5-Torsion in the Shafarevich–Tate Group of a Family of Elliptic Curves

Cheryl DeLorme Beaver

Sandia National Laboratories, Albuquerque, New Mexico 87185
E-mail: cbeaver@sandia.gov

Communicated by K. Rubin
Received August 14, 1998

We compute the \( \phi \)-Selmer group for a family of elliptic curves, where \( \phi \) is an isogeny of degree 5, then find a practical formula for the Cassels–Tate pairing on the \( \phi \)-Selmer groups and use it to show that a particular family of elliptic curves have non-trivial 5-torsion in their Shafarevich–Tate group.

1. INTRODUCTION

Let \( K \) be a number field, \( E/K \) an elliptic curve defined over \( K \), and \( E(K) \) the Mordell–Weil group of points on \( E \) with coordinates in \( K \). Denote by \( \text{III}(E/K) \) the Shafarevich–Tate group of \( E/K \). The Shafarevich–Tate group arises frequently in the study of elliptic curves although much about its size and structure remains mysterious. The group is believed to be finite and the conjecture of Birch and Swinnerton-Dyer asserts that its cardinality is a factor in the leading term of the \( L \)-series of the elliptic curve at \( s=1 \).

Kolyvagin [8] proved that \( E(\mathbb{Q}) \) and \( \text{III}(E/\mathbb{Q}) \) are both finite for a certain class of modular curves. Rubin [16] showed that if \( E \) is an elliptic curve defined over an imaginary quadratic field, \( K \), with complex multiplication by \( \mathcal{O}_K \), then \( L(E/K, 1) \neq 0 \), \( \text{III}(E/K) \) is finite. Although finiteness of the Shafarevich–Tate group has been proven in some cases, a general result is far from being achieved and we instead try to gather information about its cardinality. For example how large is the \( m \)-torsion subgroup? In the past, the 2- and 3-torsion in \( \text{III}(E/K) \) have been studied with the most success. Kramer [10] used a descent procedure to produce a family of elliptic curves with arbitrarily large 2-torsion in \( \text{III}(E/K) \); and Cassels [2] showed that the 3-torsion can be arbitrarily large by constructing certain quadratic twists of \( E \). Here we will give a method for finding non-trivial 5-torsion

Part of this research was done at MSRI under NSF Grant DMS-9701755.
elements in the Shafarevich–Tate group of a family of elliptic curves by using the Cassels–Tate pairing.

Main Results. Suppose that $\phi: E \to E'$ is an isogeny of elliptic curves of degree $m$. Denote by $S_d(E/K)$ the $d$-Selmer group of $E/K$ and by $\Sha_d(E/K)$ the $\phi$-torsion in the Shafarevich–Tate group of $E/K$. The Mordell–Weil group, Selmer group, and Shafarevich–Tate group are related by the following exact sequence

$$0 \to E'(K)/\phi E(K) \to S_d(E/K) \to \Sha_d(E/K) \to 0.$$ 

There is an alternating pairing on $\Sha(E/K)$, called the Cassels–Tate pairing, which is non-degenerate modulo the divisible subgroup. The Cassels–Tate pairing restricted to $S_d(E/K)$ lifts to a pairing on $S_d(E/K)$ which is trivial on elements coming from $E'(K)/\phi E(K)$ and which we will also call the Cassels–Tate pairing $\langle \cdot, \cdot \rangle: S_d(E/K) \times S_d(E/K) \to \mathbb{Q}/\mathbb{Z}$.

It is, in general, difficult to give a readily computable, practical formula for the pairing. However, under certain conditions, which hold for various families of curves, we are able to write the pairing down as a sum of local pairings which are easily computable. Since $\Sha_d$ is the quotient of $S_d$ by $(E'/\phi E)$, knowledge of the Selmer group and a formula for the pairing gives us a method by which we can hope to deduce information about the Shafarevich–Tate group. McCallum [11] has shown this idea to work in finding non-trivial $p$-torsion in the quotient of the Fermat curve $x^p + y^p = 1$, for $p$ satisfying certain conditions. His formula for computing the pairing involved finding a $p$-adic approximation for a certain function. Here, we apply his idea to a family of elliptic curves, but instead of the $p$-adic approximation, we find explicit formulas for the pairing in terms of local Hilbert norm residue symbols.

In particular, we consider elliptic curves, $E'$, whose 5-torsion is isomorphic over $\mathbb{Q}$ to $\mathbb{Z}/5 \mathbb{Z} \oplus \mu_5$. The following equation (see Rubin and Silverberg [15], and Klein [7, 6]) parametrizes this family of curves

$$y^2 = x^3 - \frac{u^{20} - 228u^{15} + 494u^{10} + 228u^5 + 1}{48} x + \frac{u^{30} + 522u^{25} - 10005u^{20} - 10005u^{10} - 522u^5 + 1}{864}. \quad (1)$$

Let $\hat{\phi}: E' \to E$ be the isogeny with kernel $\mathbb{Z}/5 \mathbb{Z}$. If $E'$ is given by (1), then $E'/(\mathbb{Z}/5 \mathbb{Z}) := E$ will denote the quotient of $E'$ by this unique subgroup of order 5 with trivial Galois action. For a family of these curves chosen
by defining $E'$ by Eq. (1) with values of $u \in \mathbb{Q}$ satisfying a certain divisibility condition at 5, we show that we can determine the $\phi$-Selmer group of $E'/\mathbb{Q}$ simply by looking at the primes, $v$, of split multiplicative reduction for $E'$ together with a certain number, $\lambda_v \in \mathbb{P}^1(F_5)$, associated to each such prime. The number $\lambda_v$ is related to the Tate parametrization of a certain 5-torsion point on $E'$ over the local field $\mathbb{Q}_v$. For a precise definition of $\lambda_v$, see Section 4.2. If $u$ is an integer and $v$ a prime, denote by $\text{ord}_v(u)$ the exact power of $v$ dividing $u$. Throughout, let

$$M = \{ \text{primes of bad reduction for } E' \}. \quad (2)$$

We state the main results of the paper next.

**Theorem 1.1.** Suppose that $E'$ can be given by (1) with $u \in \mathbb{Q}$, $\text{ord}_5(u) > 0$ and $E \cong E'/(\mathbb{Z}/5\mathbb{Z})$. Let $M$ be as in (2) and

$$M' = \{ v \in M \mid E' \text{ has split multiplicative reduction at } v \}$$

and

$$\Sigma = \{ v \in M' \mid v \equiv 1 \pmod{5} \text{ and } \lambda_v = \infty \}. $$

Denote by $U$ the subgroup of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^5$ generated modulo 5th powers by the primes in $M' - \Sigma$. Then there is an isomorphism

$$S_\phi(E/\mathbb{Q}) \cong \{ n \in U \mid n^{(v-1)/5} \equiv 1 \pmod{v} \forall v \in \Sigma \}. $$

For the family of curves under consideration, the Cassels–Tate pairing can be given in terms of a finite sum of local pairings on a subset of these primes of split multiplicative reduction. The local pairings can then be given in terms of the local Hilbert Norm Residue symbol raised to the power $\lambda_v$. In what follows, $\zeta$ is a certain 5th root of unity to be specified later (Section 4) and if $\epsilon$ and $\epsilon'$ are 5th roots of unity, then we’ll write $\text{Ind}_v \epsilon' = k$ if $\epsilon^k = \epsilon'$ for $k \in \frac{1}{5} \mathbb{Z}/\mathbb{Z}$.

