EXPLICIT ISOGENY DESCENT ON ELLIPTIC CURVES

ROBERT L. MILLER AND MICHAEL STOLL

Abstract. In this note, we consider an ℓ-isogeny descent on a pair of elliptic curves over $\mathbb{Q}$. We assume that $\ell > 3$ is a prime. The main result expresses the relevant Selmer groups as kernels of simple explicit maps between finite-dimensional $\mathbb{F}_\ell$-vector spaces defined in terms of the splitting fields of the kernels of the two isogenies. We give examples of proving the ℓ-part of the Birch and Swinnerton-Dyer conjectural formula for certain curves of small conductor.

1. Introduction

Let $E/\mathbb{Q}$ be an elliptic curve. Then it is known [24] that the group $E(\mathbb{Q})$ of rational points on E is a finitely generated abelian group. Its finite torsion subgroup is easily determined, but so far there is no method known that can provably determine the rank r of $E(\mathbb{Q})$ for an arbitrary given curve E. There is another abelian group associated to $E/\mathbb{Q}$, the *Shafarevich-Tate group* $Ш(\mathbb{Q}, E)$. It is conjectured to be finite for all elliptic curves; however, this is only known for curves of analytic rank 0 or 1.

The *analytic rank* is the order of vanishing of the L-series $L(E, s)$ associated to E at the point $s = 1$. The conjecture of Birch and Swinnerton-Dyer states that the analytic rank equals the rank, and moreover gives a relation between the leading term of the Taylor expansion of $L(E, s)$ at $s = 1$ and various local and global data associated to E, including the order of $Ш(\mathbb{Q}, E)$. Kolyvagin [20] has shown that the first part of the conjecture holds when the analytic rank is at most 1, that in this case $Ш(\mathbb{Q}, E)$ is finite, and the second part of the conjecture holds up to a rational factor involving only primes in a certain finite set (depending on E).

The two groups $E(\mathbb{Q})$ and $Ш(\mathbb{Q}, E)$ are related by objects that can (in principle) be computed: for each $\ell \geq 1$, there is a finite computable group $\mathrm{Sel}^{(\ell)}(\mathbb{Q}, E)$, the *$\ell$-Selmer group* of E, and an exact sequence of abelian groups

$$0 \longrightarrow E(\mathbb{Q})/\ell E(\mathbb{Q}) \longrightarrow \mathrm{Sel}^{(\ell)}(\mathbb{Q}, E) \longrightarrow Ш(\mathbb{Q}, E)[\ell] \longrightarrow 0\,.$$

If ℓ is a prime number, then all groups involved are $\mathbb{F}_\ell$-vector spaces, and we obtain the relation

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}^{(\ell)}(\mathbb{Q}, E) = r + \dim_{\mathbb{F}_\ell} E(\mathbb{Q})[\ell] + \dim_{\mathbb{F}_\ell} Ш(\mathbb{Q}, E)[\ell]\,.$$

Date: 23 January, 2011.

This can be used to obtain upper bounds for r on the one hand, but also leads to information on $\text{Ш}(\mathbb{Q}, E)$ when r is known (for example when the analytic rank is at most 1). In particular, if

$$\dim_{\mathbb{F}_\ell} \operatorname{Sel}^{(\ell)}(\mathbb{Q}, E) = r + \dim_{\mathbb{F}_\ell} E(\mathbb{Q})[\ell]\,,$$

then it follows that the ℓ-primary part of $\text{Ш}(\mathbb{Q}, E)$ is trivial. The computation of the ℓ-Selmer group is referred to as an *ℓ-descent on E*. How this can be done is discussed in some detail in [31]. The computation involves obtaining information on class groups and unit groups in number fields of degree up to ℓ^2-1, so this often will be infeasible when $\ell \geq 5$. Even when there is a rational ℓ-isogeny $\phi : E \to E'$, one usually has to deal with a field of degree $\ell^2 - \ell$. In this case, an alternative approach is to compute Selmer groups associated to ϕ and the dual isogeny ϕ'. The information obtained still provides upper bounds for the rank r and the ℓ-torsion of $\text{Ш}(\mathbb{Q}, E)$ (and $\text{Ш}(\mathbb{Q}, E')$), but the latter may fail to be sharp.

There is already a considerable amount of work in the literature in specific cases. In the following, we try to give an overview, which we do not claim to be exhaustive. Cremona uses 2-isogeny descents in [5] for a large number of curves, to determine the ranks of the Mordell-Weil groups $E(\mathbb{Q})$. In addition, online notes [7] describe how to extend these descents to full 2-descents, in cases where the information gained is inconclusive. Frey [18] uses 2-isogeny descent for curves of the form $y^2 = x^3 \pm p^3$ for primes $p > 3$ to determine their ranks in terms of congruence conditions on p. The general theory of 2-isogeny descents is presented in detail in [34, Chapter X].

Selmer [32, 33] and later Cassels [3] studied cubic twists of the cubic Fermat curve and considered among other things 3-isogenies and the multiplication by $\sqrt{-3}$ map for these curves. Satgé [28] considers the 3-isogeny from the curve given by $y^2 = x^3 + A$ to its twist $y^2 = x^3 - 27A$, for arbitrary A. He determines the Selmer group of this isogeny over $\mathbb{Q}$ by identifying it with a certain subgroup of $\operatorname{Hom}(G_{\mathbb{Q}(\sqrt{A})}, \mathbb{Z}/3\mathbb{Z})$. Jeechul Woo in his Ph.D. thesis [38] works out the theory and formulae for 3-isogeny descent in the presence of a rational 3-torsion point. Nekovář considers quadratic twists of the Fermat curve in [25] and computes the Selmer groups of rational 3-isogenies. Quer [27] uses the connection between 3-isogeny Selmer groups and class groups of quadratic fields to exhibit quadratic imaginary fields of 3-rank 6, based on elliptic curves of the form $y^2 = x^3 + k$ with rank 12. Top [36] demonstrates that the technique Quer uses applies to any elliptic curve admitting a rational 3-isogeny. DeLong [9] finds a formula for the dimension of the Selmer groups of these 3-isogenies which also relates the 3-ranks of the associated quadratic fields. Elkies and Rogers [12] use explicit formulas for 3-isogeny descents to construct elliptic curves of the form $x^3 + y^3 = k$ of ranks 8 through 11 over $\mathbb{Q}$.

Goins [19] uses 4-isogenies on the way to performing full 4-descents on the family $y^2 + xy + ay = x^3 + ax^2$ where $\sqrt{-a} \in \mathbb{Q}^*$. Flynn and Grattoni [16] consider isogenies coming from rational points of prime power order and exhibit an element of the Shafarevich-Tate group of order 13. Their PARI programs are available at [17].

Beaver computes Selmer groups for isogenies of degree 5 in [1] and uses an explicit formula for the Cassels-Tate pairing to find nontrivial elements of the Shafarevich-Tate group of order 5. Fisher gives general results regarding descents over rational isogenies of degree $\ell = 5$ and $\ell = 7$ in [13, 14], which also include tables of many specific cases.

Cremona, Fisher, O'Neil, Simon and Stoll [8] work out the general theory for full n-descents. Schaefer relates in [29] Selmer groups for isogenies of abelian varieties over number fields to class groups. In [30] he realizes the connecting homomorphism in Galois cohomology as evaluation of a certain function called the descent map (see Section 2 below) on divisors. With Stoll he explains in [31] how to do a descent for any isogeny of odd prime power degree ℓ^e. One important result, which is also used here, is that the set of bad primes can be reduced to those above ℓ and those with the property that one of the corresponding Tamagawa numbers is divisible by ℓ.

In this note, we will expand on [31] and show how such an ℓ-isogeny descent can be performed with only little explicit computation. Our main result is given in Theorem 11. It expresses the relevant Selmer groups as kernels of simle explicit maps between finite-dimensional $\mathbb{F}_\ell$ vector spaces. The maps and spaces are defined in terms of the splitting fields of the kernels of the two isogenies involved. See Section 3 below for an explanation of the underlying idea. Our result makes the computation of the Selmer group sizes very easy and straight-forward. This can be used to obtain bounds on the rank and/or the size of the ℓ-torsion subgroup of the Shafarevich-Tate groups of the two curves involved. The result takes a particularly simple form when the kernel of ϕ is generated by a rational point, see Corollary 16.

