrices. We will write $\chi\colon \mathrm{Gal}\big(\bar{F}/F\big) \to \mathbb{F}_p^\times$ for the character of the Galois group on $E'[\hat{\varphi}]$. Then the character on $E[\varphi]$ is $\omega\chi^{-1}$, where ω is the Teichmüller character introduced above. The representation now is of the form $\rho = \left(\begin{smallmatrix} \omega\chi^{-1} & * \\ 0 & \chi \end{smallmatrix}\right)$.

Corollary 5. *Suppose $p > 2$. If $F \cap \mathbb{Q}(\mu_p) = \mathbb{Q}$ and the group $H^1\big(G, E[p]\big)$ is non-trivial, then E admits exactly one isogeny $\varphi\colon E \to E'$ of degree p that is defined over F.*

Proof. By Lemma 3, we know that there is no non-trivial homothety in G. Then Lemma 4 implies that G is contained in a Borel subgroup. Hence there is a subgroup of order p in $E[p]$ fixed by the Galois group. If there were a second subgroup of order p fixed by the Galois group, then in a suitable basis of $E[p]$ the group G would consist of diagonal matrices. It would follow that G has order coprime to p and therefore that the cohomology group is trivial. Therefore, there is a unique isogeny defined over F of degree p. □

3 Proof of Theorem 1

We begin by assuming that E is defined over a number field F such that $F \cap \mathbb{Q}(\mu_p) = \mathbb{Q}$.

Lemma 6. *The cohomology group $H^1(G; E[2])$ always vanishes.*

Proof. The group $\mathrm{GL}_2(\mathbb{F}_2)$ is isomorphic to the symmetric group on 3 letters. For any cyclic subgroup of $\mathrm{GL}_2(\mathbb{F}_2)$ of order 2 generated by h, we may compute $H^1\big(\langle h\rangle, E[2]\big)$ as the quotient of the kernel of the norm $N_G = 1 + h$ on $E[2]$ modulo the image of $h - 1$. Because $p = 2$, this group is trivial.

For a general subgroup $G \leqslant \mathrm{GL}_2(\mathbb{F}_2)$, let H be the intersection of G with the normal subgroup of order 3. We have $H^1\big(H, E[2]\big) = 0$ because the order of H is coprime to 2. We also have $H^1\big(G/H, E[2]^H\big) = 0$ because H is either of order 3 and only fixes 0 in $E[2]$, or H is trivial and this group is $H^1\big(\langle h\rangle, E[2]\big) = 0$. By the inflation-restriction sequence, we conclude that $H^1\big(G, E[2]\big) = 0$. □

Lemma 7. *Let $H < \mathrm{GL}_2(\mathbb{F}_p)$ be the subgroup generated by $h = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. We have an isomorphism*

$$H^1\big(H, E[p]\big) \cong \mathbb{F}_p,$$

and the action of an element $g = \left(\begin{smallmatrix} u & w \\ 0 & v \end{smallmatrix}\right)$ in the normalizer $N(H)$ of H on this cohomology group is multiplication by $u^{-1}v^2$.

Proof. The cohomology of the cyclic group H is computed to be

$$H^1\big(H, E[p]\big) \cong \frac{\ker\big(\sum_{a=0}^{p-1} h^a\big)}{\mathrm{im}(h-1)} = \frac{\ker(0)}{\mathrm{im}\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)} \cong \mathbb{F}_p.$$

The explicit isomorphism $i\colon H^1\big(H, E[p]\big) \to \mathbb{F}_p$ sends a cocycle $\xi\colon H \to E[p]$ to the second coordinate of $\xi(h)$. Let now $g = \left(\begin{smallmatrix} u & w \\ 0 & v \end{smallmatrix}\right)$ be an element of $N(H)$ with $u, v \in \mathbb{F}_p^\times$. Then the action of g on $\xi \in H^1\big(H, E[p]\big)$ is as follows.

$$\begin{aligned}
\big(g \star \xi\big)(h) &= g\,\xi\big(g^{-1}hg\big) \\
&= g\,\xi\big(h^{u^{-1}v}\big) \\
&= g\,\big(h^{u^{-1}v-1} + \cdots + h + 1\big)\xi(h) \\
&= \left(\begin{smallmatrix} u & 0 \\ 0 & v \end{smallmatrix}\right)\left(\begin{smallmatrix} u^{-1}v & * \\ 0 & u^{-1}v \end{smallmatrix}\right)\left(\begin{smallmatrix} * \\ i(\xi) \end{smallmatrix}\right)
\end{aligned}$$

Here the terms denoted by $*$ are unknown entries which do not alter the result that

$$i\big(g \star \xi\big) = u^{-1}\,v^2\,i(\xi).$$ □

For the remainder of this section we will assume that $p > 2$ and E satisfies $H^1\big(G, E[p]\big) \neq 0$; we wish to show that we fall into one of the cases listed in the Theorem 1.

Lemma 8. *Suppose $p > 2$. Then G satisfies $H^1\big(G, E[p]\big) \neq 0$ if and only if $p \not\equiv 1 \pmod 3$ and there exists a basis of $E[p]$ such that G consists of all matrices of the form $\left(\begin{smallmatrix} v^2 & w \\ 0 & v \end{smallmatrix}\right)$ with $v \in \mathbb{F}_p^\times$ and $w \in \mathbb{F}_p$. In this case, the cohomology group is isomorphic to $\mathbb{F}_p$ and the representation ρ is of the form $\left(\begin{smallmatrix} \chi^2 & * \\ 0 & \chi \end{smallmatrix}\right)$, where χ^3 is the Teichmüller character ω.*

Proof. By Corollary 5, we may view G as a group of upper triangular matrices containing the subgroup H generated by element $h = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ of order p.

Since H is a normal subgroup of G, we can use the inflation-restriction sequence to show that

$$H^1\big(G, E[p]\big) \longrightarrow H^1\big(H, E[p]\big)^{G/H}$$

is an isomorphism because G/H is of order coprime to p. Because we assumed that $H^1\big(G, E[p]\big)$ is non-trivial, by Lemma 7 we must have that G/H acts trivially on $H^1\big(H, E[p]\big)$, that $H^1\big(G, E[p]\big)$ has precisely p elements, and that all elements in G must be of the form $\left(\begin{smallmatrix} v^2 & w \\ 0 & v \end{smallmatrix}\right)$ with $w \in \mathbb{F}_p$ and $v \in \mathbb{F}_p^\times$.

Recall that the character χ is such that $\rho = \left(\begin{smallmatrix} \omega\chi^{-1} & * \\ 0 & \chi \end{smallmatrix}\right)$. We now deduce that $\chi^2 = \omega\chi^{-1}$ and hence $\chi^3 = \omega$. Since we assumed $F \cap \mathbb{Q}(\mu_p) = \mathbb{Q}$, the determinant ω from G to $\mathbb{F}_p^\times$ must be surjective. As the determinant of the typical element in G is v^3 with $v \in \mathbb{F}_p^\times$, we must conclude that either $p = 3$ or $p \equiv 2 \pmod 3$, and that G is equal to the group of all matrices of the form $\left(\begin{smallmatrix} v^2 & w \\ 0 & v \end{smallmatrix}\right)$. □

Corollary 9. *If $p = 3$, we have $H^1\big(G, E[3]\big) \neq 0$ if and only if E has a 3-torsion point and no other isogenies defined over F.*

Proof. This can only occur if the group G is the group of matrices of the form $\left(\begin{smallmatrix} 1 & w \\ 0 & v \end{smallmatrix}\right)$ of order 6. This is precisely the case when $E(F)[3]$ is of order 3 and no other isogenies are defined over F. □

Lemma 10. *If $p = 5$, we have $H^1\big(G, E[5]\big) \neq 0$ if and only if the quadratic twist of E by $D = 5$ has a 5-torsion point and no other isogenies defined over F.*

Proof. This happens precisely when we have

$$\rho = \begin{pmatrix} \omega^2 & * \\ 0 & \omega^{-1} \end{pmatrix}$$

Here ω^2 is the quadratic character corresponding to the non-trivial extension $F\big(\sqrt{5}\big)/F$ contained in $F(\mu_5)$. Let $E^\dagger$ be the quadratic twist of E by $D = 5$. Then we have the desired form of representation ρ if and only if the representation $\rho^\dagger$ on $E^\dagger[5]$ is now of the form $\left(\begin{smallmatrix} 1 & * \\ 0 & \omega \end{smallmatrix}\right)$. We conclude that this occurs if and only if $E^\dagger(F)[5]$ has five points and $E^\dagger$ has no other isogenies of degree 5 defined over F. □

Theorem 11. *Let E be an elliptic curve defined over a number field F with $F \cap \mathbb{Q}(\mu_p) = \mathbb{Q}$. Let $K = F\big(E[p]\big)$ and $G = \mathrm{Gal}(F/K)$. Then $H^1\big(G, E[p]\big) = 0$ except in the following cases:*

- *$p = 3$, there is a rational 3-torsion point in $E(F)$, and there are no other 3-isogenies from E defined over F.*
- *$p = 5$ and the quadratic twist of E by $D = 5$ has a rational point of order 5, but no other isogenies of degree 5 defined over F.*
- *$p \geqslant 11$, $p \equiv 2 \pmod 3$, there is a unique isogeny $\varphi\colon E \to E'$ of degree p defined over F, its kernel $E[\varphi]$ acquires a rational point over $F \cdot \mathbb{Q}(\mu_p)^+$, and $E[\varphi] \cong \mu_p^{\otimes(p+1)/3}$.*

There are only finitely many cases for each prime p with $p > 17$.

Proof. The only remaining cases to prove are those where $p > 5$. As we may assume $p \equiv 2 \pmod 3$, one sees that

$$\rho = \begin{pmatrix} \omega^{\frac{p+1}{3}} & * \\ 0 & \omega^{\frac{2-p}{3}} \end{pmatrix}.$$

This explains the condition in the cases $p \geqslant 11$ in the above list.

