SELMER COMPANION CURVES

BARRY MAZUR AND KARL RUBIN

ABSTRACT. We say that two elliptic curves E_1, E_2 over a number field K are *n-Selmer companions* for a positive integer n if for every quadratic character χ of K, there is an isomorphism $\mathrm{Sel}_n(E_1^\chi/K) \cong \mathrm{Sel}_n(E_2^\chi/K)$ between the n-Selmer groups of the quadratic twists E_1^χ, E_2^χ. We give sufficient conditions for two elliptic curves to be n-Selmer companions, and give a number of examples of non-isogenous pairs of companions.

1. INTRODUCTION

There has recently been much interest in the relative densities of p-Selmer ranks of elliptic curves in families consisting of all quadratic twists of a given elliptic curve E over a fixed number field K. There are

- conjectures about these relative densities [9],
- some theorems for $p = 2$ for elliptic curves over $K = \mathbf{Q}$ with full 2-torsion rational [4, 17]
- some theorems for $p = 2$ for elliptic curves over arbitrary number fields K with other restrictions on the rational 2-torsion [5, 6]

The results here are still fragmentary, but the general sense of these conjectures and results is that the relative densities of the sets of characters χ such that E^χ has a fixed p-Selmer rank (the characters being ordered appropriately . . .) are expected to depend only on a few of the basic features of the elliptic curve E and number field K. For example, if $p = 2$ and $\mathrm{Gal}(K(E[2])/K) \cong S_3$, then these densities depend only on a single parameter, a rational number $\delta(E, K) \in [0, 1]$ that we call the *disparity* [6]. Moreover, if K has a real embedding then $\delta(E, K) = 1/2$, so for such E and K these densities are absolute constants.

At the present we have no results at all giving rank densities of p-Selmer groups of quadratic twist families when $p > 2$. For example, fix a number field K, a prime number p, and an elliptic curve E over K. We expect that the ranks of the p-Selmer groups in the family of all quadratic twists of E over K are unbounded, but we can prove this for no triple (K, p, E) with $p > 2$. Nonetheless, we have precise expectations [9] for the statistics governing p-rank densities in this context.

In view of this type of constancy of densities of Selmer ranks, let us consider the Selmer rank function itself, rather than its statistics, and formulate the following inverse question. For every positive integer n, let $\mathrm{Sel}_n(E/K)$ denote the n-Selmer group of E over K (see Definition 6.2), and for every quadratic character χ of K, we denote by E^χ the quadratic twist of E by χ.

Question 1.1. *For a fixed prime p and number field K, how much information about E can be read off from the function $\chi \mapsto \dim_{\mathbf{F}_p} \mathrm{Sel}_p(E^\chi/K)$?*

This leads us to the following definition.

Definition 1.2. We will say that two elliptic curves E_1, E_2 over K are *n-Selmer companions* if for every quadratic character χ of K there is a group isomorphism

$$\mathrm{Sel}_n(E_1^\chi/K) \cong \mathrm{Sel}_n(E_2^\chi/K).$$

If $n = \prod p_i^{k_i}$, then E_1 and E_2 are n-Selmer companions if and only if they are $p_i^{k_i}$-Selmer companions for every i. For this reason we will restrict in what follows to the case where n is a prime power.

If E_1 and E_2 are isogenous over K by an isogeny of prime degree ℓ, then so are E_1^χ and E_2^χ for every χ, and the induced maps $\mathrm{Sel}_n(E_1^\chi/K) \to \mathrm{Sel}_n(E_1^\chi/K)$ are isomorphisms for every n prime to ℓ. Thus in this case E_1 and E_2 are n-Selmer companions for every n prime to ℓ. For this reason we are mainly interested in non-isogenous n-Selmer companions, although the case of isogenies of degree dividing n is still interesting.

Our main result is Theorem 3.1 below, which gives sufficient conditions for a pair of curves to be p^k-Selmer companions for a prime power p^k.

For example, we will show (see §4) that the following pairs of non-isogenous curves, given with their labels from [2], are p^k-Selmer companions for p^k as listed, over every number field K (and in particular over $\mathbf{Q}$):

p^k	label	curve
4	1242L1	$y^2 + xy + y = x^3 - x^2 + x + 1$
	1242K1	$y^2 + xy + y = x^3 - x^2 - 1666739 - 2448131309$
5	676B1	$y^2 = x^3 + x^2 - 4x - 12$
	676E1	$y^2 = x^3 - 28561x + 1856465$
7	1026N1	$y^2 + xy + y = x^3 - x^2 - 34601x - 2468631$
	1026O1	$y^2 + xy + y = x^3 - x^2 - 4241x + 107353$
9	6555D1	$y^2 + y = x^3 - x^2 + 59335x + 3888371$
	6555E1	$y^2 + y = x^3 - x^2 - 33735977475x - 2384987222304844$

A natural open problem is to give necessary and sufficient conditions for p-companionship, with a prime p. We have not found any example of a pair of p-Selmer companions having different conductors, or having different Galois action on their p-torsion points. In §7 we give some results relating the conductors of Selmer companions.

It also seems natural to expect that a given elliptic curve can have only finitely many p-Selmer companions, even if we allow the prime p to vary. It is not difficult to show that for a given E_1/K and fixed p, there are only finitely many E_2/K satisfying the hypotheses of Theorem 3.1, because all such curves must have the same set of primes of bad reduction. See Proposition 7.1.

Finally, much of what we do in this paper applies more generally to the Bloch-Kato Selmer groups [1] attached to a motive. The subtlest problem in the general case, as in the case of elliptic curves, is to understand the local condition at p in the definition of the Bloch-Kato p^k-Selmer group, and how it changes under twists. It would be of interest to try to express that local condition only in terms of finite congruence information related to the motive.

Notation. If K is a field, we let $\bar{K}$ denote a fixed algebraic closure of K, and $G_K = \text{Gal}(\bar{K}/K)$. Let $\mathcal{X}(K) := \text{Hom}(G_K, \{\pm 1\})$ be the group of quadratic characters of K.

If E is an elliptic curve over K and m is a positive integer, then $E[m]$ will denote the kernel of multiplication by m on E.

If K is a local field and E is an elliptic curve over K, then we will say that E has potentially good reduction if E has good reduction over some finite extension F of K, *including* the case where E has good reduction over K, i.e., $F = K$. Similarly we will say that E has potentially multiplicative reduction if E has multiplicative reduction over a finite extension F of K, including the case where E has multiplicative reduction over K.

2. Elliptic curves over local fields

For this section suppose that K is a finite extension of $\mathbf{Q}_\ell$ for some rational prime ℓ, and E is an elliptic curve over K with potentially multiplicative reduction. Let $\text{ord}_K : K^\times \twoheadrightarrow \mathbf{Z}$ denote the valuation on K.

Definition 2.1. There is a unique character $\psi = \psi_{E/K} \in \mathcal{X}(K)$ such that the twist E^ψ has split multiplicative reduction (see for example [12, §1.12]). We will call ψ the *splitting character* of E/K.

The next proposition is due to Tate [19, Theorem 1].

Proposition 2.2 (Tate [19])**.** *There is a Tate parameter $q = q_E \in K^\times$ with $\text{ord}_K(q) < 0$, and an isomorphism*

$$\tau_{E/K} : \bar{K}^\times/q^{\mathbf{Z}} \xrightarrow{\sim} E(\bar{K}).$$

If E has split multiplicative reduction, then $\tau_{E/K}$ is G_K-equivariant. In general, we have

$$\tau_{E/K}(u^\sigma) = \psi(\sigma)\tau_{E/K}(u)^\sigma$$

for every $\sigma \in G_K$, where ψ is the splitting character of E/K.

Let $\boldsymbol{\mu}_m$ denote the group of m-th roots of unity in $\bar{K}$, and

$$\epsilon_m : G_K \to \text{Aut}(\boldsymbol{\mu}_m) \xrightarrow{\sim} (\mathbf{Z}/m\mathbf{Z})^\times$$

the mod m cyclotomic character.

Definition 2.3. For $m > 0$, define the canonical subgroup

$$\mathcal{C}_{E/K}[m] := \tau_{E/K}(\boldsymbol{\mu}_m) \subset E[m].$$

Lemma 2.4. *There is a G_K-isomorphism $\mathcal{C}_{E/K}[m] \cong \boldsymbol{\mu}_m \otimes \psi_{E/K}$, i.e., $\mathcal{C}_{E/K}[m]$ is a cyclic group of order m on which G_K acts by the character $\epsilon_m\psi_{E/K}$.*

Proof. This is immediate from Proposition 2.2. □

Let $j(E)$ denote the j-invariant of E.

Lemma 2.5. *Suppose E_1, E_2 are elliptic curves over K with potentially multiplicative reduction, p is a prime, and $p \nmid \text{ord}_K(j(E_1))$. Suppose further that either $p \neq 2$, or E_1 and E_2 have multiplicative reduction.*

Then for every $k \geq 1$ and every G_K-isomorphism $\lambda : E_1[p^k] \xrightarrow{\sim} E_2[p^k]$, we have

$$\lambda(\mathcal{C}_{E_1/K}[p^k]) = \mathcal{C}_{E_2/K}[p^k].$$

Proof. Let q_i be the Tate parameter of E_i/K, and ψ_i the splitting character. Let $\tau_i = \tau_{E_i/K}$ be the map of Proposition 2.2.

Fix a G_K-isomorphism $\lambda : E_1[p^k] \xrightarrow{\sim} E_2[p^k]$. By Proposition 2.2, for every $\sigma \in G_K$ and $\beta \in (\bar{K}^\times/q_i^{\mathbf{Z}})[p^k]$, we have

$$(1) \qquad \psi_i(\sigma)\tau_i(\beta)^\sigma - \tau_i(\beta) = \tau_i(\beta^\sigma/\beta) \in \tau_i(\boldsymbol{\mu}_{p^k}) = \mathcal{C}_{E_i/K}[p^k].$$

Define

$$B_i = \{z^\sigma - z : z \in E_i[p^k],\ \sigma \in G_K,\ \text{and}\ \psi_1(\sigma) = \psi_2(\sigma) = 1\}.$$

Then by (1) we have $B_i \subset \mathcal{C}_{E_i/K}[p^k]$, and since λ is G_K-equivariant we have $\lambda(B_1) = B_2$.