We have used the results to finish off the verification of the full Birch and Swinnerton-Dyer conjecture for a number of elliptic curves of conductor up to 5000. For a more precise statement of this result, see Theorem 20.

2. Generalities

Let $\ell > 3$ be a prime, and let E be an elliptic curve over $\mathbb{Q}$ such that E has a rational ℓ-isogeny. We remark that everything we do in this paper still works for $\ell = 3$, under the condition that E and E' have no special fibers of type IV or IV*. For simplicity, we do not discuss this case in more detail. Note that a full 3-descent as described in [8] is usually feasible (and an implementation is available in MAGMA, for example), so for practical purposes, it is of particular interest to be able to deal with the case $\ell > 3$.

Let $\phi : E \to E'$ be the isogeny, and let $\phi' : E' \to E$ be the dual isogeny. Vélu [37] gives explicit formulae for ϕ and E' in terms of E. (Note that the model given for E' may not be minimal.) Our reference for the following will be [31].

We have an exact sequence of Galois modules

$$0 \longrightarrow E'[\phi'] \longrightarrow E' \xrightarrow{\phi'} E \longrightarrow 0\,. \tag{2.1}$$

The *ϕ'-Selmer group* $\mathrm{Sel}^{(\phi')}(\mathbb{Q}, E')$ sits in the Galois cohomology group $H^1(\mathbb{Q}, E'[\phi'])$; it is defined to be the kernel of the diagonal map in the following diagram whose (exact) rows are obtained by taking Galois cohomology of (2.1) over $\mathbb{Q}$ and over all completions $\mathbb{Q}_v$, respectively.

$$\begin{tikzcd}
E(\mathbb{Q}) \arrow[r, "\delta"] \arrow[d] & H^1(\mathbb{Q}, E'[\phi']) \arrow[r] \arrow[d] \arrow[dr] & H^1(\mathbb{Q}, E') \arrow[d] \\
\prod_v E(\mathbb{Q}_v) \arrow[r, "\delta"] & \prod_v H^1(\mathbb{Q}_v, E'[\phi']) \arrow[r] & \prod_v H^1(\mathbb{Q}_v, E')
\end{tikzcd}$$

The *Shafarevich-Tate group* $\text{Ш}(\mathbb{Q}, E')$ is the kernel of the right-most vertical map in the diagram. This leads to the exact sequence

$$0 \longrightarrow E(\mathbb{Q})/\phi'(E'(\mathbb{Q})) \xrightarrow{\delta} \mathrm{Sel}^{(\phi')}(\mathbb{Q}, E') \longrightarrow \text{Ш}(\mathbb{Q}, E')[\phi'] \longrightarrow 0\,.$$

By the usual yoga (see [31, p. 1222]), we find that

$$H^1(\mathbb{Q}, E'[\phi']) \cong \bigl(K^\times/(K^\times)^\ell\bigr)^{(1)}\ ,$$

where K is the field of definition of any nontrivial point P in the kernel $E[\phi]$, and the superscript (1) denotes the subgroup on which the automorphism induced by $P \mapsto aP$ acts as $z \mapsto z^a$ (for $a \in \mathbb{F}_\ell^\times$ such that aP is in the same Galois orbit as P). If we define[1]

$$\begin{aligned} K(S,\ell) &= \{\alpha(K^\times)^\ell : \ell \mid v_{\mathfrak{p}}(\alpha) \text{ for all primes } \mathfrak{p} \text{ of } K \text{ not above some } p \in S\} \\ &\subset \frac{K^\times}{(K^\times)^\ell}\,, \end{aligned}$$

then the image of the Selmer group is contained in $K(S,\ell)^{(1)}$, where S contains ℓ and the primes p such that ℓ divides one of the Tamagawa numbers $c_p(E)$ or $c_p(E')$ (see [31, Prop. 3.2]). Note that if $E(\mathbb{Q})[\phi] \neq 0$, then we have that $K = \mathbb{Q}$ and $K(S,\ell)^{(1)} = \mathbb{Q}(S,\ell)$.

[1] There is a variant of this definition that requires $K(\sqrt[\ell]{\alpha})/K$ to be unramfied outside primes above primes in S. This does not make a difference when $\ell \in S$. For our purposes, the definition given here is more convenient. Note that it will be used later with sets S possibly not containing ℓ.

We fix our notations by requiring that $E[\phi] \subset E(\mathbb{R})$ and $E'[\phi'] \cap E'(\mathbb{R}) = 0$. This puts a definite order on the pair (E, E').

Let $F \in K(E)$ be the *descent map*, i.e., F has a zero of order ℓ at P and a pole of order ℓ at the origin O of E, and is normalized such that in terms of the local parameter $t = y/x$ at O (we fix a globally minimal Weierstrass equation for E), we have

$$F(t) = t^{-\ell}(1 + tf(t)),$$

for some power series $f(t)$ over K. Then the connecting homomorphism δ in the sequence above can be identified with

$$F : E(\mathbb{Q}) \longrightarrow K(S,\ell)^{(1)},$$

where we set $F(O) = 1$ and $F(P) = 1/F(-P)$ (if $P \in E(\mathbb{Q})$). We let $K_p = K \otimes_{\mathbb{Q}} \mathbb{Q}_p$, then there is a canonical homomorphism $r_p : K^\times/(K^\times)^\ell \to K_p^\times/(K_p^\times)^\ell$. The function F induces a map $F_p : E(\mathbb{Q}_p) \to K_p^\times/(K_p^\times)^\ell$.

We then have

$$\text{Sel}^{(\phi')}(\mathbb{Q}, E') = \{\xi \in K(S,\ell)^{(1)} : r_p(\xi) \in F_p(E(\mathbb{Q}_p)) \text{ for all } p \in S\} \tag{2.2}$$

as a subgroup of $K(S,\ell)^{(1)}$.

In the following, we want to make the expression on the right hand side of equation (2.2) as explicit as possible.

3. The basic idea

We begin with a definition that is needed below.

Definition 1. For S a finite set of primes and K a number field, let

$$K(S,\ell)^* = \prod_{p\in S} \frac{\mathcal{O}_{K,p}^\times}{(\mathcal{O}_{K,p}^\times)^\ell},$$

where $\mathcal{O}_{K,p} = \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is the p-adic completion of the ring of integers of K. If S and S' are finite disjoint sets of primes, then there is an obvious canonical map

$$K(S,\ell) \longrightarrow K(S',\ell)^*.$$

(Note that for $p \notin S$, an element of $K(S,\ell)$ always has a representative that is a p-adic unit.)

According to equation (2.2) above, we need to find the subgroup of $K(S,\ell)^{(1)}$ consisting of elements satisfying certain local conditions at the primes $p \in S$. This will be made fairly easy if these local conditions are of a simple nature. The simplest possible cases certainly occur when the 'local image' $F_p(E(\mathbb{Q}_p))$ is either trivial or the full local group $H_p = \bigl(K_p^\times/(K_p^\times)\bigr)^{(1)}$. Another easy situation is when the local image is exactly the part U_p of the local group that comes from p-adic units, since in that case, we can just drop p from S.

Lemma 2. *We now assume that for each $p \in S$, we are in one of the three cases mentioned above, and we set*

$$S_1 = \{p \in S : F_p(E(\mathbb{Q}_p)) = H_p\} \quad \textit{and} \quad S_2 = \{p \in S : F_p(E(\mathbb{Q}_p)) = 0\}\,.$$

Then

$$\operatorname{Sel}^{(\phi')}(\mathbb{Q}, E') = \ker\bigl(\alpha : K(S_1, \ell)^{(1)} \to K(S_2, \ell)^*\bigr)\,.$$

Here α is the canonical map from Definition 1.

Proof. First we show that the Selmer group is contained in $K(S_1, \ell)^{(1)}$. This means that for all $p \in S \setminus S_2$, the local image is contained in U_p. But for all these primes, we have by assumption that the image is either trivial or equals U_p, so the condition is satisfied.