**Theorem 1.2.** Suppose that $E'$ can be given by (1) with $u \in \mathbb{Q}$, $\text{ord}_5(u) > 0$ and $E \cong E'/(\mathbb{Z}/5\mathbb{Z})$. Let $M'$ be as in the Theorem 1.1 and

$$S = \{ v \in M' \mid v \equiv 1 \pmod{5} \}. $$

Then for $n, m \in S_\phi(E/\mathbb{Q})$, the Cassels–Tate pairing is given by

$$\langle n, m \rangle = \sum_{v \in S} \text{Ind}_v (n_v, m_v)^{-\lambda_v} \mod \mathbb{Z} $$
where $(\cdot, \cdot)$ is the local Hilbert norm residue symbol on $\mathbb{Q}_p^* / (\mathbb{Q}_p^*)^5$, and for $n \in \mathbb{Z}_p(E/\mathbb{Q})$, $n_v$ denotes the image of $n$ in $\mathbb{Q}_p^* / (\mathbb{Q}_p^*)^5$ under the map induced by the isomorphism of Theorem 1.1.

Since an element $n \in \mathbb{Z}_p(E/\mathbb{Q})$ maps to a non-trivial element of $\mathbb{Z}_p(E/\mathbb{Q})$ if $n$ is not in the kernel of the pairing, we can use the above information to find a sub-family of these curves with non-trivial 5-torsion in their Shafarevich–Tate group.

**Corollary 1.3.** Suppose that $E'$ can be given by (1) with $u \in \mathbb{Z}$, $\text{ord}_5(u) > 0$, $\text{ord}_{11}(u) = 0$, $u$ chosen so that $t = u^2 + u - 1$ is not divisible by any primes congruent to 1 modulo 5, and $\lambda_{11} \neq 0$. Let $E \approx E' / (\mathbb{Z}/5\mathbb{Z})$. Then $\mathbb{Z}_p(E/\mathbb{Q})$ contains a subgroup isomorphic to $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

2. BACKGROUND

**Notation.** If $K$ is a number field, denote by $M_K$ the complete set of non-equivalent valuations on $K$. Note that for $K = \mathbb{Q}$, $M_\mathbb{Q}$ is just the set of rational primes together with the “prime” at $\infty$. Denote by $K_v$ a completion of $K$ with respect to the metric induced by a prime $v$ and by $F_v$ the residue field. If $\phi: E \to E'$ is an isogeny of elliptic curves, denote by $E_\phi$ the kernel of $\phi$, and by $\hat{\phi}: E' \to E$ the dual isogeny. Define $H^1(K, A)$ to be the cohomology of the Galois module $A$ taken with respect to the absolute Galois group $\text{Gal}(K/K)$. If $\gamma$ is a cocycle in $H^1(K, A)$, then write $\gamma_v$ for the restriction of $\gamma$ to $\text{Gal}(K_v/K_v)$ in the local cohomology group $H^1(K_v, A)$. Finally, denote by $e_\phi$ the Weil pairing.

For an elliptic curve, $E$, defined over a number field $K$, the Shafarevich–Tate group of $E(K)$, $\text{III}(E/K)$, is defined by

$$\text{III}(E/K) = \ker \{ H^1(K, E) \to \prod_{v \in M_K} H^1(K_v, E) \}.$$

Suppose that $\phi: E \to E'$ is an isogeny of elliptic curves of degree $m$. We have the usual exact sequence

$$0 \longrightarrow E_\phi \longrightarrow E \overset{\phi}{\longrightarrow} E' \longrightarrow 0.$$  

Taking $\text{Gal}(\bar{K}/K)$ cohomology we get a long exact sequence from which we extract a short exact Kummer sequence

$$0 \longrightarrow E'(K)/\phi E(K) \overset{i_\phi}{\longrightarrow} H^1(K, E_\phi) \longrightarrow H^1(K, E) \overset{e_\phi}{\longrightarrow} 0.$$
Here $i_\phi$ denotes the usual coboundary map: $P' \mapsto \{ \gamma: \sigma \mapsto Q^\sigma - Q \}$ where $Q \in E(\bar{K})$ is such that $\phi Q = P'$. For each $v \in M_K$, we get an analogous sequence by replacing $K$ by $K_v$ and taking cohomology with respect to $\text{Gal}(\bar{K}_v/K_v)$. The sequences patch together to form the following commutative diagram

$$
\begin{array}{cccc}
E'(K)/\phi E(K) & \xrightarrow{i_\phi} & H^1(K, E_\phi) & \xrightarrow{} & H^1(K, E_\phi) \\
\prod_{v \in M_K} E'(K_v)/\phi E(K_v) & \xrightarrow{\phi_v} & \prod_{v \in M_K} H^1(K_v, E_\phi) & \xrightarrow{} & \prod_{v \in M_K} H^1(K_v, E_\phi).
\end{array}
$$

The $\phi$-Selmer group of $E/K$ is defined to be

$$
S_\phi(E/K) = \ker \{ H^1(K_v, E_\phi) \rightarrow \prod_{v \in M_K} H^1(K_v, E_\phi) \}
$$

$$
= \{ \gamma \in H^1(K_v, E_\phi) \mid \gamma_v \in \text{Im}(i_{\phi,v}) \forall v \in M_K \}. \quad (3)
$$

We see that the kernel of the far right vertical arrow of the above commutative diagram is the $\phi$-torsion in $\Sha(E/K)$ and so can be realized as a quotient of the $\phi$-Selmer group

$$
0 \rightarrow E'(K)/\phi E(K) \rightarrow S_\phi(E/K) \rightarrow \Sha_\phi(E/K) \rightarrow 0.
$$

There is little known on methods to compute $\Sha_\phi(E/K)$ directly, but we do have some hope of computing the $\phi$-Selmer group. This of course would give us a bound on the size of $\Sha_\phi(E/K)$; however, we wouldn’t be able to determine much more (for example even whether it was trivial) without some additional information. The Cassels–Tate pairing gives us a way to get an extra piece of information. The pairing, defined by Cassels for elliptic curves and by Tate in general, is defined as a pairing on

$$
\langle , \rangle: \Sha(E/K) \times \Sha(E/K) \rightarrow \mathbb{Q}/\mathbb{Z}
$$

which is non-degenerate modulo the infinitely divisible subgroup. We can restrict the Cassels–Tate pairing to the kernel of an isogeny $\phi$ and lift it to a pairing on $S_\phi(E/K)$ which is trivial on elements coming from $E'(K)/\phi E(K)$. We will denote this pairing by $\langle , \rangle$ as well:

$$
\langle , \rangle: S_\phi(E/K) \times S_\phi(E/K) \rightarrow \mathbb{Q}/\mathbb{Z}.
$$
3. DEFINITION OF THE PAIRING

Denote by $\mu_m$ the $m$-th roots of unity. We will assume that the elliptic curve $E'$ comes equipped with a fixed isomorphism of $\text{Gal}(\overline{K}/K)$-modules

$$\hat{i}: E_m' \cong \mathbb{Z}/m\mathbb{Z} \oplus \mu_m$$

and that an isogeny $\hat{\phi}$ is chosen so that

$$E'_\hat{\phi} = \hat{i}^{-1}(\mathbb{Z}/m\mathbb{Z}).$$

The dual isogeny, $\phi: E \to E'$, then has kernel $E_{\phi} \cong \mu_m$ and $E \cong E'/i(\mathbb{Z}/m\mathbb{Z})$. Thus we have the following commutative diagram.

$$\begin{array}{ccc}
E'_{\phi} & \xrightarrow{\phi} & E_{\phi} \\
\downarrow & & \downarrow \\
\mathbb{Z}/m\mathbb{Z} & \xrightarrow{i} & \mathbb{Z}/m\mathbb{Z} \oplus \mu_m \\
\end{array}$$

It is clear that these conditions imply that the map $\hat{\phi}: E_m' \to E_{\phi}$ has a (Galois equivariant) section $s: E_{\phi} \to E_m'$.

