DESCENT VIA ISOGENY ON ELLIPTIC CURVES WITH LARGE RATIONAL TORSION SUBGROUPS

E.V. FLYNN AND C. GRATTONI

Abstract. We outline implementations in PARI of various algorithms related to descent via isogeny on elliptic curves. We describe, in this context, variations of standard inequalities which assist in the computation of members of the Tate-Shafarevich group. We apply these techniques to several examples: in one case we use descent via 9-isogeny to determine the rank of an elliptic curve; in another case we find nontrivial members of the 9-part of the Tate-Shafarevich group, and in a further case, nontrivial members of the 13-part of the Tate-Shafarevich group.

1. Introduction

Recall that an elliptic curve defined over a field K is a smooth projective curve of genus 1 with at least one rational point. In projective coordinates, we will take this point to be $[0,1,0]$, and we will describe $\mathcal{E}$ by the following homogeneous equation:

$$\mathcal{E} : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

where $a_i \in K$. However, as a matter of convention, we will almost always refer to $\mathcal{E}$ by the affine chart such that $\mathcal{E}$ is described by an equation of the form

$$\mathcal{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_i \in K$ and $\mathcal{O}$ is an added point at infinity corresponding to the rational projective point $[0,1,0]$. For general background on elliptic curves see, for example, [20],[29]. For the sake of convenience, we adopt Silverman's notation [29] of often referring to $\mathcal{E}(\overline{K})$ as simply $\mathcal{E}$. In this way, it is necessary to interpret the expression "for some $P \in \mathcal{E}$" as "for some $P \in \mathcal{E}(\overline{K})$." Finally, while we will address this theorem in more detail in later sections, we recall the Mordell-Weil theorem, which states that for any elliptic curve $\mathcal{E}$ defined over a number field K, $\mathcal{E}(K) \cong \mathcal{E}_{\rm tors}(K) \times \mathbb{Z}^r$, where $r \in \mathbb{Z}^+$. We call r the *rank* of $\mathcal{E}(K)$.

Finding this number r will be the fundamental question that this article will address. The canonical method for attempting to solve this problem is by doing a complete 2-descent: attempting to compute $\mathcal{E}(\mathbb{Q})/[2]\mathcal{E}(\mathbb{Q})$ by checking whether certain twists of $\mathcal{E}$ (homogeneous spaces) have any rational points. See Chapter X of [29] for a complete account of this method. In this article, we will use a general technique outlined in [27] to construct an explicit method for doing a descent via isogeny on a certain class of elliptic curves where the isogeny is not the multiplication-by-2 map. More specifically, our method of descent via isogeny will apply when $\phi : \mathcal{E} \to \widehat{\mathcal{E}}$ is a $\mathbb{Q}$-rational isogeny between elliptic curves defined over $\mathbb{Q}$, where the kernel of the isogeny is cyclically generated by a $\mathbb{Q}$-rational point on $\mathcal{E}$ of prime power order. In accordance with Schaefer's method, we will do this without having to describe any homogeneous spaces; as he points

Date: 15 September, 2006.
1991 *Mathematics Subject Classification.* Primary 11G30; Secondary 11G10, 14H40.
Key words and phrases. Elliptic Curves, Isogeny, Tate-Shafarevich Group.

out, avoiding these spaces can be convenient as they can become quite difficult to describe as the degree of our isogeny increases. Note that because of a result by Mazur (see Theorem 2 or [22], Theorem 4.1) and the fact that we are only considering curves with a rational torsion point of prime power order, we know that our isogeny must have degree d where $d \in \{2, 3, 4, 5, 7, 8, 9\}$. Further, descents via 2- and 3-isogeny have been exhaustively described in other works, so we will largely avoid these cases. Examples of performing a descent via 2-isogeny on a hyperelliptic curve that avoids homogeneous spaces can be found in Chapter 11 of [5], while the traditional method of descent via 2-isogeny can be found in [29], X.4.10. Descent via 3-isogeny is described in [11],[33], and 3-descents are also discussed in [2],[13],[28]. Methods of performing a 4-descent can be found in [18],[23]. In addition, [1] works with 5-descents, Thomas Fisher describes a method of descent via 5- and 7-isogeny in [14],[15], and [30] discusses a method for performing an 8-descent. See also [9],[10]. Our method of descent via 9-isogeny does not seem to be addressed in other sources.

While our particular method is only feasible for curves with nontrivial rational torsion subgroups or for curves with a torsion subgroup defined over a low degree number field, this is still a worthwhile endeavor for several reasons. Firstly, the traditional method for computing the rank of $\mathcal{E}(\mathbb{Q})$ depends on computing its 2-Selmer group, which will only yield the rank of $\mathcal{E}(\mathbb{Q})$ when the 2-part of the Tate-Shafarevich group (often called Sha and denoted $Ш(\mathcal{E}/\mathbb{Q})$) is trivial. While anecdotal evidence indicates that it is somewhat unlikely that a randomly selected curve should have nontrivial elements in the 2-part of the Tate-Shafarevich group, it is still useful to have the option of doing alternate descents on a curve should a 2-descent happen to fail. Further, doing different descents allows one to discover more about the Tate-Shafarevich group, which has wider applications to the theory of elliptic curves (see [6],[35]).

2. Notation

Now let $\mathcal{E}$ be an elliptic curve defined over $\mathbb{Q}$ described by a Weierstrass equation

$$\mathcal{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1}$$

where each $a_i \in \mathbb{Q}$. We denote the group of rational points on $\mathcal{E}$ by $\mathcal{E}(\mathbb{Q})$. Further, we let $\Delta(\mathcal{E})$ be the discriminant of $\mathcal{E}$, and we let $\Delta_{\min}(\mathcal{E})$ be the discriminant of the minimal model for $\mathcal{E}$. For any elliptic curve $\mathcal{E}$ and finite prime $p \in \mathbb{Z}^+$, let $\mathcal{E}'_p$ denote the reduction of $\mathcal{E}$ at p so that

$$\mathcal{E}'_p : y^2 + a'_1xy + a'_3y = x^3 + a'_2x^2 + a'_4x + a'_6,$$

where a'_i is the reduction of a_i in $\mathbb{F}_p$. We see that this map takes a point $(x_0, y_0) \in \mathcal{E}(\mathbb{Q})$ to $(x'_0, y'_0) \in \mathcal{E}'_p(\mathbb{F}_p)$, where x'_0 and y'_0 are the reductions of x_0 and y_0 at p. Let $\mathbb{Q}(\mathcal{E})$ denote the function field of $\mathcal{E}$, which can be described by $\mathbb{Q}(x, y)$, where x and y satisfy the Weierstrass equation for $\mathcal{E}$.