Now we check that the elements in the kernel of α are exactly those that satisfy the local conditions at all $p \in S$. If $p \in S \setminus (S_1 \cup S_2)$, then the local image equals U_p, and this condition is already taken care of since $p \notin S_1$. If $p \in S_1$, then the local image is all of H_p, and therefore there is no condition. Finally, if $p \in S_2$, then the local image is trivial, which means that the Selmer group elements are represented by elements of $K(S_1, \ell)$ that are ℓth powers in K_p. Since $p \notin S_1$, we can always find a representative that is a unit in K_p; then the condition says that the image in $\mathcal{O}_{K,p}^\times/(\mathcal{O}_{K,p}^\times)^\ell$ is trivial. Since

$$\ker \alpha = \bigcap_{p \in S_2} \ker\Bigl(K(S_1, \ell)^{(1)} \to \frac{\mathcal{O}_{K,p}^\times}{(\mathcal{O}_{K,p}^\times)^\ell}\Bigr)\,,$$

the claim follows. □

We denote by K', F', F'_p, H'_p, U'_p etc. the objects corresponding to K, F, F_p, H_p, U_p etc. for the dual isogeny. Then it is a fact that there is a perfect pairing

$$H_p \times H'_p \longrightarrow \frac{\frac{1}{\ell}\mathbb{Z}}{\mathbb{Z}} \cong \mathbb{F}_\ell$$

(induced by cup product and the Weil pairing on H^1's) such that the images of F_p and F'_p are exact annihilators of each other. (See [23, Cor. I.2.3 and I.3.4]; the last statement follows from the compatibility of the two pairings.) In particular, $\operatorname{im}(F_p) = 0$ is equivalent to $\operatorname{im}(F'_p) = H'_p$, and $\operatorname{im}(F_p) = H_p$ is equivalent to $\operatorname{im}(F'_p) = 0$. In addition, we find that the $\mathbb{F}_\ell$-dimensions satisfy

$$\dim H_p = \dim H'_p = \dim \operatorname{im}(F_p) + \dim \operatorname{im}(F'_p)\,.$$

If $p \neq \ell$, then by Lemma 3.8 in [29], we have

$$\#\frac{E(\mathbb{Q}_p)}{\phi'(E'(\mathbb{Q}_p))} = \#\operatorname{im}(F_p) = \frac{c_p(E)}{c_p(E')}\#E'(\mathbb{Q}_p)[\phi']$$

and an analogous relation for ϕ. If $p = \ell$, then the last expression has to be multiplied by $\ell^{v_\ell(\gamma')}$, where $(\phi')^*(\omega_E) = \gamma'\omega_{E'}$ and ω_E, $\omega_{E'}$ are the differentials associated to a minimal Weierstrass model. This prompts the following definition.

Definition 3. We set $w = v_\ell(\gamma')$.

We define γ by $\phi^*(\omega_{E'}) = \gamma\omega_E$, then $\gamma\gamma' = \ell$, and so we have $v_\ell(\gamma) = 1 - w$. We obtain

$$\dim \operatorname{im}(F_p) + \dim \operatorname{im}(F'_p) = \dim E(\mathbb{Q}_p)[\phi] + \dim E'(\mathbb{Q}_p)[\phi'] + \begin{cases} 0 & \text{if } p \neq \ell, \\ 1 & \text{if } p = \ell. \end{cases}$$

We will need to determine w. This is done in the following lemma. We denote by $\Omega(E) = \int_{E(\mathbb{R})} |\omega_E|$ the real period of E. Recall that we had fixed E to be the curve with $E(\mathbb{R})[\phi] \neq 0$ (and therefore, we have $E'(\mathbb{R})[\phi'] = 0$).

Lemma 4. *We have $\Omega(E)/\Omega(E') = \ell^w$.*

Proof. Since $E'(\mathbb{R})[\phi'] = 0$, ϕ' is an isomorphism from $E'(\mathbb{R})$ to $E(\mathbb{R})$. Hence

$$|\gamma'|\Omega(E') = \int_{E'(\mathbb{R})} |\gamma'\omega_{E'}| = \int_{E'(\mathbb{R})} |(\phi')^*\omega_E| = \int_{E(\mathbb{R})} |\omega_E| = \Omega(E)\,.$$

We know that $\phi^*\omega_{E'}$ is an integral multiple of ω and that $\phi'^*\omega_E$ is an integral multiple of $\omega_{E'}$; also $(\phi' \circ \phi)^*\omega_E = \ell\omega_E$. Therefore, $|\gamma'| = 1$ (and $w = 0$) or $|\gamma'| = \ell$ (and $w = 1$), and the claim follows. □

Since we can easily compute the real periods using a system like MAGMA, Sage or PARI-gp, w can be determined for any given isogeny. In some cases, the periods are computed with respect to the given model, so it is important to use globally minimal models of the two curves to get correct results.

We will show below in Section 4 that when $p \in S$, but $p \neq \ell$, then we always have either trivial or full local image, and that the two cases are distinguished by looking at the quotient $c_p(E)/c_p(E')$. The only possible problem can therefore occur when $p = \ell$. If ℓ divides one of the Tamagawa numbers $c_\ell(E)$ or $c_\ell(E')$, then the result is the same as for $p \neq \ell$. Otherwise, we see by the above that the following holds.

Lemma 5. *Assume that $\ell \nmid c_\ell(E)c_\ell(E')$.*

(1) *If $E'(\mathbb{Q}_\ell)[\phi'] = 0$ and $w = 0$, then $\operatorname{im}(F_\ell) = 0$ and $\operatorname{im}(F'_\ell) = H'_\ell$.*
(2) *If $E(\mathbb{Q}_\ell)[\phi] = 0$ and $w = 1$, then $\operatorname{im}(F_\ell) = H_\ell$ and $\operatorname{im}(F'_\ell) = 0$.*

Since $\mathbb{Q}_\ell$ does not contain μ_ℓ, it is not possible that both $E(\mathbb{Q}_\ell)[\phi]$ and $E'(\mathbb{Q}_\ell)[\phi']$ are nontrivial. The cases that are left are therefore

- $E'(\mathbb{Q}_\ell)[\phi'] \neq 0$ and $w = 0$ and
- $E(\mathbb{Q}_\ell)[\phi] \neq 0$ and $w = 1$.

Then both local images at ℓ are one-dimensional subspaces of the two-dimensional space H_ℓ or H'_ℓ. It will turn out that $\operatorname{im}(F'_\ell) = U'_\ell$ in the first and $\operatorname{im}(F_\ell) = U_\ell$ in the second of the two cases. So we will be able to compute at least one of the two Selmer groups $\operatorname{Sel}^{(\phi')}(\mathbb{Q}, E')$ and $\operatorname{Sel}^{(\phi)}(\mathbb{Q}, E)$ easily. There is a formula due to Cassels that relates the sizes of these two groups, see Section 6 below. This allows us to deduce the size of the other Selmer group. Cassels' formula may also be useful when both Selmer groups can be computed by our methods, since one of the two number fields K and K' may be significantly easier to deal with (for example because it is of lower degree). We can then compute the easier group and deduce the size of the other one by Cassels' formula.

4. Tate Curves

We note that for all primes $\ell \neq p \in S$, we have that ℓ divides $c_p(E)$ or $c_p(E')$, and that our assumptions imply that if $\ell \mid c_p(E)c_p(E')$ for any prime p, then both curves must have split multiplicative reduction at p.

Our reference for the following is [35, § V.3], in particular Theorem V.3.1. If an elliptic curve E has split multiplicative reduction at p, then there is $q \in \mathbb{Q}_p^\times$ with $v(q) > 0$ such that $E(\mathbb{Q}_p) \cong \mathbb{Q}_p^\times / q^{\mathbb{Z}}$. The subgroup of points with nonsingular reduction is $E(\mathbb{Q}_p)^0 \cong \mathbb{Z}_p^\times$, and the kernel of reduction is $E(\mathbb{Q}_p)^1 \cong (1 + p\mathbb{Z}_p)$. Therefore we find that

$$E(\mathbb{Q}_p)^0 / E(\mathbb{Q}_p)^1 \cong \mathbb{Z}_p^\times / (1 + p\mathbb{Z}_p) \cong \mathbb{F}_p^\times$$

(as must be the case for split multiplicative reduction) and that the component group is

$$\Phi_p = E(\mathbb{Q}_p)/E(\mathbb{Q}_p)^0 \cong \mathbb{Z}/v_p(q)\mathbb{Z}$$

where the isomorphism is induced by the valuation on $\mathbb{Q}_p^\times$. In particular, the Tamagawa number is $c_p(E) = v_p(q)$. This description of $E(L)$ carries over to all finite extensions L of $\mathbb{Q}_p$.