The existence of a section allows a slight simplification in the definition of the pairing. For a general description see ([12], Milne I.6.9). Let $a, a' \in \mathbb{H}_i(E/K)$ and choose $b, b'$ in $H^1(K, E_{\phi})$ mapping to $a, a'$ respectively. By the definition of $\mathbb{H}(E/K)$, for each $v \in M_K$, $a$ maps to zero in $H^1(K_v, E)$ and so it is clear from the diagram

Diagram 1
that \( b_v \) can be lifted to an element \( b_{v,1} \in H^1(K_v, E_m) \) that is in the image of \( E'(K_v) \). At this point, the general definition requires us to lift \( b \) to a cochain \( b_1 = s_* b \), which considerably simplifies the rest of the definition. Now \( b_{v,1} - b_{1,v} \) maps to zero under \( H^1(K_v, E_m) \rightarrow H^1(K_v, E_\phi) \) and so is the image of an element \( c_v \in H^1(K_v, E_\phi) \). The pairing is defined to be

\[
\langle b, b' \rangle = \sum_{v \in M_K} \text{inv}_v(c_v \cup b'_v), \tag{4}
\]

where the cup product is induced from the Weil pairing (cf. [20], III.8)

\[ e_\phi^*: E_\phi^* \times E_\phi \rightarrow \mu_m, \]

and \( \text{inv}_v \) is the canonical isomorphism \( H^2(K_v, \mu_m) \rightarrow \mathbb{Q}/\mathbb{Z} \) (cf. [1], VI.1).

The strategy is to reduce the description of the pairing into terms which can be easily computed. Following McCallum [11], we do this by considering local bilinear pairings:

\[
\langle x, y \rangle_v : E'(K_v)/\phi E(K_v) \times E'(K_v)/\phi E(K_v) \rightarrow \mathbb{Q}/\mathbb{Z}.
\]

For each \( v \in M_K \), we have a diagram analogous to Diagram 1. Let \( x, y \in E'(K_v)/\phi E(K_v) \). Let \( x_1 \) be a lifting of \( x \) to \( E'(K_v)/mE'(K_v) \). Then \( i_{\phi,1}(x_1) \) and \( i_\phi(x) \) both have the same image in \( H^1(K_v, E_m) \), so \( (i_{\phi,1}(x_1) - i_\phi(x)) \) is the image of an element \( c_v \in H^1(K_v, E_\phi) \). Define

\[
\langle x, y \rangle_v = \text{inv}_v[c_v \cup i_\phi(y)]. \tag{5}
\]

Note that the definition of the Selmer group (3) shows that for each \( v \in M_K \), there is an obvious map:

\[
I_{\phi,1}: S_\phi(E/K) \rightarrow E'(K_v)/\phi E(K_v)
\]

\[ x \mapsto R_x. \]

We use \( I_{\phi,1} \) to map the Selmer group into the local groups \( E'(K_v)/\phi E(K_v) \). The Cassels–Tate pairing can then be expressed in terms of the local pairings.

**Theorem 3.1.** The Cassels–Tate pairing on \( S_\phi(E/K) \times S_\phi(E/K) \) may be expressed as a sum of local pairings

\[
\langle b, b' \rangle = \sum_{v \in M_K} \langle I_{\phi,1}(b), I_{\phi,1}(b') \rangle_v \mod \mathbb{Z}.
\]
Proof. We have that $x = I_{\Phi}(b)$, $y = I_{\Phi}(b')$, $s_\Phi b_{\Phi}(x) = b_{\Phi}$, $i_{\Phi}(x_1) = b_{\Phi}$, and $i_{\Phi}(y) = b_{\Phi}$, so the $c_\Phi$ in (5) is the same as the $c_\Phi$ in (4).

We can immediately reduce this to a finite sum.

Lemma 3.2. Let $E, E'$ be as above and suppose $x, y \in E'(\Q)/\phi E'(\Q)$. If $v$ is a real valuation and $m$ is odd, or $v$ is non-archimedean and $E'$ has good reduction at $v$ then $\langle x, y \rangle_v = 0$.

Proof. If $v$ is a real valuation and $m$ is odd, then clearly the pairing is trivial. If $v$ is non-archimedean and $E'$ has good reduction at $v$ then the corresponding cocycles are unramified in $H^1(G, E_v)$ and $H^1(G, E'_v)$ and so pair trivially (c.f. [12] I.2.6).

4. A FAMILY OF CURVES

We now specialize to the case $m = 5$ with $K = \Q$. For the formulas below we refer to [15]. Consider the family of elliptic curves parametrized by Eq. (1).

The curve has associated discriminant

$$\Delta(u) = -u^5(u^{10} + 11u^5 - 1)^5.$$  (6)

From now on, we will suppose that $E'$ is given by this equation for an arbitrary (but fixed) $u \in \Q$, and we will always assume $u$ is in lowest terms. Let

$$x_0(u) = \frac{u^{10} + 12u^8 - 12u^7 + 24u^6 + 30u^5 + 60u^4 + 36u^3 + 24u^2 + 12u + 1}{12},$$

$$y_0(u) = \frac{1}{2} u(u^4 - 3u^3 + 4u^2 - 2u + 1)(u^4 + 2u^3 + 4u^2 + 3u + 1)^2$$  (7)

and define $P' = (x_0(u), y_0(u)) \in E'(\Q)$. Fix a 5th root of unity $\zeta$ and define $R' = (x_0(\zeta u), y_0(\zeta u))$. It is easy to check that the points $P'$ and $R'$ are independent points of order 5. Since $P' \in E'(\Q)$, it generates a subgroup isomorphic to $\Z/5\Z$ as a Gal($\Q$/Q)-module. Furthermore, if $\sigma \in \text{Gal}(\Q/\Q)$, then $\sigma R' = \chi(\sigma) R' + (1 - \chi(\sigma)) P'$ where $\chi: G \rightarrow (\Z/5\Z)^*$ is the cyclotomic character. Hence, $Q' = P' - R'$ generates the subgroup isomorphic to $\mu_5$ as a Gal($\Q$/Q)-module. Thus, choosing $P'$ and $Q'$ as a basis for the 5-torsion induces an isomorphism

$$i: E'_5 \rightarrow \Z/5\Z \times \mu_5.$$  (8)
We then choose the isogeny $\hat{\phi}: E' \to E$ to be the one with kernel $E_{\hat{\phi}} = \langle P \rangle \cong \mathbb{Z}/5\mathbb{Z}$. Writing $Q = \phi Q'$, the dual isogeny $\phi: E \to E'$ has kernel $E_{\phi} = \langle Q \rangle \cong \mu_5$. Finally, the Galois map $\hat{\phi}: E'_5 \to E_5$ has a natural section
\[ s: E_{\hat{\phi}} \to E'_5 \]
\[ Q \to Q'. \]

Our curves $E, E'$ together with the isogenies $\phi, \hat{\phi}$ satisfy the conditions set forth in Section 3 and so the previous description of the Cassels–Tate pairing applies.

In order to compute the Cassels–Tate pairing we focus on the local pairings at 5 and primes of bad reduction for $E'$, since by Lemma 3.2 the local pairings are trivial otherwise. The family of curves parametrized by (1) has some nice reduction properties which we will see cause the local pairing to be trivial everywhere except at primes where $v \equiv 1 \pmod{5}$ is a prime of bad reduction for $E'$.

4.1. Tate curves

Whenever an elliptic curve has multiplicative reduction at a prime $v$, there is a Tate curve that can be associated to it. The following Theorem characterizes this association. A nice account of the theory of Tate curves can be found in [18], V.3–5.

**Theorem 4.1.1.** [Tate]

(i) If $E'/\mathbb{Q}$ has split multiplicative reduction at $v$, then there is a $q \in \mathbb{Q}_v$, with $|q|_v < 1$ such that

\[ E'(\mathbb{Q}_v) \cong \mathbb{Q}^*/q^\mathbb{Z} \]

as $\text{Gal}(\mathbb{Q}_v/\mathbb{Q})$-modules.