Choose $\gamma \in \bar{K}$ with $\gamma^p = q_1$. We have $\operatorname{ord}_K(q_1) = -\operatorname{ord}_K(j(E_1))$, so $\operatorname{ord}_K(q_1)$ is prime to p and $[K(\gamma) : K] = p$. We will show that there is a $\sigma \in G_K$ such that $\gamma^\sigma \neq \gamma$ and $\psi_1(\sigma) = \psi_2(\sigma) = 1$.

Case 1: E_1 and E_2 have multiplicative reduction. Since $\operatorname{ord}_K(q_1)$ is prime to p, $K(\gamma)/K$ is ramified, so there is a σ in the inertia group $I_K \subset G_K$ such that $\gamma^\sigma \neq \gamma$. If E_1 and E_2 have multiplicative reduction, then ψ_1 and ψ_2 are unramified, so $\psi_1(\sigma) = \psi_2(\sigma) = 1$.

Case 2: $p > 2$. Since $[K(\gamma) : K] = p$, we have $\gamma \notin K(\boldsymbol{\mu}_p)$. Thus we can choose $\sigma_0 \in G_{K(\boldsymbol{\mu}_p)}$ such that $\gamma^{\sigma_0} \neq \gamma$. Let $\sigma = \sigma_0^2$. Since $p \neq 2$ and σ_0 fixes $\gamma^{\sigma_0}/\gamma \in \boldsymbol{\mu}_p$, we have that $\gamma^\sigma/\gamma = (\gamma^{\sigma_0}/\gamma)^2 \neq 1$. Since ψ_1 and ψ_2 are quadratic characters, we also have $\psi_1(\sigma) = \psi_2(\sigma) = 1$.

Now choose $\beta \in \bar{K}$ with $\beta^{p^k} = q_1$. Then β^σ/β is a primitive p^k-th root of unity, so $\tau_1(\beta^\sigma/\beta)$ generates $\mathcal{C}_{E_1/K}[p^k]$, and by (1) we have that $\tau_1(\beta^\sigma/\beta) \in B_1$. Therefore $B_1 = \mathcal{C}_{E_1/K}[p^k]$, so

$$\lambda(\mathcal{C}_{E_1/K}[p^k]) = \lambda(B_1) = B_2 \subset \mathcal{C}_{E_2/K}[p^k].$$

The final inclusion must be an equality because both groups have order p^k by Lemma 2.4. □

3. Main theorem

Suppose for this section that K is a number field. Fix a prime p and a power p^k of p, $k \geq 1$. Our main result is the following.

Theorem 3.1. *Suppose E_1 and E_2 are elliptic curves over K. Let S_i be the set of primes of K where E_i has potentially multiplicative reduction. Let $m = p^{k+1}$ if $p \leq 3$, and $m = p^k$ if $p > 3$. Suppose further that:*

(i) *there is a G_K-isomorphism $E_1[m] \cong E_2[m]$,*

(ii) *$S_1 = S_2$,*

(iii) *for all $\mathfrak{l} \in S_1 = S_2$, the isomorphism of (i) sends $\mathcal{C}_{E_1/K_\mathfrak{l}}[m]$ to $\mathcal{C}_{E_2/K_\mathfrak{l}}[m]$,*

(iv) *for every $\mathfrak{p}$ of K above p, either*

  - *$\mathfrak{p} \in S_1 = S_2$, or*
  - *$k = 1$, E_1 and E_2 have good reduction at $\mathfrak{p}$, and the ramification degree $e(\mathfrak{p}/p)$ is less than $p - 1$.*

Then for every finite extension F of K, and every $\chi \in \mathcal{X}(F)$, there is a canonical isomorphism

$$\operatorname{Sel}_{p^k}(E_1^\chi/F) \cong \operatorname{Sel}_{p^k}(E_2^\chi/F).$$

In particular E_1 and E_2 are p^k-Selmer companions over every number field containing K.

A slightly stronger version of Theorem 3.1 will be proved in §6 below. We first give some remarks, consequences and examples.

Remark 3.2. The proof of Theorem 3.1 will show that $\mathrm{Sel}_{p^k}(E_1^\chi/F)$, $\mathrm{Sel}_{p^k}(E_2^\chi/F)$ are actually equal inside $H^1(F, E_1^\chi[p^k]) = H^1(F, E_2^\chi[p^k])$, where we use the isomorphism $E_1[p^k] \cong E_2[p^k]$ to identify $H^1(F, E_1^\chi[p^k])$ with $H^1(F, E_2^\chi[p^k])$. See Definition 6.2 and the remarks following it.

Remark 3.3. A careful reading of the proof will show that when $p = 3$, if E_1 and E_2 have no primes of additive reduction of Kodaira type II, IV, II*, or IV*, then we can take $m = 3^k$ instead of 3^{k+1} in the hypotheses of Theorem 3.1. See Remark 5.2. In particular if E is semistable, we can take $m = 3^k$ instead of $m = 3^{k+1}$.

Corollary 3.4. *Suppose K' is a number field with a unique prime $\mathfrak{p}$ above p. Suppose E_1 and E_2 are elliptic curves over K' with potentially multiplicative reduction at $\mathfrak{p}$, and with potentially good reduction at all primes different from $\mathfrak{p}$. Let $m = p^{k+1}$ if $p \le 3$, and $m = p^k$ if $p > 3$. Then E_1 and E_2 are p^k-Selmer companions over every number field K containing $K'(E_1[m], E_2[m])$.*

Proof. Fix any group isomorphism $\lambda : E_1[m] \to E_2[m]$ that takes $\mathcal{C}_{E_1/K'_{\mathfrak{p}}}[m]$ to $\mathcal{C}_{E_2/K'_{\mathfrak{p}}}[m]$. If K is a field containing $K'(E_1[m], E_2[m])$, then λ is G_K-equivariant because G_K acts trivially on both sides. We have $S_1 = S_2$ is the set of all primes of K above $\mathfrak{p}$, so all hypotheses of Theorem 3.1 are satisfied. □

Remark 3.5. One can also twist elliptic curves by characters of order $\ell > 2$. In this case the twist E^χ is an abelian variety of dimension $\ell - 1$, with an action of the group of ℓ-th roots of unity. One can study the $\mathfrak{n}$-Selmer groups $\mathrm{Sel}_{\mathfrak{n}}(E^\chi/K)$, where $\mathfrak{n}$ is an ideal of the cyclotomic field of ℓ-th roots of unity, and ask when two elliptic curves E_1, E_2 have the property that $\mathrm{Sel}_{\mathfrak{n}}(E_1^\chi/K) \cong \mathrm{Sel}_{\mathfrak{n}}(E_2^\chi/K)$ for every character χ of G_K of order ℓ. An analogue of Theorem 3.1 holds in this case, with a similar proof.

4. EXAMPLES

Suppose we are given elliptic curves E_1, E_2 over K. We next introduce some tools to prove in practice that E_1 and E_2 satisfy the hypotheses of Theorem 3.1. Let $m = p^k$ or p^{k+1} as in Theorem 3.1.

Remark 4.1. The most difficult hypothesis of Theorem 3.1 to check is (i), the existence of a G_K-isomorphism $E_1[m] \cong E_2[m]$. When $m \le 5$ this can be done by computing explicitly the (genus zero) family of all elliptic curves E over K with $E[m] \cong E_1[m]$, and checking whether E_2 belongs to this family.

For larger m the problem is more subtle. A necessary condition for the existence of such an isomorphism is that for every prime $\mathfrak{l}$ of K where E_1 and E_2 have good reduction, the traces of Frobenius $\mathrm{Frob}_{\mathfrak{l}}$ acting on $E_1[m]$ and $E_2[m]$ are the same. In some cases this necessary condition can be turned into a sufficient condition (see for example [7]). We will take a more brute force approach, and for candidate curves that satisfy the necessary condition on traces for many primes, we will simply construct an isomorphism directly.

We will discuss both of these approaches in more detail in Appendix A. It is expected that for m sufficiently large (depending on K) there are *no* pairs of non-isogenous elliptic curves E_1, E_2 over K with $E_1[m] \cong E_2[m]$ as G_K-modules.

If E is an elliptic curve, let $j(E)$ denote its j-invariant.

Remark 4.2. It is well-known (see for example [18]) that an elliptic curve E has potentially multiplicative reduction at a prime $\mathfrak{l}$ if and only if $\mathrm{ord}_{\mathfrak{l}}(j(E)) < 0$. Thus $S_1 = S_2$ if and only if $j(E_1)$ and $j(E_2)$ have the same primes in their denominators. This makes it very easy to check hypothesis (ii) of Theorem 3.1.

Hypothesis (iii) can often be verified by using Lemma 2.5.

Example 4.3. Consider the first example of the Introduction, with $K = \mathbf{Q}$, $p^k = 4$, and

$$E_1 : y^2 + xy + y = x^3 - x^2 + x + 1,$$
$$E_2 : y^2 + xy + y = x^3 - x^2 - 1666739 - 2448131309.$$

These are the curves 1242L1 and 1242K1, respectively, in [2]. The following proposition can be proved using the method of §A.2 of Appendix A, using computations in Sage [16] and PARI/GP [14]. Its proof will be sketched at the end of §A.2

Proposition 4.4. *There is a $G_{\mathbf{Q}}$-isomorphism $E_1[8] \cong E_2[8]$.*

Computing the j-invariants gives

$$(2) \qquad\qquad j(E_1) = \frac{3^3 \cdot 7^3}{2 \cdot 23}, \quad j(E_2) = \frac{3 \cdot 987697^3}{2^{49} \cdot 23}$$

so $S_1 = S_2 = \{2, 23\}$. Combined with Proposition 4.4, this shows that Theorem 3.1(i,ii,iv) are satisfied. For $\ell \in \{2, 23\}$ both E_1 and E_2 have multiplicative reduction at ℓ, and $\mathrm{ord}_{\ell}(j(E_1))$ is odd, so Lemma 2.5 shows that Theorem 3.1(iii) is satisfied.

Thus all hypotheses of Theorem 3.1 are satisfied, and we conclude that E_1 and E_2 are 4-Selmer companions over every number field.

The third and fourth examples of the introduction, with $p^k = 7$ and 9, are proved in exactly the same way, using §A.2 to construct a $G_{\mathbf{Q}}$-isomorphism $E_1[m] \cong E_2[m]$. For the $p^k = 9$ example, we use Remark 5.2 below so that (since E_1 and E_2 are semistable) we can take $m = 9$ in Theorem 3.1 instead of $m = 27$.