The ℓ-torsion subgroup of E is generated by μ_ℓ and q_ℓ, where $q_\ell^\ell = q$. So we have a point of order ℓ in $E(\mathbb{Q}_p)$ if either $\mu_\ell(\mathbb{Q}_p)$ is nontrivial, which means $p \equiv 1 \bmod \ell$, or if q is an ℓth power in $\mathbb{Q}_p$. In any case, the cyclic subgroups of order ℓ are μ_ℓ and the subgroups generated by some q_ℓ. The first kind of subgroup is always defined over $\mathbb{Q}_p$, the second kind only if $q_\ell \in \mathbb{Q}_p^\times$.

In the first case, the corresponding isogenous curve is $E'(\mathbb{Q}_p) \cong \mathbb{Q}_p^\times/(q^\ell)^{\mathbb{Z}}$, where the isogeny ϕ is induced by $z \mapsto z^\ell$. The dual isogeny ϕ' is induced by the identity map, which implies that $E(\mathbb{Q}_p)/\phi'(E'(\mathbb{Q}_p))$ is trivial. Note that we have $c_p(E') = v_p(q^\ell) = \ell v_p(q) = \ell c_p(E)$.

In the second case, the corresponding isogenous curve is $E'(\mathbb{Q}_p) \cong \mathbb{Q}_p^\times / q_\ell^{\mathbb{Z}}$, with isogeny ϕ induced by the identity. The dual isogeny ϕ' is induced by $z \mapsto z^\ell$, so we have $E(\mathbb{Q}_p)/\phi'(E'(\mathbb{Q}_p)) \cong \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^\ell$, and $c_p(E) = \ell c_p(E')$.

This leads to the following result.

Lemma 6. *Let p be a prime number.*

1. *If $c_p(E') = \ell c_p(E)$, then $\operatorname{im}(F_p) = 0$ and $\operatorname{im}(F'_p) = H'_p$.*
2. *If $c_p(E) = \ell c_p(E')$, then $\operatorname{im}(F_p) = H_p$ and $\operatorname{im}(F'_p) = 0$.*

If $\ell \neq p \in S$, then we are in one of these two cases.

Proof. We have seen in the discussion above that if the curves E and E' have split multiplicative reduction at p, then we are in one of the two cases. The claims on the local images follow from $\operatorname{im}(F_p) \cong E(\mathbb{Q}_p)/\phi'(E'(Q_p))$ and $\operatorname{im}(F'_p) \cong E'(\mathbb{Q}_p)/\phi(E(\mathbb{Q}_p))$ and the discussion preceding the statement of the lemma. If $\ell \neq p \in S$, then we must have split multiplicative reduction, therefore the first part applies. □

5. The local image at ℓ

As mentioned at the end of Section 3, the only cases that are left to consider are when $\ell \nmid c_\ell(E)c_\ell(E')$ and either

$$E'(\mathbb{Q}_\ell)[\phi'] \neq 0 \text{ and } w = 0\,, \qquad \text{or} \qquad E(\mathbb{Q}_\ell)[\phi] \neq 0 \text{ and } w = 1\,.$$

Note that the case $\ell \mid c_\ell(E)c_\ell(E')$ is taken care of by Lemma 6.
We now have the following result.

Lemma 7. *Assume that $\ell \nmid c_\ell(E)c_\ell(E')$.*

1. *If $E'(\mathbb{Q}_\ell)[\phi'] \neq 0$ and $w = 0$, then $\operatorname{im}(F'_\ell) = U'_\ell$ and $U_\ell = H_\ell$.*
2. *If $E(\mathbb{Q}_\ell)[\phi] \neq 0$ and $w = 1$, then $\operatorname{im}(F_\ell) = U_\ell$ and $U'_\ell = H'_\ell$.*

Proof. It suffices to prove the second assertion (say), the other one following by symmetry. We have $E(\mathbb{Q}_\ell)[\phi] \neq 0$, so that the kernel is generated by some $P \in E(\mathbb{Q}_\ell)$, and $H_\ell \cong \mathbb{Q}_\ell^\times/(\mathbb{Q}_\ell^\times)^\ell$. Since ℓ does not divide $c_\ell(E)$, the point P must have nonsingular reduction. In terms of a minimal integral Weierstrass equation, the descent map is then given by a polynomial $f(x) + g(x)y \in \mathbb{Z}_\ell[x, y]$ (with $\deg f \leq (\ell-1)/2$ and g monic of degree $(\ell-3)/2$). It follows that $F_\ell(Q)$ is a unit for all points $Q \in E(\mathbb{Q}_\ell)$ that do not reduce to the same point as the origin or P. For points in the same residue class as P, we use that $F_\ell(Q) = 1/F_\ell(-Q)$. For points in the kernel of reduction, we use that $F_\ell(Q) = F_\ell(Q-P)/F_\ell(-P)$. So we see that $\operatorname{im}(F_\ell) \subset U_\ell$. Since both sides are of dimension 1 (for $\operatorname{im}(F_\ell)$ we use the assumption $w = 1$ here), they must be equal. The statement on U'_ℓ follows by inspection of $H'_\ell \cong \big(\mathbb{Q}_\ell(\mu_\ell)^\times/(\mathbb{Q}_\ell(\mu_\ell)^\times)^\ell\big)^{(1)}$, which is generated by the images of the units ζ and $1 + \lambda^\ell$, where ζ is a primitive ℓth root of unity and $\lambda = 1 - \zeta$. □

6. Cassels' formula

We make the following definition.

Definition 8.

$$\Sigma_1 = \{p : c_p(E) = \ell c_p(E')\} \quad \text{and} \quad \Sigma_2 = \{p : c_p(E') = \ell c_p(E)\}\,.$$

Then $S = \Sigma_1 \cup \Sigma_2 \cup \{\ell\}$. Note that by the discussion in Section 4, $\Sigma_1 \cup \Sigma_2$ is exactly the set of primes where E (or equivalently, E') has split multiplicative reduction.

Cassels [4] has established a formula relating the sizes of $\mathrm{Sel}^{(\phi')}(\mathbb{Q}, E')$ and $\mathrm{Sel}^{(\phi)}(\mathbb{Q}, E)$. It reads as follows.

$$\frac{\#\,\mathrm{Sel}^{(\phi)}(\mathbb{Q}, E)}{\#\,\mathrm{Sel}^{(\phi')}(\mathbb{Q}, E')} = \frac{\#E(\mathbb{Q})[\phi]}{\#E'(\mathbb{Q})[\phi']}\,\frac{\Omega(E')}{\Omega(E)} \prod_q \frac{c_q(E')}{c_q(E)}$$

If $E(\mathbb{Q})[\phi] = 0$, then the right hand side is (by Lemma 4 and Definition 8) $\ell^{\#\Sigma_2 - \#\Sigma_1 - w}$. Otherwise it is $\ell^{\#\Sigma_2 - \#\Sigma_1 + 1 - w}$. (Note that $E'(\mathbb{Q})[\phi'] = 0$ according to our convention, since the nontrivial points in this kernel are not real.) In terms of $\mathbb{F}_\ell$-dimensions, this says the following.

Lemma 9.

$$\dim \mathrm{Sel}^{(\phi)}(\mathbb{Q}, E) + \#\Sigma_1 + w = \dim \mathrm{Sel}^{(\phi')}(\mathbb{Q}, E') + \#\Sigma_2 + \dim E(\mathbb{Q})[\phi]\,.$$

We can combine the information from both Selmer groups in the following way.