Further, let $\phi : \mathcal{E} \to \widehat{\mathcal{E}}$ be an isogeny of degree d defined over $\mathbb{Q}$, where we usually take d to be a power of a prime. We let $\mathcal{E}[\phi]$ denote the $\overline{\mathbb{Q}}$-rational points in the kernel of ϕ, and we let $\mathcal{E}(\mathbb{Q})[\phi]$ denote the rational points in the kernel of ϕ. Let $\mathbb{Q}(\widehat{\mathcal{E}})$ be the function field of $\widehat{\mathcal{E}}$, which we will often denote as $\mathbb{Q}(X, Y)$ where X and Y satisfy the Weierstrass equation for $\widehat{\mathcal{E}}$. We denote the dual isogeny mapping from $\widehat{\mathcal{E}}$ to $\mathcal{E}$ as $\widehat{\phi}$. As a matter of taste, we choose to call $\widehat{\mathcal{E}}$ the *dual curve* to $\mathcal{E}$, and we will denote the coefficients of the Weierstrass

equation for $\widehat{\mathcal{E}}$ with capital letters so that

$$\widehat{\mathcal{E}} : y^2 + A_1xy + A_3y = x^3 + A_2x^2 + A_4x + A_6,$$

where each $A_i \in \mathbb{Q}$. If we need to differentiate further between $\mathcal{E}$ and $\widehat{\mathcal{E}}$, we will use capital X's and Y's when working with the dual curve.

3. Finding One-Parameter Families of Elliptic Curves with Prescribed Torsion Subgroups

It is a classical result that the set of elliptic curves defined over $\mathbb{Q}$ which contain a rational point of order $d \in \{4, 5, 6, 7, 8, 9, 10, 12\}$ lie in a one-parameter family. This is a result of the following two theorems.

Theorem 1. *Any elliptic curve $\mathcal{E}/\mathbb{Q}$ with at least one rational point other than $\mathcal{O}$ that is not of order 2 or 3 is birationally equivalent to an elliptic curve in the form, $\mathcal{E} : y^2 + (1-w)xy + vy = x^3 + vx^2$ where $v, w \in \mathbb{Q}$. We call this Tate normal form (see [20], 4.1).*

Proof: This is a standard result, which can be found in [29], VIII, Exercise 8.13.a. □

Theorem 2 (Mazur)**.** *Let $X_1(d)$ be the modular curve whose rational points parametrize the family of elliptic curves possessing a rational point of order $d \geqslant 2$. Then $X_1(d)$ is of genus 0 if and only if $d \in \{2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$. Further, if $\mathcal{E}$ is an elliptic curve defined over $\mathbb{Q}$ and $P \in \mathcal{E}_{tors}(\mathbb{Q})$, then the order of P must be in $\{2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$.*

Proof: For the fact about the genus of $X_1(d)$, see [7], 2.2.4-5. For the classification of rational torsion on elliptic curves, see [22], Theorem 4.1. □

Remark 1. We see that if we assume that $\mathcal{E} : y^2 + (1-w)xy + vy = x^3 + vx^2$ is an elliptic curve with a rational point of order $d \geqslant 4$ at $(0, 0)$, then we can use the group law on the curve to find the relation between v and w induced by $d(0, 0) = \mathcal{O}$. If d is even it is simpler to use $(d/2)(0, 0) = (-d/2)(0, 0)$, and if d is odd we can use $(d'+1)(0, 0) = (-d')(0, 0)$, where $d = 2d'+1$. This relation between v and w is essentially a model for the modular curve $X_1(d)$. Further, we see from Mazur's theorem that when $d \in \{4, 5, 6, 7, 8, 9, 10, 12\}$ that we may actually parametrize the equation for $X_1(d)$ (since we can find rational parametrizations of genus 0 curves). This implies that the family of curves with a rational point of order $d \in \{4, 5, 6, 7, 8, 9, 10, 12\}$ lies in a one parameter family of the form

$$\{\mathcal{E}_t^d : y^2 + j_d(t)xy + k_d(t)y = x^3 + k_d(t)x^2 : t \in \mathbb{Q}, \Delta(\mathcal{E}_t^d) \neq 0\}. \tag{2}$$

where $j_d(t)$ and $k_d(t)$ are as follows:

Table 1. *The following gives $j_d(t), k_d(t)$ such that $E_t^d : y^2 + j_d(t)xy + k_d(t)y = x^3 + k_d(t)x^2$.*

d	$j_d(t)$	$k_d(t)$
4	1	t
5	$t+1$	t
6	$1-t$	$-t(t+1)$
7	$1-t-t^2$	$t^2(t+1)$
8	$\dfrac{-2t^2+1}{t+1}$	$-t(2t+1)$
9	t^3+t^2+1	$t^2(t^3+2t^2+2t+1)$
10	$1-\dfrac{t^3+3t^2+2t}{t^2+6t+4}$	$\dfrac{t^5+3t^4+2t^3}{t^4+12t^3+44t^2+48t+16}$
12	$\dfrac{6t^4-8t^3+2t^2+2t-1}{t^3-3t^2+3t-1}$	$\dfrac{-12t^6+30t^5-34t^4+21t^3-7t^2+t}{t^4-4t^3+6t^2-4t+1}$

4. Isogenies

In this section, we sketch the method from [34] for constructing isogenies between elliptic curves with nontrivial rational torsion.

Let $\phi : \mathcal{E} \to \widehat{\mathcal{E}}$ be a $\mathbb{Q}$-rational isogeny of elliptic curves, defined over $\mathbb{Q}$, where $\mathcal{E}$ is described by a Weierstrass equation as in (1):

$$\mathcal{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Definition 1. We associate the following values, called the *Tate values*, to an elliptic curve given by a Weierstrass equation as above:

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6. \end{aligned}$$

As usual, let $\mathcal{E}[\phi]$ denote the kernel of ϕ. Let $P = (x, y)$ be a generic point in the function field of $\mathcal{E}$, $\mathbb{Q}(\mathcal{E}) \cong \mathbb{Q}(x, y)$. Note that $x \in \mathbb{Q}(\mathcal{E})$ is the function that takes a point to its x-coordinate, so if $P = (1, 2)$, $x(P) = x((1, 2)) = 1$. Similarly, we have $y(P) = y((1, 2)) = 2$. Then consider the following two functions:

$$\begin{aligned} X(P) &= x(P) + \sum_{Q \in \mathcal{E}[\phi] - \{\mathcal{O}\}} \Big(x(P+Q) - x(Q) \Big) \\ Y(P) &= y(P) + \sum_{Q \in \mathcal{E}[\phi] - \{\mathcal{O}\}} \Big(y(P+Q) - y(Q) \Big). \end{aligned}$$

