EXPLICIT DESCENT VIA 4-ISOGENY ON AN ELLIPTIC CURVE

EDRAY HERBER GOINS

Abstract. We work out the complete descent via 4-isogeny for a family of rational elliptic curves with a rational point of order 4; such a family is of the form \( y^2 + x y + a y = x^3 + a x^2 \) where \( \sqrt{-a} \in \mathbb{Q}^\times \). In the process we exhibit the 4-isogeny and the isogenous curve, explicitly present the principal homogeneous spaces, and discuss examples by computing the rank.

1. Introduction

For each \( t \in \mathbb{Q}^\times \) we have the rational elliptic curve

\[
E_t : \quad v^2 = u^3 + (t^2 + 2) u^2 + u \quad \text{where} \quad [4] (-1, t) = \mathcal{O}.
\]

This curve is studied in detail in [2], where, among other things, it is shown that the torsion subgroup \( T \) of \( E_t(\mathbb{Q}) \) is completely classified as being either

\[
T \simeq \begin{cases} \mathbb{Z}/4\mathbb{Z} & \text{or} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \quad & \text{if} \quad t = (s^2 - 1)/s \quad \text{for} \quad s \in \mathbb{Q}^\times, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \quad & \text{if} \quad t = (s^2 - 1)/s \quad \text{and} \quad s = (r^2 - 1)/(2 r) \quad \text{for} \quad r \in \mathbb{Q}^\times. 
\end{cases}
\]

On the other hand, the rank of \( E_t(\mathbb{Q}) \) may be computed by a descent via two-isogeny coming from the rational point \([2] (-1, t) = (0, 0)\) of order 2, as implemented in computer packages such as MAGMA [1]. Unfortunately, there may be a global obstruction in computing the rank due to nontrivial elements in the Shafarevich-Tate group, so one can only find a lower bound on the rank in general. In this exposition, I show how to compute the rank of \( E_t(\mathbb{Q}) \) by exploiting instead the rational point \((-1, t)\) of order 4 i.e. I work out a descent via four-isogeny.

The main result of this paper is the following:

Theorem 1.1. Fix \( t \in \mathbb{Q}^\times \), and denote the elliptic curves

\[
E_t : \quad v^2 = u^3 + (t^2 + 2) u^2 + u,
\]

\[
E'_t : \quad V^2 = U^3 - 2 (t^2 - 4) U^2 + (t^2 + 4)^2 U,
\]

\[
E''_t : \quad v^2 = u^3 + (t^2 - 4) u^2 - 4 t^2 u.
\]

(1) There are isogenies \( \phi : E_t \to E'_t \) of degree 4 with kernel generated by \((-1, t)\), and \( \varphi : E_t \to E''_t \) of degree 2 generated by \([2] (-1, t) = (0, 0)\).

\textbf{2000 Mathematics Subject Classification.} 14G05, 11G05, 11D25.

\textbf{Key words and phrases.} elliptic curve, rank, torsion, descent, isogeny.
(2) Upon identifying the Selmer groups as subgroups of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^4$ and $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, respectively; and Shafarevich-Tate groups as a collection of homogeneous spaces, there is an exact diagram

$$
0 \longrightarrow \frac{E_t(Q)}{\phi(E'_t(Q))} \overset{\delta'}{\longrightarrow} S^{(\phi)}(E'_t/Q) \longrightarrow \text{III}(E'_t/Q)[\hat{\phi}] \longrightarrow 0
$$

(1.4)

$$
0 \longrightarrow \frac{E_t(Q)}{\phi(E''_t(Q))} \overset{\delta''}{\longrightarrow} S^{(\hat{\phi})}(E''_t/Q) \longrightarrow \text{III}(E''_t/Q)[\hat{\varphi}] \longrightarrow 0
$$

where we have the connecting homomorphisms

$$
\delta': (-1,t) \mapsto -4t^2 \quad \delta'': (0,0) \mapsto t^2 + 4
$$

(1.5)

while the maps into the Shafarevich-Tate groups send $d \mapsto \{C'_{d,t}/Q\}$ and $d \mapsto \{C''_{d,t}/Q\}$ in terms of

$$
C'_{d,t}: \quad d \left( \frac{w - \frac{z^2}{4t^2}}{2} \right) z^2 = \left( \frac{w^2 - d}{2} \right)^2,
$$

$$
C''_{d,t}: \quad d W^2 = d^2 + (t^2 + 2) d Z^2 + Z^4.
$$

(1.6)

(3) The composition

$$
\psi': C'_{d,t} \xrightarrow{\eta} C''_{d,t} \xrightarrow{\psi''} E_t
$$

in terms of the maps $\eta$ and $\psi''$ sending

$$
(z,w) \mapsto \left( -\frac{d}{2t} \frac{z^2}{(w^2 - d)}, \frac{d}{2t} \frac{z^2 (w^2 + d)}{(w^2 - d)^2} \right), \quad (Z,W) \mapsto \left( \frac{d}{Z^2}, -\frac{d W}{Z^4} \right);
$$

(1.7)

satisfy the congruence $\delta'(\psi'(P)) \equiv d \mod (\mathbb{Q}^\times)^4$.

I mention that the article [4] outlines a similar algorithm using a 4-descent by considering a diagram such as

$$
0 \longrightarrow \frac{E(Q)}{4E(Q)} \longrightarrow S^{(4)}(E/Q) \longrightarrow \text{III}(E/Q)[4] \longrightarrow 0
$$

(1.9)

$$
0 \longrightarrow \frac{E(Q)}{2E(Q)} \longrightarrow S^{(2)}(E/Q) \longrightarrow \text{III}(E/Q)[2] \longrightarrow 0
$$

(I have learned that Tom Womack is working on implementation of a similar algorithm for a future version of MAGMA.) The paper at hand may be considered a refinement of this algorithm, even though I present the algorithm for a limited family of elliptic curves possessing a 4-isogeny.

I am motivated to implement such an algorithm by the search for elliptic curves $E_t$ with $T \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ having “large” rank. In [2], there is an elliptic curve with rank 3 corresponding to $r = 15/76$. Moreover, the author, along with Garikai Campbell, conjectured that if

$$
r \in \left\{ \frac{15}{56}, \frac{24}{65}, \frac{11}{69}, \frac{7}{88}, \frac{12}{97} \right\}
$$

(1.10)
then \( E_t(\mathbb{Q}) \) will have rank at least 4. Randall Rathbun has informed me that if we assume the validity of the conjectures of Birch and Swinnerton-Dyer then our conjecture is false; in fact the curves have rank not greater than 2. This is apparently because the Shafarevich-Tate groups in the sequence

\[
0 \longrightarrow \text{III}(E_t/\mathbb{Q})[\phi] \longrightarrow \text{III}(E_t/\mathbb{Q})[4] \longrightarrow \text{III}(E'_t/\mathbb{Q})[\hat{\phi}] \longrightarrow 0
\]

are quite large. Explicitly, for these five values of \( r \) we have \( \#\text{III}(E'_t/\mathbb{Q})[\hat{\phi}] \geq 2^4 \).

The authors would like to thank Garikai Campbell, John Cremona, Lloyd Kilford, William Stein, and Randall Rathbun for helpful conversations.

### Contents

1. Introduction 1
2. Descent via Four-Isogeny 3
   2.1. The 4-Isogeny 3
   2.2. The Isogenous Curve 4
   2.3. The Connecting Homomorphism 6
   2.4. The Weil-Châtelet Group 8
   2.5. Selmer and Shafarevich-Tate Groups 9
   2.6. Complete Descent via 4-Isogeny 10
3. Descent via Two-Isogeny 10
   3.1. The 2-Isogenies 11
   3.2. Complete Descent via 2-Isogeny 12
   3.3. Modified Descent via 4-Isogeny 13
4. Examples 14
   4.1. Example: \( T \simeq \mathbb{Z}/4\mathbb{Z} \) 14
   4.2. Example: \( T \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \) 15
   4.3. Example: \( T \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \) 16
References 19

2. Descent via Four-Isogeny

For this section, we fix \( t \in \mathbb{Q}^\times \) and drop the notation involving \( t \).

2.1. The 4-Isogeny. We begin by explicitly describing the 4-isogeny and the isogenous elliptic curve.

**Proposition 2.1.** The elliptic curve \( E_t \) is rationally equivalent to

\[
E : \quad y^2 + x y + a y = x^3 + a x^2 \quad \text{where} \quad a = -\frac{1}{4t^2}, \quad [4] (0, 0) = \mathcal{O};
\]

and is 4-isogenous to the elliptic curve

\[
E' : \quad Y^2 + X Y + A Y = X^3 + A X^2 \quad \text{where} \quad A = \frac{t^2 + 4}{64}.
\]

Moreover, the isogeny \( \phi : E \to E' \) sends \( (0, 0) \to \mathcal{O} \).
One can easily show that any rational elliptic curve with a rational point of order 4 is birationally equivalent to a curve in the form above for some \( a \in \mathbb{Q}^\times \). Indeed, see Exercise 8.13(a) as well as pg. 217. The condition \( \sqrt{-a} \in \mathbb{Q}^\times \) is special to simplify the formulas to follow.