(ii) If $E'/\mathbb{Q}$ has non-split multiplicative reduction at $v$, then there is a $q \in \mathbb{Q}_v$, with $|q|_v < 1$ such that

\[ E'(\mathbb{Q}_v) \cong \mathbb{Q}^*/q^\mathbb{Z} \]

as $\text{Gal}(\mathbb{Q}_v/L)$-modules where $L$ is the unique unramified quadratic extension of $\mathbb{Q}_v$, and

\[ E'(\mathbb{Q}_v) \cong \{u \in L^* \mid \text{Norm}_{L/\mathbb{Q}_v}(u) \equiv q^\mathbb{Z}\}/q^\mathbb{Z}. \]

Examination of the Tate parametrizations for $E'$, together with the isomorphism of $\text{Gal}(\mathbb{Q}/\mathbb{Q})$-modules, $E_5 \cong \mathbb{Z}/5\mathbb{Z} \oplus \mu_5$, allows us to characterize the reduction behavior of $E'$ at all primes.
4.1.2. Let $E$ be given by (1) with $u \in \mathbb{Q}$, with $P', Q'$ as above. If $v \equiv 1 \pmod{5}$, then $E_5(\mathbb{Q}_v) = \langle P' \rangle$. Suppose that $v \neq 5$ is a prime of bad reduction for $E'$. Then $E'$ has multiplicative reduction at $v$. Furthermore, the reduction is split multiplicative if $v \equiv -1 \pmod{5}$.

Proof. By assumption, $E_5 \equiv \langle P' \rangle \oplus \langle Q' \rangle$ where $P'$ is a $\mathbb{Q}$-rational point and $Q'$ has coordinates in $\mathbb{Q}(\zeta)$ where $\zeta$ is a 5th root of unity. Hence, for all $v$, $\langle P' \rangle \subseteq E_5(\mathbb{Q}_v)$; however if $v \equiv 1 \pmod{5}$, then $\mathbb{Q}_v$ does not contain the 5th roots of unity and so $\langle Q' \rangle \notin E_5(\mathbb{Q}_v)$; hence $E_5(\mathbb{Q}_v) = \langle P' \rangle$.

Since $E'(\mathbb{Q})$ has a point of order 5, then by work of Frey ([4], Theorem 2) we know that any prime $v \neq 5$ of bad reduction has multiplicative reduction.

Now suppose that $E'$ has non-split multiplicative reduction at $v \neq 5$. By assumption $E'(\mathbb{Q}_v)$ always has at least one subgroup of order 5, thus Theorem 4.1.1(ii) implies that $L/\mathbb{Q}_v$ must contain 5th roots of unity not contained in $\mathbb{Q}_v$. This can only be possible if $v \equiv -1 \pmod{5}$. In particular, if $v \equiv -1 \pmod{5}$, then we must have split-multiplicative reduction.

Proposition 4.1.3. Let $E$ be given by (1) with $u \in \mathbb{Q}$ such that $\text{ord}_v(u) > 0$. Then $E'$ has split multiplicative reduction at $5$.

Proof. If $\text{ord}_v(u) > 0$, then the equation $E': y^2 = x^3 + a(u)x + b(u)$ as given by (1) is a minimal model at 5 since $a(u), b(u) \in \mathbb{Z}_5^\times$. Since $\Delta(u) = -4a^3(u^6 + 11u^2 + 1)^5$ then $\text{ord}_v(\Delta) > 0$ and we have bad reduction at 5. Furthermore, since $a(u) \in \mathbb{Z}_5^\times$ the reduction type is multiplicative (c.f. [20], VII.1).

Since $E'(\mathbb{Q}_5)$ contains a subgroup of order 5, but no quadratic extension $L/\mathbb{Q}_5$ contains the 5th roots of unity, we can conclude by Theorem 4.1.1(ii) that the multiplicative reduction cannot be non-split.

4.2. The image of the maps $i_{\phi,v}$

The determination of both the Selmer group and a formula for the Cassels–Tate pairing depends on the image of the local $\phi$-coboundary maps, $i_{\phi,v}$, at primes of bad reduction for $E'$. The key to analyzing these maps lies in finding the image of the (local) 5-coboundary maps

$$i_{5,v}: E'(\mathbb{Q}_v)/5E'(\mathbb{Q}_v) \to H^1(\mathbb{Q}_v, E'_5).$$

We analyze these maps by considering the Tate isomorphism and an associated parameter, $\lambda_v$.

To each $v \in M_\mathbb{Q}$ at which $E'$ has multiplicative reduction, we will associate a number $\lambda_v \in \mathbb{P}^1(F_5)$ defined as follows. Recall that we have made a choice of global points $P' \in E'(\mathbb{Q})$ and $Q' \in E'(\mathbb{Q}(\mu_5))$ giving us a
decomposition $E_5 = \langle P' \rangle \oplus \langle Q' \rangle$ as in (8). Let $\nu$ be a prime of multiplicative reduction for $E'$. Suppose that an embedding $\sigma: \mathbb{Q}(\mu_5) \to \mathbb{Q}_5$ has been chosen and denote the image of $P'$ and $Q'$ under the embedding by the same symbols. Denote by $\tau$ the Tate isomorphism referred to in Theorem 4.1.1:

$$\tau: \mathbb{Q}_5^\times / \mathbb{Z}^\times \to E'(\mathbb{Q}_5).$$

Write

$$\tau(\mu_5) = \langle aP' + bQ' \rangle \subset E_5, \quad 0 \leq a, b \leq 4. \quad (9)$$

Define

$$\lambda_\nu = \frac{a}{b} \in \mathbb{P}^1(F_5) = F_5 \cup \{ \infty \}.$$ 

Note that the ratio, $\lambda_\nu$, is well defined modulo 5 for any choice of generator $aP' + bQ'$; however, unless $\lambda_\nu = 0, \infty$, $\lambda_\nu$ does depend on our choice, $\sigma$, of embedding.

**Lemma 4.2.1.** Suppose $E'$ is given by (1) with $u \in \mathbb{Q}$.

If $\nu$ is a prime of multiplicative reduction for $E'$, the local 5-coboundary map gives an isomorphism

$$i_{\nu,5}: E'(\mathbb{Q}_5)/5E'(\mathbb{Q}_5) \to H^1(\mathbb{Q}_\nu, \langle aP' + bQ' \rangle),$$

where $a$ and $b$ are as in (9). Furthermore, with $\lambda_\nu, P'$, and $Q'$ as above,

(i) If $\nu \equiv 1 \pmod{5}$ is a prime of split multiplicative reduction, then

$$\lambda_0 = 0; \text{ i.e., } i_{\nu,5}(E'(\mathbb{Q}_\nu)/5E'(\mathbb{Q}_\nu)) \cong H^1(\mathbb{Q}_\nu, \langle Q' \rangle).$$

(ii) If $\nu$ is a prime of non-split multiplicative reduction, then

$$\lambda_\nu = \infty; \text{ i.e., } i_{\nu,5}(E'(\mathbb{Q}_\nu)/5E'(\mathbb{Q}_\nu)) \cong H^1(\mathbb{Q}_\nu, \langle P' \rangle).$$

**Proof.** The Tate parametrization, $\tau$, gives rise to the following commutative diagram where $\tilde{\tau}$ is induced by $\tau$.

$$
\begin{array}{c}
0 \\ \\
\mathbb{Q}_\nu^\times (\mathbb{Q}_\nu^\times)^5 \xrightarrow{\tilde{\tau}} E'(\mathbb{Q}_\nu)/5E'(\mathbb{Q}_\nu) \xrightarrow{\tilde{i}} 0 \\
\downarrow {\lambda_\nu} \\
0 \xrightarrow{0} H^1(\mathbb{Q}_\nu, \mu_5) \xrightarrow{\tilde{i}} H^1(\mathbb{Q}_\nu, E'_5) \xrightarrow{\cdots} \\
\downarrow \\
\end{array}
$$


It follows that

\[ i_{*\sigma}(E'(Q_v)/5E'(Q_v)) \cong H^1(Q_v, \tau(\mu_s)) = H^1(Q_v, E'_s). \]

In other words, if \( \tau(\mu_s) = \langle aP + bQ' \rangle \), we have the isomorphism:

\[ i_{*\sigma}; E'(Q_v)/5E'(Q_v) \to H^1(Q_v, \langle aP + bQ' \rangle) \]

as claimed.