The curve E and its unique isogeny φ of degree p defined over F represent a point on the modular curve $Y_0(p)$ defined over F. For $p = 11$ and $p = 17$, the curve $Y_0(p)$ is of genus 1; for all larger primes $p \equiv 2 \pmod 3$ it is of genus at least two. Therefore there are only finitely many $\bar{\mathbb{Q}}$-isomorphism classes of curves E/F with an isogeny of degree p defined over F. Only a single twist in each class can have ρ of the above shape. Hence there are only finitely many exceptions for $p > 17$. □

We specialize now to the field $F = \mathbb{Q}$ where the points on $Y_0(p)$ are well-known.

Lemma 12. *If $F = \mathbb{Q}$ and $p > 5$, we have $H^1\big(G, E[p]\big) \neq 0$ if and only if E is the curve labeled as 121c2 in Cremona's tables.*

Proof. For all those p, there are only a finite number of $\bar{\mathbb{Q}}$-isomorphism classes of elliptic curves E with a p-isogeny defined over $\mathbb{Q}$. Mazur's theorem [16] shows that there are no rational points on $Y_0(p)$ except for three points on $Y_0(11)$ and two points on $Y_0(17)$. All of these five examples have no other automorphisms than ± 1. Hence, all elliptic curves $E/\mathbb{Q}$ representing one of them are quadratic twists of each other.

Let us first look at $p = 11$. The j-invariants of the three families are -121, -32768, and -24729001, and the representation ρ must now be of the form $\left(\begin{smallmatrix} \omega^4 & * \\ 0 & \omega^7 \end{smallmatrix}\right)$. We start with the last. The curve 121c2 is an example of an elliptic curve with j-invariant -24729001. Using SageMath [23], we find a point P of order 11 in $E\big(\mathbb{Q}(\mu_{11})\big)$. Its x-coordinate in the global minimal model given above is $11\zeta^9+11\zeta^8+22\zeta^7+22\zeta^6+22\zeta^5+22\zeta^4+11\zeta^3+11\zeta^2+39$, where ζ is a primitive 11-th root of unity. One finds that $\sigma(P) = 5P$ for the Galois element with $\sigma(\zeta) = \zeta^2$. Therefore the action of Galois on the group generated by P is given by ω^4. The isogeny with P in its kernel is defined over $\mathbb{Q}$ and it is the only isogeny on E defined over $\mathbb{Q}$. Therefore the group G is precisely of the form required. Hence $H^1\big(G, E[p]\big)$ has p elements. No quadratic twist of E could have the same property.

With similar computation one finds that the group G for the curve 121b1 with j-invariant -32768 is of the form $\left(\begin{smallmatrix} \omega^8 & * \\ 0 & \omega^3 \end{smallmatrix}\right)$ and for the curve 121c1 with j-invariant -121 it is $\left(\begin{smallmatrix} \omega^7 & * \\ 0 & \omega^4 \end{smallmatrix}\right)$. No quadratic twist of these curves could have the required form for G.

For $p = 17$, the representation ρ must now be of the form $\left(\begin{smallmatrix} \omega^6 & * \\ 0 & \omega^{11} \end{smallmatrix}\right)$. In particular, for any prime $\ell \neq 11$ of good reduction for E, the Frobenius element is sent to a matrix of the form $\left(\begin{smallmatrix} \ell^6 & * \\ 0 & \ell^{11} \end{smallmatrix}\right)$. We conclude that we must have $\ell^6 + \ell^{11} \equiv a_\ell \pmod{p}$, where a_ℓ is the trace of Frobenius. This gives an easy criterion to rule out specific curves.

There are two j-invariants of elliptic curves that admit a 17-isogeny over $\mathbb{Q}$: $-297756989/2$ and $-882216989/131072$. In fact, these values were computed by Vélu and published on page 80 of [1]. We pick a curve E for each of these j-invariants. The curves 14450p1 and 14450n1 are examples. Now for both curves, it is easy to show that $\pm 3^6 \pm 3^{11} \not\equiv a_3 \pmod{17}$ for any choice of the signs as $a_3 = \pm 2$. Therefore no quadratic twist of E will satisfy the congruence that we need. Thus $H^1\big(G, E[p]\big) = 0$ for all curves with a degree-17 isogeny. Similar computations were done by Greenberg in Remark 2.1.2 in [12]. □

This concludes the proof of Theorem 1.

4 Vanishing of the second cohomology

We continue to assume that E is defined over a number field F such that $F \cap \mathbb{Q}(\mu_p) = \mathbb{Q}$.

Lemma 13. *Let p be a prime. Then $H^2\big(G, E[p]\big) = 0$ except if $p > 2$, E admits a p-isogeny $\varphi\colon E \to E'$ and no other p-isogenies over F, and $E'[\hat{\varphi}]$ contains an F-rational p-torsion point. If this cohomology group is non-zero then it contains p elements.*

We could also write the condition in the lemma as either that $E[\varphi] \cong \mu_p$ or that χ is trivial.

Proof. As before, only the cases when p divides the order of G are of interest.

We again discuss the case $p = 2$ separately. A Sylow subgroup of G is a cyclic group of order 2 generated by h, and the restriction $H^2\big(G, E[p]\big) \to H^2\big(\langle h\rangle, E[p]\big)$ is an inclusion. However, $H^2\big(\langle h\rangle, E[p]\big)$ can be computed as the Tate cohomology group $\hat{H}^0\big(\langle h\rangle, E[p]\big)$, which is zero.

For $p > 2$, we have to deal with the cases when G contains $\mathrm{SL}\big(E[p]\big)$ and when G is contained in a Borel subgroup.

In the first case, G is actually the full group $\mathrm{GL}\big(E[p]\big)$ as the Weil pairing forces the determinant to be surjective. If Z is the center of G, then $H^i\big(Z, E[p]\big) = 0$ for all $i \geqslant 0$. The Hochschild-Serre spectral sequence implies that $H^i\big(G, E[p]\big) = 0$ for all $i \geqslant 0$.

Now we may assume that G is contained in the Borel subgroup of upper-triangular matrices. If there is more that one isomorphism class of p-isogeny leaving E which is defined over F, then G is of order coprime to p and hence $H^2\big(G, E[p]\big) = 0$. Therefore, we may assume that G contains the unique p-Sylow

H generated by $h = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Since H is normal and G/H is of order coprime to p, the restriction

$$H^2\big(G, E[p]\big) \cong H^2\big(H, E[p]\big)^{G/H}$$

is an isomorphism.

Fix an injective homomorphism $\psi\colon H \to \mathbb{Q}/\mathbb{Z}$. Let $\delta\colon H^1\big(H, \mathbb{Q}/\mathbb{Z}\big) \to H^2\big(H, \mathbb{Z}\big)$ be the connecting homomorphism. Then we have an isomorphism $\hat{H}^0\big(H, E[p]\big) \to H^2\big(H, E[p]\big)$ given by sending a point $P \in E[p]$ to the cup product $\delta\psi \cup P$. For $p > 2$, the Tate cohomology group $\hat{H}^0\big(H, E[p]\big)$ is equal to the usual cohomology group $H^0\big(H, E[p]\big) = E[\varphi]$, which has p elements.

Let $g = \left(\begin{smallmatrix} u & w \\ 0 & v \end{smallmatrix}\right) \in G$. On the one hand, it acts on P by multiplication by u. On the other hand, it acts on ψ by multiplication by $u^{-1}v$ because

$$(g \star \psi)(h) = g\,\psi\big(g^{-1}hg\big) = \psi\big(h^{u^{-1}v}\big) = u^{-1}v\,\psi(h).$$

It follows that g acts on the generator of $H^2\big(H, E[p]\big)$ by multiplication by $uu^{-1}v = v$. Unless all such $g \in G$ have $v = 1$, we conclude that the second cohomology group vanishes. Otherwise it has p elements, and this occurs if and only if $E'[\hat{\varphi}]$ contains a rational p-torsion point. □

5 Application to the conjecture of Birch and Swinnerton-Dyer and p-descent

The vanishing of the Galois cohomology group we consider is used when trying to extend Kolyvagin's results to find a sharper bound on the Birch and Swinnerton-Dyer conjecture for elliptic curves of analytic rank at most 1. This was the original motivation in Cha's work [3]. In [13], the authors attempt to extend Cha's results, but there is a mistake in the proof of their Lemma 5.4 and consequently their Theorem 3.5 is not correct. The latter is also copied as Theorem 5.3 in [17]. Using our results above, we can now state and prove a corrected version of Theorem 3.5 in [13]. We refer to the original paper for the notations.

Theorem 14. *Let $E/\mathbb{Q}$ be an elliptic curve of analytic rank at most 1. Let p be an odd prime. Let F a quadratic imaginary field satisfying the Heegner hypothesis and suppose p does not ramify in $F/\mathbb{Q}$. Suppose that (E, p) does not appear in the list of Theorem 1 and that E is not isogenous to an elliptic curve over $\mathbb{Q}$ such that the dual isogeny contains a rational p-torsion point. Then the p-adic valuation of the order of the Tate-Shafarevich group is bounded by twice the index of the Heegner point.*

Proof. In their proof, only the vanishing of $H^1\big(G, E[p]\big)$ and $H^2\big(G, E[p]\big)$ are needed for the argument. Under our assumptions they both vanish by Theorem 1 and Lemma 13. One has also to note that, as pointed out in [17], the assumption in their theorem that E does not admit complex multiplication is not used in the proof. Finally, the paper [13] needs that F is not included in $K = \mathbb{Q}\big(E[p]\big)$ to conclude that $H^i\big(\mathrm{Gal}(F(E[p])/F), E[p]\big)$ also vanishes for $i = 1$ and 2. This is guaranteed by the Heegner hypothesis and the assumption that p does not ramify in F, as F and K then have disjoint sets of ramified primes. □

The following is a short-cut in the usual p-descent for E =121c2 and $p = 11$. It is not a new result as it appears already in [18] as Example 7.4. However it illustrates that the non-trivial class in $H^1\big(G, E[p]\big)$ can be of use.