**Proof.** Starting with the curve \( u^2 = u^3 + (t^2 + 2)u^2 + u \), make the substitution

\[
x = \frac{u + 1}{4t^2} \quad \text{and} \quad y = \frac{v - tu}{8t^3} \implies (-1, t) \mapsto (0, 0).
\]

Then \( E \) has the Weierstrass equation above. Following the ideas in [8] we produce an isogeny \( \phi : E \to E' \) such that the cyclic subgroup

\[
E[\phi] = \{ (0, 0), (-a, 0), (0, -a), \mathcal{O} \}
\]

is the kernel. We choose such a map that sends \((x, y) \mapsto (X, Y)\) in terms of

\[
X = -A + \left(\frac{t(x + 2a)(2y + x + a)}{8x(x + a)}\right)^2,
\]

\[
Y = X^2 - (x + a)^2 \left(\frac{(2y + x + a) - 2tx(x + 2a)}{8x(x + a)}\right)^4.
\]

The new curve \( E' \) has a rational point of order 4, but we choose the dual isogeny \( \hat{\phi} : E' \to E \) such that

\[
E'[\hat{\phi}] = \left\{ \left( -2A, A \frac{2 + it}{4} \right), (-A, 0), \left( -2A, A \frac{2 - it}{4} \right), \mathcal{O} \right\}
\]

where \( i = \sqrt{-1} \). This map sends \((x, y) \mapsto (x, y)\) in terms of

\[
x = -a + \left( \frac{X(2Y + X + A)}{2t(X + A)(X + 2A)} \right)^2,
\]

\[
y = x^2 - \left( \frac{2(X + 2A)(2Y + X + A) - tX(X + A)}{4t(X + A)(X + 2A)} \right)^4.
\]

One checks that \( \hat{\phi} \circ \phi = [4] \) is the “multiplication-by-4” map on \( E \), while \( \phi \circ \hat{\phi} = [4] \) is the “multiplication-by-4” map on \( E' \).

### 2.2. The Isogenous Curve.

The following proposition shows how the size of \( E(\mathbb{Q})/4E(\mathbb{Q}) \) is related to the size of \( E(\mathbb{Q})/\phi(E'(\mathbb{Q})) \).

**Proposition 2.2.** Let \( \phi : E \to E' \) be the isogeny in Proposition 2.1 and \( \hat{\phi} : E' \to E \) denote its dual.

1. The following sequence is exact if and only if \( \sqrt{t^2 + 4} \in \mathbb{Q}^\times \):

\[
0 \longrightarrow \frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} \overset{\phi}{\longrightarrow} \frac{E(\mathbb{Q})}{4E(\mathbb{Q})} \overset{\phi}{\longrightarrow} \frac{E(\mathbb{Q})}{\phi(E'(\mathbb{Q}))} \longrightarrow 0.
\]

2. Both \( E(\mathbb{Q}) \) and \( E'(\mathbb{Q}) \) have the same rank.

3. The torsion subgroup \( T' \) of \( E'(\mathbb{Q}) \) is \( \mathbb{Z}/8\mathbb{Z} \) when \( \sqrt{t + \sqrt{t^2 + 4}} \in \mathbb{Q}^\times \), and \( \mathbb{Z}/4\mathbb{Z} \) otherwise.

**Proof.** The dual isogeny induces the exact sequence

\[
0 \longrightarrow \frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} \overset{\phi}{\longrightarrow} \frac{E(\mathbb{Q})}{\phi(E(\mathbb{Q}))} \longrightarrow \frac{E(\mathbb{Q})}{4E(\mathbb{Q})} \longrightarrow \frac{E(\mathbb{Q})}{\phi(E'(\mathbb{Q}))} \longrightarrow 0.
\]
We compute the first term in this sequence. From above, \( E'(\mathbb{Q})[\hat{\phi}] = \{(-A,0), \mathcal{O}\} \) has order 2. \( E[4] \) is generated by \( P = (0,0) \) and

\[
(2.10) \quad Q = \left( -\frac{2a}{1+\alpha}, \frac{8a^3}{(1+\alpha)^2(1+i\alpha)} \right) \quad \text{where} \quad \alpha = \sqrt[4]{\frac{t^2+4}{t^2}}.
\]

One verifies that \( \phi(P) = \mathcal{O} \) while \( \phi([2]Q) = (-A,0) \). Clearly \( Q \not\in E(\mathbb{Q})[4] \), while

\[
(2.11) \quad [2]Q = \left( -\frac{1+\alpha^2}{8}, \frac{(1+\alpha^2)^2}{32} \right) \in E(\mathbb{Q})[4] \iff \sqrt{t^2+4} \in \mathbb{Q}^\times.
\]

Hence \( E'(\mathbb{Q})[\hat{\phi}] = \phi(E(\mathbb{Q})[4]) \) if and only if \( t^2 + 4 \) is a square.

Second, the statement that isogenous elliptic curves have the same rank is well-known: As \( E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \) is finite the rank of \( E'(\mathbb{Q}) \) cannot be greater than the rank of \( E(\mathbb{Q}) \). Similarly, \( E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q})) \) is finite so we must have equality with the rank.

As for the torsion, it is easy to see that \((0,0) \in E'(\mathbb{Q}) \) is a rational point of order 4. By Mazur's Theorem, either \( E'[2] \subseteq E'(\mathbb{Q}) \) or else the torsion subgroup is of the form \( \mathbb{Z}/4n\mathbb{Z} \) for \( n = 1, 2, 3 \). We begin by showing that not all of the 2-torsion is rational. The points \( (X,Y) \) of order 2 satisfy \( 2Y + X + A = 0 \), so that

\[
(2.12) \quad (X + A) \left( 4X^2 + X + A \right) = -4 \left( Y^2 + XY + AY - X^3 - AX^2 \right) = 0.
\]

\((-A,0)\) is one rational point of order 2 corresponding to the linear factor, but the quadratic factor has discriminant \(-1\) so that polynomial has no rational roots.

Next we show that there are no rational points of order 3. Assume that \( (X,Y) \) is such a point. One computes that the 3-division polynomial of \( E' \) is

\[
(2.13) \quad \psi_3(X,t) = 3X^4 + (1 + 4A)X^3 + 3AX^2 + 3A^2X + A^3.
\]

We make the substitution

\[
(2.14) \quad \sigma = -\frac{3X + 4A}{X} \quad \text{and} \quad \tau = \frac{3X + 4A}{X + 2A}t.
\]

Note that \( X(X+2A) \neq 0 \) because otherwise \( (X,Y) \) would be a point of order 4. Also, \( 3X + 4A \neq 0 \): if not, then \( (X,Y) = (-A\beta/3, -A\beta/9) \) in terms of a root of the quadratic \( \beta^2 + 3\beta + 48A \). However, this quadratic has discriminant \(-3(t^2+1)\) which is not a square, so \( (X,Y) \) is not a rational point. Hence \( \sigma \) and \( \tau \) are well-defined and nonzero. Solving for \( X \) and \( t \) transforms the 3-division polynomial as

\[
(2.15) \quad \psi_3 \left( -\frac{4A}{\sigma + 3}, \frac{\tau(\sigma + 1)}{2\sigma} \right) = \frac{A^3(\sigma + 1)^2}{\sigma(\sigma + 3)^4} \left[ \tau^2 - \sigma(\sigma + 1)(\sigma - 3) \right]
\]
so that \((\sigma, \tau)\) is a rational point on the elliptic curve \( \tau^2 = \sigma(\sigma + 1)(\sigma - 3) \). However, one checks that the only such (affine) rational points satisfy \( \tau = 0 \), a contradiction.