Lemma 1. ([34], *Equation 2*) *Let $\phi : \mathcal{E} \to \widehat{\mathcal{E}}$ be as above. Then $\mathbb{Q}(\widehat{\mathcal{E}}) \cong \mathbb{Q}(X, Y)$. That is, if $P = (x, y)$, then $\phi(P) = \phi((x, y)) = (X, Y)$.*

Proof: See [34], Equation 2, though this is fairly transparent since $\mathcal{E}[\phi]$ is clearly the kernel of the maps X and Y. □

Definition 2. Let $\phi : \mathcal{E} \to \widehat{\mathcal{E}}$ be as above. Let $\mathcal{E}[\phi]_2$ denote the points of order 2 in $\mathcal{E}[\phi]$. Further, let R be a subset of $\mathcal{E}[\phi] - \{\mathcal{O}\} - \mathcal{E}[\phi]_2$ such that

$$\mathcal{E}[\phi] - \{\mathcal{O}\} - \mathcal{E}[\phi]_2 = R \cup (-R) \text{ and } R \cap (-R) = \varnothing.$$

Then we define $S = R \cup \mathcal{E}[\phi]_2$.

Definition 3. For any $Q \in \mathcal{E}$, we define the following quantities associated with Q:

$$\begin{aligned}
&Q = (x_Q, y_Q)\\
&g_Q^x = 3x_Q^2 + 2a_2x_Q + a_4 - a_1y_Q\\
&g_Q^y = -2y_Q - a_1x_Q - a_3\\
&s_Q = \begin{cases} g_Q^x & \text{if } Q \in \mathcal{E}[\phi]_2 \\ 2g_Q^x - a_1g_Q^y = 6x_Q^2 + b_2x_Q + b_4 & \text{if } Q \notin \mathcal{E}[\phi]_2 \end{cases}\\
&u_Q = (g_Q^y)^2 = 4x_Q^3 + b_2x_Q^2 + 2b_4x_Q + b_6.
\end{aligned}$$

Theorem 3. (*see* [34]) *Let $\phi : \mathcal{E} \to \widehat{\mathcal{E}}$ and S be as above. Let*

$$s = \sum_{Q \in S} s_Q \text{ and } w = \sum_{Q \in S} (u_Q + x_Q s_Q).$$

Then $\widehat{\mathcal{E}}$ satisfies the following Weierstrass equation:

$$\widehat{\mathcal{E}} : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + (a_4 - 5s)X + (a_6 - b_2s - 7w).$$

Proof: See [34], where this relation between X and Y is obtained via a computation using the formal groups of $\mathcal{E}$ and $\widehat{\mathcal{E}}$. □

Remark 2. We can use Vélu's method to find an isogeny $\phi : \mathcal{E}_t^d \to \widehat{\mathcal{E}}_t^d$ for the elliptic curves from Table 1, as well as the Weierstrass equation for $\widehat{\mathcal{E}}_t^d$. Further, we can compute the explicit formula for the dual isogeny, $\widehat{\phi}$ by repeating Vélu's method. Namely, we start with $\widehat{\mathcal{E}}_t^d$ to find an isogeny to $\widehat{\widehat{\mathcal{E}}}_t^d$, which can be birationally transformed to $\mathcal{E}_t^d$. Note that to do this, we need to determine the kernel of the dual isogeny, $\widehat{\mathcal{E}}_t^d[\widehat{\phi}]$, by factoring the d^{th} division polynomial of $\widehat{\mathcal{E}}_t^d$. We summarize these results as follows.

Recall that we denote our original family of curves as in (2):

$$\{\mathcal{E}_t^d : y^2 + j_d(t)xy + k_d(t)y = x^3 + k_d(t)x^2 : t \in \mathbb{Q}, \Delta(\mathcal{E}_t^d) \neq 0\}.$$

Similarly, we have our associated family of dual curves, where $\widehat{\mathcal{E}}_t^d$ is dual to $\mathcal{E}_t^d$ for $d \in \{4, 5, 7, 8, 9\}$ and any $t \in \mathbb{Q}$ such that $\mathcal{E}_t^d$ is an elliptic curve, which we list in the following tables for $d = 4, 5, 7, 8, 9$.

Table 2. *The following gives* $l_d(t), m_d(t)$ *such that* $\widehat{\mathcal{E}}_t^d : y^2 + j_d(t)xy + k_d(t)y = x^3 + k_d(t)x^2 + l_d(t)x + m_d(t)$.

d	$l_d(t)$
4	$-5(t^2+t)$
5	$5t(t^2-2t-1)$
7	$5t(t^6-7t^4-14t^3-14t^2-7t-1)$
8	$\dfrac{-5t(17t^6+51t^5+59t^4+33t^3+5t^2-3t-1)}{t^3+3t^2+3t+1}$
9	$5t(t^{10}+t^9-8t^8-33t^7-72t^6-108t^5-114t^4-81t^3-37t^2-10t-1)$

d	$m_d(t)$
4	$t(3t^2-12t-1)$
5	$t(t^4-10t^3-5t^2-15t-1)$
7	$t(t^{10}-8t^9-46t^8-107t^7-202t^6-343t^5-393t^4-258t^3-94t^2-19t-1)$
8	$\dfrac{-275t^{11}-1290t^{10}-2597t^9-2948t^8-2251t^7-1475t^6-913t^5-422t^4-107t^3-8t^2+t}{t^5+5t^4+10t^3+10t^2+5t+1}$
9	$t^{17}-7t^{16}-63t^{15}-230t^{14}-641t^{13}-1639t^{12}-3691t^{11}-6707t^{10}-9425t^9-10174t^8$ $-8456t^7-5379t^6-2559t^5-865t^4-190t^3-24t^2-t$

Remark 3. We have made available at [17] the PARI [24] function TorsionCurve, which takes a torsion order $d \in \{4,5,6,7,8,9\}$ and a parameter $t \in \mathbb{Q}$ and returns a 5 component vector $[a_1,a_2,a_3,a_4,a_6]$ corresponding to an elliptic curve in Tate normal form with a point of order d whose Weierstrass coefficients are determined by the parameter t. For example, TorsionCurve$(5,4)$ returns the vector $[5,4,4,0,0]$, which describes the elliptic curve

$$\mathcal{E} : y^2 + 5xy + 4y = x^3 + 4x^2.$$

In addition, we have written a function, DualCurve, which takes a torsion order $d \in \{4,5,6,7,8,9\}$ and a parameter $t \in \mathbb{Q}$ and uses Vélu's method to return a 5 component vector $[A_1,A_2,A_3,A_4,A_6]$ corresponding to the dual curve to TorsionCurve(d, t). In addition, IsogenyPhi(d, t, [x, y]) uses Vélu's method to map a (general or explicit) point on $\mathcal{E}_t^d/\mathcal{E}_t^d[\phi]$ by ϕ to $\widehat{\mathcal{E}}_t^d$. Similarly, IsogenyDual(d, t, [x, y]) takes a (general or explicit) point on $\widehat{\mathcal{E}}_t^d/\widehat{\mathcal{E}}_t^d[\widehat{\phi}]$ and maps it by $\widehat{\phi}$ to $\mathcal{E}_t^d$.