Example 4.5. Consider the second example of the Introduction, with $K = \mathbf{Q}$, $p^k = 5$, and

$$E_1 : y^2 = x^3 + x^2 - 4x - 12$$
$$E_2 : y^2 = x^3 - 28561x + 1856465$$

These are the curves $676B1$ and $676E1$, respectively, in [2]. We will prove the following proposition in §A.1 of Appendix A.

Proposition 4.6. *There is a $G_{\mathbf{Q}}$-isomorphism $E_1[5] \cong E_2[5]$.*

Both E_1 and E_2 have conductor $676 = 2^2 \cdot 13^2$, $j(E_1) = -208$, and $j(E_2) = 1168128$. Thus E_1, E_2 have good reduction at 5 and potentially good reduction everywhere, so $S_1 = S_2$ is the empty set and all hypotheses of Theorem 3.1 are satisfied. We conclude that E_1 and E_2 are 5-Selmer companions over every number field.

The strategy of Example 4.5, along with the method described in §A.1 of Appendix A, works in exactly the same way to give many more examples of p-Selmer companions over $\mathbf{Q}$ with $p = 2, 3$ or 5.

5. Elliptic curves over local fields, continued

For this section let K be a finite extension of $\mathbf{Q}_\ell$ or of $\mathbf{R}$. Fix a rational prime power p^k. For every elliptic curve E/K, let $\kappa_E = \kappa_{E/K}$ denote the Kummer map

$$\kappa_{E/K} : E(K) \longrightarrow H^1(K, E[p^k]).$$

For the proof of Theorem 3.1 we need to understand the image of κ_E. We will consider several cases.

5.1. **Potentially good reduction.**

Lemma 5.1. *Suppose that either K is archimedean, or K is nonarchimedean of residue characteristic different from p and E has bad, potentially good reduction.*

(i) *If $p \leq 3$, then* $\mathrm{image}(\kappa_E)$ *is represented by the cocycles*

$$\{c_t : t \in E[p^{k+1}], p^k t \in E(K)\},$$

where c_t is defined by $c_t(\sigma) = t^\sigma - t$ for $\sigma \in G_K$.
(ii) *If $p > 3$, or if v is archimedean and $p > 2$, then* $\mathrm{image}(\kappa_E) = 0$.

Proof. We consider the archimedean and nonarchimedean cases separately.

Case 1: K is archimedean. In this case (ii) is clear, because G_K has order 1 or 2 so $H^1(K, E[p^k]) = 0$.

For every p, the map $E(K)[p] \to E(K)/p^k E(K)$ is surjective, so $\mathrm{image}(\kappa_E) = \kappa_E(E(K)[p])$. If $s \in E(K)[p]$, then $\kappa_E(s)$ is represented by the cocycle c_t for (every) $t \in E[p^{k+1}]$ with $p^k t = s$. This proves (i) in this case.

Case 2: K is nonarchimedean of residue characteristic different from p and E has bad, potentially good reduction. Consider the filtration

$$E_1(K) \subset E_0(K) \subset E(K)$$

where $E_0(K)$ is the subgroup of points with nonsingular reduction, and $E_1(K)$ is the subgroup of points that reduce to zero [15, Chapter VII]. Then $E_1(K)$ is a pro-ℓ-group, where ℓ is the residue characteristic of K. Since E has additive reduction, $E_0(K)/E_1(K)$ is isomorphic to the additive group of the residue field of K, also an ℓ-group. The description of $E(K)/E_0(K)$ in [18] shows that the p-part of $E(K)/E_0(K)$ is killed by p, and is trivial if $p > 3$. Hence $E(K)/p^k E(K) = 0$ if $p > 3$, and $E(K)[p] \to E(K)/p^k E(K)$ is surjective for every p. Therefore $\mathrm{image}(\kappa_E) = 0$ if $p > 3$, and (as in Case 1) $\mathrm{image}(\kappa_E) = \kappa_E(E(K)[p])$ is represented by the cocycles $\{c_t : t \in E[p^{k+1}], p^k t \in E(K)\}$ if $p \leq 3$. This completes the proof. $\square$

Remark 5.2. Suppose $p = 3$. If K is nonarchimedean and the Kodaira type of the reduction of E is not II, IV, II*, or IV*, then [18] shows that $E(K)/E_0(K)$ has order prime to 3. Thus in those cases we have $\mathrm{image}(\kappa_E) = 0$, just as when $p > 3$. This allows us to take $m = 3^k$ instead of $m = 3^{k+1}$ in Theorem 3.1 in this case (see Remark 3.3).

Lemma 5.3. *Suppose K is nonarchimedean of residue characteristic different from p, and E_1, E_2 are elliptic curves over K with potentially good reduction. If $m \geq 3$ and $E_1[m] \cong E_2[m]$ as G_K-modules, then either both E_1 and E_2 have good reduction, or both have bad reduction.*

Proof. By [13, Proposition 7.1(b)], if one of E_1, E_2 has good reduction, then the other cannot have additive reduction. The lemma follows directly.   □

5.2. **Potentially multiplicative reduction.** Recall that if E has potentially multiplicative reduction, then Proposition 2.2 gives a parameter q and an isomorphism $\tau_{E/K} : \bar{K}^\times/q^{\mathbf{Z}} \to E(\bar{K})$.

Lemma 5.4. *Suppose E/K has split multiplicative reduction. Then $\mathrm{image}(\kappa_E)$ is the image of the composition*

$$K^\times \longrightarrow H^1(K, \boldsymbol{\mu}_{p^k}) \longrightarrow H^1(K, E[p^k])$$

where the first map is the classical Kummer map, and the second is induced by the inclusion $\tau_{E/K} : \boldsymbol{\mu}_{p^k} \hookrightarrow E[p^k]$.

Proof. This follows directly from the commutativity of the diagram

$$
\begin{array}{ccc}
K^\times & \longrightarrow & H^1(K, \boldsymbol{\mu}_{p^k}) \\
\tau_{E/K} \downarrow & & \downarrow \tau_{E/K} \\
E(K) & \xrightarrow{\kappa_E} & H^1(K, E[p^k]).
\end{array}
$$

□

Definition 5.5. Suppose L is a quadratic extension of K. Let $N_{L/K} : L^\times \to K^\times$ be the norm map, and let $\psi \in \mathcal{X}(K)$ be the quadratic character attached to L/K. Let $\boldsymbol{\mu}_{p^k} \otimes \psi$ denote a copy of $\boldsymbol{\mu}_{p^k}$ with G_K acting by $\epsilon_{p^k}\psi$ instead of ϵ_{p^k}, and define a twisted Kummer map

$$\nu_{L/K} : \ker(N_{L/K}) \longrightarrow H^1(K, \boldsymbol{\mu}_{p^k} \otimes \psi)$$

where for $x \in \ker(N_{L/K})$, we choose $u \in \bar{K}$ such that $u^{p^k} = x$, and then $\nu_{L/K}(x)$ is represented by the cocycle $\sigma \mapsto (u^\sigma)^{\psi(\sigma)}/u$. We leave it as an exercise to show that $\sigma \mapsto (u^\sigma)^{\psi(\sigma)}/u$ is indeed a cocycle with values in $\boldsymbol{\mu}_{p^k} \otimes \psi$, when $x \in \ker(N_{L/K})$.

Lemma 5.6. *Suppose E/K has potentially multiplicative reduction, with nontrivial splitting character ψ (i.e., E/K does not have split multiplicative reduction). Let $q \in K^\times$ be the Tate parameter, and let L be the quadratic extension of K attached to ψ. Let $\mathcal{H}$ be the image of the composition*
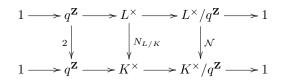
$$\ker(N_{L/K}) \xrightarrow{\nu_{L/K}} H^1(K, \boldsymbol{\mu}_{p^k} \otimes \psi) \xrightarrow{\tau_{E/K}} H^1(K, E[p^k]).$$

  (i) *If $p > 2$, or if $p = 2$ and $q \notin N_{L/K}L^\times$, then $\mathrm{image}(\kappa_E) = \mathcal{H}$.*
  (ii) *Suppose $p = 2$ and $q = N_{L/K}(\beta)$ with $\beta \in L^\times$. Then $\mathrm{image}(\kappa_E)$ is the subgroup of $H^1(K, E[p^k])$ generated by $\mathcal{H}$ and the class of the cocycle*

$$\sigma \mapsto \tau_{E/K}((\alpha^\sigma)^{\psi(\sigma)}/\alpha)$$

  where $\alpha \in \bar{K}^\times$ and $\alpha^{2^k} = \beta$.

Proof. Consider the commutative diagram with exact rows

$$1 \longrightarrow q^{\mathbf{Z}} \longrightarrow L^{\times} \longrightarrow L^{\times}/q^{\mathbf{Z}} \longrightarrow 1$$
$$\downarrow{2} \qquad \downarrow{N_{L/K}} \qquad \downarrow{\mathcal{N}}$$
$$1 \longrightarrow q^{\mathbf{Z}} \longrightarrow K^{\times} \longrightarrow K^{\times}/q^{\mathbf{Z}} \longrightarrow 1$$

where we denote by $\mathcal{N}$ the right-hand norm map. The snake lemma shows that the map $\ker(N_{L/K}) \to \ker(\mathcal{N})$ is surjective if $q \notin N_{L/K}L^{\times}$, and if $q = N_{L/K}(\beta)$ then the cokernel of that map has order 2, and $\ker(\mathcal{N})$ is generated by the image of $\ker(N_{L/K})$ and β.

Proposition 2.2 shows that we have a commutative diagram

$$\ker(N_{L/K}) \xrightarrow{\nu_{L/K}} H^1(K, \boldsymbol{\mu}_{p^k} \otimes \psi)$$
$$\downarrow{\tau_{E/K}} \qquad\qquad \downarrow{\tau_{E/K}}$$
$$E(K) \xrightarrow{\kappa_E} H^1(K, E[p^k]),$$

and $\tau_{E/K} : \ker(\mathcal{N}) \to E(K)$ is an isomorphism. (To see this last fact, note that $\tau_{E/K} : L^{\times}/q^{\mathbf{Z}} \to E(L)$ is a group isomorphism satisfying $\tau_{E/K}(u^{\sigma}) = -\tau_{E/K}(u)^{\sigma}$ if σ is the nontrivial automorphism of L/K, so $\tau_{E/K}(u) \in E(K)$ if and only if $u^{\sigma} = u^{-1}$, i.e., if and only if $\mathcal{N}(u) = 1$.) It follows that $\text{image}(\kappa_E) = \mathcal{H}$ if $p > 2$ or if $q \notin N_{L/K}L^{\times}$, and if $q = N_{L/K}(\beta)$ then $\text{image}(\kappa_E)$ is generated by $\mathcal{H}$ and $\kappa_E(\tau_{E/K}(\beta))$.