For a prime of split multiplicative reduction, Theorem 4.1.1(i) tells us that \( \tau \) is Galois equivariant and so \( \langle aP + bQ' \rangle \) corresponds to the subgroup of \( E'_s \) on which the Galois group acts by \( \mu_s \). If \( v \not\equiv 1 \pmod{5} \), then by Lemma 4.1.2, \( E'_3(Q_v) = \langle P' \rangle \) and so we must have that \( \tau(\mu_s) = \langle Q' \rangle \); i.e., \( a = 0 \Rightarrow \lambda_v = 0 \).

If \( v \) is a prime of non-split multiplicative reduction for \( E' \), then Theorem 4.1.1(ii) tells us that \( \tau \) is not Galois equivariant, but the action is twisted by a quadratic character, \( \chi \), which acts by taking a 5th root of unity to its inverse. Thus as \( \text{Gal}(\bar{Q}/Q) \)-modules, \( \tau(\mu_s) \equiv \mu_3(\chi) \equiv \mathbb{Z}/5\mathbb{Z} \). Since we have non-split reduction, Lemma 4.1.2 tells us \( v \not\equiv 1 \pmod{5} \) and \( E'_3(Q_v) = \langle P' \rangle \). If follows that \( \tau(\mu_s) = \langle P' \rangle \); i.e., \( b = 0 \Rightarrow \lambda_v = \infty \).

Proposition 4.2.2. Suppose that \( E' \) is given by (1) for a choice of \( u \in \mathbb{Z} \) with \( \text{ord}_5(u) > 0 \) such that \( t = u^2 + u - 1 \) is not divisible by any prime congruent to 1 modulo 5. Then if \( v \equiv 1 \pmod{5} \) is a prime of bad reduction for \( E' \), \( \lambda_v \neq \infty \).

Proof. Suppose that \( v \equiv 1 \pmod{5} \) is a prime of bad reduction for \( E' \). According to definition (9), to show that \( \lambda_v \neq \infty \), we must show that \( \tau(\mu_s) \neq \langle P' \rangle \). Suppose that \( \zeta \in \mu_s \). The image of \( \zeta \) under the Tate map, \( \pi(\zeta) = (x(\pi(\zeta)), y(\pi(\zeta))) \) (see [18], V.3 for explicit formulas) tells us that \( x(\pi(\zeta)) \) is a unit if and only if \( y(\pi(\zeta)) \) is a unit.

We now consider the coordinates of \( P' \). Let \( E' \) given by Eq. (1) with \( u \in \mathbb{Z} \) chosen so that \( t = u^2 + u - 1 \) is not divisible by any primes congruent to 1 mod 5. The discriminant of \( E' \) is given by

\[ A = -u^5(u^2 + u - 1)^5 (u^4 - 3u^3 + 4u^2 - 2u + 1)^5 (u^4 + 2u^3 + 4u^2 + 3u + 1)^5. \]
For simplicity write
\[ t = u^2 + u - 1, \quad s = u^4 - 3u^3 + 4u^2 - 2u + 1, \quad r = u^4 + 2u^3 + 4u^2 + 3u + 1, \]
so that
\[ A = -(utsr)^5. \]

By assumption \( v \nmid t \) and so we must have that \( v \mid (urs) \). Now consider the formula (7) for the \( y \)-coordinate of \( P' \),
\[ y(P') = \frac{1}{2}u(u^4 - 3u^3 + 4u^2 - 2u + 1)(u^4 - 3u^3 + 4u^2 + 3u + 1)^2 = \frac{1}{2}urs^2. \]

Notice that
\[ v \mid (urs) \Rightarrow v \mid y(P'), \]
thus \( y(P') \) is not a unit. On the other hand, \( \text{GCD}(x(P'), y(P')) \mid 12 \) and so for \( v \equiv 1 \pmod{5} \), \( x(P') \) is a unit. Hence, \( \tau(\zeta) \neq P' \), for all \( \zeta \in H_5 \) and we conclude that \( \lambda_v \neq \infty \). \( \square \)

We now have enough machinery set up to determine the Selmer group and the Cassels–Tate pairing.

4.3. The Selmer Group

Recall that the \( \phi \)-Selmer group is defined in terms of the image of the local coboundary maps, \( i_{\phi,v} \):
\[ S_{\phi}(E/Q) = \{ \gamma \in H^1(Q, E_{\phi}) \mid \gamma_v \in \text{Im}(i_{\phi,v}) \forall v \in M_Q \}. \]

There is another interpretation of the Selmer group as a subgroup of \( \mathbb{Q}^*/(\mathbb{Q}^*)^2 \). It is in this form that we will describe the Selmer group as it is much easier to work with from the computational viewpoint.

By assumption, \( E_{\phi}^0 = i^{-1}(\mathbb{Z}/5 \mathbb{Z}) \). Let \( P' \) be the generator of \( E_{\phi}^0 \) chosen above. The Weil pairing induces an isomorphism
\[ E_{\phi} \cong H_5 \]
\[ x \mapsto e_{\phi}(x, P') \]
which in turn induces an isomorphism

$$j_P: H^1(Q, E_p) \to H^1(Q, \mu_s) = \mathbb{Q}^*(\mathbb{Q}^*)^5$$

(10)

where the last equality is the canonical identification from Kummer theory.

Using the diagram below

$$\begin{array}{ccc}
0 & \longrightarrow & E'(Q)/\phi(E(Q)) \\
\downarrow & & \downarrow \\
0 & \longrightarrow & H^1(Q, E_p) \xrightarrow{j_P} \mathbb{Q}^*(\mathbb{Q}^*)^5 \\
\end{array}$$

we get the following description of $S_d(E/Q)$:

$$S_d(E/Q) = \{ x \in \mathbb{Q}^*/(\mathbb{Q}^*)^5 \mid x_v \in \text{Im}(j_P \circ i_{\phi,v}) \forall v \in M \}.$$  

From now on, we will identify $S_d(E/Q)$ with this subgroup of $\mathbb{Q}^*/(\mathbb{Q}^*)^5$. The definition implies that to find $S_d$ we must know the images of all of the local coboundary maps; however, the next lemma tells us that we can restrict our attention to the coboundary maps at primes of bad reduction. As before (2) let $M$ be the set of primes of bad reduction for $E'$.

**Lemma 4.3.1.** Suppose that $E'$ is given by (1) with $u \in \mathbb{Q}$, ord$_5(u) > 0$ and $E \cong E'/\mathbb{Z}/5\mathbb{Z}$. Let $N = \{ a \mid \text{ord}_v(a) \equiv 0 \pmod{5} \text{ if } v \notin M \} < \mathbb{Q}^*/(\mathbb{Q}^*)^5$. Then

$$S_d(E/Q) = \{ a \in N \mid a_v \in \text{Im}(j_P \circ i_{\phi,v}) \forall v \in M \}.$$  

**Proof.** Elements of the Selmer group are unramified outside the set of primes of bad reduction for $E'$ (note that by our conditions, $5 \notin M$). An element $a \in \mathbb{Q}^*/(\mathbb{Q}^*)^5$ represents an unramified cocycle in $H^1(Q_v, E_p)$ if and only if ord$_v(a) \equiv 0 \pmod{5}$ (c.f. [20], X.4).

We are now ready to prove the first main result, Theorem 1.1.