Example 1. Consider $\mathcal{E} : y^2 + 8xy + 7y = x^3 + 7x^2$, which is given by TorsionCurve$(5,7)$. Then the dual curve is given by DualCurve$(5,7)$, and is described by the following Weierstrass equation:

$$\widehat{\mathcal{E}} : y^2 + 8xy + 7y = x^3 + 7x^2 + 1190x - 9660.$$

We can quickly find the point $(14, 28) \in \mathcal{E}(\mathbb{Q})$, which has infinite order in $\mathcal{E}(\mathbb{Q})$. Therefore, $(14, 28) \notin \mathcal{E}[\phi]$. So we can use IsogenyPhi$(5, 7, [14, 28])$ to see that $\phi((14, 28)) = (349/36, 6493/216)$. We can now apply IsogenyDual$(5, 7, [349/36, 6493/216])$, which yields

$$[-29111531/2842596, 335859771193/4792616856],$$

which precisely says that

$$\widehat{\phi}((349/36, 6493/216)) = (-29111531/2842596, 335859771193/4792616856).$$

It can be easily verified that this point equals $[5](14, 28)$, which is compatable with the fact that $\widehat{\phi} \circ \phi = [5]$ on $\mathcal{E}$.

5. The $\widehat{\phi}$-Selmer and Tate-Shafarevich Groups

In this section, we will recall some general background on the ϕ-Selmer and Tate-Shafarevich groups, which arise by taking cohomology on the exact sequence

$$0 \to \widehat{\mathcal{E}}(\overline{\mathbb{Q}})[\widehat{\phi}] \to \widehat{\mathcal{E}}(\overline{\mathbb{Q}}) \xrightarrow{\widehat{\phi}} \mathcal{E}(\overline{\mathbb{Q}}) \to 0. \tag{3}$$

Note that all of the results in this section generalize to the case when $\mathcal{E}$ is an elliptic curve defined over a number field K and $\widehat{\phi} : \widehat{\mathcal{E}} \to \mathcal{E}$ is an isogeny defined over K.

Remark 4. For the sake of brevity, we adopt the notation $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and $G_p = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ where $p \in \{q : q \in \mathbb{Z}^+ \text{ is prime or } q = \infty\}$. As usual, when $p = \infty$, $\mathbb{Q}_\infty := \mathbb{R}$.

Proposition 1. ([29], *X.4*) *Let $\widehat{\phi} : \widehat{\mathcal{E}} \to \mathcal{E}$ be a $\mathbb{Q}$-rational isogeny of elliptic curves defined over $\mathbb{Q}$. Then the following diagram is commutative where δ is the connecting homomorphism that arises from taking Galois cohomology on the sequence from (3):*

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathcal{E}(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q})) & \xrightarrow{\delta} & H^1(G, \widehat{\mathcal{E}}(\overline{\mathbb{Q}})[\widehat{\phi}]) & \longrightarrow & H^1(G, \widehat{\mathcal{E}}(\overline{\mathbb{Q}}))[\widehat{\phi}] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \prod_p \mathcal{E}(\mathbb{Q}_p)/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q}_p)) & \xrightarrow{\delta} & \prod_p H^1(G_p, \widehat{\mathcal{E}}(\overline{\mathbb{Q}}_p)[\widehat{\phi}]) & \longrightarrow & \prod_p H^1(G_p, \widehat{\mathcal{E}}(\overline{\mathbb{Q}}_p))[\widehat{\phi}] & \longrightarrow & 0
\end{array}$$

Definition 4. Let $\widehat{\phi} : \widehat{\mathcal{E}} \to \mathcal{E}$ be a $\mathbb{Q}$-rational isogeny of elliptic curves defined over $\mathbb{Q}$. We define the $\widehat{\phi}$-Selmer group of $\widehat{\mathcal{E}}/\mathbb{Q}$, denoted $\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})$, to be

$$\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q}) = ker\left(H^1(G, \widehat{\mathcal{E}}(\overline{\mathbb{Q}})[\widehat{\phi}]) \to \prod_p H^1(G_p, \widehat{\mathcal{E}}(\overline{\mathbb{Q}}_p))\right).$$

Definition 5. Similarly, we define the Tate-Shafarevich group of $\widehat{\mathcal{E}}/\mathbb{Q}$, denoted $Ш(\widehat{\mathcal{E}}/\mathbb{Q})$, to be

$$Ш(\widehat{\mathcal{E}}/\mathbb{Q}) = ker\left(H^1(G, \widehat{\mathcal{E}}(\overline{\mathbb{Q}})) \to \prod_p H^1(G_p, \widehat{\mathcal{E}}(\overline{\mathbb{Q}}_p))\right).$$

Lemma 2. ([29], *X.4.2.a*) *Let $\mathcal{E}$ be an elliptic curve defined over $\mathbb{Q}$, and let $\widehat{\phi} : \widehat{\mathcal{E}} \to \mathcal{E}$ be a $\mathbb{Q}$-rational isogeny. Then the following is an exact sequence:*

$$0 \to \mathcal{E}(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q})) \to Sel^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q}) \to Ш(\widehat{\mathcal{E}}/\mathbb{Q})[\widehat{\phi}] \to 0.$$

Proof: This is clear from the definitions of the $\widehat{\phi}$-Selmer group and the Tate-Shafarevich group (this sequence is simply extracted from the commutative diagram in Proposition 1). □

Lemma 3. ([29], *X.4.4*) *Let $\mathcal{E}$ be an elliptic curve defined over $\mathbb{Q}$ and let $\widehat{\phi}:\widehat{\mathcal{E}}\to\mathcal{E}$ be a $\mathbb{Q}$-rational isogeny. Let $d=deg(\widehat{\phi})=deg(\phi)$. Then $Sel^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})\subseteq H^1(Gal(\overline{\mathbb{Q}}/\mathbb{Q}),\widehat{\mathcal{E}}(\overline{\mathbb{Q}})[\widehat{\phi}];T)$ for the following finite set:*

$$T=\{p : p|\Delta_{min}(\mathcal{E}) \text{ or } p|d \text{ or } p=\infty\}. \tag{4}$$