Proposition 15. *The Tate-Shafarevich group of the curve 121c2 does not contain any non-trivial elements of order 11. The full Birch and Swinnerton-Dyer conjecture holds for this curve.*

Proof. Set $p = 11$. Let $\varphi\colon E \to E'$ be the p-isogeny defined over $\mathbb{Q}$. We saw before that $E[\varphi] \cong \mathbb{F}_p(4)$ and $E'[\hat{\varphi}] \cong \mathbb{F}_p(7)$ where $\mathbb{F}_p(k)$ is the 1-dimensional $\mathbb{F}_p$-vector space with the Galois group acting by the character ω^k.

Let F be the maximal extension of $\mathbb{Q}$ which is unramified at all finite places $\ell \neq p$. Write $\mathcal{G} = \mathrm{Gal}\big(F/\mathbb{Q}\big)$ and $\mathcal{H} = \mathrm{Gal}\big(F/\mathbb{Q}(\zeta)\big)$ where ζ is a primitive p-th root of 1. Let $\Gamma = \mathcal{G}/\mathcal{H}$. Since $|\Gamma|$ is

coprime to p, we have an isomorphism $H^1\big(\mathcal{G}, E[\varphi]\big) \cong H^1(\mathcal{H}, E[\varphi])^{\Gamma}$. Now Dirichlet's unit theorem can be used to compute

$$H^1\big(\mathcal{H}, \mathbb{F}_p(1)\big) = H^1\big(\mathcal{H}, \mu_p\big) \cong \mathbb{F}_p(1) \oplus \bigoplus_{i=0}^{4} \mathbb{F}_p(2\,i)$$

as a $\mathbb{F}_p[\Gamma]$-module; see for instance Corollary 8.6.12 (or 8.7.3 in the second edition) in [19]. Since $H^1\big(\mathcal{H}, \mathbb{F}_p(k)\big) \cong H^1\big(\mathcal{H}, \mathbb{F}_p(1)\big)(k-1)$, the group $H^1\big(\mathcal{G}, \mathbb{F}_p(k)\big)$ is a sum of copies of $\mathbb{F}_p$ corresponding to the copies of $\mathbb{F}_p(1-k)$ in $H^1\big(\mathcal{H}, \mathbb{F}_p(1)\big)$. We deduce that $H^1\big(\mathcal{G}, E[\varphi]\big)$ is trivial and that $H^1\big(\mathcal{G}, E'[\hat{\varphi}]\big)$ is 1-dimensional.

Since $K/\mathbb{Q}$ is only ramified at p, we have an inflation map $H^1\big(G, E'[\hat{\varphi}]\big) \to H^1\big(\mathcal{G}, E'[\hat{\varphi}]\big)$. By Theorem 1 and the above, this is now an isomorphism and our explicit cocycle ξ can be viewed as a generator for $H^1\big(\mathcal{G}, E'[\hat{\varphi}]\big)$.

The $\hat{\varphi}$-Selmer group $\mathrm{Sel}^{\hat{\varphi}}$ is defined to be the kernel of the map

$$H^1\big(\mathcal{G}, E'[\hat{\varphi}]\big) \to H^1\big(\mathbb{Q}_p, E'\big)[\hat{\varphi}].$$

An explicit local computation shows that $\hat{\varphi}\colon E'(\mathbb{Q}_p) \to E(\mathbb{Q}_p)$ is surjective. Therefore $H^1\big(\mathbb{Q}_p, E'\big)[\hat{\varphi}] \cong H^1\big(\mathbb{Q}_p, E'[\hat{\varphi}]\big)$. Since $K/\mathbb{Q}$ is totally ramified at p, the decomposition group of $K/\mathbb{Q}$ at the unique place above p in K is equal to G. Therefore ξ also inflates to a non-trivial element in $H^1\big(\mathbb{Q}_p, E'[\hat{\varphi}]\big)$. It follows that the generator of $H^1\big(\mathcal{G}, E'[\hat{\varphi}]\big)$ does not lie in the Selmer group. Therefore $\mathrm{Sel}^{\hat{\varphi}}$ is trivial.

Since $H^1\big(\mathcal{G}, E[\varphi]\big) = 0$, the φ-Selmer group Sel^{φ} is trivial. The usual exact sequence

$$\mathrm{Sel}^{\varphi} \longrightarrow\!\!\!\!\!\rightarrow \mathrm{Sel}^{p}(E/\mathbb{Q}) \longrightarrow\!\!\!\!\!\rightarrow \mathrm{Sel}^{\hat{\varphi}}$$

shows now that the p-Selmer group $\mathrm{Sel}^{p}(E/\mathbb{Q})$ is trivial. Therefore the rank of E is zero and the p-primary part of the Tate-Shafarevich group $Ш(E/\mathbb{Q})$ is trivial.

As explained in Theorem 8.5 in [17], the only prime at which one has to check the Birch and Swinnerton-Dyer conjecture after the Heegner point computations done there is $p = 11$. Therefore, this completes the proof of the conjecture for this specific elliptic curve. □

The main result of [17] (based on [18] and [8]) by Miller and his collaborators states that the Birch and Swinnerton-Dyer conjecture holds for all elliptic curves of conductor at most 5000 and analytic rank at most 1. As a consequence of the error in [13], the verification for some curves in this list is not complete. The following is a description how we performed the necessary computations to fill in the gaps for all these curves. See also [24] for the correction of the corresponding bug in SageMath.

From the change in Theorem 14, it follows that only curves E contained in the list of Theorem 1 could have been affected when verifying the p-part of the conjecture. The case 121c2 was verified in Proposition 15. The exceptional cases with $p = 3$ are already dealt with in Theorem 9.1 in [18], as they were already considered exceptional cases there. That only leaves the curves with non-vanishing $H^1\big(G, E[5]\big)$. For the following list of curves, we had to perform a 5-descent to verify the conjecture: 50a3, 50a4, 75a2, 150b3, 150b4, 175c2, 275b1, 325d2, 550b1, 550f3, 775c1, 950a1, 1050d2, 1425b1, 1450a1, 1650b1, 1650b2, 1650c2, 1650d2, 1950b2, 1975d1, 2175f2, 2350e2, 2550f2, 2850a1, 2850a2, 2850g2, 2950a1, 3075d1, 3075g2, 3325c1, 3550d1, 3850k2, 3950a1, 4350a1, 4350a2, 4425c1, 4450a1, 4450f2, 4650e1, 4650k2, 4650m2. The methods in [18] are sufficient in all these cases. If the rank is 1, then even the weaker bound in their Corollary 7.3 is enough. Otherwise, if the rank is 0, the Selmer groups for φ and $\hat{\varphi}$ are trivial as one finds quickly by looking at a few local conditions.

6 Results for $i > 1$

We now turn to the question of finding all cases of elliptic curves E/F and primes p such that the group $H^1\big(G_i, E[p^i]\big)$ does not vanish for some $i > 1$. We continue to assume that $F \cap \mathbb{Q}(\mu_p) = \mathbb{Q}$ and we will assume now that $p > 2$.

By Lemma 3 and Lemma 4, we know that all these groups vanish unless there is an isogeny $\varphi\colon E \to E'$ defined over F. Therefore, we may continue to assume the existence of φ and that the group G is contained

in the Borel subgroup of upper triangular matrices. This fixes (up to scalar) the first basis element of $E[p]$ and we still have some flexibility about the second; if there is a second subgroup of $E[p]$ fixed by the Galois group, we will choose the second basis element in there. Unlike in the case $i = 1$, we may not yet assume that p divides the order of G.

In what follows we will write expressions like $G = \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$. By this we mean that G is equal to the group of all matrices of this form in $\mathrm{GL}_2(\mathbb{F}_p)$, so $*$ on the diagonal can take any non-zero value and $*$ in the top right corner can be any value in $\mathbb{F}_p$.

Let M be the additive group of 2×2-matrices with coefficients in $\mathbb{F}_p$. Then $G \leqslant \mathrm{GL}_2(\mathbb{F}_p)$ acts on M by conjugation. We would like to determine $\mathrm{Hom}_G\big(M, E[p]\big)$. We do so by computing first $\mathrm{Hom}_G\big(M, E[\varphi]\big)$ and $\mathrm{Hom}_G\big(M, E'[\hat{\varphi}]\big)$.

Lemma 16. *Suppose first $p > 3$. The group $\mathrm{Hom}_G\big(M, E[\varphi]\big)$ is trivial except in the following cases.*

- *If $G = \left(\begin{smallmatrix} 1 & 0 \\ 0 & * \end{smallmatrix}\right)$ in a suitable basis of $E[p]$, then $\mathrm{Hom}_G\big(M, E[\varphi]\big)$ has dimension 2 over $\mathbb{F}_p$.*
- *If $G = \left(\begin{smallmatrix} * & 0 \\ 0 & 1 \end{smallmatrix}\right)$ in a suitable basis of $E[p]$, this group has dimension 1.*
- *If $G = \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$, this group has dimension 1.*
- *If $G \leqslant \left\{ \left(\begin{smallmatrix} u & w \\ 0 & u^2 \end{smallmatrix}\right) \;\middle|\; u \in \mathbb{F}_p^\times, w \in \mathbb{F}_p \right\}$, this group has dimension 1.*

If $p = 3$, the list is the same with one modification to the second and to the last case above.