Finally, we are in the case where we distinguish between \( \mathbb{Z}/4\mathbb{Z} \) and \( \mathbb{Z}/8\mathbb{Z} \). Say that \( R = (X,Y) \) is a rational point of order 8. Then \( [2]R \) is a point of order 4, so without loss of generality say \( [2]R = P \). By considering the \( X \)-coordinates we have

\[
(2.16) \quad X([2]R) = \frac{X^4 - A(X + A)}{(X + A)(4X^2 + X + A)} = 0 \quad \implies \quad X^2 - \sqrt{A}(X + A) = 0.
\]
Hence $\sqrt{A} \in \mathbb{Q}^\times$. In fact, make the substitution

$$\gamma = \sqrt{t + \sqrt{t^2 + 4}} \quad \Rightarrow \quad t = \frac{\gamma^4 - 4}{2 \gamma^2} \quad \text{and} \quad A = \left(\frac{\gamma^4 + 4}{16 \gamma^2}\right)^2.$$  \hfill (2.17)

The discriminant of the quadratic $X^2 - \sqrt{A}(X + A)$, namely $\gamma^2$, must be a square since its roots are rational; hence $\gamma \in \mathbb{Q}^\times$. Then the rational point of order 8 is

$$R = \left(\frac{(\gamma^4 + 4)(\gamma^2 + 2\gamma + 2)}{64 \gamma^3}, \frac{(\gamma^4 + 4)(\gamma^2 + 2\gamma + 2)}{1024 \gamma^5}\right).$$  \hfill (2.18)

The converse is clear i.e. if $[8]R = \mathcal{O}$ then $\sqrt{t + \sqrt{t^2 + 4}} \in \mathbb{Q}^\times$. \hfill $\square$

2.3. The Connecting Homomorphism. There is a natural bijection between the crossed homomorphisms $H^1\left(\text{Gal}(\mathbb{Q}/\mathbb{Q}), E\right)$ and $WC\left(E/\mathbb{Q}\right)$, the collection of equivalence classes of homogeneous spaces for $E$, usually called the Weil-Châtelet group. We will find it more convenient to work with the isogenous curve $E'$: The exact sequence

$$0 \longrightarrow E'[\hat{\phi}] \longrightarrow E' \xrightarrow{\hat{\phi}} E \longrightarrow 0$$  \hfill (2.19)

implies, through Galois cohomology, the exact sequence

$$0 \longrightarrow \frac{E(\mathbb{Q})}{\hat{\phi}(E'(\mathbb{Q}))} \xrightarrow{\delta_E} H^1\left(\text{Gal}(\mathbb{Q}/\mathbb{Q}), E'[\hat{\phi}]\right) \longrightarrow WC\left(E'/\mathbb{Q}\right)$$  \hfill (2.20)

via the connecting homomorphism $\delta_E$. We make such a homomorphism explicit by considering a generalization of the Weil pairing.

**Proposition 2.3.**

1. There is a pairing $e_\phi : E'[\hat{\phi}] \times E[\hat{\phi}] \rightarrow \mu_4$ that is bilinear, alternating, non-degenerate, and Galois invariant; which satisfies

$$e_\phi(T', T) = \sqrt{-1} \quad \text{when} \quad T' = \left(-2A, \frac{2 + \sqrt{-1}t}{4}\right), \quad T = (0, 0).$$  \hfill (2.21)

2. The pairing $b : E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q})) \times E[\hat{\phi}] \rightarrow \mathbb{Q}^\times/(\mathbb{Q}^\times)^4$ defined by

$$\left((x, y), [m](0, 0)\right) \mapsto \begin{cases} a^{-m} & (x, y) = (0, 0), \\ (x^2 - y)^m & \text{otherwise;} \end{cases}$$  \hfill (2.22)

is bilinear and non-degenerate on the left.

3. Upon identifying $E'[\hat{\phi}] \simeq \mu_4$ as $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules we have

$$H^1\left(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), E'[\hat{\phi}]\right) \simeq \mathbb{Q}^\times/(\mathbb{Q}^\times)^4.$$  \hfill (2.23)

4. The composition of these maps

$$\frac{E(\mathbb{Q})}{\hat{\phi}(E'(\mathbb{Q}))} \times E[\hat{\phi}] \xrightarrow{b} \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^4} \xrightarrow{\delta_0} H^1\left(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), E'[\hat{\phi}]\right)$$  \hfill (2.24)

relates the connecting homomorphisms by

$$e_\phi(\delta_E(P)(\sigma), T) = \delta_Q\left(b(P, T)\right)(\sigma) \quad \text{for all} \quad \sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}).$$  \hfill (2.25)

In particular, we may identify $\delta_E : P \mapsto \delta_Q\left(b(P, T)\right)$ when $T = (0, 0)$. 

\text{\textbf{In particular, we may identify $\delta_E : P \mapsto \delta_Q\left(b(P, T)\right)$ when $T = (0, 0)$.}}
Proof: We follow the construction of the Weil pairing in [7, §8, pgs. 95–99], but we make the formulas explicit. Consider the function \( f \in \mathbb{Q}(E) \) defined as
\[
 f(x, y) = x^2 - y. 
\]
One checks that
\[
x^2 - y = 0 \implies x^4 = y^2 + xy + ay - x^3 - ax^2 = 0 \implies (x, y) = (0, 0); 
\]
so that the divisor of this function is \( \text{div}(f) = 4((0, 0)) - 4(\mathcal{O}) \). Similarly, we consider the function \( g \in \mathbb{Q}(E') \) defined by
\[
g(X,Y) = \frac{2(2X + A) (2Y + X + A) - tX(X + A)}{4t(X + A)(X + 2A)}; 
\]
the formulas in (2.27) show that \( f \circ \hat{\phi} = g^4 \). For \( P' \in E'({\overline{\mathbb{Q}}}) \) and \( T' \in E'[\hat{\phi}] \) we have
\[
g(P' \oplus T')^4 = f \left( \hat{\phi}(P') \oplus \hat{\phi}(T') \right) = f \left( \hat{\phi}(P') \oplus \mathcal{O} \right) = g(P')^4. 
\]
We define the pairing \( e_\phi : E'[\hat{\phi}] \times E[\hat{\phi}] \rightarrow \mu_4 \) by
\[
e_\phi(T', T) = \left( \frac{g(P' \oplus T')}{g(P')} \right)^m \text{ where } T = [m](0, 0). 
\]
The bilinear, alternating, non-degenerate, and Galois invariant properties follow from the arguments given in [7, §8, pgs. 95–99]. In particular, one verifies that
\[
 T' = \left( -2A, A \frac{2 + \sqrt{-1}t}{4} \right), \quad T = (0, 0) \implies e_\phi(T', T) = \frac{g(P' \oplus T')}{g(P')} = \sqrt{-1}. 
\]
Consider the map \( b : E(\mathbb{Q}) \times E[\hat{\phi}] \rightarrow \mathbb{Q}^\times/(\mathbb{Q}^\times)^4 \). First we show it is well-defined. As shown above, \( x^2 - y = 0 \) if and only if \( (x, y) = (0, 0) \). On the other hand, we have by assumed bilinearity
\[
b\left( (0, 0), [m](0, 0) \right) = b\left( [-1](0, 0), [m](0, 0) \right)^{-1} = a^{-m}. 
\]
Now we show that this map can be extended to the quotient. When \( (x, y) = \hat{\phi}(X,Y) \) then \( x^2 - y \) is a fourth-power by (2.27) so that the map extends to a well-defined map \( b : E(\mathbb{Q})/\hat{\phi}(E(\mathbb{Q})) \times E[\hat{\phi}] \rightarrow \mathbb{Q}^\times/(\mathbb{Q}^\times)^4 \). The fact that \( b \) is a non-degenerate pairing follows from the same arguments as with the Weil pairing above.

Fix \( d \in \mathbb{Q}^\times \), and consider the map \( \xi : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow E'[\hat{\phi}] \) defined by
\[
\xi : \quad \sigma \mapsto \xi_\sigma = [m]\left( -2A, A \frac{2 + \sqrt{-1}t}{4} \right) \quad \text{whenever} \quad \frac{\sigma(\sqrt{d})}{\sqrt{d}} = (-1)^{m/2}. 
\]
The map \( \xi \) is a 1-cocycle, so has a cohomology class \( \{\xi\} \in H^1\left( \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), E'[\hat{\phi}] \right) \).

Identify translation by this point with the Galois action i.e. \( (X,Y)^\sigma = (X,Y) \oplus \xi_\sigma \).

From the map \( d \mapsto d^4 \) we find the well-known Kummer sequence
\[
(2.33) \quad 1 \longrightarrow E'[\hat{\phi}] \simeq \mu_4 \longrightarrow \mathbb{Q}^\times \longrightarrow \mathbb{Q}^\times \longrightarrow 1 \quad \text{of Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\text{-modules}, \text{so from Galois cohomology we find the exact sequence} 
\]
\[
(2.34) \quad 1 \longrightarrow \mathbb{Q}^\times/(\mathbb{Q}^\times)^4 \overset{\delta_\xi}{\longrightarrow} H^1\left( \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), E'[\hat{\phi}] \right) \longrightarrow H^1\left( \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathbb{Q}^\times \right), 
\]
where \( \delta_\xi : d \mapsto \{\xi\} \). Hilbert’s Theorem 90 states the last term is trivial; hence the third part of the proposition holds.
To show the fourth part of the proposition, fix \( P \in E(\mathbb{Q}) \), choose \( P' \in E'(\overline{\mathbb{Q}}) \) satisfying \( P = \hat{\phi}(P') \), and denote \( \xi = \delta_E(P) \). For any \( \sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \) we have

\[
e_{\phi}(\delta_E(P)(\sigma), T) = e_{\phi}(\xi_{\sigma}, [m]|(0, 0)) = \left( \frac{g(P' \oplus \xi_{\sigma})}{g(P')} \right)^m = \left( \frac{g(P')^{\sigma}}{g(P')} \right)^m = (\delta_{Q}(d)(\sigma))^m = \delta_{Q}(b(P, T))(\sigma).
\]

where we have identified \( E'[\phi] \simeq \mu_4 \) and set \( d = f(P) \equiv b(P, (0, 0)) \).