Lemma 10. *Let r denote the rank of $E(\mathbb{Q})$ (and $E'(\mathbb{Q})$). Then we have*

$$\begin{aligned} r + \dim Ш(\mathbb{Q}, E)[\ell] &\le r + \dim Ш(\mathbb{Q}, E')[\phi'] + \dim Ш(\mathbb{Q}, E)[\phi] \\ &= \dim \mathrm{Sel}^{(\phi')}(\mathbb{Q}, E') + \dim \mathrm{Sel}^{(\phi)}(\mathbb{Q}, E) - \dim E(\mathbb{Q})[\phi] \\ &= 2 \dim \mathrm{Sel}^{(\phi')}(\mathbb{Q}, E') - \#\Sigma_1 + \#\Sigma_2 - w \\ &= 2\big(\dim \mathrm{Sel}^{(\phi)}(\mathbb{Q}, E) - \dim E(\mathbb{Q})[\phi]\big) + \#\Sigma_1 - \#\Sigma_2 + w\,. \end{aligned}$$

The same bound holds for $\dim Ш(\mathbb{Q}, E')[\ell]$. In particular, we get an upper bound for $\dim Ш(\mathbb{Q}, E)[\ell]$ and $\dim Ш(\mathbb{Q}, E')[\ell]$ if we know the rank r and the size of one of the two Selmer groups.

Proof. Note first that we have $E(\mathbb{Q})[\phi] = E(\mathbb{Q})[\ell]$. The only nontrivial part of this statement is that $E(\mathbb{Q})[\ell] \neq 0$ implies $E(\mathbb{Q})[\phi] \neq 0$. But if there is a rational ℓ-torsion point on E and $E(\mathbb{Q})[\phi] = 0$, then $E[\phi] \cong \mu_\ell$ by the Weil pairing, contradicting our assumption that $E[\phi] \subset E(\mathbb{R})$.

We have the exact sequences

$$0 \longrightarrow \frac{E(\mathbb{Q})}{\phi'(E'(\mathbb{Q}))} \longrightarrow \mathrm{Sel}^{(\phi')}(\mathbb{Q},E') \longrightarrow Ш(\mathbb{Q},E')[\phi'] \longrightarrow 0$$
$$0 \longrightarrow \frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} \longrightarrow \mathrm{Sel}^{(\phi)}(\mathbb{Q},E) \longrightarrow Ш(\mathbb{Q},E)[\phi] \longrightarrow 0$$
$$0 = E'(\mathbb{Q})[\phi'] \longrightarrow \frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} \longrightarrow \frac{E(\mathbb{Q})}{\ell E(\mathbb{Q})} \longrightarrow \frac{E(\mathbb{Q})}{\phi'(E'(\mathbb{Q}))} \longrightarrow 0$$
$$0 \longrightarrow Ш(\mathbb{Q},E)[\phi] \longrightarrow Ш(\mathbb{Q},E)[\ell] \longrightarrow Ш(\mathbb{Q},E')[\phi'] \,,$$

and we know that

$$\dim E(\mathbb{Q})/\ell E(\mathbb{Q}) = r + \dim E(\mathbb{Q})[\ell] = r + \dim E(\mathbb{Q})[\phi] \,.$$

From this, we can deduce that

$$\begin{aligned} r + \dim Ш(\mathbb{Q},E)[\ell] &\le r + \dim Ш(\mathbb{Q},E')[\phi'] + \dim Ш(\mathbb{Q},E)[\phi] \\ &= \dim \frac{E(\mathbb{Q})}{\phi'(E'(\mathbb{Q}))} + \dim \frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} - \dim E(\mathbb{Q})[\phi] \\ &\qquad + \dim Ш(\mathbb{Q},E')[\phi'] + \dim Ш(\mathbb{Q},E)[\phi] \\ &= \dim \mathrm{Sel}^{(\phi')}(\mathbb{Q},E') + \dim \mathrm{Sel}^{(\phi)}(\mathbb{Q},E) - \dim E(\mathbb{Q})[\phi] \\ &= 2\dim \mathrm{Sel}^{(\phi')}(\mathbb{Q},E') - \#\Sigma_1 + \#\Sigma_2 - w \\ &= 2\dim \mathrm{Sel}^{(\phi)}(\mathbb{Q},E) + \#\Sigma_1 - \#\Sigma_2 + w - 2\dim E(\mathbb{Q})[\phi] \,. \end{aligned}$$

For the last two equalities, we use Lemma 9.
To get the bound for $\dim Ш(\mathbb{Q},E')[\ell]$, we use the exact sequence

$$0 \longrightarrow Ш(\mathbb{Q},E')[\phi'] \longrightarrow Ш(\mathbb{Q},E')[\ell] \longrightarrow Ш(\mathbb{Q},E)[\phi] \,.$$

□

If $Ш(\mathbb{Q},E)$ (or equivalently, $Ш(\mathbb{Q},E')$) is finite, then the dimensions of $Ш(\mathbb{Q},E')[\phi']$ and $Ш(\mathbb{Q},E)[\phi]$ are even, and it follows that the rank r has the same parity as $\#\Sigma_1 + \#\Sigma_2 + w$. Recall that $\Sigma_1 \cup \Sigma_2$ is the set of primes of split multiplicative reduction. By [11, Theorem 5] the root number $\varepsilon(E/\mathbb{Q})$ for E is given in terms of local Artin symbols and the local root number at ℓ:

$$\varepsilon(E/\mathbb{Q}) = (-1)^{1+\#\Sigma_1+\#\Sigma_2}\varepsilon(E/\mathbb{Q}_\ell) \prod_{p\neq\ell \text{ additive}} \left(-1, \mathbb{Q}_p(P)/\mathbb{Q}_p\right) \,.$$

Since the parity conjecture is known for Selmer groups [10, Theorem 1.4] and we are assuming $Ш(\mathbb{Q},E)$ is finite, this implies by the above observation that $(-1)^{\#\Sigma_1+\#\Sigma_2+w} = \varepsilon(E/\mathbb{Q})$. Combining this with the product formula for the Artin symbol and the fact that the Artin symbol is trivial for primes $p \neq \ell$ of semistable reduction (see [11] again) and at infinity according to our normalization, this gives us a formula for the local root number at ℓ:

$$\varepsilon(E/\mathbb{Q}_\ell) = (-1)^{1-w}(-1, \mathbb{Q}_\ell(P)/\mathbb{Q}_\ell)\,.$$

7. The main result

We apply Lemma 2 and obtain the following expressions for the Selmer groups

Theorem 11. *Let $\phi : E \to E'$ be an isogeny of prime degree $\ell > 3$ of elliptic curves over $\mathbb{Q}$, with dual isogeny $\phi' : E' \to E$, and assume that $\ker(\phi) \subset E(\mathbb{R})$. Let K and K' be the splitting fields of $E[\phi]$ and $E'[\phi']$, respectively, and define Σ_1, Σ_2 and w as in Definitions 8 and 4 above.*
If $\ell \nmid c_\ell(E)c_\ell(E')$, $w = 1$ and $E(\mathbb{Q}_\ell)[\phi] = 0$, then let $S_1 = \Sigma_1 \cup \{\ell\}$, else let $S_1 = \Sigma_1$.
If $\ell \nmid c_\ell(E)c_\ell(E')$, $w = 0$ and $E'(\mathbb{Q}_\ell)[\phi'] = 0$, then let $S_2 = \Sigma_2 \cup \{\ell\}$, else let $S_2 = \Sigma_2$.
Let

$$\alpha : K(S_1, \ell)^{(1)} \longrightarrow K(S_2, \ell)^* \quad \textit{and} \quad \beta : K'(S_2, \ell)^{(1)} \longrightarrow K'(S_1, \ell)^*$$

be the canonical maps.
Then $\mathrm{Sel}^{(\phi')}(\mathbb{Q}, E') = \ker\alpha$ unless $\ell \nmid c_\ell(E)c_\ell(E')$, $w = 0$ and $E'(\mathbb{Q}_\ell)[\phi'] \neq 0$, and $\mathrm{Sel}^{(\phi)}(\mathbb{Q}, E) = \ker\beta$ unless $\ell \nmid c_\ell(E)c_\ell(E')$, $w = 1$ and $E(\mathbb{Q}_\ell)[\phi] \neq 0$.
In the two excluded cases, we still have inclusions $\mathrm{Sel}^{(\phi')}(\mathbb{Q}, E') \subset \ker\alpha$ and $\mathrm{Sel}^{(\phi)}(\mathbb{Q}, E) \subset \ker\beta$, respectively.

We see that in each case, we obtain an explicit description for at least one of the two Selmer groups, which we can therefore determine fairly easily. We repeat the observation that this is sufficient to obtain a bound on the ℓ-torsion in Ш, compare Lemma 10.