**Proof of Theorem 1.1.** By the previous lemma, we know that

$$S_d(E/Q) = \{ a \in N \mid a_v \in \text{Im}(j_P \circ i_{\phi,v}) \forall v \in M \},$$

where $M$ is as in (2) and $N$ is as in Lemma 4.11. To complete the description of the $\phi$-Selmer group, we need to determine the image of $j_P \circ i_{\phi,v}$ for all $v \in M$ and determine the conditions necessary for an element of $N$ to be in all of the images.
Suppose that \( v \in M \) and consider the following commutative diagram

\[
\begin{array}{c}
0 \longrightarrow E(Q_v)/\phi E(Q_v) \longrightarrow H^1(Q_v, E') \\
0 \longrightarrow E'(Q_v)/SE'(Q_v) \longrightarrow H^1(Q_v, E'_x) \\
0 \longrightarrow E'(Q_v)/\phi E(Q_v) \longrightarrow H^1(Q_v, E'_x) \\
0 & 0
\end{array}
\]

It follows that

\[
i_{v,\phi}(E'(Q_v)/\phi E(Q_v)) \cong \tilde{\phi}_v(i_{v,\phi}(E'(Q_v)/SE'(Q_v))).
\]

To determine the images explicitly, we partition the primes \( v \in M \) into three categories:

(A) \( E' \) has split multiplicative reduction at \( v \) with \( v \not \equiv 1 \pmod{5} \), or \( v \equiv 1 \pmod{5} \) with \( \lambda_v \neq \infty \).

(B) \( E' \) has non-split multiplicative reduction at \( v \).

(C) \( E' \) has split multiplicative reduction at \( v \) with \( v \equiv 1 \pmod{5} \) and \( \lambda_v = \infty \).

For primes in case (A), Lemma 4.2.1 tells us that

\[
i_{5,\phi}(E'(Q_v)/SE'(Q_v)) = H^1(Q_v, \langle aP + bQ' \rangle), \quad b \neq 0.
\]

Furthermore,

\[
\phi(Q') = Q \Rightarrow \phi(\langle aP + bQ' \rangle) \cong E_d = \langle Q \rangle,
\]

thus

\[
i_{5,\phi}(E'(Q_v)/\phi E(Q_v)) = \phi_v(H^1(Q_v, \langle aP + bQ' \rangle)) = H^1(Q_v, E_d),
\]

and so

\[
\text{Im}(j_P \circ i_{5,\phi}) = \mathbb{Q}_v^\times/(\mathbb{Q}_v^\times)^3.
\]

In case (B), Lemma 4.2.1(ii) tells us that

\[
i_{5,\phi}(E'(Q_v)/SE'(Q_v)) \cong H^1(Q_v, \langle P' \rangle).
\]
Since $\hat{\phi}P^r = O$, we get that

$$i_{\phi,*}(E'(\mathbb{Q}_v)/\phi E(\mathbb{Q}_v)) = \hat{\phi}_*(H^1(\mathbb{Q}_v, \langle P^r \rangle)) = \{1\}, \quad (11)$$

thus

$$\text{Im}(j_{P^r} \circ i_{\phi,*}) = \{1\}.$$ 

Finally, in case (C) Lemma 4.2.1 tells us that

$$i_{S,v}(E'(\mathbb{Q}_v)/5E'(\mathbb{Q}_v)) = H^1(\mathbb{Q}_v, \langle P^* \rangle)$$

and so using the same argument as in (B),

$$\text{Im}(j_{P^r} \circ i_{\phi,*}) = \{1\}.$$ 

To complete our description of the $\phi$-Selmer group, we must determine which elements of $N$ are in all of the images $j_{P^r} \circ i_{\phi,*}$. The image of $j_{P^r} \circ i_{\phi,*}$ for primes in case (A) is all of $\mathbb{Q}_v^* / (\mathbb{Q}_v^*)^5$ and consequently no conditions are imposed on elements of $N$ to be in the image of these maps. In the case of (B) and (C), we have that the image is trivial. Thus an element of $N$ must be a 5th power in $\mathbb{Q}_v^*$ for each of these primes in order to be in the Selmer group. Note that $v$ itself is not a 5th power in $\mathbb{Q}_v^*$. Therefore if $a \in S_v(E/\mathbb{Q})$, then $\text{ord}_v(a) \equiv 0 \pmod{5}$ for all $v$ in the sets (B) and (C). If $v$ is a prime of non-split multiplicative reduction (as in (B)), then we have seen that $v \not\equiv 1 \pmod{5}$ (and $v \neq 5$). In this case, every element of $\mathbb{Q}_v^*/(\mathbb{Q}_v^*)^5$ is a 5th power. In the case of (C), we have that $v \equiv 1 \pmod{5}$ and so an element $a \in \mathbb{Q}_v^*/(\mathbb{Q}_v^*)^5$ is a 5th power if and only if $a^{\frac{1}{5}} \equiv 1 \pmod{v}$. This completes the proof of the theorem.

**Corollary 4.3.2.** If $E'$ is given by (1) with $u \in \mathbb{Z}$, $\text{ord}_v(u) > 0$, $t = u^2 + u - 1$ not divisible by any primes congruent to 1 modulo 5, and $E \equiv E'/(\mathbb{Z}/5\mathbb{Z})$ then $S_\phi(E/\mathbb{Q})$ is generated, modulo 5th powers, by the images of the primes of split multiplicative reduction.

**Proof.** By Proposition 4.2.2, the set $\Sigma$ in the statement of Theorem 1.1 is empty and the result follows from the theorem.

**4.4. The Local Pairings**

We proceed to compute the Cassels–Tate pairing by looking at the local pairings. Recall that the local pairings are defined by (see Section 5):

$$\langle x, y \rangle_v = \text{inv}_v[\epsilon_v \cup i_{\phi,*}(y)],$$

where $\epsilon_v \in H^1(\mathbb{Q}_v, E'_\phi)$ is an element that maps to $i_{S,v}(x_1) - s_\phi i_{\phi,*}(x)$. 

40 CHERYL DELORME BEAVER
Lemma 4.4.1. Suppose that $E'$ is given by (1) with $u \in \mathbb{Q}$, $\ord(u) > 0$ and $E \cong E'(\mathbb{Z}/5\mathbb{Z})$. Let $x, y \in E'(\mathbb{Q}_5)/\phi E(\mathbb{Q}_5)$. If $v \in M$ with $\lambda_v = \infty$ or $\lambda_v = 0$, then $(x, y)_v = 0$.

Proof. If $v \in M$ with $\lambda_v = \infty$, then $H^1(\mathbb{Q}_5, E'_5) \cong H^1(\mathbb{Q}_5, \langle P' \rangle)$ and, as we saw in the proof of Theorem 1.1, Eq. (11)

$$i_{v,1}(E'(\mathbb{Q}_5)/\phi E(\mathbb{Q}_5)) = \{0\}.$$  

Thus for any $y \in E'(\mathbb{Q}_5)/\phi E(\mathbb{Q}_5)$, $i_{v,1}(y) = 0$ and so the local pairing is

$$\langle x, y \rangle_v = \text{inv}_v([c_v \cup 0] = 0.$$  

If $v \in M$ with $\lambda_v = 0$, then we have that the image of $i_{5,v}$ in $H^1(\mathbb{Q}_5, E_5)$ is isomorphic to $H^1(\mathbb{Q}_5, \langle Q' \rangle)$. Furthermore, the image of the section $s_1$ also lies in $H^1(\mathbb{Q}_5, \langle Q' \rangle)$. It follows that if $c_v \in H^1(\mathbb{Q}_5, E'_5) = H^1(\mathbb{Q}_5, \langle P' \rangle)$ is an element mapping to $i_{5,(x)}(x) - s_1 i_{5,1}(x) \in H^1(\mathbb{Q}_5, \langle Q' \rangle)$ then $c_v = 0$ and the pairing, $(x, y)_v = \text{inv}_v([0 \cup i_v(y)] = 0$, is again trivial.

It remains to compute the local pairing at the primes of bad reduction for $E'$ with $\lambda_v \neq 0$, $\infty$. Note that by Lemma 4.1.2 and Lemma 4.2.1 these are the primes with $v \equiv 1 (\mod 5)$. In this case, the local fields, $\mathbb{Q}_v$, contain the 5th roots of unity. Again suppose that an embedding, $\sigma: \mathbb{Q}(\mu_5) \hookrightarrow \mathbb{Q}_v$, has been chosen. Denote the image of the global points $P'$, $Q$, and $Q'$ with respect to this embedding by the same symbol.