- *If $G = \left(\begin{smallmatrix} * & 0 \\ 0 & 1 \end{smallmatrix}\right)$ in a suitable basis of $E[3]$, this group has dimension 2.*

Proof. If $f\colon M \to E[\varphi]$ is fixed by $g \in G$, then $f(m) = g \cdot f(g^{-1}mg)$ for all $m \in M$. Let α, β, γ, and δ be the images in $E[\varphi]$ under f of $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ respectively. Then the above equation for m being one of the these four matrices yields four equations that have to hold for all $g = \left(\begin{smallmatrix} u & w \\ 0 & v \end{smallmatrix}\right) \in G$:

$$\begin{aligned} \alpha &= u \cdot (\alpha + u^{-1}w\,\beta) \\ \beta &= u \cdot (u^{-1}v\,\beta) \\ \gamma &= u \cdot (-v^{-1}w\,\alpha - u^{-1}v^{-1}w^2\,\beta + uv^{-1}\,\gamma + v^{-1}w\,\delta) \\ \delta &= u \cdot (\delta - u^{-1}w\,\beta) \end{aligned} \tag{3}$$

From these equations, we deduce the following:

$$\begin{aligned} f \text{ is fixed by } \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) &\iff \beta = 0 \text{ and } \alpha = \delta \\ f \text{ is fixed by } \left(\begin{smallmatrix} 1 & 0 \\ 0 & v \end{smallmatrix}\right) \text{ for some } v \neq 1 &\iff \beta = \gamma = 0 \\ f \text{ is fixed by } \left(\begin{smallmatrix} u & 0 \\ 0 & 1 \end{smallmatrix}\right) \text{ for some } u \neq \pm 1 &\iff \alpha = \gamma = \delta = 0 \\ f \text{ is fixed by } \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right) &\iff \alpha = \delta = 0 \end{aligned}$$

Assume first that G is contained in $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$. Since the determinant must be surjective, G is either $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 1 & 0 \\ 0 & * \end{smallmatrix}\right)$, after choosing a suitable second basis element for $E[p]$. In both cases, the above allows us to verify the statements in the lemma. The case when G is contained in $\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$ is very similar, except that when $p = 3$, in which case we are in the group of matrices with $v = u^2$ and we can only apply the fourth equation instead of the third.

Assume now that G contains an element $\left(\begin{smallmatrix} u & w \\ 0 & v \end{smallmatrix}\right)$ with $v \neq 1$ and one with $u \neq 1$. Then $\beta = 0$ by the second equation in (3). From the last two equations, we deduce that $\alpha = \delta = 0$. Now the equations (3) simplify to one equation $(1 - u^2v^{-1})\gamma = 0$. Therefore, if G is contained in the group of matrices with $v = u^2$, then the dimension of $\mathrm{Hom}_G\big(M, E[\varphi]\big)$ is 1 and $p > 3$ as otherwise all $g \in G$ have $v = 1$, otherwise the space is trivial. □

Recall that $E'[\hat{\varphi}]$ is the kernel of the dual isogeny.

Lemma 17. *Suppose $p > 2$. The group $\mathrm{Hom}_G\big(M, E'[\hat{\varphi}]\big)$ is trivial except in the following cases. If G is contained in $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$ or if $G = \left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$ or if $G = \left\{\left(\begin{smallmatrix} v^2 & 0 \\ 0 & v \end{smallmatrix}\right) \mid v \in \mathbb{F}_p^\times\right\}$ in a suitable basis for $E[p]$, then $\mathrm{Hom}_G\big(M, E'[\hat{\varphi}]\big)$ has dimension 1. If $G = \left(\begin{smallmatrix} * & 0 \\ 0 & 1 \end{smallmatrix}\right)$ in a suitable basis of $E[p]$, then it has dimension 2.*

Proof. This is analogous to the proof of the previous lemma. The equations (3) become equations where the u at the start of the right hand side of each equation is replaced by a v. This new set of equations can be rewritten as follows.

$$\begin{aligned} (1-v)\alpha &= u^{-1}vw\,\beta \\ (1-u^{-1}v^2)\beta &= 0 \\ (1-u)\gamma &= w(\delta-\alpha) - u^{-1}w^2\beta \\ (1-v)\delta &= -u^{-1}vw\,\beta \end{aligned} \tag{4}$$

From here, the computations are again straightforward for the cases when G is contained in $\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$. If G is contained in the group $\left\{\left(\begin{smallmatrix} v^2 & w \\ 0 & v \end{smallmatrix}\right) \mid v \in \mathbb{F}_p^\times, w \in \mathbb{F}_p\right\}$, it is either equal to this group, in which case the cohomology group in question is trivial, or it is equal to a subgroup of order $p-1$. In the latter case, we may change the choice of basis of $E[p]$ to get G to be equal to $\left\{\left(\begin{smallmatrix} v^2 & 0 \\ 0 & v \end{smallmatrix}\right) \mid v \in \mathbb{F}_p^\times\right\}$, in which case $\alpha = \gamma = \delta = 0$, but β is free. In all other cases it is trivial. □

The exact sequence

$$0 \longrightarrow \mathrm{Hom}_G\big(M, E[\varphi]\big) \longrightarrow \mathrm{Hom}_G\big(M, E[p]\big) \xrightarrow{\varphi} \mathrm{Hom}_G\big(M, E'[\hat{\varphi}]\big) \tag{5}$$

connects the results from the previous two lemmas.

Proposition 18. *If $p > 3$, the group $\mathrm{Hom}_G\big(M, E[p]\big)$ vanishes except when, for some choice of basis of $E[p]$, it is one of the following subgroups.*

G	$= \left(\begin{smallmatrix} 1 & 0 \\ 0 & * \end{smallmatrix}\right)$	$= \left(\begin{smallmatrix} * & 0 \\ 0 & 1 \end{smallmatrix}\right)$	$= \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$	$\leqslant \left(\begin{smallmatrix} u & * \\ 0 & u^2 \end{smallmatrix}\right)$	$= \left(\begin{smallmatrix} v^2 & 0 \\ 0 & v \end{smallmatrix}\right)$
$\dim_{\mathbb{F}_p} \mathrm{Hom}_G\big(M, E[p]\big)$	3	3	2	1	1

If $p = 3$, the group $\mathrm{Hom}_G\big(M, E[p]\big)$ vanishes except when, for some choice of basis of $E[p]$, it is one of the following subgroups.

G	$= \left(\begin{smallmatrix} 1 & 0 \\ 0 & * \end{smallmatrix}\right)$	$= \left(\begin{smallmatrix} * & 0 \\ 0 & 1 \end{smallmatrix}\right)$	$= \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$	$= \left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$
$\dim_{\mathbb{F}_3} \mathrm{Hom}_G\big(M, E[3]\big)$	3	4	2	1

Here we have chosen a suitable second basis element in $E[p]$ as in the previous lemmas. Of course, the first two cases are in fact the same when the basis elements are swapped.

Proof. If $\mathrm{Hom}_G\big(M, E'[\hat{\varphi}]\big) = 0$, then the exact sequence (5) reduces this to Lemma 16. Otherwise, we have to check if the homomorphisms $f\colon M \to E'[\hat{\varphi}]$ lift to homomorphisms $e\colon M \to E[p]$ that are G-equivariant. In the following four cases, they all lift indeed. We will just give the explicit map which form a basis of $\mathrm{Hom}_G\big(M, E[p]\big)$ modulo the image from $\mathrm{Hom}_G\big(M, E[\varphi]\big)$. One can verify without difficult that they are G-equivariant.

G	$= \left(\begin{smallmatrix} 1 & 0 \\ 0 & * \end{smallmatrix}\right)$	$= \left(\begin{smallmatrix} * & 0 \\ 0 & 1 \end{smallmatrix}\right)$	$= \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$	$= \left(\begin{smallmatrix} v^2 & 0 \\ 0 & v \end{smallmatrix}\right)$
$e\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 0 \\ a \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 \\ d \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 0 \\ b \end{smallmatrix}\right)$

There is only the case $G = \left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$ left to treat. The generator of $\mathrm{Hom}_G\big(M, E'[\hat{\varphi}]\big)$ is given by $f\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = a + d$. We will show that f does not lift to a map $e\colon M \to E[p]$. Denote by $\left(\begin{smallmatrix} \alpha \\ 1 \end{smallmatrix}\right)$ the image of $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ under such an e and by $\left(\begin{smallmatrix} \beta \\ 0 \end{smallmatrix}\right)$ the image of $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$. Then we must have for all $u \neq 1$ and w in $\mathbb{F}_p$ that

$$\left(\begin{smallmatrix} \beta \\ 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} u & w \\ 0 & 1 \end{smallmatrix}\right) e \left(\begin{smallmatrix} 0 & u^{-1}w \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} u & w \\ 0 & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} u^{-1}w\beta \\ 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} w\beta \\ 0 \end{smallmatrix}\right).$$

Hence $\beta = 0$. Again for all u and w, we should have that

$$\left(\begin{smallmatrix}\alpha\\1\end{smallmatrix}\right) = \left(\begin{smallmatrix}u & w\\0 & 1\end{smallmatrix}\right) e \left(\begin{smallmatrix}1 & u^{-1}w\\0\end{smallmatrix}\right) = \left(\begin{smallmatrix}u & w\\0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}\alpha\\1\end{smallmatrix}\right) = \left(\begin{smallmatrix}u\alpha+w\\1\end{smallmatrix}\right).$$

However, this cannot hold for all choices no matter what α is. □

Definition. Let E/F be an elliptic curve. We will say that G_i is *greatest possible* if it consists of all the matrices in $\mathrm{GL}_2(\mathbb{Z}/p^i\mathbb{Z})$ that reduce to a matrix in G modulo p. Equivalently, M_i is the kernel of the map $\mathrm{GL}_2(\mathbb{Z}/p^i) \to \mathrm{GL}_2(\mathbb{F}_p)$.

We will show that if $p > 2$ and $i > 1$, then G_i is greatest possible if and only if G_2 is greatest possible: Since $G_i \to G_{i-1}$ is surjective, by induction it suffices to prove that the kernel H_{i-1} contains all matrices of the form $1 + p^{i-1}A \in \mathrm{GL}_2(\mathbb{Z}/p^i)$. If G_2 is greatest possible, then for any $A \in M_2(\mathbb{F}_p)$ there exists an element $g \in G_i$ whose image in $\mathrm{GL}_2(\mathbb{Z}/p^2)$ is $1 + pA$. Then $g^{p^{i-2}}$ has image $(1 + p^{i-1}A)$ in $\mathrm{GL}_2(\mathbb{Z}/p^i)$ by taking binomial expansions, and so G_i contains all of H_{i-1}.

Proposition 19. *Let $p > 2$ be a prime and let E/F be an elliptic curve. Suppose G lies in the Borel subgroup of upper triangular matrices and that G_2 is greatest possible. If G is not among the exceptional cases in Theorem 1 or in Proposition 18, then $H^1\big(G_i, E[p^j]\big) = 0$ for all $i \geqslant j \geqslant 1$.*

Proof. The short exact sequence (2) implies that if $H^1\big(G_{i+1}, E[p^{j-1}]\big)$ and $H^1\big(G_{i+1}, E[p]\big)$ are zero, then so is $H^1\big(G_{i+1}, E[p^j]\big)$. By induction on j, it suffices to prove the proposition in the case $j = 1$.