Theorem 4. ([28], *Proposition 3.2*) *Let $\mathcal{E}$, ϕ, T, and d be as in Lemma 3. Let $c_{\mathcal{E},p}$ be the Tamagawa number for $\mathcal{E}$ at p, and let $c_{\widehat{\mathcal{E}},p}$ be the Tamagawa number for $\widehat{\mathcal{E}}$ at p (see Definition 7). Then*

$$Sel^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})\subseteq H^1(Gal(\overline{\mathbb{Q}}/\mathbb{Q}),\widehat{\mathcal{E}}(\overline{\mathbb{Q}})[\widehat{\phi}];S)$$

where

$$S=T-\{p :\ gcd(d,c_{\mathcal{E},p})=\ gcd(d,c_{\widehat{\mathcal{E}},p})=1\}. \tag{5}$$

Theorem 5. ([29], *X.4.2.b*) *Let $\mathcal{E}$ be an elliptic curve defined over $\mathbb{Q}$ and let $\widehat{\phi}:\widehat{\mathcal{E}}\to\mathcal{E}$ be a $\mathbb{Q}$-rational isogeny. Then $Sel^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})$ is finite.*

Remark 5. Whenever we refer to the set S, we will assume it is the above set from (5). We need not worry about confusing the set S associated to $\mathcal{E}$ and the set S' associated to $\widehat{\mathcal{E}}$ when $\widehat{\phi}:\mathcal{E}\to\widehat{\mathcal{E}}$ is a $\mathbb{Q}$-rational isogeny of $\mathbb{Q}$-rational elliptic curves: it will always be the case that $S=S'$; see [8], II.12.

6. A General Method for Computing $\mathrm{Sel}^{(\widehat{\phi})}(\mathcal{E}/\mathbb{Q})$

Definition 6. Let $\mathcal{E}$ be an elliptic curve defined over $\mathbb{Q}$, and let $\widehat{\phi}:\widehat{\mathcal{E}}\to\mathcal{E}$ be a $\mathbb{Q}$-rational isogeny. Let S be the finite set of places associated to $\mathcal{E}$ described in (5). Then we define $\mathbb{Q}(S,d)\subseteq\mathbb{Q}^*/(\mathbb{Q}^*)^d$ to be the following group:

$$\mathbb{Q}(S,d)=\{k\in\mathbb{Q}^*/(\mathbb{Q}^*)^d : \mathrm{ord}_p(k)\equiv 0 \bmod d \text{ for all } p\notin S\}. \tag{6}$$

Proposition 2. ([29], *X.1.1 and Exercise 10.1*) *Let $\mathcal{E}$ be an elliptic curve defined over $\mathbb{Q}$ and let $\phi:\mathcal{E}\to\widehat{\mathcal{E}}$ be a degree-d $\mathbb{Q}$-rational isogeny such that $\mathcal{E}[\phi]\subseteq\mathcal{E}(\mathbb{Q})$ is cyclically generated by a point $T\in\mathcal{E}(\mathbb{Q})$. Then there exists an injective homomorphism:*

$$F:\mathcal{E}(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q}))\quad\to\quad\mathbb{Q}(S,d).$$

Further, for any $P\in\mathcal{E}(\mathbb{Q})$ such that $P\neq T,\mathcal{O}$, $F(P)\equiv f_T(P)\ mod(\mathbb{Q}^*)^d$ where $f_T\in\mathbb{Q}(\mathcal{E})$ is such that $div(f_T)=d\cdot T-d\cdot\mathcal{O}$ and $f_T\circ\widehat{\phi}=g_T^d$ for some $g_T\in\mathbb{Q}(\widehat{\mathcal{E}})$.

Remark 6. This implies that the $\widehat{\phi}$-Selmer group of an elliptic curve defined over $\mathbb{Q}$ is isomorphic to a subgroup of $\mathbb{Q}(S,d)\subseteq\mathbb{Q}^*/(\mathbb{Q}^*)^d$. This fact and the commutative diagram from Proposition 1 give us an effective method of computing $\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})$. Namely, following the construction from [27], we see that

Proposition 2 and the diagram from Proposition 1 lead to the following commutative diagram:

$$\begin{array}{ccc} \mathcal{E}(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q})) & \xrightarrow{F} & \mathbb{Q}(S,d) \\ \downarrow & & \downarrow \prod \beta_p \\ \prod_p \mathcal{E}(\mathbb{Q}_p)/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q}_p)) & \xrightarrow{\prod F_p} & \prod_p \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^d \end{array}$$

Note that $\beta_p : \mathbb{Q}(S,d) \to \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^d$ is the map induced by the natural embeddding $\mathbb{Q}^* \to \mathbb{Q}_p^*$, and F_p is the same map as F with its domain extended to $\mathcal{E}(\mathbb{Q}_p)/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q}_p))$. We will address this in more depth in Section 8.

Lemma 4. (*see* [27]) *Let $\mathcal{E}$ be an elliptic curve defined over $\mathbb{Q}$ and let $\widehat{\phi} : \widehat{\mathcal{E}} \to \mathcal{E}$ be a $\mathbb{Q}$-rational isogeny of degree d such that $\mathcal{E}[\phi] \subseteq \mathcal{E}(\mathbb{Q})$. Then*

$$Sel^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q}) \cong \bigcap_{p\in S} \beta_p^{-1}\left(F_p\Big(\mathcal{E}(\mathbb{Q}_p)/\widehat{\phi}\big(\widehat{\mathcal{E}}(\mathbb{Q}_p)\big)\Big)\right) \subseteq \mathbb{Q}(S,d) \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^d.$$

Proof: This follows directly from the diagram in Proposition 1 and by our construction in Proposition 2. □

Remark 7. Though it is technically imprecise to do so, we will often refer to

$$\bigcap_{p\in S} \beta_p^{-1}\left(F_p\Big(\mathcal{E}(\mathbb{Q}_p)/\widehat{\phi}\big(\widehat{\mathcal{E}}(\mathbb{Q}_p)\big)\Big)\right) \subseteq \mathbb{Q}(S,d) \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^d$$

as the $\widehat{\phi}$-Selmer group of $\widehat{\mathcal{E}}$ instead of a group *isomorphic* to $\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})$.