If $a, b \in \mathbb{Q}_v^*/(\mathbb{Q}_v^*)^5$, then let $x \in \mathbb{Q}_v$ be such that $x^5 = a$, $b$ any element of $\mathbb{Q}_v^*$ mapping to $b$ and $[b, \mathbb{Q}_v]$ the Artin symbol. The Hilbert norm residue symbol at 5 is defined by

$$(\cdot, \cdot): \mathbb{Q}_v^*/(\mathbb{Q}_v^*)^5 \times \mathbb{Q}_v^*/(\mathbb{Q}_v^*)^5 \rightarrow \mu_5$$

$$(a, b) \mapsto a^{[b, \mathbb{Q}_v]} - 1.$$  

Kummer Theory gives isomorphisms $\mathbb{Q}_v^*/(\mathbb{Q}_v^*)^5 \cong H^1(\mathbb{Q}_v, \mu_5)$, and we have

$$\mu_5 \cong H^1(\mathbb{Q}_v, \mu_5 \otimes \mu_5)$$

$$\xrightarrow{\text{via}}$$

$$H^2(\mathbb{Q}_v, \mu_5) \otimes H^1(\mathbb{Q}_v, \mu_5) \xrightarrow{\text{inv} \otimes 1} (\mathbb{Q}/\mathbb{Z}) \otimes \mu_5 \rightarrow \mu_5.$$  

According to [17] Serre XIV.2, Proposition 5, with these identifications, the Hilbert pairing may be identified with the cup product pairing:

$$(\cdot, \cdot): H^1(\mathbb{Q}_v, \mu_5) \otimes H^1(\mathbb{Q}_v, \mu_5) \rightarrow H^2(\mathbb{Q}_v, \mu_5 \otimes \mu_5).$$

Recall that the map $j_{P'}$ (10) gives us an isomorphism $H^1(\mathbb{Q}_v, E_{P'}) \cong H^1(\mathbb{Q}_v, \mu_5)$. With $Q$ a generator for $E_{P'}$, we define an analogous isomorphism $j_Q$:

$$j_Q: H^1(\mathbb{Q}_v, E_{P'}) \rightarrow H^1(\mathbb{Q}_v, \mu_5).$$
LEMMA 4.4.2. The following diagram commutes

\[
\begin{array}{ccc}
\text{inv}(\cup) : \ H^1(\mathbb{Q}_v, E'[\ell]) \times H^1(\mathbb{Q}_v, E'[\ell]) & \longrightarrow & \mathbb{Q}/\mathbb{Z} \\
& \downarrow i_\rho & \downarrow j_\rho \\
\text{Ind}_{\text{ind}Q, P}(\cdot, \cdot) : \mathbb{Q}_v^*/(\mathbb{Q}_v^*)^5 \times \mathbb{Q}_v^*/(\mathbb{Q}_v^*)^5 & \longrightarrow & \mathbb{Q}/\mathbb{Z},
\end{array}
\]

where \( e = e_\rho(Q, P') \).

The proof of this lemma can be found in McCallum [11]. This diagram allows us to get a relation between our local pairing, given by the first row, with the Hilbert norm residue symbol given by the second row. This relationship is stated explicitly in the following lemma.

LEMMA 4.4.3. If \( v \in M \) with \( \lambda_v \neq 0, \infty \), then for \( x, y \in E'(\mathbb{Q}_v)/\phi E(\mathbb{Q}_v) \),

\[
\langle x, y \rangle_v = \text{Ind}_{\text{ind}Q, P'}(j_{\rho} \circ i_{\phi_v}(x), j_{\rho} \circ i_{\phi_v}(y))^{-\zeta_v},
\]

where \( \langle \cdot, \cdot \rangle_v \) is the Hilbert norm residue symbol.

Proof. Suppose that \( v \in M \) with \( \lambda_v \neq 0, \infty \). By Lemma 4.1.2 and Lemma 4.2.1 we must have that \( v \equiv 1 \pmod{5} \). Thus \( \mathbb{Q}_v^* \) contains the 5th roots of unity.

For \( x, y \in E'(\mathbb{Q}_v)/\phi E(\mathbb{Q}_v) \), the cohomology classes of \( i_{\phi_v}(x) \) and \( i_{\phi_v}(y) \) can be represented by the cocycles \( \{ \tau \mapsto n_1 \tau \} \) and \( \{ \zeta \mapsto m_2 \zeta \} \), respectively. We know by Lemma 4.2.1 that the image of \( i_{\phi_v} \) is isomorphic to \( H^1(\mathbb{Q}_v, \langle aP' + bQ' \rangle) \), depending on the Tate parametrization, with \( ab \neq 0 \) where we’ve set \( \lambda_v = \frac{a}{b} \).

Write \( Z = Q' + \lambda_v P' \). Let \( x_1 \) be a lifting of \( x \) to \( E'(\mathbb{Q}_v)/\phi E(\mathbb{Q}_v) \), representing \( i_{\phi_v}(x) \) by the cocycle \( \{ \tau \mapsto (r_1 Q' + r_2 \lambda_v P') \} \) and using the fact that \( \phi(i_{\phi_v}(x_1) - s_\ast i_{\phi_v}(x)) \) can then be represented by \( \phi((r_1 Q' + r_2 \lambda_v P') - n_v Q') = r_1 Q' - n_v Q' = 0 \), we get \( r_v = n_v \) (since our choice of cocycle is unique since \( E_3 \) is \( \mathbb{Q}_v \)-rational) and so the cohomology class of \( c_v \in H^1(\mathbb{Q}_v, E'[\ell]) \) which maps to \( (i_{\phi_v}(x_1) - s_\ast i_{\phi_v}(x)) \) corresponds to \( n_v \lambda_v P' \) and can be represented by the cocycle \( \{ \tau \mapsto n_v \lambda_v P' \} \).

Write \( \zeta = e_\rho(Q, P') \). The above identifications together with Lemma 4.4.2 and (12) then give us that \( \langle x, y \rangle_v = \text{inv}_{\text{ind}Q, P'}(c_v \cup i_{\phi_v}(y)) \) can be represented by

\[
\text{inv}_{\text{ind}Q, P' \cup m_2 Q} \sim \text{Ind}_{\text{ind}Q, P'}(j_{\rho} \circ i_{\phi_v}(x), j_{\rho} \circ i_{\phi_v}(y))^{-\zeta_v},
\]

\[
\sim \text{Ind}_{\text{ind}Q, P'}(\zeta^{-n_v \lambda_v}, \zeta m_2)^{-\zeta_v},
\]

\[
\sim \text{Ind}_{\text{ind}Q, P'}((\zeta^{m_2})^{-n_v \lambda_v})^{-\zeta_v},
\]

\[
\sim \text{Ind}_{\text{ind}Q, P'}(j_{\rho} \circ i_{\phi_v}(x), j_{\rho} \circ i_{\phi_v}(y))^{-\zeta_v}.
\]
The proof of Theorem 1.2 with $\zeta = \zeta(P, P')$ is now very simple.

**Proof of Theorem 1.2.** If $E$ is given by (1) with $\text{ord}_d(u) > 0$ then Lemma 4.1.2 and Proposition 4.1.3 tell us that all primes of bad reduction for $E$ have multiplicative reduction. The theorem then follows from Lemma 4.4.1 and Lemma 4.4.3.

**Computations.** Let $a$ and $b$ be 2 elements of $\mathbb{Q}_v^*$ with valuations $\alpha$ and $\beta$ respectively. Define $c = (-1)^{\alpha} \frac{a}{b}$. The local Hilbert symbol can be given by $(a, b)_v = \frac{c}{v}(-1)^{\alpha}$. Theorem 1.2 tells us that all primes of bad reduction for $E$ have multiplicative reduction. The theorem then follows from Lemma 4.4.1 and Lemma 4.4.3.

We are finally ready to prove Corollary 1.3.

**Proof of Corollary 1.3.** We will accomplish this proof by exhibiting 2 elements which we can guarantee to be in the Selmer group, namely 5 and 11, that pair non-trivially under the Cassels–Tate pairing. This shows that $\text{Sel}(E/\mathbb{Q})$ is non-trivial and the result follows, since by the alternating property of the Cassels–Tate pairing the order of 5 must be a square.