For $i = 1$, the statement follows from Theorem 1. We assume now that it holds for $i \geqslant 1$. By assumption M_{i+1} is isomorphic to the group $(1 + p\,\mathrm{Mat}_2\big(\mathbb{Z}/p^i\big)) \subset \mathrm{GL}_2(\mathbb{Z}/p^{i+1})$ and H_i is isomorphic to the group M of all matrices with coefficients in $\mathbb{F}_p$. Using Proposition 18, we find

$$H^1\big(M_{i+1}, E[p]\big)^G = \mathrm{Hom}_G\big(M_{i+1}, E[p]\big) \cong \mathrm{Hom}_G\big(M, E[p]\big) = 0$$

because all elements in the kernel of the map $M_{i+1} \to M$ are p'th powers. (Note that this requires $p > 2$.) Now considering the inflation-restriction sequence

$$0 \longrightarrow H^1\big(G, E[p]\big) \longrightarrow H^1\big(G_{i+1}, E[p]\big) \longrightarrow H^1\big(M_{i+1}, E[p]\big)^G \tag{6}$$

yields that $H^1\big(G_{i+1}, E[p]\big) = 0$. □

Lemma 20. *Let $p > 2$ be a prime and E/F an elliptic curve such that G_2 is greatest possible. If G is among the exceptional cases in Theorem 1 or in Proposition 18 then $H^1\big(G_i, E[p^i]\big) \neq 0$ for all $i \geqslant 2$.*

Proof. We claim that the sequence (6) is part of a short exact sequence. The next term in the sequence is $H^2\big(G, E[p]\big)$, and so it suffices to show that the map $H^1(M_{i+1}, E[p])^G \to H^2\big(G, E[p]\big)$ is zero. By Lemma 13, the target group is trivial unless $G = \left(\begin{smallmatrix}* & *\\0 & 1\end{smallmatrix}\right)$. If $p > 3$ and $G = \left(\begin{smallmatrix}* & *\\0 & 1\end{smallmatrix}\right)$, then the source group $H^1(M_{i+1}, E[p])^G$ vanishes. If $p = 3$ and $G = \left(\begin{smallmatrix}* & *\\0 & 1\end{smallmatrix}\right)$, the source is cyclic and generated by a cocycle $\xi\colon M_{i+1} \to E[3]$ such that $\left(\begin{smallmatrix}a & b\\c & d\end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix}c/3\\0\end{smallmatrix}\right)$. The image of ξ in $H^2\big(G, E[p]\big)$ is zero because the formula $\left(\begin{smallmatrix}a & b\\c & d\end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix}ac/3\\0\end{smallmatrix}\right)$ lifts it to a cocycle $G_{i+1} \to E[3]$.

Therefore, the dimension of $H^1(G_{i+1}, E[p])$ is the sum of the dimensions of the two groups surrounding it in the sequence (6). In all cases, this dimension is strictly larger than the dimension of the group of p-torsion points of E defined over F.

Now we turn to sequence (2) with $i \geqslant 2$. In all cases, the dimension of $H^1\big(G_i, E[p]\big)$ is strictly larger than the dimension of $E(F)[p^{i-1}]/pE(F)[p^i]$ (which is at most 1 because $E(F)[p^{i-1}]$ must be cyclic by the assumption on F). We conclude that $H^1\big(G_i, E[p^i]\big)$ is non-trivial. □

So far we have been able to treat all cases in which G_i is greatest possible and $F \cap \mathbb{Q}(\mu_p) = \mathbb{Q}$. We will now restrict our attention to $F = \mathbb{Q}$ and $p > 3$. Luckily, for the large majority of elliptic curves over $\mathbb{Q}$ the groups G_i are indeed greatest possible. The following is a summary of the results in [12] and in [11].

Theorem 21. *Let $p > 3$ and $i > 1$. Let $E/\mathbb{Q}$ be an elliptic curve with an isogeny of degree p defined over $\mathbb{Q}$. Then G_i is greatest possible except in two cases:*

- *when $p = 7$ and the curve is the quadratic twist of a curve of conductor 49, or*
- *when $p = 5$ and there is an isogeny $\psi\colon E \to E''$ of degree 25 defined over $\mathbb{Q}$.*

We will now treat the two exceptional cases, starting with $p = 5$.

Lemma 22. *Let $E/\mathbb{Q}$ be an elliptic curve and suppose there is an cyclic isogeny $\psi\colon E \to E' \to E''$ of degree $p^2 = 25$ defined over $\mathbb{Q}$. Then $H^1\big(G_2, E[p^2]\big) = 0$ if and only if $H^1\big(G_i, E[p^i]\big) = 0$ for all $i > 1$. This vanishing holds except if $G = \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$, if $G = \left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$, or if E appears in Theorem 1 as an exception.*

For instance, it is non-vanishing if E admits a rational 5-torsion point or if E' admits a rational 5-torsion point. The curves 11a3 and 11a2 are examples of these two situations where $H^1\big(G, E[p]\big) = 0$, yet $H^1\big(G_i, E[p^i]\big) \neq 0$ for all $i > 1$ because there are two 5-isogenies 11a3 $\to$ 11a1 $\to$ 11a2 with only 11a3 and 11a1 having a rational 5-torsion point. The cohomology group $H^1\big(G_2, E[25]\big)$ is also non-trivial for 11a1 by Proposition 19.

Proof. Note that there are no elliptic curves with rational points of order 25 and there are no cyclic isogenies over $\mathbb{Q}$ of degree $p^3 = 125$. Greenberg shows in Theorem 2 in [12] that the index of G_2 in $\mathrm{GL}_2\big(\mathbb{Z}/25\big)$ is divisible by 5 but not 25. Hence the group G_2 can be identified with a subgroup of the upper triangular matrices modulo p^2, but the top left entry is not constant 1 modulo p^2 and the top right corner is not constant zero modulo p. Since the index is only divisible by 5 once, the group G_2 consists of all the upper triangular matrices that reduce to an element of G.

We wish to use the same strategy as in the proof of Proposition 19, but we have to show that G-fixed part of $H^1\big(M_2, E[p]\big)$ is still zero despite $M_2 \neq M$. This time M_2 can be identified with upper triangular matrices modulo p and the computations are slightly easier. One finds that $\mathrm{Hom}_G\big(M_2, E[\varphi]\big)$ has dimension 2 if $G = \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$ and 0 in all other cases. Similarly, the dimension of $\mathrm{Hom}_G\big(M_2, E'[\hat{\varphi}]\big)$ is equal to 2 if $G = \left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$ and zero otherwise. (Alternatively, it is not too hard to show by direct calculation that the dimension of $\mathrm{Hom}_G\big(M_2, E[p]\big)$ is 2 if $G = \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$, 1 if $G = \left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$, and 0 otherwise.)

Hence if we assume that neither $G = \left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$ nor $G = \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$ nor $G = \left\{ \left(\begin{smallmatrix} v^2 & w \\ 0 & v \end{smallmatrix}\right) \;\middle|\; v \in \mathbb{F}_p^\times, w \in \mathbb{F}_p \right\}$, then $H^1\big(G_i, E[p^i]\big) = 0$ for all $i \geqslant 1$ with the same proof as in Proposition 19.

If $G = \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$, then one can show as in Lemma 20 that $H^1\big(G_i, E[p^i]\big)$ is non-zero for all $i > 1$. Similarly for $G = \left\{ \left(\begin{smallmatrix} v^2 & w \\ 0 & v \end{smallmatrix}\right) \;\middle|\; v \in \mathbb{F}_p^\times, w \in \mathbb{F}_p \right\}$.

Finally if $G = \left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$, then one may compute $H^1\big(G_2, E[p^2]\big)$ directly: the group G_2 consists of all upper triangular matrices modulo p^2 whose lower right entry is congruent to 1 modulo p. Let H be the subgroup generated by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Then the method used in the proof of Theorem 1 shows that the subgroup of $H^1\big(H, E[p^2]\big)$ fixed by the action of G_2/H is trivial. However $H^1\big(G_2/H, E[p^2]^H\big) \cong \mathbb{Z}/p\mathbb{Z}$ implies then that $H^1\big(G_2, E[p^2]\big) \cong \mathbb{Z}/p\mathbb{Z}$ where an explicit isomorphism sends a cocycle ξ to the first coordinate of $\xi\left(\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1+p \end{smallmatrix}\right)\right)$ in $p\mathbb{Z}/p^2\mathbb{Z}$. From the exact sequence (2), one deduces that $H^1\big(G_2, E[p]\big)$ is non-trivial and again this implies that all $H^1\big(G_i, E[p^i]\big)$ are non-zero for $i > 1$. □

Lemma 23. *Let $E/\mathbb{Q}$ be a quadratic twist of a curve of conductor 49 and let $p = 7$. Then $H^1\big(G_i, E[p^i]\big) = 0$ for all $i \geqslant 1$.*

Proof. Assume first that E is one of the curves of conductor 49. By assumption E has complex multiplication by $\mathcal{O}$, where $\mathcal{O}$ is either $\mathbb{Z}[\sqrt{-7}]$ or the ring of integers in $\mathbb{Q}(\sqrt{-7})$. Since $\mathbb{Q}(\sqrt{-7}) \subset K$, the subgroup $\mathrm{Gal}(K/\mathbb{Q}(\sqrt{-7})) < G$ acts by $\mathcal{O}$-linear endomorphisms on $E[7^i]$. By scaling with the period, we may choose points p and $\sqrt{-7} \cdot p$ as a basis for $E[7^i]$. Any lift of these forms a $\mathbb{Z}_7$-basis of the Tate module T_7E. The endomorphism $a + b\sqrt{-7}$ with a, $b \in \mathbb{Q} \cap \mathbb{Z}_7$ acts via $\left(\begin{smallmatrix} a & b \\ -7b & a \end{smallmatrix}\right)$ on $T_7(E)$.