Suppose $p = 2$ and $q = N_{L/K}(\beta)$, and choose $\alpha \in \bar{K}^{\times}$ with $\alpha^{2^k} = \beta$. Then by definition $\kappa_E(\tau_{E/K}(\beta))$ is represented by the cocycle $\sigma \mapsto \tau_{E/K}(\alpha)^{\sigma} - \tau_{E/K}(\alpha)$, and by Proposition 2.2

$$\tau_{E/K}(\alpha)^{\sigma} - \tau_{E/K}(\alpha) = \psi(\sigma)\tau_{E/K}(\alpha^{\sigma}) - \tau_{E/K}(\alpha) = \tau_{E/K}((\alpha^{\sigma})^{\psi(\sigma)}/\alpha).$$

This completes the proof of the lemma. $\qquad\square$

Lemma 5.7. *Let $m = 2^{k+1}$ if $p = 2$, and $m = p^k$ if $p > 2$. Suppose E_1 and E_2 are elliptic curves over K with potentially multiplicative reduction, and there is a G_K-isomorphism $E_1[m] \cong E_2[m]$ that identifies $\mathcal{C}_{E_1/K}[m]$ with $\mathcal{C}_{E_2/K}[m]$.*

    (i) *The splitting characters of E_1 and E_2 are equal.*
    (ii) *Suppose $p = 2$. Let q_i be the Tate parameter of E_i, and $\pi_1 \in \bar{K}^{\times}$ with $\pi_1^{2^k} = q_1$. Then there is an $x \in K^{\times}$ and an odd integer n such that $q_2^n = q_1 x^m$ and $\tau_{E_1/K}(\pi_1) = \tau_{E_2/K}(\pi_1 x^2)$ in $E_1[2^k] = E_2[2^k]$.*

Proof. Since $\mathcal{C}_{E_1/K}[m]$ and $\mathcal{C}_{E_1/K}[m]$ are isomorphic G_K-modules, and $m > 2$, assertion (i) follows directly from Lemma 2.4.

Suppose $p = 2$, and let $\lambda : E_1[m] \to E_2[m]$ be the G_K-isomorphism. We will abbreviate $\tau_i := \tau_{E_i/K}$. Replacing λ by an odd multiple of λ if necessary, we may assume that the diagram

(3)
$$\boldsymbol{\mu}_m \underset{\tau_2}{\overset{\tau_1}{}} \begin{array}{c} E_1[m] \\ \downarrow{\lambda} \\ E_2[m] \end{array}$$

commutes.

Fix $\beta_1 \in \bar{K}^\times$ such that $\beta_1^m = q_1$. Then $\tau_1(\beta_1) \in E_1[m]$, and we fix $\beta_2 \in \bar{K}^\times$ such that $\tau_2(\beta_2) = \lambda(\tau_1(\beta_1))$. Since $\tau_2(\beta_2) \in E_2[m]$, we have $\beta_2^m \in q_2^{\mathbf{Z}}$, say $\beta_2^m = q_2^n$. If n is even, then $\beta_2^{m/2} = \pm q_2^{n/2}$, so $\tau_2(\beta_2^{m/2}) = \tau_2(\pm 1) \in \mathcal{C}_{E_2/K}[m]$. But $\tau_1(\beta_1^{m/2}) \notin \mathcal{C}_{E_1/K}[m]$, so this is impossible and n must be odd.

Let ψ denote the common splitting character of E_1 and E_2. By Proposition 2.2, for every $\sigma \in G_K$ we have

$$\tau_i(\beta_i^\sigma/\beta_i) = \tau_i(\beta_i^\sigma) - \tau_i(\beta_i) = \psi(\sigma)\tau_i(\beta_i)^\sigma - \tau_i(\beta_i).$$

Applying λ we see that $\lambda(\tau_1(\beta_1^\sigma/\beta_1)) = \tau_2(\beta_2^\sigma/\beta_2)$. But $\beta_i^\sigma/\beta_i \in \boldsymbol{\mu}_m$, so by (3) we have $\beta_1^\sigma/\beta_1 = \beta_2^\sigma/\beta_2$. Thus $(\beta_2/\beta_1)^\sigma = \beta_2/\beta_1$ for every $\sigma \in G_K$, so $\beta_2/\beta_1 \in K$.

Let $x = \beta_2/\beta_1$. Then $q_2^n = q_1 x^m$, and if we take $\pi_1 = \beta_1^2$ then $\pi_1^{2^k} = q_1$ and

$$\tau_2(\pi_1 x^2) = \tau_2(\pi_1 \beta_2^2/\beta_1^2) = \tau_2(\beta_2^2) = \lambda(\tau_1(\beta_1^2)) = \lambda(\tau_1(\pi_1)).$$

This proves (ii). $\qquad\square$

5.3. The group scheme kernel of p^k.

Let $\mathcal{O}$ be the ring of integers of K and $\mathbf{F}$ the residue field. Let $\mathcal{E}$ be the Néron model of E, so $\mathcal{E}$ is a smooth group scheme over $\mathcal{O}$. Let $\mathcal{E}^0$ be its connected component at the identity, so $\mathcal{E}^0$ is an open subgroup scheme of $\mathcal{E}$. Let $\mathcal{E}^0_{/\mathbf{F}} \subset \mathcal{E}_{/\mathbf{F}}$ be the closed fibers of these group schemes, and $\Phi = \mathcal{E}_{/\mathbf{F}}/\mathcal{E}^0_{/\mathbf{F}}$ the group of components of the closed fiber, viewed as a (finite étale) group scheme over $\mathbf{F}$. Let $\mathcal{E}[p^k]$ the kernel of multiplication by p^k on $\mathcal{E}$; this is a group scheme over $\mathcal{O}$ with finite generic fiber.

Proposition 5.8. *Suppose that multiplication by p induces a faithfully flat morphism $\mathcal{E} \to \mathcal{E}$ over $\mathcal{O}$. Then $\mathcal{E}[p^k]$ is a quasi-finite flat group scheme over $\mathcal{O}$, and* image(κ_E) *is the image of the composition*

$$H^1_{\mathrm{fppf}}(\mathrm{Spec}(\mathcal{O}), \mathcal{E}[p^k]) \longrightarrow H^1_{\mathrm{fppf}}(\mathrm{Spec}(K), \mathcal{E}[p^k]) \xrightarrow{\sim} H^1(K, E[p^k])$$

where H^1_{fppf} means cohomology of abelian group schemes, computed in the fppf *topology.*

Proof. This follows from [8, Lemma 5.1(iii)]. The long exact cohomology sequence attached to $0 \to \mathcal{E}[p^k] \to \mathcal{E} \xrightarrow{p^k} \mathcal{E} \to 0$ gives

$$\longrightarrow H^0_{\mathrm{fppf}}(\mathrm{Spec}(\mathcal{O}), \mathcal{E}) \xrightarrow{p^k} H^0_{\mathrm{fppf}}(\mathrm{Spec}(\mathcal{O}), \mathcal{E})$$
$$\longrightarrow H^1_{\mathrm{fppf}}(\mathrm{Spec}(\mathcal{O}), \mathcal{E}[p^k]) \longrightarrow H^1_{\mathrm{fppf}}(\mathrm{Spec}(\mathcal{O}), \mathcal{E})[p^k].$$

We have $H^0_{\mathrm{fppf}}(\mathrm{Spec}(\mathcal{O}), \mathcal{E}) = E(K)$, and $H^1_{\mathrm{fppf}}(\mathrm{Spec}(\mathcal{O}), \mathcal{E})[p^k] = H^1(\mathbf{F}, \Phi)[p^k]$ by [8, Lemma 5.1(iii)]. It follows from our assumption on p that $\Phi[p^k] = 0$, so the upper left vertical map in the following commutative diagram is an isomorphism:

$$
\begin{array}{ccc}
H^0_{\mathrm{fppf}}(\mathrm{Spec}(\mathcal{O}), \mathcal{E})/p^k H^0_{\mathrm{fppf}}(\mathrm{Spec}(\mathcal{O}), \mathcal{E}) & \xrightarrow{\cong} & E(K)/p^k E(K) \\
\Big\downarrow{\scriptstyle\cong} & & \Big\downarrow{\scriptstyle\kappa_E} \\
H^1_{\mathrm{fppf}}(\mathrm{Spec}(\mathcal{O}), \mathcal{E}[p^k]) & & \\
\Big\downarrow & & \\
H^1_{\mathrm{fppf}}(\mathrm{Spec}(K), \mathcal{E}[p^k]) & \longrightarrow & H^1(K, E[p^k]).
\end{array}
$$

The proposition follows. $\qquad\square$

Remark 5.9. If K has residue characteristic p, then multiplication by p induces a faithfully flat endomorphism of $\mathcal{E}$ if and only if E has good or multiplicative reduction and p does not divide the order of Φ.

6. Proof of Theorem 3.1

The following is a slightly stronger version of Theorem 3.1. We will prove Theorem 6.1 below, and then derive Theorem 3.1 from it. Fix a prime power p^k and a number field K. Recall that for every field F, we let $\mathcal{X}(F) = \mathrm{Hom}(G_F, \{\pm 1\})$.

Theorem 6.1. *Suppose E_1 and E_2 are elliptic curves over K. Let S_i be the set of primes of K where E_i has potentially multiplicative reduction. Let $m = p^{k+1}$ if $p \le 3$, and $m = p^k$ if $p > 3$. Suppose further that:*

(i) *there is a G_K-isomorphism $E_1[m] \cong E_2[m]$,*

(ii) *$S_1 = S_2$,*

(iii) *for all $\mathfrak{l} \in S_1 = S_2$, the isomorphism of (i) sends $\mathcal{C}_{E_1/K_{\mathfrak{l}}}[m]$ to $\mathcal{C}_{E_2/K_{\mathfrak{l}}}[m]$,*

(iv) *for every prime v above p, either*

- *E_1 and E_2 have potentially multiplicative reduction at v, or*
- *$p > 2$, E_1 and E_2 have good reduction at v, and the isomorphism of (i) extends to an isomorphism $\mathcal{E}_1[p^k] \cong \mathcal{E}_2[p^k]$ over $\mathrm{Spec}(\mathcal{O}_{K_v})$, where the group scheme $\mathcal{E}_i[p^k]$ is the kernel of multiplication by p^k in the Néron model of E_i.*

Then for every finite extension F of K, and every $\chi \in \mathcal{X}(F)$, there is a canonical isomorphism

$$\mathrm{Sel}_{p^k}(E_1^\chi/F) \cong \mathrm{Sel}_{p^k}(E_2^\chi/F).$$

In particular E_1 and E_2 are p^k-Selmer companions over every number field containing K.