7. The Map $F : \mathcal{E}_t^d(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{E}}_t^d(\mathbb{Q})) \to \mathbb{Q}(S,d)$

Remark 8. Let $\phi : \mathcal{E}_t^d \to \widehat{\mathcal{E}}_t^d$ be a rational degree-d isogeny of elliptic curves over $\mathbb{Q}$ where $d \in \{4,5,7,8,9\}$ as in Tables 1 and 2. Then we can use the construction of F in Proposition 2 and the IsPrincipal function in Magma [21] applied to $d\cdot T - d\cdot\mathcal{O}$ (which computes f_T such that $\mathrm{div}(f_T) = d\cdot T - d\cdot\mathcal{O}$), to find the maps

$$F : \mathcal{E}_t^d(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{E}}_t^d(\mathbb{Q})) \to \mathbb{Q}(S,d) : (x,y) \mapsto F((x,y)). \tag{7}$$

We summarize these results in the following table.

Table 3. *The following gives the map $F(x,y)$ in (7).*

$deg(\phi)$	F
4	$x^2 - y$
5	$(x+1)y - x^2$
7	$(t-1)x^3 + (y-t^2)x^2 + (y-2ty)x + yt^2$
8	$x^4 + (4t+3)x^3 + \dfrac{2t^3+5t^2+(-4y+4)t+(-3y+1)}{t+1}x^2 + (-6yt-4y)x + (-2yt^2-3yt-y)$
9	$(-t^2-2)x^4 + (-2t^4-t^3-2t^2+(y-1))x^3 + (-t^6-2t^5-3t^4-2t^3+(3y-1)t^2+3y)x^2$ $+(3yt^4+2yt^3+3yt^2+y)x + (yt^6+2yt^5+3yt^4+2yt^3+yt^2)$

Remark 9. We have made available at [17] the PARI function Fo([x, y], d, t]), which takes as input a torsion order $d \in \{4, 5, 6, 7, 8, 9\}$, a parameter $t \in \mathbb{Q}$, and rational point on the curve $P \in \mathcal{E}_t^d$, and returns $F(P) \in \mathbb{Q}(S, d)$. For example, Fo($[-7, 49], 5, 7$) returns 343, which gives us that $F : \mathcal{E}_7^5 \to \mathbb{Q}(S, 5)$ is such that $F((-7, 49)) = 7^3$.

8. Local Considerations

Let $\mathcal{E}$ be an elliptic curve defined over $\mathbb{Q}$ and let $\widehat{\phi} : \widehat{\mathcal{E}} \to \mathcal{E}$ be a degree-d isogeny where d is a power of a prime and $\mathcal{E}[\phi] \subseteq \mathcal{E}(\mathbb{Q})$. In this section, we will state a version of Hensel's Lemma and demonstrate how it can be used to compute many of the quantities we need to determine $\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})$. First, we will use the lemma to find representatives for $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^d$ that correspond with the elements of $\mathbb{Q}(S, d)$ under our local map

$$\beta_p : \mathbb{Q}(S, d) \to \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^d \qquad \text{where } p < \infty.$$

Next, we will we will discuss how to extend the map

$$F : \mathcal{E}_t^d(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{E}}_t^d(\mathbb{Q})) \to \mathbb{Q}(S, d)$$

to

$$F_p : \mathcal{E}_t^d(\mathbb{Q}_p)/\widehat{\phi}(\widehat{\mathcal{E}}_t^d(\mathbb{Q}_p)) \to \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^d \qquad \text{where } p < \infty,$$

and how to use this map to algorithmically find generators for $\mathcal{E}_t^d(\mathbb{Q}_p)/\widehat{\phi}(\widehat{\mathcal{E}}_t^d(\mathbb{Q}_p))$.

Finally, we will consider the case $p = \infty$ and show how to do the analogous computations when we take the localization of $\mathbb{Q}$ at ∞, the real numbers.

We first statement a version of Hensel's Lemma.

Lemma 5. *(Hensel's Lemma) Let K be a number field and let $v \in M_K^0$ be a non-Archimedean valuation. Then let K_v be the completion of K with respect to the absolute value $|\cdot|_v$, and let $\mathcal{O}_v = \{x \in K_v : |x|_v \leqslant 1\}$ be its associated ring of integers. If $f(x) \in \mathcal{O}_v[x]$ and $\alpha_0 \in \mathcal{O}_v$ are such that $|f(\alpha_0)|_v < |f'(\alpha_0)|^2$, then there exists a unique $\alpha \in \mathcal{O}_v$ such that $f(\alpha) = 0$ and*

$$|\alpha - \alpha_0|_v \leqslant \left| \frac{f(\alpha_0)}{f'(\alpha_0)} \right|_v .$$

Proof: See [25], 2.1.5. □

Remark 10. Using this version of Hensel's Lemma, we can describe the local quotient group $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^d$ and the associated map $\beta_p : \mathbb{Q}(S, d) \to \mathbb{Q}_p^*/(\mathbb{Q}_p)^d$ for $p \neq \infty$, as follows. Let $S = \{p_1, p_2, \ldots, p_k\}$ be a set of rational primes that generate a subgroup of $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^d$ where d is a power of a prime. Recall from (6) that in our case, we denote this group $\mathbb{Q}(S, d)$ where S is from (5). If d is even, then -1 is not a d^{th} power in $\mathbb{Q}$, so

$$\mathbb{Q}(S, d) = \langle -1, p_1, \ldots, p_k : (-1)^2 = 1 \text{ and } p_i^d = 1 \rangle.$$

If d is odd, then -1 is a d^{th} power, so

$$\mathbb{Q}(S, d) = \langle p_1, \ldots, p_k : p_i^d = 1 \rangle.$$

In order to compute $\beta_p(\mathbb{Q}(S, d))$, we just need to check which of our elements from $\mathbb{Q}(S, d)$ become equivalent in $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^d$ using Hensel's Lemma. For example, if $|d|_p = 1$ and p_1 and p_2 are distinct primes in $\mathbb{Q}(S, d)$

such that $p_1 \cdot p_2^{d-1}$ is a d^{th} power in $\mathbb{F}_p$, then Hensel's Lemma implies that $x^d - p_1 \cdot p_2^{d-1}$ has a solution in $\mathbb{Q}_p$: that is, it is a d^{th}-power in $\mathbb{Q}_p$. Hence $p_1 \cdot p_2^{d-1} = 1$ in $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^d$, so $p_1 = p_2$ in $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^d$.

We can illustrate this more concretely with a numerical example.