2.4. The Weil-Châtelet Group. The full collection of homogeneous spaces in the Weil-Châtelet group is too large for interest in this exposition, so instead we consider the image \( WC(E'/\mathbb{Q})[\phi] \) of the crossed homomorphisms studied above. Recall that \( WC(E'/\mathbb{Q}) \) consists of equivalence classes \( \{C'/\mathbb{Q}\} \) of certain rational curves, where a class is trivial if and only if \( C'(\mathbb{Q}) \) is nonempty.

**Proposition 2.4.**

1. The composite map

\[
\frac{\mathbb{Q}^*}{(\mathbb{Q}^*)^4} \xrightarrow{\delta_i} H^1 \left( \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), E'[\phi] \right) \longrightarrow WC(E'/\mathbb{Q})
\]

sends \( d \mapsto \{C_d'/\mathbb{Q}\} \), where

\[
C_d': \quad d (w + a z^2) z^2 = (w^2 - d)^2.
\]

2. There is an isomorphism \( \theta : C_d' \xrightarrow{\bar{\theta}} E' \) defined over \( \overline{\mathbb{Q}} \) such that

\[
\psi': \quad C_d' \xrightarrow{\bar{\theta}} E' \xrightarrow{\hat{\phi}} E, \quad (z, w) \mapsto \left( \frac{w}{z^2}, \frac{w^2 - d}{z^4} \right).
\]

**Proof.** We construct a homogeneous space corresponding the cohomology class \( \{\xi\} \in H^1 \left( \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), E'[\phi] \right) \) following the exposition in [1, §3, pgs. 287 - 296]. Fix \( d \in \mathbb{Q}^* \), and consider the functions \( z, w \in \overline{\mathbb{Q}}(E') \) defined implicitly by

\[
z = \frac{\sqrt{d}}{g(P')} \quad \text{and} \quad \frac{1}{z} = \frac{1}{w} = \frac{1}{g([-1]P')} \quad \text{where} \quad P' = (X, Y).
\]

It is easy to check that the point \((z, w)\) is on \( C_d' \) as defined above. We show these functions are Galois invariant. To this end, choose \( \sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \), and say that \( \sigma(\sqrt{d}) = (-1)^{m/2} \sqrt{d} \). For any integer \( n \) we have

\[
\sigma \left( \frac{\sqrt[n]{P'}}{g([n]P')} \right) = (-1)^{mn/2} \frac{\sqrt[n]{P'}}{g([n]P')},
\]

where \( T' = [n] \xi_{\sigma} \) and \( T = (0, 0) \). It follows from Proposition 2.3 that \( e_{\phi}(T', T) = (-1)^{mn/2} \). Hence the equations defining \( z \) and \( w \) are Galois invariant, so that \( z \) and \( w \) themselves are Galois invariant.

This defines a map \( E' \rightarrow C_d' \) sending \((X, Y) \mapsto (z, w)\) in terms of

\[
z = \sqrt{d} \frac{4t(X + A)(X + 2A)}{2(X + 2A)(2Y + X + A) - tX(X + A)}, \quad w = \sqrt{d} \frac{2(X + 2A)(2Y + X + A) + tX(X + A)}{2(X + 2A)(2Y + X + A) - tX(X + A)}.
\]
The inverse map \( \theta : C'_d \to E' \) – which can be found by considering \( g(P') \pm g([-1]P') \) – sends \((z, w) \mapsto (X, Y)\) in terms of
\[
(2.42) \quad X = 4A \frac{w - \sqrt{d}}{\sqrt{d}z - 2(w - \sqrt{d})}, \quad Y = (X + A) \frac{-\sqrt{d}z + t(w + \sqrt{d})}{2 \sqrt{d}z}.
\]

One checks using the formulas in (2.7) that the composition \( \psi = \hat{\phi} \circ \theta \) is the map \((z, w) \mapsto (w/z^2, (w^2 - d)/z^4)\). \(\square\)

### 2.5. Selmer and Shafarevich-Tate Groups

Combining the exact sequences introduced above, we have the exact diagram

\[
\begin{array}{ccccccccc}
0 & \longrightarrow & E'(\mathbb{Q}) & \longrightarrow & S^{(\phi)}(E/\mathbb{Q}) & \longrightarrow & \mathbb{II}(E/\mathbb{Q}) & \longrightarrow & 0 \\
& & \phi \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E(\mathbb{Q}) & \longrightarrow & S^{(4)}(E/\mathbb{Q}) & \longrightarrow & \mathbb{II}(E/\mathbb{Q})[4] & \longrightarrow & 0 \\
& & \phi \downarrow & & \downarrow & & \phi \downarrow & & \\
0 & \longrightarrow & E(\mathbb{Q}) & \longrightarrow & S^{(\hat{\phi})}(E'/\mathbb{Q}) & \longrightarrow & \mathbb{II}(E'/\mathbb{Q})[\hat{\phi}] & \longrightarrow & 0 \\
& & \phi \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & 0
\end{array}
\]

where the Selmer and Shafarevich-Tate groups are defined as
\[
(2.44) \quad S^{(\phi)}(E/\mathbb{Q}) = \ker \left\{ H^1(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), E[\phi]) \to \prod_{\nu} WC(E/\mathbb{Q}_{\nu}) \right\};
\]
\[
\quad \mathbb{II}(E/\mathbb{Q}) = \ker \left\{ WC(E/\mathbb{Q}) \to \prod_{\nu} WC(E/\mathbb{Q}_{\nu}) \right\};
\]

taking the product over all places \(\nu\) of \(\mathbb{Q}\). One can compute the rank of \(E(\mathbb{Q})\) with the explicit map in Proposition 2.3 – assuming that \(\mathbb{II}(E'/\mathbb{Q})[\hat{\phi}]\) is trivial.

**Proposition 2.5.** Let \(\Sigma\) be the finite set of places of \(\mathbb{Q}\) consisting of \(2, \infty\), and those primes occurring in the factorization of \(t\) and \(t^2 + 4\). We have
\[
(2.45) \quad S^{(\hat{\phi})}(E'/\mathbb{Q}) \simeq \left\{ d = \pm \prod_{p \in \Sigma} p^{\nu_p} \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^4 \mid C'_d(\mathbb{Q}_{\nu}) \neq \emptyset \text{ for all } \nu \in \Sigma \right\},
\]
\[
\quad \mathbb{II}(E'/\mathbb{Q})[\hat{\phi}] \simeq \left\{ \{C'_d/\mathbb{Q}\} \in WC(E'/\mathbb{Q})[\hat{\phi}] \mid C'_d(\mathbb{Q}_{\nu}) \neq \emptyset \text{ for all } \nu \in \Sigma \right\}.
\]

**Proof.** We may identify the Selmer group with a subgroup of \(\mathbb{Q}/(\mathbb{Q}^\times)^4\) by the isomorphism in Proposition 2.3. The subgroup \(WC(E'/\mathbb{Q})[\hat{\phi}] \subseteq WC(E'/\mathbb{Q})\) consists of the equivalence classes \(\{C'_d/\mathbb{Q}\}\). By definition, a class \(\{C'_d/\mathbb{Q}\} \in WC(E'/\mathbb{Q})\) is trivial if and only if \(C'_d(\mathbb{Q}_{\nu})\) is nonempty. \(\square\)
2.6. Complete Descent via 4-Isogeny. We collect the results proved thus far into one statement.

**Theorem 2.6.** Fix $t \in \mathbb{Q}^\times$, and let $E_t$ and $E'_t$ denote the elliptic curves

\[(2.46) \quad E_t : \quad v^2 = u^3 + (t^2 + 2) u^2 + u, \quad E'_t : \quad V^2 = U^3 - 2 (t^2 - 4) U^2 + (t^2 + 4)^2 U.\]

1. There is an isogeny $\phi : E_t \to E'_t$ of degree 4 with kernel generated by $(-1, t)$.
2. Upon identifying the Selmer and Shafarevich-Tate groups as in Proposition 2.5, there is an exact sequence

\[(2.47) \quad 0 \to E_t(\mathbb{Q}) \xrightarrow{\delta} S(\hat{\phi}(E'_t/\mathbb{Q})) \to \text{III}(E'_t/\mathbb{Q})[\hat{\phi}] \to 0\]

where $\delta$ sends $[m] (-1, t) \mapsto (-4 t^2)^m$ and $(u, v) \mapsto u^2 + 2 (t^2 + 1) u + 1 - 2 t v$ otherwise; while the second map sends $d \mapsto \{C'_{d,t}/\mathbb{Q}\}$ in terms of

\[(2.48) \quad C'_{d,t} : \quad d \left( - \frac{z^2}{4 t^2} \right) z^2 = (w^2 - d)^2.\]

3. The map $\psi' : C'_{d,t} \to E_t$ sending

\[(2.49) \quad (z, w) \mapsto \left( \frac{4 t^2 (w^2 - d)^2}{d z^4}, \frac{4 t^3 (w^2 - d) (w^2 + d)}{d z^4} \right)\]

satisfies the congruence $\delta' \left( \psi'(P) \right) \equiv d \pmod{(\mathbb{Q}^\times)^4}$.