Definition 6.2. The p^k-*Selmer group* $\mathrm{Sel}_{p^k}(E/K) \subset H^1(K, E[p^k])$ of an elliptic curve E over K is

$$\mathrm{Sel}_{p^k}(E/K) := \ker\big(H^1(K, E[p^k]) \longrightarrow \bigoplus_v H^1(K_v, E[p^k])/\mathrm{image}(\kappa_{E/K_v})\big).$$

A G_K-isomorphism $E_1[p^k] \cong E_2[p^k]$ allows us to identify

$$H^1(K, E_1[p^k]) = H^1(K, E_2[p^k]), \quad H^1(K_v, E_1[p^k]) = H^1(K_v, E_2[p^k]) \text{ for every } v.$$

We will show that under the hypotheses of Theorems 3.1 and 6.1, with these identifications, for every v and for every $\chi \in \mathcal{X}(K_v)$, the images of the horizontal Kummer maps

(4)
$$
\begin{array}{ccc}
E_1^\chi(K_v) & \xrightarrow{\kappa_{E_1^\chi/K_v}} & H^1(K_v, E_1[p^k]) \\
& & \| \\
E_2^\chi(K_v) & \xrightarrow{\kappa_{E_2^\chi/K_v}} & H^1(K_v, E_2[p^k])
\end{array}
$$

are equal. It will then follow from the definition that $\mathrm{Sel}_{p^k}(E_1^\chi/K) = \mathrm{Sel}_{p^k}(E_2^\chi/K)$ inside $H^1(K, E_1[p^k]) = H^1(K, E_2[p^k])$ for every χ. This gives the canonical isomorphisms referred to in Theorems 3.1 and 6.1.

Proof of Theorem 6.1. Suppose E_1 and E_2 satisfy the hypotheses of Theorem 6.1. We will show that $\mathrm{image}(\kappa_{E_1^\chi/K_v}) = \mathrm{image}(\kappa_{E_2^\chi/K_v})$ for every place v of K and every $\chi \in \mathcal{X}(K)$. Note that except in the case where $v \mid p$ and E_1, E_2 have

good reduction at p (Case 5 below), if the pair (E_1, E_2) satisfies the hypotheses of Theorem 6.1, then so does the pair (E_1^χ, E_2^χ) for every $\chi \in \mathcal{X}(K)$. Thus in Cases 1-4, it is enough to consider $\chi = 1$. We will identify $E_1[p^k]$ with $E_2[p^k]$ using the given isomorphism, and denote this G_K-module simply by $E[p^k]$.

We split the proof into several cases.

Case 1: $v \mid \infty$. By Lemma 5.1, image(κ_{E_i/K_v}) is zero if $p > 2$, and is completely determined by the G_K-module $E_i[2^{k+1}]$ if $p = 2$. But if $p = 2$ then by assumption $E_1[2^{k+1}] \cong E_2[2^{k+1}]$ as G_K-modules, so image(κ_{E_1/K_v}) = image(κ_{E_2/K_v}).

Case 2: $v \nmid \infty$ and E_1 has bad, potentially good reduction at v. By our assumptions, $v \nmid p$ and E_2 also has potentially good reduction at v. By Lemma 5.3, the reduction of E_2 is also bad. By Lemma 5.1, we again see that image(κ_{E_i/K_v}) is zero if $p > 3$, and in general is completely determined by the G_K-module $E_i[m]$, so image(κ_{E_1/K_v}) = image(κ_{E_2/K_v}).

Case 3: $v \nmid p\infty$ and E_1 has good reduction at v. By our assumptions, E_2 has potentially good reduction at v. By Lemma 5.3, the reduction of E_2 is also good. It follows that for $i = 1, 2$, the image of κ_{E_i/K_v} is the unramified subgroup of $H^1(K_v, E[p^k])$ (see [3, Lemma 4.1]), i.e.,

$$\text{image}(\kappa_{E_i/K_v}) = \ker\big(H^1(K_v, E[p^k]) \to H^1(K_v^{\mathrm{ur}}, E[p^k])\big)$$

where K_v^{ur} is the maximal unramified extension of K_v. Since this subgroup is independent of i, we have image(κ_{E_1/K_v}) = image(κ_{E_2/K_v}).

Case 4: $v \nmid \infty$ and E_1 has potentially multiplicative reduction at v. By our assumptions, E_2 also has potentially multiplicative reduction at v, and the images of $H^1(K_v, \boldsymbol{\mu}_{p^k}) \to H^1(K_v, E_i[p^k])$ are identified by the isomorphism $E_i[p^k] \cong E_2[p^k]$.

Suppose first that E_1 has split multiplicative reduction. Then so does E_2 (by Lemma 5.7(i)), and then Lemma 5.4 shows that image(κ_{E_1/K_v}) = image(κ_{E_2/K_v}).

Now suppose E_1 does not have split multiplicative reduction, and let L be the quadratic extension corresponding to the splitting character of E_1/K_v. By Lemma 5.7(i), the splitting characters of E_1 and E_2 are equal. Let q_i be the Tate parameter of E_i. By Lemma 5.7(ii), if $p = 2$ we have $q_1 \in N_{L/K_v}L^\times \iff q_2 \in N_{L/K_v}L^\times$.

If $p > 2$, or if $p = 2$ and $q_1, q_2 \notin N_{L/K_v}L^\times$, then it follows from Lemma 5.6(i) that image(κ_{E_1/K_v}) = image(κ_{E_2/K_v}).

Finally, suppose that $p = 2$ and $q_1 \in N_{L/K_v}L^\times$, say $q_1 = N_{L/K_v}(\beta_1)$. Let $x \in K_v^\times$ and the odd integer n be as in Lemma 5.7(ii), so $q_2^n = q_1 x^m$, and we set $\beta_2 = (\beta_1 x^{2^k})^n$ so $N_{L/K_v}(\beta_2) = q_2^n$. Fix $\alpha_1 \in \bar{K}_v^\times$ with $\alpha_1^{2^k} = \beta_1$, and set $\alpha_2 = (\alpha_1 x)^n$, so $\alpha_2^{2^k} = \beta_2$. Using Lemma 5.6(ii), to show that image(κ_{E_1/K_v}) = image(κ_{E_2/K_v}) it is enough to show that the two cocycles

$$c_i : \sigma \mapsto \tau_{E_i/K_v}((\alpha_i^\sigma)^{\psi(\sigma)}/\alpha_i)$$

generate the same subgroup of $H^1(K_v, E[2^k])$, for $i = 1, 2$.

If σ fixes L (i.e., $\psi(\sigma) = 1$), then $((\alpha_i^\sigma)^{\psi(\sigma)}/\alpha_i)^{2^k} = \beta_i^\sigma/\beta_i = 1$, so

$$(\alpha_2^\sigma)^{\psi(\sigma)}/\alpha_2 = \alpha_2^\sigma/\alpha_2 = ((x^\sigma \alpha_1^\sigma)/(x\alpha_1))^n = (\alpha_1^\sigma/\alpha_1)^n = ((\alpha_1^\sigma)^{\psi(\sigma)}/\alpha_1)^n \in \boldsymbol{\mu}_{2^k},$$

since $x \in K_v$. By hypothesis (iii) we have

$$\tau_{E_1/K_v}(\boldsymbol{\mu}_{2^k}) = \mathcal{C}_{E_1/K_v}[2^k] = \mathcal{C}_{E_2/K_v}[2^k] = \tau_{E_2/K_v}(\boldsymbol{\mu}_{2^k})$$

inside $E_1[2^k] = E_2[2^k]$, and n is odd, so c_1 and c_2 generate the same subgroup of $H^1(K_v, E[2^k])$.

If σ does not fix L (i.e., $\psi(\sigma) = -1$), then $(\alpha_i^\sigma)^{\psi(\sigma)}/\alpha_i = 1/(\alpha_i^\sigma \alpha_i)$, and $(\alpha_1^\sigma \alpha_1)^{2^k} = \beta_1^\sigma \beta_1 = N_{L/K_v}(\beta_1) = q_1$, so by Lemma 5.7(ii) applied with $\pi_1 = \alpha_i^\sigma \alpha_i$ we have

$$\tau_{E_1/K_v}((\alpha_1^\sigma)^{\psi(\sigma)}/\alpha_1) = \tau_{E_2/K_v}(x^{-2}(\alpha_1^\sigma)^{\psi(\sigma)}/\alpha_1)$$
$$= \tau_{E_2/K_v}(((\alpha_2^\sigma)^{\psi(\sigma)}/\alpha_2)^n) = n\tau_{E_2/K_v}((\alpha_2^\sigma)^{\psi(\sigma)}/\alpha_2).$$

Thus $c_1 = nc_2$ in $H^1(K_v, E[2^k])$, and n is odd, so c_1 and c_2 generate the same subgroup. Thus $\text{image}(\kappa_{E_1/K_v}) = \text{image}(\kappa_{E_2/K_v})$ in Case 4.

Case 5: $v \mid p$, $p > 2$, E_1 and E_2 have good reduction at v, and the isomorphism $E_1[p^k] \cong E_2[p^k]$ extends to an isomorphism $\mathcal{E}_1[p^k] \cong \mathcal{E}_2[p^k]$. In this case Proposition 5.8 shows that $\text{image}(\kappa_{E_1/K_v}) = \text{image}(\kappa_{E_2/K_v})$. More generally, suppose $\chi \in \mathcal{X}(K_v)$, and let L be the quadratic extension of K_v cut out by χ. Then Proposition 5.8 shows that $\text{image}(\kappa_{E_1/L}) = \text{image}(\kappa_{E_2/L})$, and this isomorphism preserves the natural action of $\text{Gal}(L/K_v)$. Let σ denote the nontrivial element of $\text{Gal}(L/K_v)$, and for every $\mathbf{Z}_p[\text{Gal}(L/K_v)]$-module M, define $M^- := \{m \in M : m^\sigma = -m\}$. Since $p > 2$, one verifies easily using the Hochschild-Serre spectral sequence that for $i = 1, 2$ we have

$$E_i^\chi(K_v)/p^k E_i^\chi(K_v) = (E_i(L)/p^k E_i(L))^-, \quad H^1(K_v, E_i^\chi[p^k]) = H^1(L, E_i[p^k])^-,$$
$$\text{image}(\kappa_{E_i^\chi/K_v}) = \text{image}(\kappa_{E_i/L})^-$$

and we conclude that $\text{image}(\kappa_{E_1^\chi/K_v}) = \text{image}(\kappa_{E_2^\chi/K_v})$.