Proof. We observe that in all relevant cases, the sets S_1 and S_2 correspond to those defined in Lemma 2. For primes $p \neq \ell$, this follows from Lemma 6, which also covers the case $p = \ell$ when $\ell \mid c_\ell(E)c_\ell(E')$. The remaining cases for $p = \ell$ are dealt with in Lemmas 5 and 7. In the cases where we do not claim equality, we fail to take into account the local condition at ℓ (which is of codimension 1 in $U_\ell = H_\ell$ or $U'_\ell = H'_\ell$). □

This provides some easy bounds on the Selmer groups. To make this more precise, we observe the following. We denote the class number of a number field K by h_K.

Lemma 12. *Let $K/\mathbb{Q}$ be a Galois extension with Galois group a subgroup of $\mathbb{F}_\ell^\times$. Let S be a set of primes. If $\ell \nmid h_K$, then*

$$\dim_{\mathbb{F}_\ell} K(S, \ell)^{(1)} = \#S' + 1$$

if K is totally real but $K \neq \mathbb{Q}$, or $K = \mathbb{Q}(\mu_\ell)$ with the standard action on μ_ℓ, and

$$\dim_{\mathbb{F}_\ell} K(S,\ell)^{(1)} = \#S'$$

otherwise. In each case $S' \subset S$ is the subset of primes that are totally split in K.

Proof. The case $K = \mathbb{Q}$ is clear. In general there is an exact sequence

$$0 \longrightarrow U_S/U_S^\ell \longrightarrow K(S,\ell) \longrightarrow \mathrm{Cl}_S(K)[\ell] \longrightarrow 0$$

where U_S is the group of S-units of K and $\mathrm{Cl}_S(K)$ is the S-class group. The assumption $\ell \nmid h_K$ implies that $\mathrm{Cl}_S(K)[\ell] = 0$. By the Dirichlet unit theorem, the group U_S has torsion-free rank $\#S_K + \#\Sigma_K - 1$, where S_K is the set of places of K above primes in S and Σ_K is the set of infinite places of K. Let $G \subset \mathbb{F}_\ell^\times$ be the (cyclic) Galois group of $K/\mathbb{Q}$. The representation of G on the $\mathbb{Q}$-vector space $U_S \otimes_{\mathbb{Z}} \mathbb{Q}$ must involve all characters of G of fixed order $n \mid \#G$ with the same multiplicity m_n. Let K_n be the the subfield of K of degree n. Then

$$\sum_{k \mid n} m_k \varphi(k) = \#S_{K_n} + \#\Sigma_{K_n} - 1$$

for all $n \mid \#G$. We then have $\dim K(S,\ell)^{(1)} = m_{\#G}$ (plus 1 if $\mu_\ell \subset K$ with the standard action). It can be checked that for $K \neq \mathbb{Q}$, the unique solution of this system of linear equations has $m_{\#G} = \#(S \cup \{\infty\})'$. This gives the result when $K \neq \mathbb{Q}(\mu_\ell)$, since then the S-unit group has no ℓ-torsion. For $K = \mathbb{Q}(\mu_\ell)$, we get an additional dimension from μ_ℓ when $\mathbb{F}_\ell^\times$ acts on it in the standard way. □

This applies to our situation in the following way.

Corollary 13. *In the situation of Theorem 11, the following assertions hold.*

(1) *If $\ell \nmid h_K$, then we have*

$$\dim K(S_1,\ell)^{(1)} = \#\Sigma_1 + 1 - \dim E(\mathbb{Q})[\phi]\,,$$

and therefore (writing $\text{Ш}[\ell]$ *for either* $\text{Ш}(\mathbb{Q},E)[\ell]$ *or* $\text{Ш}(\mathbb{Q},E')[\ell]$*)*

$$r + \dim \text{Ш}[\ell] \le \#\Sigma_1 + \#\Sigma_2 + 2(1 - \dim E(\mathbb{Q})[\phi]) - w\,.$$

(2) *If $\ell \nmid h_{K'}$, then we have*

$$\dim K'(S_2,\ell)^{(1)} = \#\Sigma_2 + \dim E(\mathbb{Q})[\phi]\,,$$

and therefore (writing $\text{Ш}[\ell]$ *for either* $\text{Ш}(\mathbb{Q},E)[\ell]$ *or* $\text{Ш}(\mathbb{Q},E')[\ell]$*)*

$$r + \dim \text{Ш}[\ell] \le \#\Sigma_1 + \#\Sigma_2 + w\,.$$

Proof.

(1) First note that for all $p \in \Sigma_1$, p is totally split in K (since by the discussion in Section 4, we have $E(\mathbb{Q}_p)[\phi] \neq 0$). If $S_1 \neq \Sigma_1$, then we have $E(\mathbb{Q}_\ell)[\phi] = 0$, and so the additional element ℓ of S_1 does not split completely. In the notation of Lemma 12, we thus have $S'_1 = \Sigma_1$. Also, K is totally real. The claim on the dimension of $K(S_1, \ell)^{(1)}$ follows. By Theorem 11, we have

$$\mathrm{Sel}^{(\phi')}(\mathbb{Q}, E') \subset \ker \alpha \subset K(S_1, \ell)^{(1)}\,,$$

so $\dim \mathrm{Sel}^{(\phi')}(\mathbb{Q}, E') \leq \#\Sigma_1 + 1 - \dim E(\mathbb{Q})[\phi]$. Lemma 10 now gives the estimate on $r + \dim Ш[\ell]$.

(2) In the same way as in part (1), we find that $S'_2 = \Sigma_2$. Now K' is not totally real, so Lemma 12 gives the dimension of $K'(S_2, \ell)^{(1)}$ as stated. The estimate then follows using Lemma 10 as in part (1).

□

Example 14. Let $\ell \geq 11$ be a prime, and let $\phi : E \to E'$ be an ℓ-isogeny of elliptic curves of conductor ℓ^2 (such that $E[\phi] \subset E(\mathbb{R})$ as usual). By work of Mazur [21] we have $\ell \leq 163$, and we find that in fact this applies to exactly the following curves E (with $\ell = 11, 19, 43, 67, 163$):

121a2, 121b1, 121c2, 361a1, 1849a1, 4489a1 and 26569a1.

(We use the labeling of the Cremona database [6].)

By [34, Proposition VII.4.1], the points in $E[\phi]$ and $E'[\phi']$ are defined over an abelian extension of $\mathbb{Q}$ of degree dividing $\ell - 1$ and only ramified at ℓ. By the Kronecker-Weber theorem [26, Theorem V.1.10], all such number fields are contained in $\mathbb{Q}(\mu_\ell)$. The field $K = \mathbb{Q}(P)$ for any $P \in E[\phi] \setminus \{0\}$ is totally real, hence contained in the maximal totally real subfield $\mathbb{Q}(\mu_\ell)^+$ of $\mathbb{Q}(\mu_\ell)$. By [2], for example, it is known that ℓ does not divide the class number of $\mathbb{Q}(\mu_\ell)^+$. Since $[\mathbb{Q}(\mu_\ell)^+ : K]$ divides $\ell - 1$ and hence is coprime to ℓ, this implies that $\ell \nmid h_K$. If ℓ is a regular prime, i.e., $\ell \neq 67$, then $\ell \nmid h_{K'}$ as well.

Since K is totally ramified at ℓ, we have that $[\mathbb{Q}_\ell(P) : \mathbb{Q}_\ell] = [K : \mathbb{Q}]$. Again by work of Mazur, E has no rational ℓ-torsion, implying that $K \neq \mathbb{Q}$. This implies $P \notin E(\mathbb{Q}_\ell)$, so $E(\mathbb{Q}_\ell)[\phi] = 0$. In the same way, we see that $E'(\mathbb{Q}_\ell)[\phi'] = 0$.