**Proof.** The curves $E_t$ and $E'_t$ are related to $E$ and $E'$ by the transformation

\[(2.50) \quad x = \frac{u + 1}{4 t^2}, \quad y = \frac{v - t u}{8 t^3} \quad \text{and} \quad X = \frac{U - (t^2 + 4)}{64}, \quad Y = \frac{V - 4 U}{512}.\]

The first statement follows from Proposition 2.4. The image of $\delta$ in the second statement follows from Proposition 2.5, Proposition 2.4, and the congruence

\[(2.51) \quad x^2 - y \equiv (u^2 + 2 (t^2 + 1) u + 1) - 2 t v \pmod{(\mathbb{Q}^\times)^4};\]

while the image of the second map follows from Proposition 2.4. The third statement follows from Proposition 2.4 where we write the map $\psi'$ in terms of $u$ and $v$ rather than $x$ and $y$. From the identity

\[(2.52) \quad (u, v) = \psi'(z, w) \Rightarrow (u^2 + 2 (t^2 + 1) u + 1) - 2 t v = d \left( \frac{2 t}{z} \right)^4\]

we find the congruence $(u^2 + 2 (t^2 + 1) u + 1) - 2 t v \equiv d \pmod{(\mathbb{Q}^\times)^4}$. \(\square\)

3. Descent via Two-Isogeny

The descent algorithm associated to the rational point of order 4 described in the previous section can be refined to exploit the 2-isogeny coming from the doubling of this point.
3.1. The 2-Isogenies. We begin by factoring the 4-isogeny.

**Proposition 3.1.** Let $\phi : E \to E'$ as in Proposition 2.1 and denote the curve

$$E'' : \quad v^2 = u^2(u - 4)(u + t^2).$$

There exist rational 2-isogenies $\varphi : E \to E''$ and $\eta : E' \to E''$ such that $\phi = \hat{\eta} \circ \varphi$.

**Proof.** The isogeny $\phi$ and the “multiplication-by-2” map on $E$ induce the following exact diagram:

$$\begin{array}{cccccc}
0 & 0 & 0 & 0 \\
\downarrow & \downarrow & \downarrow & \downarrow \\
0 & \to E[\phi] \cap E[2] \to E[2] \to \phi(E[2]) \to 0 \\
\downarrow & \downarrow & \downarrow & \downarrow \\
0 & \to E[2] \to E \to E' \simeq E/E[\phi] \to 0 \\
\downarrow & \downarrow & \downarrow & \downarrow \\
0 & \to 2E[\phi] \to E \to E'' := E/2E[\phi] \to 0 \\
\downarrow & \downarrow & \downarrow & \downarrow \\
0 & 0 & 0 & 0
\end{array}$$

We will construct isogenies $\varphi : E \to E''$ and $\eta : E' \to E''$ with kernels

$$(3.3) \quad E[\varphi] = 2E[\phi] = \{(a, 0), \mathcal{O}\} \quad \text{and} \quad E'[\eta] = \phi(E[2]) = \{(-A, 0), \mathcal{O}\}.$$ 

To this end, assume without loss of generality that $E = E_t$ and $E' = E'_t$ as in Theorem 2.6, where now $(u, v) = (0, 0)$ and $(U, V) = (0, 0)$ are the rational points of order 2. Following the exposition in [7], we define the isogenies

$$(3.4) \quad \varphi : E \to E'', \quad (u, v) \mapsto \left(\frac{u + 1}{u}, \frac{1 - u^2}{u^2}v\right);$$

$$(3.5) \quad \eta : E' \to E'', \quad (U, V) \mapsto \left(\frac{V^2}{4U^2}, \frac{(t^2 + 4)^2 - U^2}{8U^2}V\right);$$

with dual isogenies

$$(3.6) \quad \hat{\varphi} : E'' \to E, \quad (u, v) \mapsto \left(\frac{v^2}{4(u + t^2)^2}, \frac{-4t^2 + 2t^2u + u^2}{8(u + t^2)^2}v\right);$$

$$(3.7) \quad \hat{\eta} : E'' \to E', \quad (u, v) \mapsto \left(\frac{v^2}{u^2}, \frac{-4t^2 - u^2}{u^2}v\right).$$

One checks that $\hat{\varphi} \circ \varphi = \{2\}$ and $\hat{\eta} \circ \eta = \{2\}$ are the “multiplication-by-2” maps on $E$, and $E'$, respectively. Moreover, one checks that $\phi = \hat{\eta} \circ \varphi$ and $\hat{\phi} = \hat{\varphi} \circ \eta$.

□
3.2. Complete Descent via 2-Isogeny. The previous proposition implies the following exact diagram as a refinement of the diagram in (2.43):

\[
\begin{array}{c}
0 \quad 0 \quad 0 \\
\downarrow \quad \downarrow \quad \downarrow \\
E''(\mathbb{Q})[\hat{\varphi}] \quad \eta(E''(\mathbb{Q})[\hat{\varphi}]) \\
\varphi \downarrow \quad \downarrow \quad \downarrow \\
E''(\mathbb{Q}) \quad \eta(E''(\mathbb{Q})) \\
\varphi \downarrow \quad \downarrow \quad \downarrow \\
E(\mathbb{Q}) \quad \phi(E''(\mathbb{Q})) \\
\delta \downarrow \quad \downarrow \quad \downarrow \\
S(\phi)(E''/\mathbb{Q}) \quad \eta \downarrow \\
\varphi \downarrow \quad \downarrow \quad \downarrow \\
S(\phi)(E''/\mathbb{Q}) \quad \eta \downarrow \\
0 \quad 0 \quad 0
\end{array}
\]

The first (nontrivial) row in the diagram above comes from the explicit relation

\[
E''(\mathbb{Q})[\hat{\varphi}] = \{(-t^2,0), \mathcal{O}\} \quad \text{yet} \quad (u,v) = \eta(U, V) \implies u = \frac{V^2}{4U^2} > 0;
\]

while the second and fourth rows are related to a descent via 2-isogeny. We recall the main results for the latter:

**Proposition 3.2.** Fix \( t \in \mathbb{Q}^\times \), denote \( E_t \) as in Theorem 2.6, and denote \( E''_t \) as in Proposition 3.1.

(1) There is an exact sequence

\[
\begin{array}{c}
0 \quad \to \quad E_t(\mathbb{Q})[\hat{\varphi}] \\
\varphi \downarrow \quad \downarrow \\
E_t(\mathbb{Q}) \quad \phi(E''(\mathbb{Q})) \\
\delta \downarrow \quad \downarrow \\
S(\phi)(E''/\mathbb{Q}) \quad \eta \downarrow \\
\varphi \downarrow \quad \downarrow \\
S(\phi)(E''/\mathbb{Q}) \quad \eta \downarrow \\
0 \quad 0 \quad 0
\end{array}
\]

where \( \delta'' \) sends \([m](0,0) \mapsto (t^2 + 2)^m\) and \((u,v) \mapsto u\) otherwise; while the second map sends \( d \mapsto \{C''_{d,t}/\mathbb{Q}\} \) in terms of

\[
C''_{d,t} : \quad dW^2 = d^2 + (t^2 + 2) dZ^2 + Z^4.
\]

(2) The map \( \psi' : C''_{d,t} \to E_t \) in Theorem 2.6 factors as the composition

\[
\begin{array}{c}
C''_{d,t} \quad \eta' \quad C''_{d,t} \quad \psi'' \quad E_t \\
\eta \quad \psi'' \quad E_t
\end{array}
\]

where \( \eta' \) and \( \psi'' \) are the maps sending

\[
(z,w) \mapsto \left( -\frac{d}{2t(w^2-d)}, \frac{d}{2(w^2-d)^2} \right), \quad (Z,W) \mapsto \left( \frac{d}{Z^2}, -\frac{dW}{Z^3} \right).
\]
In the Proposition above we identify, as in Proposition \ref{4-IsogenyProp} the Selmer and Shafarevich-Tate groups as

\[
S^{(\phi)}(E''/\mathbb{Q}) \simeq \left\{ d = \pm \prod_{p \in \Sigma} p^{\nu_p} \in \mathbb{Q}_p^\times \left| C''_d(\mathbb{Q}_p) \neq \emptyset \text{ for all } \nu \in \Sigma \right. \right\},
\]

(3.12)

\[
	ext{III}(E''/\mathbb{Q})[\hat{\varphi}] \simeq \left\{ (C''_d/\mathbb{Q}) \in WC(E''/\mathbb{Q})[\hat{\varphi}] \left| C''_d(\mathbb{Q}_p) \neq \emptyset \text{ for all } \nu \in \Sigma \right. \right\}.
\]

Hence by the canonical exact sequence

\[
1 \longrightarrow \left( \frac{\mathbb{Q}_p^\times}{\mathbb{Q}_p^\times} \right)^2 \longrightarrow \left( \frac{\mathbb{Q}_p^\times}{\mathbb{Q}_p^\times} \right)^3 \longrightarrow \left( \frac{\mathbb{Q}_p^\times}{\mathbb{Q}_p^\times} \right)^2 \longrightarrow 1
\]

(3.13)

we may think of $S^{(\phi)}(E'/\mathbb{Q})$ as being a cover of $S^{(\phi)}(E''/\mathbb{Q})$.