Thus $\text{image}(\kappa_{E_1^\chi/K_v}) = \text{image}(\kappa_{E_2^\chi/K_v})$ in (4) for every v and every χ, and we conclude that E_1 and E_2 are p-Selmer companions over K.

If F is a finite extension of K, then E_1 and E_2 satisfy the hypotheses of Theorem 6.1 over F as well. Applying the proof above with F in place of K shows that E_1 and E_2 are p-Selmer companions over F. $\qquad\square$

Proof of Theorem 3.1. Theorem 3.1 is identical to Theorem 6.1 except for the second part of hypothesis (iv). Suppose $k = 1$, $\mathfrak{p} \mid p$, E_1, E_2 have good reduction at $\mathfrak{p}$, and the ramification $e(\mathfrak{p}/p) < p - 1$ (so in particular $p > 2$). By Raynaud's theorem [10, §3.5.5], the group scheme $\mathcal{E}_i[p]$ is determined by the Galois module $E_i[p]$. Hence in this case the isomorphism $E_1[p] \cong E_2[p]$ necessarily extends to an isomorphism $\mathcal{E}_1[p] \cong \mathcal{E}_2[p]$. Thus if hypotheses (i) and (iv) of Theorem 3.1 are satisfied, then hypothesis (iv) of Theorem 6.1 is satisfied. In this way Theorem 3.1 follows from Theorem 6.1. $\qquad\square$

7. Additional questions and remarks

In this section we discuss some related questions, including partial converses to Theorem 3.1. Fix a number field K.

7.1. The number of companions.

Proposition 7.1. *Fix an elliptic curve E_1 over K, and a prime power $p^k > 2$. There are only finitely many elliptic curves E_2/K (up to isomorphism) satisfying hypotheses (i) and (ii) of Theorem 3.1.*

Proof. Let

$$\Sigma = \{\text{primes } \mathfrak{l} \text{ of } K : E_1 \text{ has bad reduction at } \mathfrak{l}\} \cup \{\mathfrak{l} : \mathfrak{l} \mid p\}.$$

Suppose that E_1 and E_2 satisfy (i) and (ii) of Theorem 3.1, and $\mathfrak{l}$ is a prime of K not dividing p. If E_2 has potentially multiplicative reduction at $\mathfrak{l}$, then $\mathfrak{l} \in S_2 = S_1 \subset \Sigma$. If E_2 has additive, potentially good reduction at $\mathfrak{l}$, then so does E_1 by Lemma 5.3, so $\mathfrak{l} \in \Sigma$. Thus E_2 has good reduction at all primes outside of Σ. By the "Shafarevich Conjecture" (proved by Faltings), there are only finitely many such elliptic curves E_2/K. $\square$

7.2. Selmer parity companions.

Definition 7.2. We will say that two elliptic curves E_1, E_2 over K are *p-Selmer parity companions* if for every quadratic character χ of K we have

$$\dim_{\mathbf{F}_p} \mathrm{Sel}_p(E_1^\chi/K) \equiv \dim_{\mathbf{F}_p} \mathrm{Sel}_p(E_2^\chi/K) \pmod 2.$$

Remark 7.3. Clearly, if E_1 and E_2 are *p*-Selmer companions, then they are also *p*-Selmer parity companions.

Recall that the Shafarevich-Tate conjecture asserts that the Shafarevich-Tate groups of all elliptic curves over K are finite.

Proposition 7.4. *Suppose that the Shafarevich-Tate conjecture holds. Then E_1 and E_2 are p-Selmer parity companions for one prime p if and only if they are p-Selmer parity companions for every prime p.*

Proof. If the Shafarevich-Tate group of an elliptic curve E over K is finite, then the Cassels pairing shows that $\dim_{\mathbf{F}_p} \mathrm{Sel}_p(E/K) \equiv \mathrm{rank}(E(K)) \pmod 2$, so in particular $\dim_{\mathbf{F}_p} \mathrm{Sel}_p(E/K)$ is independent of p. The proposition follows easily. $\square$

Remark 7.5. Proposition 7.4 shows that (at least conjecturally) *p*-Selmer parity companions need not have the same Galois action on their *p*-torsion points. For example, the curves $E_1 = 1026N1$ and $E_2 = 1026O1$ over $\mathbf{Q}$ of the Introduction are 7-Selmer companions, so they are 7-Selmer parity companions, so conjecturally they are *p*-Selmer parity companions for every prime *p*. In fact, we will show unconditionally in Example 7.7 below that E_1 and E_2 are 2-Selmer parity companions. However, the discriminants of E_1 and E_2 are $-2^{17} \cdot 3^5 \cdot 19$ and $-2^3 \cdot 3^9 \cdot 19^2$, respectively, so $\mathbf{Q}(E_1[2]) \neq \mathbf{Q}(E_2[2])$.

We can use the methods and results of [6] to determine when two elliptic curves are 2-Selmer parity companions.

For every elliptic curve E/K and place v of K, let $\omega_{E,v} : \mathcal{X}(K_v) \to \{\pm 1\}$ be the map (of sets, not in general a homomorphism) given by [6, Definition 6.1].

Theorem 7.6. *Suppose E_1, E_2 are elliptic curves over K, and Σ is a finite set of places of K containing all places above 2 and ∞, and all primes where either E_1 or E_2 has bad reduction. Then E_1 and E_2 are 2-Selmer parity companions if and only if $\dim_{\mathbf{F}_2} \mathrm{Sel}_2(E_1/K) \equiv \dim_{\mathbf{F}_2} \mathrm{Sel}_2(E_2/K) \pmod 2$ and $\omega_{E_1,v} = \omega_{E_2,v}$ for every $v \in \Sigma$.*

Proof. This follows directly from [6, Proposition 6.2]. $\square$

Example 7.7. We will use Theorem 7.6 to show that the curves $E_1 = 1026N1$ and $E_2 = 1026O1$ over $\mathbf{Q}$ of the Introduction are 2-Selmer parity companions. Let $\Sigma = \{\infty, 2, 3, 19\}$. We will use the calculations of the proof of [6, Proposition 6.9] to check that $\omega_{E_1,v} = \omega_{E_2,v}$ for every $v \in \Sigma$.

Case 1 of the proof of [6, Proposition 6.9] shows that $\omega_{E_i,\infty}(\chi) = 1$ if and only if χ is the trivial character.

If $\ell = 2$ or 19, then both E_1 and E_2 have split multiplicative reduction at ℓ, so Case 2 of the proof of [6, Proposition 6.9] shows that $\omega_{E_i,\ell}(\chi) = 1$ if and only if χ is the trivial character.

The Kodaira type of the reduction of E_1 (resp., E_2) modulo 3 is IV (resp., IV*). Therefore Case 5 of the proof of [6, Proposition 6.9] shows that $\omega_{E_1,3}(\chi) = \chi(\Delta_1)$, where Δ_i is the discriminant of E_i. Since $\Delta_1/\Delta_2 = 2^{14} \cdot 3^{-4} \cdot 19^{-1}$, and 19 is a square in $\mathbf{Q}_3$, it follows that $\omega_{E_1,3} = \omega_{E_2,3}$.

Further, one can compute that $\mathrm{Sel}_2(E_1/\mathbf{Q}) = \mathrm{Sel}_2(E_2/\mathbf{Q}) = 0$, so by Theorem 7.6 we conclude that E_1 and E_2 are 2-Selmer parity companions.

The next corollary comes close to showing that hypothesis (ii) of Theorem 3.1 is a necessary condition.

Corollary 7.8. *Suppose E_1 and E_2 are 2-Selmer parity companions, and $\mathfrak{l}$ is a prime of K not dividing 2. Then:*

(i) *E_1 has split multiplicative reduction at $\mathfrak{l}$ if and only if E_2 does,*
(ii) *E_1 has potentially multiplicative reduction at $\mathfrak{l}$ if and only if E_2 does.*

In particular if S_i is the set of primes where E_i has potentially multiplicative reduction as in Theorem 3.1, and $\Sigma_2 := \{\mathfrak{l} : \mathfrak{l} \mid 2\}$, then $S_1 \cup \Sigma_2 = S_2 \cup \Sigma_2$.

Proof. By Theorem 7.6, we have $\omega_{E_1,\mathfrak{l}} = \omega_{E_2,\mathfrak{l}}$. Both assertions now follow directly from [6, Proposition 6.9]. $\square$

Corollary 7.9. *Suppose E_1 and E_2 are 2-Selmer parity companions, and $E_1[4] \cong E_2[4]$ as G_K-modules. If $\mathfrak{l}$ is a prime of K not dividing 2, then E_1 has good (resp., additive, resp., multiplicative) reduction at $\mathfrak{l}$ if and only if E_2 does.*

Proof. Combining Lemma 5.3 and Corollary 7.8, we get that

- E_1 has good reduction at $\mathfrak{l}$ if and only if E_2 does,
- E_1 has additive, potentially good reduction at $\mathfrak{l}$ if and only if E_2 does,
- E_1 has potentially multiplicative reduction at $\mathfrak{l}$ if and only if E_2 does.

In the last case, Lemma 5.7 shows that E_1 and E_2 have the same splitting character over $K_\mathfrak{l}$, so E_1 has multiplicative reduction at $\mathfrak{l}$ if and only if E_2 does. This completes the proof. $\square$

7.3. **Selmer near-companions.**

Definition 7.10. We will say that two elliptic curves E_1, E_2 over K are *n-Selmer near-companions* if there is a constant $C = C(E_1, E_2, K)$ such that for every $\chi \in \mathcal{X}(K)$ there is an abelian group A_χ and homomorphisms $\mathrm{Sel}_n(E_1^\chi/K) \to A_\chi$ and $\mathrm{Sel}_n(E_2^\chi/K) \to A_\chi$ with kernel and cokernel of order at most C.

Note that E_1 and E_2 are n-Selmer companions if and only if Definition 7.10 is satisfied with $C = 1$.