First we show that 5 and 11 are in the Selmer group. The discriminant of $E$ is given by $\Delta = -u^2(u^{10} + 11u^2 - 1)^2$. We have that $\text{ord}_{11}(11u^2) = 1$ and $u^{10} \equiv 1 \pmod{11}$, so $\text{ord}_{11}(\Delta) = \text{ord}_{11}(u^{10} + 11u^2 - 1)^2 = 5$. Furthermore, any change of coordinates changes $\Delta$ by a power of 12, so get that 11 must also divide the minimal discriminant of $E$ and is therefore a prime of bad reduction for $E$. According to Theorem 1.2, 11 is a prime of split-multiplicative reduction and by Proposition 4.1.3, 5 is also a prime of split-multiplicative reduction for $E$. Thus, since we have chosen $u$ so that $t = u^2 + u - 1$ is not divisible by any primes congruent to 1 modulo 5, Corollary 4.3.2 tells us that the Selmer group is generated by primes of split multiplicative reduction for $E$, we get that $5, 11 \in S_\ell(E/\mathbb{Q})$.

Next we consider the pairing on $\langle 5, 11 \rangle$. Theorem 1.2 tells us

$$\langle 5, 11 \rangle = \sum_{v \in S} \text{Ind}_{d(Q, P)}(5, 11)^{-\epsilon_v} \mod \mathbb{Z},$$

where $S = \{ v \in M \mid v \equiv 1 \pmod{5} \text{ with } \lambda_v \neq 0, \infty \}$. If $v \in S$, with $v \neq 11$, then both 5 and 11 are units in $\mathbb{Q}_v^*$. By the discussion above, the Hilbert pairing is trivial on units, so $\langle 5, 11 \rangle_v = 0$ and the pairing between 5 and 11 reduces to the local pairing at $v = 11$:

$$\langle 5, 11 \rangle_{11} = \text{Ind}_{d}(5, 11)^{-2} = \text{Ind}_{d}((5)^{(11-1)/5})^{-2} = \text{Ind}_{d}(5^2)^{-2} \neq 0.$$  

**Example.** We now do an explicit example for $u = 5$. In this case, the curve $E$ is

$$E': y^2 = x^3 - \frac{5525890547461}{3}x + \frac{315742662278497110547}{108},$$
the discriminant is
\[ A = -5^5(11 \cdot 29 \cdot 31 \cdot 991)^5, \]
and the rational 5-torsion point \( P \) is
\[ P = \left( \frac{1674448105}{5}, \frac{3506759}{120901020992332992024} \right). \]

Following Velu [22] we get an equation for \( E \):
\[ E: y^2 + y = x^3 - x^2 - 14128847434470x - 12090102099232992024. \]

Since \( \text{ord}_v(2) < 12 \) for all \( v \mid A \) we get that the primes of bad reduction for \( E \) are 5, 11, 29, 31, 991. By Lemma 4.1.2 and Proposition 4.1.3 we get split-multiplicative reduction at 5, 11, 31, 991 and checking directly (using, say pari-gp) we see that 29 is also a prime of split-multiplicative reduction.

Furthermore \( t = u^2 + u - 1 = 29 \) for \( u = 5 \) and so by Corollary 4.3.2 we know that the Selmer group for \( E \) is generated up to 5th powers by these primes of split multiplicative reduction; i.e.,
\[ S_q(E/\mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z})^5 \cong \langle 5, 11, 29, 31, 991 \rangle \in \mathbb{Q}^* / (\mathbb{Q}^*)^5. \]

Next we compute the kernel of the Cassels–Tate pairing using Theorem 1.2.

In our case, \( M = \{5, 11, 29, 31, 991\} \) and \( S = \{11, 31, 991\} \). By choosing a nice embedding of \( \mathbb{Q}(\mu_5) \to \mathbb{Q}_p \), we can assume \( \lambda_v = -1 \) for \( v = 11, 31, 991 \). These embeddings give us \( \zeta = 5, \zeta = 16, \zeta = 799 \) for \( v = 11, 31, 991 \) respectively (again this was done using pari-gp).

Thus the pairing becomes for \( n, m \in S_q(E/\mathbb{Q}) \):
\[ \langle n, m \rangle = \text{Ind}_5(n, m)_{11} + \text{Ind}_5(n, m)_{31} + \text{Ind}_{799}(n, m)_{991} \mod \mathbb{Z}. \]

Now it is easy to compute the kernel of the pairing—we get that it is rank one, generated by the element \( a = 5 \cdot 11 \cdot 991^4 \in S_q(\mathbb{Q}) \); i.e.,
\[ \ker(\langle , \rangle) \cong \mathbb{Z}/5\mathbb{Z}. \]

Since \( E'(\mathbb{Q})/\phi E(\mathbb{Q}) \cong \ker(\langle , \rangle) \) and \( \text{III}_q(\mathbb{Q}) \cong S_q(E/\mathbb{Q}) / (E'(\mathbb{Q})/\phi E(\mathbb{Q})) \), we see that we have one of two cases:
\[ \text{III}_q(E/\mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z})^4 \quad \text{if} \ E(\mathbb{Q}) = \emptyset, \text{ or} \]
\[ \text{III}_q(E/\mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z})^6 \quad \text{if} \ E(\mathbb{Q}) \neq \emptyset. \]

One can check that the functional equation for the \( L \)-series associated to \( E \) is \(-1\) and so \( L(E, 1) \) should have a zero of odd order. Since \( E \) is modular [23], if we can show that \( L'(E, 1) \neq 0 \), then work of Kolyvagin
and Gross and Zagier [5] tells us that $E(\mathbb{Q})$ has rank 1. We can estimate $L'(E, 1)$ via

$$L'(E, 1) = 2 \sum_{n=1}^{\infty} \frac{a_n}{n} E_1 \left( \frac{2\pi n}{\sqrt{N}} \right)$$

where the $a_n$ are the coefficients from the $L$-series of $E$, $E_1(x) = \int_{x}^{\infty} \frac{e^{-t}}{t} dt$, and $N$ is the conductor of $E$ (see [3], Section 7.5.3). If we sum the first 10,000 terms of this series (using PARI to find the $a_n$ and $E_1(x)$) we get $L'(E, 1) \approx 3.76$. According to ([19], Proposition 4.1) we calculate that the error in our estimation is off by no more than 1.25 and so in particular, $L'(E, 1) \neq 0$ and we have that $\text{Im}(E(\mathbb{Q})) \cong (\mathbb{Z}/5\mathbb{Z})^5$.

**Remark.** Experimentally, the condition that $\lambda_{11} \neq 0$ required in Corollary 1.3 seems to be satisfied most of the time. In particular, this is true for $u = 5, 10, 15, 20, 30, 35, 45, 50, 60$. In fact, after a search of all values of $u$ up to 200 satisfying the other hypotheses in the corollary, there haven't been any counterexamples to $\lambda_{11} \neq 0$. It seems likely that with a more careful study of the properties of the Tate parameterization, one should be able to show that the condition is satisfied for all $u$ in some collection of 11-adic open disks. This will be the subject of future research.

Finally, note that in general we can compute the local pairings rather easily. Once we've chosen an embedding for $\mu_5$ into $\mathbb{Q}_5$, we can compute the Hilbert norm residue symbol and $\lambda_5$ using functions in gp-pari. Thus with the aid of the computer, the algorithms presented in this paper give a method to compute the kernel of the Cassels-Tate pairing and so determine the size of the $\phi$-torsion in the Shafarevich-Tate groups of these elliptic curves.

ACKNOWLEDGMENTS

The author would like to thank her advisor William McCallum for his guidance and support in researching this topic, much of which was contained in her Ph.D. dissertation; Bjorn Poonen for his useful comments on an early draft of this paper; and Karl Rubin for many useful suggestions in editing the paper.

REFERENCES