**Proof.** The first statement follows from Proposition \ref{4-IsogenyProp} and the results from \cite{7}, so we focus on the second statement. Consider the diagram

\[
\begin{array}{ccc}
C'_{d,t} & \xrightarrow{\theta} & E'_{\ell} \\
\downarrow{\eta} & & \downarrow{\hat{\varphi}} \\
C''_{d,t} & \xrightarrow{\vartheta} & E''_{\ell}
\end{array}
\]

(3.14)

where $\theta$ is the isomorphism in (2.42) and $\vartheta$ is the isomorphism that sends

\[
\vartheta: (Z, W) \mapsto \left( 2 \frac{Z^2 + \sqrt{d} W + d}{Z^2}, 2 \sqrt{d} \frac{(t^2 + 2) Z^2 + 2 \sqrt{d} W + 2 d}{Z^3} \right);
\]

(3.15)

which has the inverse

\[
\vartheta^{-1}: (u, v) \mapsto \left( \sqrt{d} \frac{2 v}{u (u - 4)}, \sqrt{d} \frac{-4 t^2 + 2 t^2 u + u^2}{u (u - 4)} \right).
\]

(3.16)

Define the map $\eta_* : C'_{d,t} \to C''_{d,t}$ by $\eta_* = \vartheta^{-1} \circ \eta \circ \theta$. This gives the composition

\[
\psi'' \circ \eta_* = (\hat{\varphi} \circ \vartheta) \circ (\vartheta^{-1} \circ \eta \circ \theta) = (\hat{\varphi} \circ \eta) \circ \theta = \hat{\varphi} \circ \theta = \psi'.
\]

(3.17)

Moreover, one checks that $\eta_*$ maps $(z, w)$ as above. \hfill \Box

### 3.3. Modified Descent via 4-Isogeny

We present an effective version of the four-descent by using the two-descent. This is the main result of the paper.

**Theorem 3.3.** Fix $t \in \mathbb{Q}_p^\times$, and denote the elliptic curves

\[
\begin{align*}
E_{\ell} : & \quad v^2 = u^3 + (t^2 + 2) u^2 + u, \\
E'_{\ell} : & \quad V^2 = U^3 - 2 (t^2 - 4) U^2 + (t^2 + 4)^2 U, \\
E''_{\ell} : & \quad v^2 = u^3 + (t^2 - 4) u^2 - 4 t^2 u.
\end{align*}
\]

(3.18)

(1) There are isogenies $\phi : E_{\ell} \to E'_{\ell}$ of degree 4 with kernel generated by $(-1, t)$, and $\varphi : E_{\ell} \to E''_{\ell}$ of degree 2 generated by $[2] (-1, t) = (0, 0)$.
(2) Upon identifying the Selmer groups as subgroups of quotients of \( \mathbb{Q}^\times / (\mathbb{Q}^\times)^4 \) and Shafarevich-Tate groups as a collection of homogeneous spaces, there is an exact diagram

\[
\begin{array}{ccccccccc}
0 & \longrightarrow & \hat{E}_t(\mathbb{Q}) & \phi(\hat{E}_t^\prime(\mathbb{Q})) & \delta' & S(\hat{\phi})(E_t^\prime/\mathbb{Q}) & \phi(E_t^\prime(\mathbb{Q})) & \delta'' & S(\hat{\phi})(E_t^\prime/\mathbb{Q}) & \phi(E_t^\prime(\mathbb{Q})) & \longrightarrow & 0 \\
& & \downarrow & & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \hat{E}_t(\mathbb{Q}) & \phi(\hat{E}_t^\prime(\mathbb{Q})) & \delta'' & S(\hat{\phi})(E_t^\prime/\mathbb{Q}) & \phi(E_t^\prime(\mathbb{Q})) & \delta & S(\hat{\phi})(E_t^\prime/\mathbb{Q}) & \phi(E_t^\prime(\mathbb{Q})) & \longrightarrow & 0
\end{array}
\]

where we have the connecting homomorphisms

\[
\begin{align*}
\delta' : & \quad (-1, t) \mapsto -4 t^2 \\
& \quad (u, v) \mapsto u^2 + 2 (t^2 + 1) u + 1 - 2 t v \\
\delta'' : & \quad (0, 0) \mapsto t^2 + 4 \\
& \quad (u, v) \mapsto u
\end{align*}
\]

while the maps into the Shafarevich-Tate groups send \( d \mapsto \{ C_{d,t}^\prime / \mathbb{Q} \} \) and \( d \mapsto \{ C_{d,t}'' / \mathbb{Q} \} \) in terms of

\[
\begin{align*}
C_{d,t}^\prime : & \quad d W^2 = d^2 + (t^2 + 2) d Z^2 + Z^4 \\
C_{d,t}'' : & \quad d W^2 = d^2 + (t^2 + 2) d Z^2 + Z^4
\end{align*}
\]

(3) The composition

\[
\psi : \quad C_{d,t}^\prime \xrightarrow{\eta} C_{d,t}'' \xrightarrow{\psi''} E_t
\]

in terms of the maps \( \eta \) and \( \psi'' \) sending

\[
\begin{align*}
(z, w) & \mapsto \left( \frac{d z^2}{2 t (w^2 - d)}, \frac{d z^2 (w^2 + d)}{2 (w^2 - d)^2} \right) , \\
(Z, W) & \mapsto \left( \frac{d Z^2}{Z^2}, - \frac{d W}{Z^3} \right)
\end{align*}
\]

satisfy the congruence \( \delta' (\psi' (P)) \equiv d \mod (\mathbb{Q}^\times)^4 \).

Note that we abuse notation and write \( \eta \) instead of \( \eta_* \).

**Proof.** This follows directly from Theorem 2.6 and Proposition 3.2. \( \square \)

### 4. Examples

In this section we assume that the elliptic curve \( E \) and its 4-isogenous curve \( E' \) have Weierstrass equations as in Proposition 2.1.

**4.1. Example:** \( \mathbb{T} \cong \mathbb{Z}/4\mathbb{Z} \). Consider \( t = 8 \). Using the ideas in \( \mathbb{Z} \) as well as Proposition 2.2 it is easy to see that the torsion subgroup of both \( E(\mathbb{Q}) \) and \( E'(\mathbb{Q}) \) is \( \mathbb{Z}/4\mathbb{Z} \). In fact, one may use either Cremona’s mwrank or the package MAGMA so see that the Mordell-Weil groups are

\[
\begin{align*}
E(\mathbb{Q}) & \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}, \\
E'(\mathbb{Q}) & \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}, \\
E''(\mathbb{Q}) & \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}.
\end{align*}
\]

We consider the diagram in 3.10 in detail.
Performing a 2-descent with \texttt{mr} \ (recall \ that \ \( \eta : E' \to E'' \) \ and \ \( \hat{\eta} : E'' \to E \) are 2-isogenies) \ one \ computes \ the \ quantities

\[
\frac{E''(Q)}{\eta(E'(Q))} \simeq S^{(n)}(E'/Q) \simeq \{ \pm 1, \pm 2 \}, \quad \text{III}(E'/Q)[\eta] \simeq \{ 0 \};
\]

\[
\frac{E(Q)}{\hat{\eta}(E'(Q))} \simeq S^{(\hat{n})}(E''/Q) \simeq \{ \pm 1 \}, \quad \text{III}(E''/Q)[\hat{\eta}] \simeq \{ 0 \}.
\]

Considering \ the \ diagram \ in \ (4.2), \ we \ see \ that

\[
\frac{E(Q)}{\hat{\phi}(E'(Q))} \simeq S^{(\hat{\phi})}(E''/Q) \simeq \{ \pm 1 \}, \quad \text{III}(E''/Q)[\hat{\phi}] \simeq \{ 0 \}.
\]