Since E has additive reduction at ℓ and good reduction everywhere else, we find $\Sigma_1 = \Sigma_2 = \emptyset$. If $\ell = 67$, we verify that $w = 1$. Corollary 13 now shows that

$$r + \dim_{\mathbb{F}_\ell} Ш(\mathbb{Q}, E)[\ell] \leq w\,.$$

We then verify that the rank is equal to w, and we see that

$$Ш(\mathbb{Q}, E)[\ell] = Ш(\mathbb{Q}, E')[\ell] = 0\,.$$

Example 15. Consider $E = 294a1$ with 7-isogenous curve $E' = 294a2$. We find $\Sigma_1 = \emptyset$, $\Sigma_2 = \{2\}$, $w = 1$, and the rank $r = 0$. We have $K = \mathbb{Q}(\mu_7)^+$ (the maximal real subfield of $\mathbb{Q}(\mu_7)$) and $K' = \mathbb{Q}(\sqrt{-7})$. Note that Corollary 13 gives a bound of 2 for the dimension of $Ш(\mathbb{Q}, E)[7]$. So we need to look more carefully to prove that there is no 7-torsion in $Ш(\mathbb{Q}, E)$. According to Theorem 11,

$$\mathrm{Sel}^{(\phi)}(\mathbb{Q}, E) = \ker\bigl(\beta : K'(\{2\}, 7)^{(1)} \to K'(\{7\}, 7)^*\bigr) .$$

The group $K'(\{2\}, 7)$ is generated by (the classes of) $1+\sqrt{-7}$ and $1-\sqrt{-7}$; the two are swapped by the nontrivial automorphism. Therefore $K'(\{2\}, 7)^{(1)}$ is generated by their quotient. We check that $\frac{1+\sqrt{-7}}{1-\sqrt{-7}}$ is not a seventh power in $\mathbb{Q}_7(\sqrt{-7})$. This implies that β is injective, hence $\mathrm{Sel}^{(\phi)}(\mathbb{Q}, E) = 0$. Lemma 10 then gives the bound

$$\dim Ш(\mathbb{Q}, E)[7] \le 0 + 0 - 1 + 1 = 0 .$$

8. When there is rational ℓ-torsion

Now we consider the case that $E(\mathbb{Q})[\phi] \neq 0$ in some detail. From Theorem 11 and Lemma 9, we obtain the following.

Corollary 16. *Assume that we have a nontrivial point P in $E(\mathbb{Q})[\phi]$. Let $S_1 = \Sigma_1$, and set $S_2 = \Sigma_2$ if $w = 1$ or $\ell \in \Sigma_1$, $S_2 = \Sigma_2 \cup \{\ell\}$ otherwise. Let*

$$\alpha : \mathbb{Q}(S_1, \ell) \longrightarrow \mathbb{Q}(S_2, \ell)^*$$

be the canonical map. Then $\mathrm{Sel}^{(\phi')}(\mathbb{Q}, E') = \ker\alpha$, and

$$r + \dim_{\mathbb{F}_\ell} Ш(\mathbb{Q}, E)[\ell] \le 2\dim_{\mathbb{F}_\ell} \ker\alpha - \#\Sigma_1 + \#\Sigma_2 - w \le \#\Sigma_1 + \#\Sigma_2 - w .$$

Proof. The result on the Selmer group follows from Theorem 11. (Note that $E(\mathbb{Q})[\phi] \neq 0$ implies $E(\mathbb{Q}_\ell)[\phi] \neq 0$ and therefore $E'(\mathbb{Q}_\ell)[\phi'] = 0$. Note also that $p \in \Sigma_2$ implies $p \equiv 1 \bmod \ell$, so that $\ell \notin \Sigma_2$.) The general bound of Lemma 10 and the trivial fact that $\dim \mathbb{Q}(S, \ell) = \#S$ then give the estimates. □

Note that (for $p \in \Sigma_2$, which implies that $p \equiv 1 \bmod \ell$)

$$\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^\ell \cong \mu_\ell(\mathbb{F}_p) \cong \mathbb{Z}/\ell\mathbb{Z} ,$$

where the first isomorphism is given by $x \mapsto x^{(p-1)/\ell} \bmod p$. The second isomorphism depends on the choice of a generator of $\mu_\ell(\mathbb{F}_p)$. Note also that

$$\mathbb{Z}_\ell^\times/(\mathbb{Z}_\ell^\times)^\ell \cong \mathbb{Z}/\ell\mathbb{Z}$$

via $x \mapsto (x^{\ell-1} - 1)/\ell \bmod \ell$.

Example 17. Consider curve $E = 50b1$, with 5-isogenous curve 50b3. Note that $E(\mathbb{Q})[5] \neq 0$. We have $\Sigma_1 = \{2\}$, $\Sigma_2 = \emptyset$, and $w = 1$. By Corollary 16, we have $\dim \mathrm{Sel}^{(\phi')}(\mathbb{Q}, E') = 1$. The rank is zero, so we find the bound

$$\dim Ш(50b1)[5] \le 2 - 1 + 0 - 1 = 0 .$$

Example 18. For curve $E = 174\mathrm{b}1$, which is 7-isogenous to 174b2, we have $E(\mathbb{Q})[7] \neq 0$ and find $\Sigma_1 = \{2, 3\}$, $\Sigma_2 = \{29\}$; also $w = 1$. The group $\mu_7(\mathbb{F}_{29})$ is generated by 16; we have

$$16^0 = 1,\ 16^1 = 16,\ 16^2 = 24,\ 16^3 = 7,\ 16^4 = 25,\ 16^5 = 23,\ 16^6 = 20\,.$$

If we identify $\mathbb{Z}_{29}^\times/(\mathbb{Z}_{29}^\times)^7 \cong \mu_7(\mathbb{F}_{29})$ with $\mathbb{Z}/7\mathbb{Z}$ by sending 16 to 1, then 2 is mapped to 1, and 3 is mapped to 5. So α is surjective and $\dim\ker\alpha = 1$. We obtain the bound (the rank is again zero)

$$\dim Ш(174\mathrm{b}1)[7] \le 2 - 2 + 1 - 1 = 0\,.$$

Example 19. We now consider $E = 294\mathrm{b}2$ with $E(\mathbb{Q})[7] \neq 0$ and 7-isogenous curve 294b1. We find $\Sigma_1 = \{2, 3\}$, $\Sigma_2 = \emptyset$, and $w = 0$. By Corollary 16, we have

$$\mathrm{Sel}^{(\phi')}(\mathbb{Q}, E') = \ker\bigl(\mathbb{Q}(\{2,3\}, 7) \to \mathbb{Z}_7^\times/(\mathbb{Z}_7^\times)^7 \cong \mathbb{Z}/7\mathbb{Z}\bigr)\,.$$

The map is given by $a \mapsto (a^6 - 1)/7 \pmod 7$. Since both 2 and 3 have nontrivial image, we have $\dim \mathrm{Sel}^{(\phi')}(\mathbb{Q}, E') = 1$, and (the rank is zero)

$$\dim Ш(294\mathrm{b}2)[7] \le 2 - 2 + 0 - 0 = 0\,.$$

9. Application to the Birch and Swinnerton-Dyer Conjecture

Theorem 20. *Let $\phi : E \to E'$ be an isogeny of degree ℓ of elliptic curves over $\mathbb{Q}$, and assume that the analytic rank of E is 0 or 1 and the conductor of E is less than 5000. If the ℓ-primary parts of $Ш(\mathbb{Q}, E)$ and $Ш(\mathbb{Q}, E')$ are predicted by the Birch and Swinnerton-Dyer conjecture to be trivial, then they are indeed trivial. This means that the conjecture holds up to a rational factor that is a unit at ℓ.*

Proof. By the results of [13] and [22], as well as calculations based on [15], the only remaining cases are the following pairs (E, ℓ): $(121\mathrm{b}1, 11)$, $(361\mathrm{a}1, 19)$, $(441\mathrm{d}1, 7)$, $(784\mathrm{h}1, 7)$, $(1849\mathrm{a}1, 43)$, $(3025\mathrm{a}1, 11)$, $(3136\mathrm{r}1, 7)$, $(4489\mathrm{a}1, 67)$.
Four of these cases can be found in Example 14, which shows that $Ш(\mathbb{Q}, E)[\ell] = 0$ for each case. This leaves the four cases $(441\mathrm{d}1, 7)$, $(784\mathrm{h}1, 7)$, $(3025\mathrm{a}1, 11)$ and $(3136\mathrm{r}1, 7)$. For all four curves we have that $\Sigma_1 = \Sigma_2 = \emptyset$ and $w = 1$. One can verify that $\ell \nmid h_K$ and $r = 1$ in each case and so by Corollary 13, we find that $Ш(\mathbb{Q}, E)[\ell] = Ш(\mathbb{Q}, E')[\ell] = 0$. □