Example 2. Let $\mathcal{E} : y^2 + 13xy + 84y = x^3 + 84x^2$ be the elliptic curve obtained from Table 1 when $d = 9$ and $t = 2$. Note that $9(0,0) = \mathcal{O}$ and $\Delta(\mathcal{E}) = -1 \cdot 2^9 \cdot 3^8 \cdot 7^3 \cdot 37^1$. Hence $\mathbb{Q}(S, 7) = \langle 2, 3, 7, 37 \rangle$. Now Hensel's Lemma can be invoked to find that $x^9 - 2 \cdot 3$ has a solution in $\mathbb{Q}_7$. Thus, $2 \cdot 3$ is a 9^{th} power in $\mathbb{Q}_7$ so that $2 \cdot 3 = 1$ in $\mathbb{Q}_7^*/(\mathbb{Q}_7^*)^9$. This is equivalent to saying that $2 = 3^8$ in $\mathbb{Q}_7^*/(\mathbb{Q}_7^*)^9$, so that $\beta_7(2) = 2 = 3^8$.

For additional examples, see Chapter 11 of [5], which addresses the group $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$.

Remark 11. We have made available at [17] the PARI function ModuloPowLocalp(z, d, t, p), which takes as input a torsion order $d \in \{4, 5, 6, 7, 8, 9\}$, a parameter $t \in \mathbb{Q}$, a prime $p \in S$, and a rational number $z \in \mathbb{Q}$, and returns $\beta_p(z)$. For example, ModuloPowLocalp$(17, 5, 7, 5)$ returns 2^3, so that $\beta_p(17) = 2^3$.

We are now in a position to use the local map $F_p : \mathcal{E}_t^d(\mathbb{Q}_p)/\widehat{\phi}(\widehat{\mathcal{E}}_t^d(\mathbb{Q}_p)) \to \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^d$ to find generators for $\mathcal{E}_t^d(\mathbb{Q}_p)/\widehat{\phi}(\widehat{\mathcal{E}}_t^d(\mathbb{Q}_p))$ when $p < \infty$.

Example 3. Let $\mathcal{E} : y^2 - y = x^3 - x^2$ be an elliptic curve. Note that $5(0,0) = \mathcal{O}$ and that $\mathbb{Q}(S, 5) = \langle 5, 11 \rangle$. We will use Hensel's Lemma to determine whether there exists a point $(5, \alpha_1)$ on $\mathcal{E}(\mathbb{Q}_5)$ where $\alpha_1 \in \mathbb{Q}_5$ by letting $x = 5$ and letting y remain an indeterminant in our Weierstrass equation:

$$y^2 - y = 5^3 - 5^2 = 100.$$

So we let $f(y) = y^2 - y - 100$, which implies that $f'(y) = 2y$. Now let $\alpha_0 = 5^2 + 4 \cdot 5^3$, which yields

$$f(\alpha_0) = f(525) = 2^2 \cdot 5^5 \cdot 11^1 \text{ and } f'(\alpha_0) = f'(525) = 2^1 \cdot 3^1 \cdot 5^2 \cdot 7^1.$$

Hence, $|f(\alpha_0)|_5 = 5^{-5}$ and $|f'(\alpha_0)|_5^2 = 5^{-4}$ so that $|f(\alpha_0)|_5 < |f'(\alpha_0)|_5^2$, which allows us to invoke Hensel's Lemma. Namely, we know that there exists a point $(5, \alpha_1) \in \mathcal{E}(\mathbb{Q}_5)$ for some $\alpha_1 \in \mathbb{Q}_5$. Further, we could continue this method of approximation to whatever precision we desire, say $O(5^{10})$:

$$\alpha_1 = 5^2 + 4 \cdot 5^3 + 3 \cdot 5^5 + 2 \cdot 5^6 + 4 \cdot 5^7 + 4 \cdot 5^8 + 4 \cdot 5^9 + O(5^{10}).$$

Similarly, we find that $(15, \alpha_2)$ is a point on $\mathcal{E}(\mathbb{Q}_5)$ where

$$\alpha_2 = 4 \cdot 5^2 + 4 \cdot 5^3 + 4 \cdot 5^5 + 2 \cdot 5^6 + 5^7 + O(5^{10}).$$

Now recall from Table 3 that $F : \mathcal{E}(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q}))$ is given by $F((x, y)) = (x + 1)y - x^2$. By extending this to $\mathcal{E}(\mathbb{Q}_5)$, we see that

$$F_5((5, \alpha_1)) = (5 + 1)\alpha_1 - 5^2 = 4 \cdot 5^5 + 2 \cdot 5^7 + 4 \cdot 5^8 + 4 \cdot 5^9 + O(5^{10}) = 4 + 2 \cdot 5^2 + 4 \cdot 5^3 + 4 \cdot 5^4 + O(5^5).$$

Note that the latter equality follows since $5^5 = 1$ in $\mathbb{Q}_5^*/(\mathbb{Q}_5^*)^5$. Now we can truncate this value after the first term and still use Hensel's Lemma to find its image in $\mathbb{Q}_5^*/(\mathbb{Q}_5^*)^5$ (we only need to know the behaviour of $F_5((5, \alpha_1))$ modulo 5^2). Further, we see that $-1^5 \equiv 4 \cdot 11^3 \bmod 5^2$, which implies that $4 \cdot 11^3 = 1$ in $\mathbb{Q}_5^*/(\mathbb{Q}_5^*)^5$, which is equivalent to saying that $F_5((5, \alpha_1)) \cdot 11^3 = 1$ in our quotient group. That is, $F_5((5, \alpha_1)) = 11^2$. Similarly, $F_5((15, \alpha_2)) = 11$. So we see that $(5, \alpha_1)$ and $(15, \alpha_2)$ have distinct images under F_5, but are not mutually independent generators for $\mathcal{E}(\mathbb{Q}_5)/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q}_5))$.

Remark 12. This method gives us an algorithmic process for finding independent $\mathbb{Q}_p$-points on an elliptic curve, $\mathcal{E} : y^2 + (1-w)xy + vy = x^3 + vx^2$, with a map $F : \mathcal{E}(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q})) \to \mathbb{Q}(S,d)$. Further, as long as we know how many independent points we need to find, this search algorithm becomes deterministic—conveniently, Lemma 10 in a later section does precisely this. The following merely outlines a crude variation of p-adic algorithms described elsewhere in the literature (see [27],[28], for example); we have not included here any of the standard tricks for improving efficiency, such as restricting the search to homogeneous spaces.