Using \ Theorem \ 2.6 \ we \ may \ compute \ generators \ explicitly \ by \ exploiting \ the \ homogeneous \ spaces. \ The \ curves \ \( E \) \ and \ \( E' \) \ both \ have \ conductor \ \( 24 \cdot 17 \) \ so \ that \ they \ have \ good \ reduction \ away \ from \ \( \Sigma = \{ 2, 17, \infty \} \). \ The \ homogeneous \ spaces \ of \ interest \ are \ of \ the \ form

\[
C'_d : \quad d(w + a z^2) z^2 = (w^2 - d)^2, \quad a = -4^d.
\]

When \ \( d = -1 \) \ we \ find \ the \ solution \ \( \( z, w \) = (4, 0) \); \ this \ can \ be \ predicted \ from \ the \ connecting \ homomorphism \ \( \delta' : (0, 0) \mapsto a^{-1} = -1 \). \ When \ \( d = 4 \) \ we \ find \ the \ solution \ \( \( z, w \) = (16, 10) \); \ this \ maps \ to \ the \ point \ of \ infinite \ order

\[
\left( \frac{w}{z^2}, \frac{w^2 - d}{z^2} \right) = \left( \frac{5}{128}, \frac{3}{2048} \right) \in E(Q).
\]

Hence \ \( S^{(\hat{\phi})}(E'/Q) \simeq \{ \pm 1, \pm 4 \} \). \ A \ brief \ search \ shows \ that \ \( -1/2, -3/4 \) \ in \ \( E'(Q) \). \ In \ fact, \ one \ checks \ that

\[
\phi(0, 0) = \mathcal{O}, \quad \phi\left( \frac{5}{128}, \frac{3}{2048} \right) = [2] \left( \frac{1}{2}, \frac{3}{4} \right);
\]

\[
\hat{\phi}(0, 0) = [2] (0, 0), \quad \hat{\phi}\left( \frac{1}{2}, \frac{3}{4} \right) = [2] \left( \frac{5}{128}, \frac{3}{2048} \right)
\]

This \ shows \ that

\[
\frac{E(Q)}{\hat{\phi}(E'(Q))} \simeq \frac{Z}{2Z} \times \frac{Z}{2Z} \quad \text{and} \quad \frac{E'(Q)}{\hat{\phi}(E(Q))} \simeq \frac{Z}{2Z} \times \frac{Z}{4Z}.
\]

4.2. Example: \ \( T \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \). \ Consider \ \( t = 3/2 \). \ One \ computes \ that \ the \ Mordell-Weil \ groups \ are

\[
E(Q) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z},
\]

\[
E'(Q) \simeq \mathbb{Z}/8\mathbb{Z},
\]

\[
E''(Q) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.
\]

We \ consider \ Proposition \ 2.9 \ in \ more \ detail \ because \ \( \sqrt{t + \sqrt{t^2 + 4}} \) \ is \ rational.

Performing \ a \ 2-descent \ with \ \texttt{mr} \ one \ computes \ the \ quantities

\[
\frac{E''(Q)}{\eta(E'(Q))} \simeq S^{(n)}(E'/Q) \simeq \{ \pm 1 \}, \quad \text{III}(E'/Q)[\eta] \simeq \{ 0 \};
\]

\[
\frac{E(Q)}{\hat{\phi}(E''(Q))} \simeq S^{(\hat{\phi})}(E''/Q) \simeq \{ \pm 1 \}, \quad \text{III}(E''/Q)[\hat{\phi}] \simeq \{ 0 \};
\]
and so
\begin{equation}
\frac{E(Q)}{\phi(E'(Q))} \simeq S(\phi)(E'/Q) \simeq \mathbb{Z}[\hat{\phi}] \quad \text{and} \quad \frac{E'(Q)}{\phi(E(Q))} \simeq \mathbb{Z}.
\end{equation}

We now compute explicit points. The curves have good reduction away from \( \Sigma = \{2, 3, 5, \infty\} \), and the homogeneous spaces of interest are of the form
\begin{equation}
C'_d: \quad d (w + a z^2) z^2 = (w^2 - d)^2, \quad a = -3^{-2}.
\end{equation}
When \( d = -9 \) we find the solution \((z, w) = (3, -3)\); this maps to the point
\begin{equation}
\left( w \begin{array}{c}
\frac{w}{z^2}, \\
\frac{w^2 - d}{z^4}
\end{array} \right) = \left( -\frac{1}{3}, \frac{2}{9} \right) \in E(Q).
\end{equation}
(Note how we may predict \( S(\phi)(E'/Q) \simeq \{1, -9\} \) from the connecting homomorphism \( \delta': (0, 0) \mapsto a^{-1} \equiv -9 \).) In fact, the group of rational points \( E(Q) \) is generated by \((-1/3, 2/9)\) and \((0, 0)\), while the group \( E'(Q) \) is generated by \((25/64, 125/1024)\); with orders 2, 4, and 8, respectively. (Compare with the proof of Proposition 2.2 where \( \gamma = \sqrt{t + \sqrt{t^2 + 4}} = 2 \) ) We have \( \phi(0, 0) = \mathcal{O} \) while
\begin{equation}
\phi \left( \frac{1}{3}, \frac{2}{9} \right) = [4] \left( \frac{25}{64}, -\frac{125}{1024} \right) \quad \text{and} \quad \hat{\phi} \left( \frac{25}{64}, \frac{125}{1024} \right) = \left( -\frac{1}{3}, \frac{2}{9} \right) \oplus (0, 0);
\end{equation}
this shows that
\begin{equation}
\frac{E(Q)}{\phi(E'(Q))} \simeq \mathbb{Z} \quad \text{and} \quad \frac{E'(Q)}{\phi(E(Q))} \simeq \mathbb{Z} / 4\mathbb{Z}.
\end{equation}

4.3. Example: \( \mathcal{T} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \). Consider the collection of elliptic curves studied in Example 2 as discussed in the introduction; each rational \( r \) corresponds to \( t = (r^4 - 6 r^2 + 1) / (2 r^3 - 2 r) \). Bounds on the rank can be computed by \texttt{mrank} and by \texttt{MAGMA}, but these programs do not seem to be able to compute the rank exactly. For these five examples we will consider the non-negative integer \( R \) such that
\begin{equation}
E(Q) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}^R,
\end{equation}
\begin{equation}
E'(Q) \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}^R,
\end{equation}
\begin{equation}
E''(Q) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}^R.
\end{equation}

Various data about the curves is summarized in Table 1. We will see below that, assuming the conjectures of Birch and Swinnerton-Dyer, the lower bounds on \( R \) are sharp and the Shafarevich-Tate groups are non-trivial.

We focus on size of the Selmer groups. The program \texttt{mrank} computes the groups \( S^{(n)}(E'/Q) \) and \( S^{(n)}(E''(Q)) \) associated with the 2-isogenies, so it suffices to consider the group \( S(\phi)(E'/Q) \) associated with the 4-isogeny. We may compute the size of the latter Selmer group using the exact diagram in 4.4: the data is collected in Table 2. Consider the image of the torsion subgroup of \( E(Q) \) under the connecting homomorphism \( \delta': (x, y) \mapsto x^2 - y \mod (Q \times)^4 \). Quite explicitly, the torsion subgroup is generated by the points
\begin{equation}
P = \left( \frac{r^2}{(r^2 + 2 r - 1)(r^2 - 2 r - 1)}, \frac{2 r^4}{(r^2 + 2 r - 1)^2 (r^2 - 2 r - 1)^2} \right),
\end{equation}
\begin{equation}
Q = \left( \frac{r (r + 1)}{(r^2 + 2 r - 1)(r^2 - 2 r - 1)^2}, \frac{r (r + 1)^2 (r - 1)^3}{(r^2 + 2 r - 1)^2 (r^2 - 2 r - 1)^3} \right).
\end{equation}
Table 1. Data for $E_t(\mathbb{Q})$ where $t = (r^4 - 6r^2 + 1) / (2r^3 - 2r)$

| $r$  | $t$         | Set of Bad Primes $\Sigma$                     | Rank Bounds |
|------|-------------|-----------------------------------------------|-------------|
| 15   | $5651521$   | $\{2, 3, 5, 7, 41, 71, 1231, 3361, 4591, \infty\}$ | $2 \leq R \leq 4$ |
| 56   | $4890480$   | $\{2, 3, 5, 7, 41, 71, 1231, 3361, 4591, \infty\}$ | $2 \leq R \leq 4$ |
| 24   | $3580801$   | $\{2, 3, 5, 7, 13, 23, 41, 89, 967, 4801, \infty\}$ | $2 \leq R \leq 4$ |
| 65   | $11384880$  | $\{2, 3, 5, 7, 11, 29, 223, 2441, 3079, \infty\}$ | $2 \leq R \leq 4$ |
| 11   | $4806319$   | $\{2, 3, 5, 7, 11, 29, 223, 2441, 3079, \infty\}$ | $2 \leq R \leq 4$ |
| 69   | $1760880$   | $\{2, 3, 5, 7, 11, 19, 23, 79, 113, 281, 7793, \infty\}$ | $2 \leq R \leq 4$ |
| 7    | $57695201$  | $\{2, 3, 5, 7, 17, 41, 97, 109, 233, 991, 11593, \infty\}$ | $1 \leq R \leq 4$ |