The Frobenius element $\mathrm{Fr}_\ell \in \mathrm{GL}(T_7 E)$ for $\ell = 347$ has trace $a_\ell = 4$ for all four curves of conductor 49. Since ℓ splits in $\mathbb{Q}(\sqrt{-7})$, the Frobenius Fr_ℓ in $\mathrm{GL}_2(\mathbb{Z}_7)$ is a matrix of the above shape with trace 4 and determinant 347. We find that it is congruent to $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)$ modulo 7. Since G contains now the homotheties by 2 and 4, the result follows from Lemma 3.

Let now E be a quadratic twist of a curve of conductor 49. Then it is the quadratic twist of one of them by an integer D coprime to 7. The above homotheties are multiplied by a non-zero scalar and hence Lemma 3 also implies the result for E. □

Proof of Theorem 2. We combine the results from Proposition 19, Lemma 20, Lemma 22 and Lemma 23. From these we conclude immediately that $H^1\big(G_i, E[p^i]\big) = 0$ if and only if $H^1\big(G_2, E[p^2]\big) = 0$.

We are now left with making the list in Theorem 2 match with the non-vanishing cases. We start by verifying that the cohomology groups are non-vanishing in each of the five special cases in the theorem.

- First, if E contains a rational point of order p, then $G = \left(\begin{smallmatrix} 1 & 0 \\ 0 & * \end{smallmatrix}\right)$, $G = \left(\begin{smallmatrix} * & 0 \\ 0 & 1 \end{smallmatrix}\right)$, or $G = \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$. In all these cases, the cohomology groups in question do not vanish by Lemma 20 and Lemma 22.
- In the second point in the list of Theorem 2, $p = 5$ and the quadratic twist by $D = 5$ of E has a rational 5-torsion point. Then G is contained in $\left\{ \left(\begin{smallmatrix} v^2 & * \\ 0 & v \end{smallmatrix}\right) \;\middle|\; v \in \mathbb{F}_p^\times \right\}$. If G is equal to that group, then Theorem 1 and Lemma 20 or Lemma 22 imply the non-vanishing of $H^1\big(G_2, E[p^2]\big)$. Otherwise we may choose the basis of $E[p]$ so that G is contained in the diagonal matrices of this form, in which case Lemma 20 proves the assertion.
- In the third point, $p = 5$ and the quadratic twist by $D = 5$ of E' has a rational 5-torsion point. Then G is contained in $\left\{ \left(\begin{smallmatrix} u & * \\ 0 & u^2 \end{smallmatrix}\right) \;\middle|\; u \in \mathbb{F}_p^\times \right\}$. There is no isogeny of degree 25 defined over $\mathbb{Q}$ leaving from E, hence G_2 is greatest possible; therefore Lemma 20 proves the desired non-vanishing.
- If we are in the situation of the fourth point in Theorem 2, we are in the situation of Lemma 22 and $G = \left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$. Therefore $H^1\big(G_2, E[p^2]\big) \neq 0$.
- In the final point, if $p = 11$ and E is 121c2, then Theorem 1 and Lemma 20 shows the desired non-vanishing. If the curve is 121c1 instead, then $G = \left\{ \left(\begin{smallmatrix} u & * \\ 0 & u^2 \end{smallmatrix}\right) \;\middle|\; u \in \mathbb{F}_p^\times \right\}$ and Lemma 20 treats this case too.

Next, we have to check that every case when the group $H^1\big(G_2, E[p^2]\big)$ is non-trivial is among the exceptional cases of Theorem 2 above.

Let us assume first that G_2 is greatest possible and consider the cases in Lemma 20. If $G = \left(\begin{smallmatrix} 1 & 0 \\ 0 & * \end{smallmatrix}\right)$ or $G = \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$, then E has a rational p-torsion point. By Mazur's Theorem on the torsion point on elliptic curves over $\mathbb{Q}$, we know that this can only occur if $p = 5$ or $p = 7$ and we fall under the first point in the list of Theorem 2. If (E, p) appears as an exception in Theorem 1, then either $p = 5$ and we are in the situation of the second point, or $p = 11$ and we are in the last point on the list. If G is the group of all matrices of the form $\left(\begin{smallmatrix} v^2 & 0 \\ 0 & v \end{smallmatrix}\right)$, then the quadratic twist by $D = 5$ has a rational 5-torsion point and we are in the situation of the second point. Finally, assume G is contained in the group $\left\{ \left(\begin{smallmatrix} u & * \\ 0 & u^2 \end{smallmatrix}\right) \;\middle|\; u \in \mathbb{F}_p^\times \right\}$. Then $p \equiv 2 \pmod 3$. If $p = 5$, then the quadratic twist by $D = 5$ of E' has a rational 5-torsion point and we are in the third case. If $p \geqslant 11$, then the proof that there is only one curve, namely 121c1, is very analogous to Lemma 12.

Finally, we consider the cases in Lemma 22. If $G = \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$, then E has a rational 5-torsion point and we are in the first point in the list. If $G = \left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$, then E' admits a rational 5-torsion point, which is the fourth point on the list. If (E, p) appear as exceptions in Theorem 1, then we fall into the second point on the list. □

7 Numerical computations

We used Magma [2] to perform, for small primes p, the numerical computation of our cohomology group $H^1\big(G_2, V_2\big)$ for various subgroup $G_2 \leqslant \mathrm{GL}_2(\mathbb{Z}/p^2)$, where V_2 is the natural rank 2 module over $\mathbb{Z}/p^2$ on which G_2 acts. We restricted our attention to groups with surjective determinants and we only considered groups up to conjugation in $\mathrm{GL}_2(\mathbb{Z}/p^2)$.

We will continue to write M_2 for the kernel of reduction $G_2 \to \mathrm{GL}_2(\mathbb{F}_p)$ and G for its image.

7.1 $p = 2$

For the prime $p = 2$, the groups $H^1\big(G_2, V_2\big)$ are non-zero for 36 conjugacy classes of subgroup $G_2 \leqslant \mathrm{GL}_2(\mathbb{Z}/4)$ with surjective determinant. The possible cohomology groups are $\big(\mathbb{Z}/2\big)^k$ for $0 \leqslant k \leqslant 6$ and $\mathbb{Z}/4$. Non-trivial cohomology groups appear for all dimensions $1 \leqslant d \leqslant 4$ of M_2.

7.2 $p = 3$

There are 41 groups G_2 with non-vanishing $H^1\big(G_2, V_2\big)$. For thirteen of them the cohomology group is $\mathbb{Z}/3 \oplus \mathbb{Z}/3$, for one it is $\mathbb{Z}/3 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/3$ and for all others it is just $\mathbb{Z}/3$. In all non-vanishing cases the image $G \leqslant \mathrm{GL}_2(\mathbb{F}_3)$ of reduction has either non-trivial $H^0(G, V)$ or non-trivial $H^2(G, V)$, where V is the 2-dimensional vector space over $\mathbb{F}_3$ with its natural action by $G \leqslant \mathrm{GL}_2(\mathbb{F}_3)$. In other words, these numerical computations show that if the group $H^1\big(G_2, E[9]\big)$ is non-trivial for an elliptic curve $E/\mathbb{Q}$, there is an isogeny $\varphi\colon E \to E'$ defined over $\mathbb{Q}$ of degree 3 such that either φ or its dual $\hat{\varphi}$ has a rational 3-torsion point in its kernel.

The maximal order of the cohomology group appears for the group G_2 consisting of all matrices in $\mathrm{GL}_2(\mathbb{Z}/9)$ with reduction $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ modulo 3.

7.3 $p = 5$

There are 39 groups G_2 with non-vanishing $H^1\big(G_2, V_2\big)$. For two of them, the group is $\mathbb{Z}/5 \oplus \mathbb{Z}/5$, for one it is $\mathbb{Z}/25$ and for all others it is $\mathbb{Z}/5$. If we restrict to those groups for which M_2 has dimension 4, then there are five cases as found in Section 6:

G	$\left(\begin{smallmatrix} v^2 & 0 \\ 0 & v \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 1 & 0 \\ 0 & * \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} u & * \\ 0 & u^2 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} v^2 & * \\ 0 & v \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$
$\lvert G\rvert$	4	4	20	20	20
$H^1\big(G_2, V_2\big)$	$\mathbb{Z}/5$	$\mathbb{Z}/5 \oplus \mathbb{Z}/5$	$\mathbb{Z}/5$	$\mathbb{Z}/5$	$\mathbb{Z}/5$

This determines what the non-vanishing cohomology groups can be for this specific prime.

7.4 $p = 7$

Here we restricted our attention to the subgroups G_2 for which M_2 has dimension 4. Then, as previously found, there are only two cases. The group G can be of the form $\left(\begin{smallmatrix} 1 & 0 \\ 0 & * \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$. In the first case the cohomology group $H^1\big(G_2, V_2\big)$ is $\mathbb{Z}/7 \oplus \mathbb{Z}/7$; in the latter it is $\mathbb{Z}/7$.

8 Applications to local and global divisibility of rational points

The cohomology groups that we have discussed in this paper also appear in the analogue of the Grunwald–Wang problem for elliptic curves. This question was raised by Dvornicich and Zannier in [9].

Grunwald–Wang problem for elliptic curves. Let $E/\mathbb{Q}$ be an elliptic curve, $P \in E(\mathbb{Q})$, and $m > 1$. If P is divisible by m in $E(\mathbb{Q}_\ell)$ for almost all ℓ, is it true that P is divisible by m in $E(\mathbb{Q})$?

By the Chinese remainder theorem, it is sufficient to restrict to the case when $m = p^i$ is a prime power. The answer is positive if m is prime. The explicit example in [10] shows that the answer is negative for $m = 4$. In [20], it is shown that the answer is positive for all $m = p^2$ with p a prime larger than 3. To our knowledge, the case $m = 9$ has not been determined.