Theorem 7.11. *Suppose E_1 and E_2 are elliptic curves over K. Let $m = p^{k+1}$ if $p \leq 3$, and $m = p^k$ if $p > 3$. Suppose further that there is a G_K-isomorphism $E_1[m] \cong E_2[m]$. Then E_1 and E_2 are p^k-Selmer near-companions.*

Proof. If E is an elliptic curve over K and Σ is a finite set of places of K, define

$$\mathrm{Sel}_{p^k}^{\Sigma}(E/K) := \ker\big(H^1(K, E[p^k]) \longrightarrow \bigoplus_{v \notin \Sigma} H^1(K_v, E[p^k])/\mathrm{image}(\kappa_{E/K_v})\big).$$

Then the definitions yield an exact sequence

$$(5) \quad 0 \longrightarrow \mathrm{Sel}_{p^k}(E/K) \longrightarrow \mathrm{Sel}_{p^k}^{\Sigma}(E/K) \longrightarrow \bigoplus_{v \in \Sigma} H^1(K_v, E[p^k])/\mathrm{image}(\kappa_{E/K_v}).$$

Now let Σ be the finite set of places of K dividing $n\Delta_1\Delta_2\infty$, where Δ_i is the discriminant of E_i. Using the given G_K-isomorphism to identify $E_1[p^k]$ with $E_2[p^k]$, Cases 2 and 3 of the proof of Theorem 6.1 show that if $v \notin \Sigma$, then $\mathrm{image}(\kappa_{E_1^\chi/K_v}) = \mathrm{image}(\kappa_{E_2^\chi/K_v})$ for every $\chi \in \mathcal{X}(K)$. Therefore $\mathrm{Sel}_{p^k}^{\Sigma}(E_1^\chi/K) = \mathrm{Sel}_{p^k}^{\Sigma}(E_2^\chi/K)$ inside $H^1(K, E_1[p^k]) = H^2(K, E[p^k])$, and we define A_χ to be this common group. Now if we let

$$C := \prod_{v \in \Sigma} \sup_{\chi \in \mathcal{X}(K_v)} |H^1(K_v, E_1^\chi[p^k])|$$

then (5) applied to E_1^χ and E_2^χ shows that E_1 and E_2 are p^k-Selmer near-companions. $\square$

Example 7.12. Take $K = \mathbf{Q}$ and $p^k = 2$, and let E_1 and E_2 be the elliptic curves $26A1$ and $598B1$ in [2]:

$$E_1 : y^2 + xy + y = x^3 - 5x - 8,$$
$$E_2 : y^2 + xy = x^3 - x^2 + 44x + 496.$$

The method of §A.1 below allows us to verify that there is a $G_{\mathbf{Q}}$-isomorphism $E_1[4] \cong E_2[4]$, so E_1 and E_2 are 2-Selmer near-companions by Theorem 7.11. Using a little more care, we can show that $\mathrm{Sel}_{p^k}^{\Sigma}(E_1^\chi/K) = \mathrm{Sel}_{p^k}^{\Sigma}(E_2^\chi/K)$ for every χ, with $\Sigma = \{23\}$. In the exact sequences (5) for E_1^χ and E_2^χ with this Σ, the right hand group has order $[E_1(\mathbf{Q}_{23}) : 2E_1(\mathbf{Q}_{23})] = 2$, independent of χ. It follows that for every quadratic character χ of $G_{\mathbf{Q}}$ we have

$$\dim_{\mathbf{F}_2} \mathrm{Sel}_2(E_1^\chi/\mathbf{Q}) - \dim_{\mathbf{F}_2} \mathrm{Sel}_2(E_2^\chi/\mathbf{Q}) \in \{-1, 0, 1\}.$$

All three values $-1, 0, 1$ occur. (Note that E_1 has good reduction at 23 and E_2 has multiplicative reduction, so hypothesis (ii) of Theorem 3.1 does not hold.)

APPENDIX A. CHECKING THAT $E_1[m] \cong E_2[m]$

Suppose E_1 and E_2 are elliptic curves over K. In this appendix we discuss two methods for verifying that there is a G_K-isomorphism $E_1[m] \cong E_2[m]$.

A.1. **Universal families.** If $m = 3$, 4, or 5 then [11, Theorem 4.1], [13, Theorem 4.1], and [11, Theorem 5.1], respectively, give explicit models

$$(6) \qquad \tilde{E}_t : y^2 = x^3 + a(t)x + b(t), \qquad a(t), b(t) \in K[t]$$

for the family of all elliptic curves E/K with $E[m]$ symplectically G_K-isomorphic to $E_1[m]$. (A symplectic isomorphism is one that preserves the Weil pairings.) In other words, there is a symplectic G_K-isomorphism $E_1[m] \cong E_2[m]$ if and only if there is an $s \in K$ such that the specialization $\tilde{E}_s$ is isomorphic over K to E_2.

To test this, we can simply compute the j-invariant of $\tilde{E}_t$

$$J(t) := 1728 \frac{a(t)^3}{4a(t)^3 + 27b(t)^2} \in K(t),$$

and then find (the finite set of) all zeros in K of the rational function $J(t) - j(E_2)$. For each zero $s \in K$, we have that $\tilde{E}_s$ is an elliptic curve over K with $j(\tilde{E}_s) = J(s) = j(E_2)$, and it is then a simple matter to test whether $\tilde{E}_s$ is isomorphic to E_2 over K. If it is, then $E_1[m]$ is (symplectically) G_K-isomorphic to $E_2[m]$. But if for every zero $s \in K$ of $J(t) - j(E_2)$ we have that $\tilde{E}_s$ is not isomorphic over K to E_2, then there is no symplectic G_K-isomorphism $E_1[m] \cong E_2[m]$.

In the case $m = 4$, one can show that there is a G_K-isomorphism $E_1[4] \cong E_1^{\Delta}[4]$ that is *not* symplectic, where E_1^{Δ} is the quadratic twist of E_1 by its discriminant Δ. It follows that if $E_2[4]$ is G_K-isomorphic to $E_1[4]$, then $E_2[4]$ is symplectically G_K-isomorphic either to $E_1[4]$ or to $E_1^{\Delta}[4]$, so we can use the argument above to test for all G_K-isomorphisms, not just the symplectic ones.

Proof of Proposition 4.6. Let E_1 and E_2 be as in Example 4.5. Then E_1 has the short Weierstrass model $y^2 = x^3 - 5616x - 494208$. Applying [11, Theorem 5.1] with $a = -5616$ and $b = -494208$ gives an explicit model of the elliptic curve $\tilde{E}_t/\mathbf{Q}(t)$ of (6). If we set $J(t) := j(\tilde{E}_t)$ then we compute that the only rational zero of $J(t) - j(E_2)$ is $-9/22$. Specializing $\tilde{E}_t$ at $t = -9/22$ gives a Weierstrass model of an elliptic curve isomorphic over $\mathbf{Q}$ to E_2. Thus there is a (symplectic) $G_{\mathbf{Q}}$-isomorphism $E_1[5] \cong E_2[5]$. $\qquad\square$

A.2. **Constructing an explicit isomorphism.** Suppose $m = p^n$. Let $f_i(x) \in K[x]$ be the polynomial of degree $d := (p^{2n} - p^{2n-2})/2$ whose roots are the x-coordinates of the points in $E_i[p^n] - E_i[p^{n-1}]$. Suppose further that f_1 and f_2 are irreducible; this is equivalent to requiring that G_K acts transitively on $E_i[p^n]/\{\pm 1\}$ for $i = 1, 2$.

Fix a root α_1 of f_1. Suppose that f_2 also has at least one root $\alpha_2 \in K(\alpha_1)$. (If $E_1[p^n] \cong E_2[p^n]$, then, this will necessarily be the case.) Fix such a root and call it α_2. Then $K(\alpha_2) = K(\alpha_1)$, so there is a unique polynomial $\phi(x) \in K[x]$ of degree less than d such that $\phi(\alpha_1) = \alpha_2$. Since α_1 is a root of $f_2 \circ \phi$, we have that f_1 divides $f_2 \circ \phi$, so ϕ maps all roots of f_1 to roots of f_2.

Fix a prime $\mathfrak{l}$ of K such that E_1 and E_2 have good reduction at $\mathfrak{l}$, and $\mathfrak{l}$ splits completely in $K(E_1[p^n])/K$. Fix a prime of $K(E_1[p^n])$ above $\mathfrak{l}$. If $\mathbf{F}_{\mathfrak{l}}$ denotes the residue field of $\mathfrak{l}$, this choice gives us a reduction isomorphism

$$\pi : E_1(\bar{K})[p^n] \xrightarrow{\sim} E_1(\mathbf{F}_{\mathfrak{l}})[p^n].$$

Note that ϕ also maps all roots of f_1 in $\mathbf{F}_{\mathfrak{l}}$ to roots of f_2 in $\mathbf{F}_l$.

Fix a basis P_1, P_2 of $E_1(\mathbf{F}_{\mathfrak{l}})[p^n]$. Let $Q_1, Q_2 \in E_1(\mathbf{F}_{\mathfrak{l}})[p^n]$ be points such that $x(Q_i) = \phi(x(P_i))$. Define a group homomorphism $\varphi : E_1(\mathbf{F}_{\mathfrak{l}})[p^n] \to E_2(\mathbf{F}_{\mathfrak{l}})[p^n]$ by

$$\varphi(aP_1 + bP_2) = aQ_1 + bQ_2 \quad \text{for } a, b \in \mathbf{Z}/p^n\mathbf{Z}.$$

Using the reduction isomorphism π, we can lift φ to a group homomorphism $E_1[p^n] \to E_2[p^n]$, which we also denote by φ. Consider the diagram

(7)

$$
\begin{array}{ccc}
E_1[p^n] - E_1[p^{n-1}] & \xrightarrow{\quad\varphi\quad} & E_2[p^n] - E_2[p^{n-1}] \\
\pi \downarrow \cong & & \pi \downarrow \cong \\
E_1(\mathbf{F}_{\mathfrak{l}})[p^n] - E_1(\mathbf{F}_{\mathfrak{l}})[p^{n-1}] & \xrightarrow{\quad\varphi\quad} & E_2(\mathbf{F}_{\mathfrak{l}})[p^n] - E_2(\mathbf{F}_{\mathfrak{l}})[p^{n-1}] \\
\downarrow & & \downarrow \\
(E_1(\mathbf{F}_{\mathfrak{l}})[p^n] - E_1(\mathbf{F}_{\mathfrak{l}})[p^{n-1}])/\{\pm 1\} & \xrightarrow{[\phi]} & (E_2(\mathbf{F}_{\mathfrak{l}})[p^n] - E_2(\mathbf{F}_{\mathfrak{l}})[p^{n-1}])/\{\pm 1\} \\
\pi^{-1} \downarrow \cong & & \pi^{-1} \downarrow \cong \\
(E_1[p^n] - E_1[p^{n-1}])/\{\pm 1\} & \xrightarrow{[\phi]} & (E_2[p^n] - E_2[p^{n-1}])/\{\pm 1\}
\end{array}
$$

where $[\phi]$ denotes the map induced by applying the polynomial ϕ to the x-coordinates. The upper and lower squares are commutative, with vertical isomorphisms.