The remaining cases where the analytic rank of E is at most 1 and the conductor is at most 5000 are

$$E \in \{570\mathrm{l}1,\ 870\mathrm{i}1,\ 1050\mathrm{o}1,\ 1938\mathrm{j}1,\ 1950\mathrm{y}1,\ 2370\mathrm{m}1,\ 2550\mathrm{be}1,\ 3270\mathrm{h}1\}$$

for $\ell = 5$ and $E \in \{546\mathrm{f}1,\ 858\mathrm{k}1,\ 1230\mathrm{k}1\}$ for $\ell = 7$. In these cases the Birch and Swinnerton-Dyer conjecture implies that

$$Ш(\mathbb{Q}, E)(\ell) = 0 \quad \text{but} \quad Ш(\mathbb{Q}, E')(\ell) = (\mathbb{Z}/\ell\mathbb{Z})^2\,.$$

In this situation an ℓ-isogeny descent shows that $Ш(\mathbb{Q},E')[\ell]=(\mathbb{Z}/\ell\mathbb{Z})^2$, as found in [13] or using the above methods. However this shows neither that

$$Ш(\mathbb{Q},E)[\ell]=0 \quad \text{nor that} \quad Ш(\mathbb{Q},E')(\ell)=Ш(\mathbb{Q},E')[\ell]\,.$$

These cases require a second descent over $\phi' : E' \to E$, a full ℓ-descent on E, or at the very least one must show that the elements of order ℓ in $Ш(\mathbb{Q},E')$ are not divisible by ℓ. This will be the subject of a forthcoming paper with Brendan Creutz.

References

[1] C. Beaver: 5-*torsion in the Shafarevich-Tate group of a family of elliptic curves,* J. Number Th. **82** (2000), 25–46.

[2] J. Buhler, R. Crandall, R. Ernvall, T. Metsänkylä: *Irregular primes and cyclotomic invariants to four million,* Math. Comp. **61** (1993), 151–153.

[3] J.W.S. Cassels: *Arithmetic on curves of genus 1. I. On a conjecture of Selmer,* J. reine angew. Math. **202** (1959), 52–99.

[4] J.W.S. Cassels: *Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer*, J. reine angew. Math. **217** (1965), 180–189.

[5] J.E. Cremona: *Algorithms for modular elliptic curves,* Second edition, Cambridge University Press, Cambridge, 2007.

[6] J.E. Cremona: Elliptic curves database, available online at `http://www.warwick.ac.uk/staff/J.E.Cremona/ftp/data/INDEX.html`

[7] J.E. Cremona: Online notes, available as item 26 at `http://www.warwick.ac.uk/staff/J.E.Cremona/papers`

[8] J.E. Cremona, T.A. Fisher, C. O'Neill, D. Simon, M. Stoll: *Explicit n-descent on elliptic curves, I. Algebra,* J. reine angew. Math. **615** (2008), 121–155; *II. Geometry,* J. reine angew. Math. **632** (2009), 63–84; *III. Algorithms,* in preparation.

[9] M. DeLong: *A formula for the Selmer group of a rational three-isogeny,* Acta Arith. **105** (2002), 119–131.

[10] T. Dokchitser, V. Dokchitser: *On the Birch-Swinnerton-Dyer quotients modulo squares,* Ann. Math. **172** (2010), 567–596.

[11] T. Dokchitser, V. Dokchitser: *Parity of ranks for elliptic curves with a cyclic isogeny,* J. Number Th. **128** (2008), 662–679.

[12] N. Elkies, N. Rogers: *Elliptic curves $x^3+y^3=k$ of high rank,* in: …(ANTS?) Springer Lect. Notes in Comp. Sci. **3076**, pp. 184–193, 2004.

[13] T.A. Fisher: *On* 5 *and* 7 *descents for elliptic curves,* Ph.D. thesis, University of Cambridge (2000).

[14] T.A. Fisher: *Some examples of* 5 *and* 7 *descent for elliptic curves over* $\mathbb{Q}$, J. Eur. Math. Soc. (JEMS) **3** (2001), 169–201.

[15] T.A. Fisher: *Finding rational points on elliptic curves using* 6-*descent and* 12-*descent,* J. Algebra **320** (2008), 853–884.

[16] E.V. Flynn, C. Grattoni: *Descent via isogeny on elliptic curves with large rational torsion subgroups,* J. Symb. Comp. **43** (2008), 293–303.

[17] E.V. Flynn, C. Grattoni: PARI programs, available at `http://people.maths.ox.ac.uk/flynn/genus2/flynngrattoni/`.

[18] G. Frey: *Der Rang der Lösungen von $Y^2=X^3\pm p^3$ über* $\mathbb{Q}$, Manuscr. Math. **48** (1984), 71–101.

[19] E.H. Goins: *Explicit descent via* 4*-isogeny on an elliptic curve,* `arXiv:math/0411215` (2004).

[20] V.A. Kolyvagin: *Finiteness of* $E(\mathbb{Q})$ *and* $Ш(E,\mathbb{Q})$ *for a subclass of Weil curves* (Russian), Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 3, 522–540, 670–671; translation in Math. USSR-Izv. **32** (1989), no. 3, 523–541.

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

[22] R.L. Miller: *Empirical evidence for the Birch and Swinnerton-Dyer conjecture,* Ph.D. thesis, University of Washington (2010).

[23] J.S. Milne: *Arithmetic duality theorems,* Perspectives in Mathematics, vol. 1, Academic Press, Orlando, Florida, 1986.

[24] L.J. Mordell: *On the rational solutions of the indeterminate equations of the 3rd and 4th degrees*, Proc. Camb. Phil. Soc. **21** (1922), 179–192.

[25] J. Nekovář: *Class number of quadratic fields and Shimura's correspondence,* Math. Ann. **287** (1990), 577–594.

[26] J. Neukirch: *Algebraische Zahlentheorie,* Springer-Verlag, Berlin Heidelberg, 1994.

[27] J. Quer: *Corps quadratiques de* 3*-rang* 6 *et courbes elliptiques de rang* 12*,* C. R. Acad. Sci. Paris (I) **305** (1987), 215–218.

[28] P. Satgé: *Groupes de Selmer et corps cubiques,* J. Number Th. **23** (1986), 294–317.

[29] E.F. Schaefer: *Class groups and Selmer groups,* J. Number Th. **56** (1996), no. 1, 79–114.

[30] E.F. Schaefer: *Computing a Selmer group of a Jacobian using functions on the curve,* Math. Ann. **310** (1998), 447–471.

[31] E.F. Schaefer, M. Stoll: *How to do a p-descent on an elliptic curve,* Trans. Amer. Math. Soc. **356** (2004), 1209–1231.

[32] E.S. Selmer: *The diophantine equation* $ax^3+by^3+cz^3=0$*,* Acta Math. (Stockh.) **85** (1951), 203–362.

[33] E.S. Selmer: *The diophantine equation* $ax^3+by^3+cz^3=0$*. Completion of the tables,* Acta Math. (Stockh.) **92** (1954), 191–197.

[34] J.H. Silverman: *The arithmetic of elliptic curves,* Springer Graduate Texts in Mathematics **106**, Springer-Verlag, New York Berlin Heidelberg Tokyo, 1986.

[35] J.H. Silverman: *Advanced topics in the arithmetic of elliptic curves,* Springer Graduate Texts in Mathematics **151**, Springer-Verlag, New York Berlin Heidelberg, 1994.

[36] J. Top: *Descent by* 3*-isogeny and* 3*-rank of quadratic fields,* Advances in number theory (Kingston, ON, 1991), 303–317, Oxford Sci. Publ., Oxford Univ. Press, New York, 1993.

[37] J. Vélu: *Isogénies entre courbes elliptiques,* C. R. Acad. Sci. Paris, Série A **273** (1971), 238–241.

[38] J. Woo: *Arithmetic of elliptic curves and surfaces: descents and quadratic sections,* Ph.D. thesis, Harvard University (2010).

Mathematics Institute, University of Warwick, Coventry CV4 7AL, U.K.
E-mail address: `rlm@rlmiller.org`

Mathematisches Institut, Universität Bayreuth, 95440 Bayreuth, Germany
E-mail address: `Michael.Stoll@uni-bayreuth.de`