This question connects to our cohomology groups through the following reinterpretation. Suppose $m = p^i$ for our fixed prime p. Let Σ be a finite set of places in $\mathbb{Q}$. Let

$$D(E/\mathbb{Q}) = \ker\Big(E(\mathbb{Q})/p^iE(\mathbb{Q}) \to \prod_{v \notin \Sigma} E(\mathbb{Q}_v)/p^iE(\mathbb{Q}_v)\Big)$$

be the group that measures if there are points P that are locally divisible by p^i, but not globally. Let

$$L(E/\mathbb{Q}) = L(G_i) = \ker\Big(H^1\big(G_i, E[p^i]\big) \to \prod_{\substack{C \leqslant G_i \\ C \text{ cyclic}}} H^1\big(C, E[p^i]\big)\Big) \tag{7}$$

be the kernel of reduction to all the cyclic subgroups of G_i. We now assume that Σ contains all places above p and all bad places. By Chebotarev's theorem, $L(E/\mathbb{Q})$ is also the kernel of localization from $H^1\big(G_i, E[p^i]\big)$ to all $H^1(D_{w|v}, E[p^i]\big)$ where $D_{w|v}$ is the decomposition group in $K_i/\mathbb{Q}$ of a place w above v. Hence a natural notation for $L(E/\mathbb{Q})$ could be $Ш^1\big(U, E[p^i]\big)$ with U the complement of Σ in $\mathrm{Spec}(\mathbb{Z})$. The sequence

$$0 \longrightarrow D(E/\mathbb{Q}) \longrightarrow L(E/\mathbb{Q}) \longrightarrow H^1\big(G_i, E(K_i)\big)$$

is exact. Hence the answer is positive for $m = p^i$ if $H^1\big(G_i, E[p^i]\big)$ vanishes. Note that the description of $L(E/\mathbb{Q})$ in (7) is now entirely group-theoretic, and can be computed numerically with the methods described in the previous section.

Theorem 24. *Let p a prime and $i \geqslant 1$. Then the Grunwald–Wang problem for local-global divisibility by $m = p^i$ admits a positive answer for all elliptic curves $E/\mathbb{Q}$ if and only if $p > 3$ or $m = 2$ or $m = 3$.*

Proof. If we find a point P of infinite order that is a counter-example for $m = p^i$, then $p^j P$ is a counter-example for $m = p^{i+j}$ for any $j > 0$. As mentioned before, the negative answer for $m = 4$ is explained in [10]. This settles also all higher powers of 2 as their examples are points of infinite order. Counter-examples when m is a power of 3 were first found by Creutz in [7]. We will give below in Proposition 25 a new counter-example of infinite order for $m = 9$. For $p \geqslant 5$ the theorem follows from [20]. However, we wish to give a slightly simplified proof with our methods.

Assume therefore $p \geqslant 5$. We will now show that the kernel of localization $L(G_i)$ is zero. Note that by Greenberg's result in Theorem 21 and the work done in the exceptional cases in Lemma 22 and Lemma 23, we may assume that G_i is greatest possible or that $i = 2$ and M_2 consists of all matrices m such that $m - 1$ is upper triangular. In both cases the elements in $E[p^i]$ fixed by M_i are just $E[p]$. We get an exact sequence

$$0 \longrightarrow H^1\big(G, E[p]\big) \xrightarrow{\inf} H^1\big(G_i, E[p^i]\big) \longrightarrow H^1\big(M_i, E[p^i]\big).$$

First assume that $L(G_i)$ contains a non-trivial element which belongs to the image of the inflation map from $H^1\big(G, E[p]\big)$. Since the latter must now be non-trivial, G must contain the element $\bar{h} = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. By the description of M_i, we find that G_i contains the element $h = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Let C be the cyclic group generated by h and let $\bar{C}$ be its image in G. Our computations for proving Theorem 1 showed that $H^1\big(G, E[p]\big) \to H^1(\bar{C}, E[p]\big)$ is a bijection. Next, both maps in the composition

$$H^1\big(\bar{C}, E[p]\big) \longrightarrow H^1\big(\bar{C}, E[p^i]^{C \cap M_i}\big) \longrightarrow H^1\big(C, E[p^i]\big)$$

are injective: for the latter it is because any inflation map is injective, and for the first it can be read off the long exact sequence associated to the inclusion $E[p] \to E[p^i]^{C \cap M_i}$. We conclude that $H^1\big(G, E[p]\big) \to H^1\big(C, E[p^i]\big)$ is injective. This now contradicts the assumption that $L(G_i)$ contained a non-trivial element from $H^1\big(G, E[p]\big)$.

Therefore, $L(G_i)$ injects into to

$$L(M_i) = \ker\Big(H^1\big(M_i, E[p^i]\big) \to \prod_{\substack{C \leqslant M_i \\ \text{cyclic}}} H^1\big(C, E[p^i]\big)\Big),$$

where the product now runs over all cyclic subgroups of M_i. We will now prove by induction on i that $L(M_i)$ is trivial. It is known for $i = 1$.

Recall that the group H_i acts trivially on $E[p^i]$. We consider the following diagram with exact rows:

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^1\big(M_i, E[p^i]\big) & \longrightarrow & H^1\big(M_{i+1}, E[p^i]\big) & \longrightarrow & H^1\big(H_i, E[p^i]\big) \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \prod_C H^1\big(C/C \cap H_i, E[p^i]^{C \cap H_i}\big) & \longrightarrow & \prod_C H^1\big(C, E[p^i]\big) & \longrightarrow & \prod_C H^1\big(C \cap H_i, E[p^i]\big) \end{array} \tag{8}$$

where the products run over all cyclic subgroups C of M_{i+1}. Now the vertical map on the right hand side has the same kernel as

$$H^1\big(H_i, E[p^i]\big) = \mathrm{Hom}\big(H_i, E[p^i]\big) \longrightarrow \prod_{\substack{D \leqslant H_i \\ \text{cyclic}}} \mathrm{Hom}\big(D, E[p^i]\big)$$

and this map is clearly injective. Since $C \cap H_i$ fixes $E[p^i]$ the vertical map on the right in the above diagram (8) is injective by induction hypothesis because $C/C \cap H_i \cong CH_i/H_i$ will run through all cyclic subgroups of M_i at least once. Therefore the middle vertical map in (8) is injective, too.

Next, consider the following diagram with exact rows:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E[p] & \xrightarrow{\delta} & \mathrm{Hom}\big(M_{i+1}, E[p]\big) & \xrightarrow{\iota} & H^1\big(M_{i+1}, E[p^{i+1}]\big) & \xrightarrow{[p]} & H^1\big(M_{i+1}, E[p^i]\big) \\
 & & & & \downarrow & & \downarrow & & \downarrow \\
E[p^{i+1}]^C & \xrightarrow{[p]} & E[p^i]^C & \xrightarrow{\delta_C} & \mathrm{Hom}\big(C, E[p]\big) & \longrightarrow & H^1\big(C, E[p^{i+1}]\big) & \longrightarrow & H^1\big(C, E[p^i]\big)
\end{array}$$

Here C is any cyclic subgroup of M_{i+1}. The zero at the top left corner is a consequence from the fact that the M_{i+1}-fixed points in $E[p^j]$ are exactly $E[p]$ for all $1 \leqslant j \leqslant i+1$.

If $\xi \in L(M_{i+1})$, then its image under $[p]$ in $H^1\big(M_{i+1}, E[p^i]\big)$ must be trivial by what we have shown for the middle vertical map in (8). Therefore ξ is the image under ι of an element f in $\mathrm{Hom}\big(M_{i+1}, E[p]\big)$. Since $E[p]$ is p-torsion, we can identify $\mathrm{Hom}\big(M_{i+1}, E[p]\big)$ with $\mathrm{Hom}\big(M_2, E[p]\big)$. To say that ξ restricts to zero for a cyclic group $C \leqslant M_{i+1}$ forces $f\colon M_2 \to E[p]$ to be in the image of the map $\delta_C\colon E[p] \to \mathrm{Hom}\big(C, E[p]\big)$ for all cyclic subgroups C of M_2.

Now we identify M_2 with the additive subgroup $\tilde{M}_2 \leqslant \mathrm{Mat}_2(\mathbb{F}_p)$ as before. Under this identification the map δ sends a p-torsion point $T \in E[p] = \mathbb{F}_p^2$ to the map f sending a matrix $m \in \tilde{M}_2$ to $m(T)$. Thus, the restriction of f to $\mathrm{Hom}\big(\langle m\rangle, \mathbb{F}_p^2\big)$ is in the image of $\delta_{\langle m\rangle}$ for a particular $m \in \tilde{M}_2$ if and only if $f(m) \in \mathbb{F}_p^2$ belongs to the image of m. Therefore, we have shown that

$$L(M_{i+1}) = \frac{\Big\{ f \in \mathrm{Hom}\big(\tilde{M}_2, \mathbb{F}_p^2\big) \;\Big|\; f(m) \in \mathrm{im}(m)\ \forall m \in \tilde{M}_2 \Big\}}{\Big\{ f(m) = m(T) \text{ for some } T \in \mathbb{F}_p^2 \Big\}}. \tag{9}$$

We wish to show that $L(M_{i+1})$ is trivial if $\tilde{M}_2$ is the full matrix group or the upper triangular matrices. Assume first that $\tilde{M}_2$ is the full matrix group. Then f is determined by its image on the matrices with only one non-zero entry. However, the local condition of being in the image of δ_C for these matrices and the matrices $\left(\begin{smallmatrix}1&0\\1&0\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}0&1\\0&1\end{smallmatrix}\right)$ forces $f(m)$ to be just $m(T)$ for $T = f\left(\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)\right) + f\left(\left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right)\right)$. Therefore $L(M_{i+1})$ is trivial. The case when $\tilde{M}_2$ is the group of upper triangular matrices is very similar. □

The result about the vanishing of $L(G_2)$ for $p > 3$ in the above proof is reminiscent of Proposition 3.2.ii in [9]. We have reproved part of this result with a more conceptual approach. The main reason for doing so is that the general statement there is slightly incorrect. The case $\dim(M_2) = 3$ assumes that $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ belongs to G_2. However, for $p = 3$, the group G_2 generated by $\left(\begin{smallmatrix}7&8\\3&1\end{smallmatrix}\right)$ and the group of all matrices m with $m - 1$ upper-triangular is a counterexample. This group does not contain any elements of order 9 and one can compute that $L(G_2)$ is isomorphic to $\mathbb{Z}/3$.