Let S be the set of places of K where at least one of $E_1[p^n], E_2[p^n]$ is ramified, and $\mathcal{X}(K,S) \subset \mathcal{X}(K)$ the (finite) subgroup of characters unramified outside of S.

Lemma A.1. *Suppose that the center square of* (7) *is commutative. Then:*

    (i) *φ is a group isomorphism,*

    (ii) *there is a quadratic character $\psi \in \mathcal{X}(K,S)$ such that $\varphi(P^\sigma) = \psi(\sigma)\varphi(P)^\sigma$ for every $P \in E_1[p^n]$ and $\sigma \in G_K$.*

Proof. If the center square of (7) is commutative, then the entire diagram is commutative. Since $\phi \in K[x]$, the bottom map $[\phi]$ is G_K-equivariant. Since f_2 is irreducible, G_K acts transitively on $(E_2[p^n] - E_2[p^{n-1}])/\{\pm 1\}$. Hence the bottom map $[\phi]$ is surjective, so the top map ϕ is surjective, and (i) follows.

It also follows from the commutativity of (7) and the G_K-equivariance of $[\phi]$ that

(8) $$\varphi(P^\sigma) = \pm\varphi(P)^\sigma \quad \text{for every } P \in E_1[p^n] \text{ and } \sigma \in G_K.$$

For every $\sigma \in G_K$, the sets

$$\{P \in E_1[p^n] : \varphi(P^\sigma) = \varphi(P)^\sigma\}, \quad \{P \in E_1[p^n] : \varphi(P^\sigma) = -\varphi(P)^\sigma\}$$

are subgroups of $E[p^n]$. It follows from (8) that the union of these two subgroups is $E[p^n]$, and therefore one of them must be all of $E[p^n]$. Thus for every σ we can define $\psi(\sigma) = \pm 1$ so that $\varphi(P^\sigma) = \psi(\sigma)\varphi(P)^\sigma$ for every $P \in E_1[p^n]$. One sees easily that $\psi \in \mathcal{X}(K)$, and ψ is necessarily unramified outside S, so $\psi \in \mathcal{X}(K,S)$. $\qquad\square$

Suppose now that the center square of (7) is commutative. Let $\psi \in \mathcal{X}(K,S)$ be the character of Lemma A.1(ii). Then by Lemma A.1, φ induces an isomorphism $E_1[p^n] \xrightarrow{\sim} E_2^\psi[p^n]$, where E_2^ψ is the quadratic twist of E_2 by ψ. We would like to verify that ψ must be the trivial character.

Fix a basis $\chi_1, \ldots, \chi_t$ of the $\mathbf{F}_2$-vector space $\mathcal{X}(K,S)$. Suppose that for every i, $1 \le i \le t$, we can find a prime $\mathfrak{q}_i$ of K, $\mathfrak{q}_i \notin S$, such that

- $\chi_i(\mathfrak{q}_i) = -1$, $\chi_j(\mathfrak{q}_i) = 1$ if $j \neq i$,
- the traces of Frobenius of $\mathfrak{q}_i$ on $E_1[p^n]$ and $E_2[p^n]$ satisfy

$$\text{Trace}(\text{Frob}_{\mathfrak{q}_i}|E_1[p^n]) \neq -\text{Trace}(\text{Frob}_{\mathfrak{q}_i}|E_2[p^n]).$$

Choose a nontrivial character $\chi = \prod_i \chi_i^{a_i} \in \mathcal{X}(K, S)$, $a_i \in \{0, 1\}$. If $a_i \neq 0$ for some i, then by our choice of $\mathfrak{q}_i$ we have $\text{Trace}(\text{Frob}_{\mathfrak{q}_i} | E_1[p^n]) \neq \text{Trace}(\text{Frob}_{\mathfrak{q}_i} | E_2^\chi[p^n])$, so $E_1[p^n] \not\cong E_2^\chi[p^n]$. Hence ψ must be the trivial character.

All of the steps above can be handled by either Sage [16] or PARI/GP [14]. Computing the polynomial $\phi(x)$ is the only significantly time-consuming step. Finding a prime $\mathfrak{l}$, checking the commutativity of (7), and finding primes $\mathfrak{q}_i$ with appropriate traces of Frobenius is very quick. (Note that the points $Q_1, Q_2 \in E_1(\mathbf{F}_{\mathfrak{l}})[p^n]$ are only defined up to multiplication by ± 1. If the first choice does not lead to commutativity in (7), then replacing Q_1 by $-Q_1$ may still work.)

Proof of Proposition 4.4. Let E_1 and E_2 be as in Example 4.3, both of conductor $1242 = 2 \cdot 3^3 \cdot 23$, and $m = 8$. PARI/GP computes the polynomial $\phi(x)$ of degree $(8^2 - 4^2)/2 = 24$ in less than a minute on a modern desktop computer. We take $\mathfrak{l} := 19681$, and

$$P_1 := (731, 4673), P_2 := (3074, 1044) \in E_1(\mathbf{F}_{19681}).$$

Then P_1, P_2 generate $E_1[8]$, and we compute that $\phi(731) \equiv 10530 \pmod{19681}$ and $\phi(3074) \equiv 17962 \pmod{19681}$. We define φ as above using the points

$$Q_1 = (10530, 9277), Q_2 = (17962, 16270) \in E_2(\mathbf{F}_{19681}),$$

and we check directly that the center square of (7) commutes. Therefore Lemma A.1 shows that $\varphi : E_1[8] \to E_2^\psi[8]$ is a $G_\mathbf{Q}$-equivariant isomorphism, where $\psi \in \mathcal{X}(\mathbf{Q}, \{\infty, 2, 3, 23\})$. The group $\mathcal{X}(\mathbf{Q}, \{\infty, 2, 3, 23\})$ is generated by the characters $\chi_{-1}, \chi_2, \chi_{-3}, \chi_{-23}$, where χ_d is the quadratic character of $\mathbf{Q}(\sqrt{d})/\mathbf{Q}$. We find the following data, where $a_q(E_i)$ is the trace of Frobenius Frob_q.

q	$\chi_{-1}(q)$	$\chi_2(q)$	$\chi_{-3}(q)$	$\chi_{-23}(q)$	$a_q(E_1) \pmod 8$	$a_q(E_2) \pmod 8$
31	-1	1	1	1	2	2
349	1	-1	1	1	2	2
233	1	1	-1	1	2	2
241	1	1	1	-1	6	6

The argument above shows that ψ is the trivial character, so $\varphi : E_1[8] \to E_2[8]$ is a $G_\mathbf{Q}$-equivariant isomorphism. $\square$

References

[1] Bloch, S., Kato, K.: *L*-functions and Tamagawa numbers of motives. In: The Grothendieck Festschrift (Vol. I), P. Cartier, et al., eds., *Prog. in Math.* **86**, Boston: Birkhäuser (1990) 333–400.

[2] J.E. Cremona, Algorithms for modular elliptic curves. Cambridge University Press, Cambridge (1992).

[3] J.W.S. Cassels, Arithmetic of curves of genus 1. VIII. *J. Reine Angew. Math.* **217** (1965) 180-199.

[4] D.R. Heath-Brown, The size of Selmer groups for the congruent number problem II. *Invent. Math.* **118** (1994) 331–370.

[5] Z. Klagsbrun, Selmer ranks of quadratic twists of elliptic curves. Ph.D. Thesis, UC Irvine (2011).

[6] Z. Klagsbrun, B. Mazur, K. Rubin, Selmer ranks of quadratic twists of elliptic curves, to appear.

[7] A. Kraus, J. Oesterlé, Sur une question de B. Mazur. *Math. Ann.* **293** (1992), 259-275.

[8] B. Mazur, Rational points of abelian varieties with values in towers of number fields. *Invent. Math.* **18** (1972) 183–266.

[9] B. Poonen, E. Rains, *Random maximal isotropic subspaces and Selmer groups. J. Amer. Math. Soc.* **25** (2012) 245–269.

[10] M. Raynaud, Schémas en groupes de type $(p, \ldots, p)$, *Bull. Soc. Math. France* **102** (1974), 241–280.

[11] K. Rubin, A. Silverberg, Families of elliptic curves with constant mod p representations. In: Elliptic Curves, Modular Forms, & Fermat's Last Theorem (Hong Kong, 1993), J. Coates and S. T. Yau, eds. International Press, Cambridge (1995) 148-161.

[12] J-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259–331.

[13] A. Silverberg, Explicit families of elliptic curves with prescribed mod N representations. In: Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, New York (1997) 447-461.

[14] PARI/GP, version `2.4.3`. The PARI Group (2011) `http://pari.math.u-bordeaux.fr`.

[15] J. Silverman, The arithmetic of elliptic curves, *Grad. Texts in Math.* **106**, Springer, New York, 1986.

[16] Sage Mathematics Software, Version `4.7.2`. The Sage Development Team (2011) `http://www.sagemath.org`.

[17] H.P.F. Swinnerton-Dyer, The effect of twisting on the 2-Selmer group. *Math. Proc. Cambridge Philos. Soc.* **145** (2008) 513–526.

[18] J. Tate, Algorithm for determining the type of a singular fiber in an elliptic pencil. In: Modular functions of one variable (IV), *Lecture Notes in Math.* **476**, New York: Springer-Verlag (1975) 33–52.

[19] J. Tate, A review of non-archimedean elliptic functions. In: Elliptic Curves, Modular Forms, & Fermat's Last Theorem (Hong Kong, 1993), J. Coates and S. T. Yau, eds. International Press, Cambridge (1995) 162–184.

DEPARTMENT OF MATHEMATICS, HARVARD UNIVERSITY, CAMBRIDGE, MA 02138, USA
E-mail address: `mazur@math.harvard.edu`

DEPARTMENT OF MATHEMATICS, UC IRVINE, IRVINE, CA 92697, USA
E-mail address: `krubin@math.uci.edu`