Table 2. Selmer Group Computations via $\text{murank}$

| $r$  | $S^{(0)}(E'/\mathbb{Q})$ | $S^{(2)}(E''/\mathbb{Q})$ | # $S^{(\phi)}(E'/\mathbb{Q})$ |
|------|---------------------------|---------------------------|-------------------------------|
| 15   | $\langle -1, 2, 3, 5, 7, 41, 71 \rangle$ | $\langle -1, 2, 3, 5, 7, 41, 71 \rangle$ | $2^{13}$ |
| 56   | $\langle -1, 2, 3, 5, 7, 41, 89 \rangle$ | $\langle -1, 2, 3, 5, 7, 41, 89 \rangle$ | $2^{13}$ |
| 24   | $\langle -1, 2, 5, 23, 29, 33 \rangle$ | $\langle -1, 2, 5, 23, 29, 33 \rangle$ | $2^{11}$ |
| 65   | $\langle -1, 2, 5, 7, 11, 15, 57, 113, 843 \rangle$ | $\langle -1, 2, 7, 57, 11 \cdot 15 \rangle$ | $2^{12}$ |
| 11   | $\langle -1, 2, 5, 7, 11, 15, 57, 113, 843 \rangle$ | $\langle -1, 2, 5, 7, 11, 15 \rangle$ | $2^{10}$ |

having orders 2 and 8, respectively, and the connecting homomorphism $\delta'$ sends
(4.17)
$$P \mapsto -\frac{r^4}{(r^2 + 2r - 1)^2(r^2 - 2r - 1)^2}, \quad Q \mapsto \frac{r(r + 1)^3(r - 1)^3}{(r^2 + 2r - 1)^2(r^2 - 2r - 1)^2}.$$ 

For the $d \in S^{(\phi)}(E'/\mathbb{Q})$ above, consider the homogeneous spaces

(4.18) $C_d': \quad d(w + az^2)z^2 = (w^2 - d)^2$, \quad a = -\frac{r^2(r + 1)^2(r - 1)^2}{(r^2 + 2r - 1)^2(r^2 - 2r - 1)^2}.$$

Some generators $(x, y)$ on $E(\mathbb{Q})$ can be found by $\text{murank}$; these can be pulled back to a point $(z, w)$ on $C_d'(\mathbb{Q})$ via the mapping $\psi': C_d' \to E$ in Theorem 2.6. We summarize these rational points in Table 3.

Rathbun \[5\] has remarked that the points in Table 3 correspond to the complete list generators on the elliptic curve if we assume the validity of the Birch and Swinnerton-Dyer conjectures. That is, we consider the order of the vanishing of the $L$-series in order to compute the rank, as well as the relationship with the residue and regulator of the elliptic curve to compute the generators; the information is summarized in Table 3. (For more information on the BSD conjectures, consult \[6\] Chapter 4.) Notice that the $\hat{\phi}$-component of the Shafarevich-Tate group is not
Table 3. Points \((z, w) \in C'_d(\mathbb{Q})\) Corresponding to \(d \in S(\hat{\phi}(E'/\mathbb{Q}))\)

| \(r\) | \(d\) | \(z\) | \(w\) |
|------|------|------|------|
| 15/56 | \(-1 \cdot 5651521^2\) | 5651521 | 5651521 |
|      | \(2 \cdot 8733^2\) | \(86033006559349680248647\) | \(3354273204372689787801\) |
|      | \(41 \cdot 71 \cdot 8617^2\) | \(36749739714577272536\) | \(320119683924889132\) |
|      | \(3 \cdot 5 \cdot 7 \cdot 56515210^2\) | \(3790287093391733579\) | \(5724171826291368240\) |
| 24/65 | \(-1 \cdot 6769^2\) | 155687 | 6769 |
|      | \(2 \cdot 15^2\) | \(3893880282213551\) | \(45660470553\) |
|      | \(41 \cdot 89 \cdot 130^2\) | \(2376079357686320\) | \(25044578686\) |
|      | \(3 \cdot 5 \cdot 13 \cdot 527982^2\) | \(83760182508961\) | \(26347553866400\) |
| 11/69 | \(-1 \cdot 4806319^2\) | 9612638 | 4806319 |
|      | \(5 \cdot 4683^2\) | \(68687104829\) | \(585884547\) |
|      | \(23 \cdot 2453^2\) | \(107909560\) | \(42652\) |
|      | \(2 \cdot 29 \cdot 33 \cdot 215530^2\) | \(67089450748541\) | \(71568676933\) |
|      | \(100180503473972531298429\) | \(545439052560\) | \(12390148\) |
|      | \(834126406602556183512\) | \(10180503473972531298429\) | \(2401846018297942811880275\) |
| 7/88  | \(-1 \cdot 57695201^2\) | 57695201 | 57695201 |
|      | \(2 \cdot 6441^2\) | \(5596434497\) | \(41962889\) |
|      | \(7 \cdot 7658655^2\) | \(2776356\) | \(738\) |
|      | \(15608602011772334\) | \(143349694803\) | \(2275391981\) |
|      | \(26233163006176556\) | \(50569135135585\) | \(954960053\) |
| 12/97 | \(-1 \cdot 80420641^2\) | 80420641 | 80420641 |
|      | \(17 \cdot 97 \cdot 34^2\) | \(3173285824541959\) | \(1304349940207\) |
|      | \(1635 \cdot 34779^2\) | \(59077245130310\) | \(558755747\) |
|      | \(11503152325990561\) | \(11503152325990561\) | \(31422940575120\) |
always of square order; we give an explanation. For the moment, let $\hat{\phi} : E \rightarrow E'$ be any isogeny. The canonical alternating, non-degenerate, bilinear pairing

$$III(E'/\mathbb{Q}) \times III(E'/\mathbb{Q}) \rightarrow \mathbb{Q}/\mathbb{Z}$$

induces a non-degenerate, bilinear pairing

$$III(E'/\mathbb{Q})[\hat{\phi}] \times III(E'/\mathbb{Q})[\hat{\phi}] \rightarrow \mathbb{Q}/\mathbb{Z}. \tag{4.20}$$

(For more information on the Cassels pairing, consult [7, Appendix C, §17].) When $\phi$ is the “multiplication-by-$m$” map we have $III(E/\mathbb{Q})/m \cong III(E/\mathbb{Q})[m]$ – assuming that $III(E/\mathbb{Q})$ is finite – so the pairing induces an alternating, non-degenerate, bilinear pairing

$$III(E/\mathbb{Q})[m] \times III(E/\mathbb{Q})[m] \rightarrow \mathbb{Q}/\mathbb{Z}. \tag{4.21}$$

Hence $III(E/\mathbb{Q})[m]$ must have square order. In general, however, $\hat{\phi}$ might not be self-dual; that is, upon considering the short exact sequence

$$0 \rightarrow III(E/\mathbb{Q})[\hat{\phi}] \rightarrow III(E'/\mathbb{Q}) \rightarrow \frac{III(E'/\mathbb{Q})}{\phi \left( III(E/\mathbb{Q}) \right)} \rightarrow 0 \tag{4.22}$$

we might have

$$\# \frac{III(E/\mathbb{Q})}{\phi \left( III(E/\mathbb{Q}) \right)} \neq \# \frac{III(E'/\mathbb{Q})}{\phi \left( III(E'/\mathbb{Q}) \right)} \Rightarrow \frac{III(E'/\mathbb{Q})}{\phi \left( III(E'/\mathbb{Q}) \right)} \neq \frac{III(E'/\mathbb{Q})}{\phi \left( III(E'/\mathbb{Q}) \right)} \tag{4.23}.$$

**References**

[1] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[2] Garikai Campbell and Edray Herber Goins. Heron Triangles, Diophantine Problems, and Elliptic Curves. *Submitted*, 2003.

[3] Daniel Sion Kubert. Universal bounds on the torsion of elliptic curves. *Proc. London Math. Soc. (3)*, 33(2):193–237, 1976.

[4] J. R. Merriman, S. Siksek, and N. P. Smart. Explicit 4-descents on an elliptic curve. *Acta Arith.*, 77(4):385–404, 1996.

[5] Randall L. Rathbun. Personal communication. October 2003.
[6] Alice Silverberg. Open questions in arithmetic algebraic geometry. In *Arithmetic algebraic geometry (Park City, UT, 1999)*, volume 9 of *IAS/Park City Math. Ser.*, pages 83–142. Amer. Math. Soc., Providence, RI, 2001.

[7] Joseph H. Silverman. *The arithmetic of elliptic curves*. Springer-Verlag, New York-Berlin, 1986.

[8] Jacques Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A-B*, 273:A238–A241, 1971.

Department of Mathematics, California Institute of Technology, Pasadena, CA 91125

E-mail address: goins@caltech.edu