We include here a new counter-example for $m = 9$; the method is quite different from [7] where a first such example was found.

Proposition 25. *Let E be the elliptic curve labeled 243a2, given by the global minimal equation $y^2 + y = x^3 + 20$, and let $P = (-2, 3)$. Then $3\,P$ is divisible by 9 in $E(\mathbb{Q}_\ell)$ for all primes $\ell \neq 3$, but it is not divisible by 9 in $E(\mathbb{Q})$.*

Proof. Since P is a generator of the free part of this curve of rank 1, it is clear that $3P$ is not divisible by 9 in $E(\mathbb{Q})$.

Let k be the unique subfield of $\mathbb{Q}(\mu_9)$ of degree 3 over $\mathbb{Q}$ and let ζ be a primitive 9-th root of unity. Then $P' = (3\zeta^5 + 3\zeta^4 + 3, 9\zeta^4 - 9\zeta^2 + 9\zeta + 4) \in E(k)$ satisfies $3P' = P$. Thus, if $\ell \equiv \pm 1 \pmod 9$, then ℓ splits in k and hence P is divisible by 3 in $E(\mathbb{Q}_\ell)$. As a consequence, $3P$ is divisible by 9 over $\mathbb{Q}_\ell$.

For this curve and $p = 3$, the group $G = \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$ is of order 6 and $K = \mathbb{Q}(\theta)$ with $\theta^6 + 3 = 0$. Factoring the 9-division polynomial, one finds that K_2/K is an extension of degree 3. The field of definition of the points of order 9 is K_2 except for those points T with $3\,T \in E(\mathbb{Q})[3]$. Those are defined instead over a non-Galois extension of degree 3 over k.

Let $\ell \not\equiv \pm 1 \pmod 9$ and $\ell \neq 3$. Then the Frobenius element Fr_ℓ in G_2 cannot belong to $\mathrm{Gal}(K_2/k)$. Therefore Fr_ℓ does not fix any point of order 9. It follows that $\tilde{E}(\mathbb{F}_\ell)[9] = \tilde{E}(\mathbb{F}_\ell)[3]$. Consider the following commutative diagram, whose lower row is exact.

$$\begin{array}{ccccccc} & & & & P \in E(\mathbb{Q})/3E(\mathbb{Q}) & \xrightarrow{[3]} & E(\mathbb{Q})/9E(\mathbb{Q}) \\ & & & & \downarrow & & \downarrow \\ E(\mathbb{Q}_\ell)[9] & \xrightarrow{[3]} & E(\mathbb{Q}_\ell)[3] & \xrightarrow{\delta} & E(\mathbb{Q}_\ell)/3E(\mathbb{Q}_\ell) & \xrightarrow{[3]} & E(\mathbb{Q}_\ell)/9E(\mathbb{Q}_\ell) \end{array}$$

Since $\ell \neq 3$, the reduction of E at ℓ is good and hence [3] is an isomorphism on the kernel of reduction $E(\mathbb{Q}_\ell) \to \tilde{E}(\mathbb{F}_\ell)$. It follows that $E(\mathbb{Q}_\ell)[3] \cong \tilde{E}(\mathbb{F}_\ell)[3]$ and $E(\mathbb{Q}_\ell)/3E(\mathbb{Q}_\ell) \cong \tilde{E}(\mathbb{F}_\ell)/3\tilde{E}(\mathbb{F}_\ell)$ have the same size. By the above argument δ is an injective map between two groups of the same size. Thus δ is a bijection. This implies that $3P$ is divisible by 9 in $E(\mathbb{Q}_\ell)$. □

This is the counter-example of smallest conductor for $m = 9$; here is how we found that this curve is a likely candidate.

Consider curves E with a 3-isogeny where either the kernel has a rational 3-torsion point or where the kernel of the dual isogeny has a rational 3-torsion point. On the one hand, we computed (for a few thousand primes $\ell \neq 3$ of good reduction) the pairs $(a_\ell(E), \ell)$ modulo 9. On the other hand, we may determine all subgroups $G_2 \leqslant \mathrm{GL}_2(\mathbb{Z}/9)$ with surjective determinant to find the examples for which the kernel (7) is non-trivial. There are 13 such groups. The dimension of M_2 in these cases is 1, 2 or 3. For each of them we may list pairs $(\mathrm{tr}(g), \det(g))$ when g runs through all matrices $g \in G_2$.

Now, if the list of possible pairs $(a_\ell(E), \ell)$ modulo 9 agrees with one of the lists above, then G_2 could be among the groups for which the localization kernel is non-trivial. Furthermore, it is easy to check local divisibility for primes $\ell < 1000$ for all possible candidates in $3E(\mathbb{Q})/9E(\mathbb{Q})$. The above curve 243a2 was the first to pass all these tests.

Here are a few more candidates. Note that we have not formally proved that local divisibility holds by 9 holds for all primes ℓ of good reduction.

The point $P = (6, 17)$ on the curve 9747f1 gives a point $3P$ which is likely to be locally divisible by 9 for *all* primes, but not divisible by 9 globally. In this example G_2 has 54 elements.

On the curve 972d2 the point $3P$ with $P = (13, 35)$ is likely to be locally divisible by 9 for all places $\ell \neq 3$, yet not globally so. This is a curve without a rational 3-torsion point and G_2 having 54 elements again.

All the above examples have complex multiplication by the maximal order in $\mathbb{Q}(\sqrt{-3})$. The curve 722a1, with a point P having x-coordinate $\frac{27444}{169}$, is an example without complex multiplication and $|G_2| = 162$. Again, it is likely that $3P$ is locally divisible by 9 at all places $\ell \neq 19$, but $3P$ is not globally divisible by 9. The group G_2 here is probably conjugate to the one mentioned earlier as a counter-example to Proposition 3.2.ii in [9].

We have also done numerical calculation of the kernel in (7) for other primes. For $p = 5$, there are only three subgroups G_2 in $\mathrm{GL}_2(\mathbb{Z}/25)$ with non-trivial localization kernel. They all have $\dim(M_2) = 2$ and $|G| = 4$.

For $p = 2$, there are twelve cases. The dimensions of M_2 can be 1, 2, or 3. In only one of these cases is the localization kernel is $\mathbb{Z}/2 \oplus \mathbb{Z}/2$; otherwise it is $\mathbb{Z}/2$.

References

[1] B. J. Birch and W. Kuyk (eds.), *Modular functions of one variable. IV*, Lecture Notes in Mathematics, Vol. 476, Springer-Verlag, Berlin-New York, 1975.

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

[3] Byungchul Cha, *Vanishing of some cohomology groups and bounds for the Shafarevich-Tate groups of elliptic curves*, J. Number Theory **111** (2005), no. 1, 154–178.

[4] Mirela Çiperiani and Jakob Stix, *Weil-Châtelet divisible elements in Tate-Shafarevich groups II: On a question of Cassels*, to appear in Journal für die Reine und Angewandte Mathematik.

[5] John Coates, *An application of the division theory of elliptic functions to diophantine approximation*, Invent. Math. **11** (1970), 167–182.

[6] John E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997.

[7] Brendan Creutz, *On the local-glocal principle for divisibiity in the cohomology of elliptic curves*, available at `http://arxiv.org/abs/1305.5881`, 2013.

[8] Brendan Creutz and Robert L. Miller, *Second isogeny descents and the Birch and Swinnerton-Dyer conjectural formula*, J. Algebra **372** (2012), 673–701.

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

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

[11] R. Greenberg, K. Rubin, A. Silverberg, and M. Stoll, *On elliptic curves with an isogeny of degree 7*, Amer. J. Math. **136** (2014), no. 1, 77–109.

[12] Ralph Greenberg, *The image of Galois representations attached to elliptic curves with an isogeny*, Amer. J. Math. **134** (2012), no. 5, 1167–1196.

[13] Grigor Grigorov, Andrei Jorza, Stefan Patrikis, William A. Stein, and Corina Tarniţă, *Computational verification of the Birch and Swinnerton-Dyer conjecture for individual elliptic curves*, Math. Comp. **78** (2009), no. 268, 2397–2425.

[14] Benedict H. Gross, *Kolyvagin's work on modular elliptic curves*, L-functions and arithmetic (Durham, 1989), London Math. Soc. Lecture Note Ser., vol. 153, Cambridge Univ. Press, Cambridge, 1991, pp. 235–256.

[15] Ahmed Matar, *For an elliptic curve $E/\mathbb{Q}$ can the cohomology group $H^1\big(\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}), E[p]\big)$ be nontrivial?*, `http://mathoverflow.net/questions/186807`, 2014.

[16] Barry Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162.

[17] Robert L. Miller, *Proving the Birch and Swinnerton-Dyer conjecture for specific elliptic curves of analytic rank zero and one*, LMS J. Comput. Math. **14** (2011), 327–350.

[18] Robert L. Miller and Michael Stoll, *Explicit isogeny descent on elliptic curves*, Math. Comp. **82** (2013), no. 281, 513–529.

[19] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, Grundlehren der Mathematischen Wissenschaften, vol. 323, Springer, 2000.

[20] Laura Paladino, Gabriele Ranieri, and Evelina Viada, *On the minimal set for counterexamples to the local-global principle*, J. Algebra **415** (2014), 290–304.

[21] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.

[22] ———, *Cohomologie Galoisienne*, Lecture Notes in Mathematics, Vol. 5, Springer-Verlag, Berlin-New York, 1973, Cours au Collège de France, Paris, 1962–1963, Avec des textes inédits de J. Tate et de Jean-Louis Verdier, Quatrième édition.

[23] William A. Stein et al., *Sage Mathematics Software (Version 6.4)*, The Sage Development Team, 2014, available from `http://www.sagemath.org`.

[24] Christian Wuthrich, *prove_BSD for elliptic curve uses an incorrect lemma*, Bug report and fixing patch for SageMath, available at `http://trac.sagemath.org/ticket/17869`, 2015.