Step 1: Use the techniques from Remark 10 to find the image of $\mathbb{Q}(S,d)$ under the map β_p.
Step 2: Running through choices of $x_0, s \in \mathbb{Z}$, substitute $\dfrac{x_0}{p^s}$ into our Weierstrass equation for $\mathcal{E}$:

$$y^2 + (1-w)\frac{x_0}{p^s}y + vy = \left(\frac{x_0}{p^s}\right)^3 + v\left(\frac{x_0}{p^s}\right)^2.$$

Step 3: Search to see whether there exists $y_0 \in \mathbb{Q}_p$ satisfying the above polynomial. This search to increasing p-adic depth will eventually show either that the above polynomial has no $\mathbb{Q}_p$ solutions, or it will yield some $y_0 \in \mathbb{Q}$ satisfying the above polynomial to sufficient p-adic accuracy that it is guaranteed to lift to a $\mathbb{Q}_p$-solution by Hensel's Lemma. If we find a y_0 that lifts to a solution in $\mathbb{Q}_p$, continue to lift y_0 to an appropriate level of p-adic precision, then go on to Step 4.
Step 4: Use the appropriate F_p map from Table 3 to find $F_p\left(\dfrac{x_0}{p^s}, y_0\right)$.
Step 5: Use Hensel's Lemma to determine to which element of $\beta_p(\mathbb{Q}(S,d))$ is equivalent to the image of $\left(\dfrac{x_0}{p^s}, y_0\right)$ under F_p. If we did not use enough p-adic precision to determine this, go back to Step 3, lift y_0 to a higher level of precision and try again. Each time we find a point whose image under F_p is independent from the list of previous independent points found, we add that point to the list.
Step 6: When the independent points found generate a group that attain our bounds in Lemma 10, terminate the algorithm and return our list of independent local points on the curve.

Remark 13. We have made available at [17] the PARI function FpSearchp(d, t, p), which takes as input a torsion order $d \in \{4,5,6,7,8,9\}$, a parameter $t \in \mathbb{Q}$, a prime $p \in S$, and performs the above algorithm for $\mathcal{E}_t^d$ at p. For example, FpSearchp(5, 7, 7) returns 7^4, which implies that $F_7\left(\mathcal{E}_7^5(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{E}}_7^5(\mathbb{Q}))\right) = \langle 7^4\rangle$.

Remark 14. As one might expect, finding generators for $\mathcal{E}(\mathbb{R})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{R}))$ is a slightly different task than finding generators for $\mathcal{E}(\mathbb{Q}_p)/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q}_p))$. However, it is also largely a simpler process because $\mathbb{R}^*/(\mathbb{R}^*)^d$ is such a small group.

Lemma 6. *Let $\phi : \mathcal{E} \to \widehat{\mathcal{E}}$ be a degree-d $\mathbb{Q}$-rational isogeny of $\mathbb{Q}$-rational elliptic curves where d is a power of a prime. Further, suppose that $\mathcal{E}[\phi] \subseteq \mathcal{E}(\mathbb{Q})$. If $d = 2^k$, $k \geqslant 1$, then*

$$\#\mathcal{E}(\mathbb{R})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{R})) = 1 \text{ or } 2.$$

Otherwise,

$$\#\mathcal{E}(\mathbb{R})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{R})) = 1.$$

Proof: By combining the hypotheses of this lemma with Proposition 2, we see that there exists an injective homomorphism

$$F : \mathcal{E}(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q})) \to \mathbb{Q}(S,d).$$

Now, if we extend this map to the completion of $\mathbb{Q}$ at ∞ (that is $\mathbb{Q}_\infty = \mathbb{R}$), we get the following map:

$$F_\infty : \mathcal{E}(\mathbb{R})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{R})) \to \mathbb{R}^*/(\mathbb{R}^*)^d.$$

Further, we know that this map is an injection into a subgroup of $\mathbb{R}^*/(\mathbb{R}^*)^d$. When $d = 2^k$, $k \geqslant 1$, then d is even and $\mathbb{R}^*/(\mathbb{R}^*)^d = \{1\}$; otherwise the prime power d is odd and $\mathbb{R}^*/(\mathbb{R}^*)^d = \{1\}$. □

Corollary 1. *Let $\phi : \mathcal{E} \to \widehat{\mathcal{E}}$ be a degree-d $\mathbb{Q}$-rational isogeny of $\mathbb{Q}$-rational elliptic curves such that $\mathcal{E}[\phi] \subseteq \mathcal{E}(\mathbb{Q})$ where d is a power of a prime. Then we know that there exists an injective map*

$$F : \mathcal{E}(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q})) \to \mathbb{Q}(S, d)$$

where S is as in (5). If d is odd, then we can take S to be $S - \{\infty\}$ when computing $Sel^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})$.

Proof: From our previous lemma, we showed that if d is odd, then $\mathbb{R}^*/(\mathbb{R}^*)^d = \{1\}$ and $F_\infty(\mathcal{E}(\mathbb{R})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{R}))) = \{1\}$. This implies that $\beta_\infty^{-1} = F_\infty(\mathcal{E}(\mathbb{R})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{R}))) = \mathbb{Q}(S, d)$. Therefore,

$$\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q}) = \bigcap_{v \in S} \beta_v^{-1}\left(F_v\left(\mathcal{E}(\mathbb{Q}_v)/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q}_v))\right)\right) = \bigcap_{v \in S-\{\infty\}} \beta_v^{-1}\left(F_v\left(\mathcal{E}(\mathbb{Q}_v)/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q}_v))\right)\right).$$

Hence, we may take S to be $S - \{\infty\}$. □

Remark 15. If d is even, then we need a method of determining whether $\#\mathcal{E}(\mathbb{R})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{R})) = 1$ or 2. That is, whether $F_\infty(\mathcal{E}(\mathbb{R})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{R}))) = \{1\}$ or $F_\infty(\mathcal{E}(\mathbb{R})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{R}))) = \{\pm 1\}$. Note that F extends to F_∞ as follows:

$$F_\infty(P) = \begin{cases} 1 & \text{if } F(P) > 0 \\ -1 & \text{if } F(P) < 0. \end{cases}$$

Hence, this problem reduces to the problem of determining whether there exists a point $P \in \mathcal{E}(\mathbb{R})$ such that $F_\infty(P) = -1$. Since we can always extract square roots of non-negative numbers in $\mathbb{R}$, this is not a difficult task. Let $\mathcal{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x^2 + a_6$ be an elliptic curve with $k(0,0) = \mathcal{O}$ for $k = 2^j$. If we treat our Weierstrass equation as a polynomial in y, we can use the quadratic formula to get

$$y = \frac{-(a_1x + a_3) \pm \sqrt{(a_1x + a_3)^2 + 4(x^3 + a_2x^2 + a_4x^2 + a_6)}}{2}.$$

Then we have

$$F((x,y)) = F\left(\left(x, \frac{-(a_1x + a_3) \pm \sqrt{(a_1x + a_3)^2 + 4(x^3 + a_2x^2 + a_4x + a_6)}}{2}\right)\right).$$

So we can split F into two functions in x:

$$g_1(x) = F\left(\left(x, \frac{-(a_1x + a_3) + \sqrt{(a_1x + a_3)^2 + 4(x^3 + a_2x^2 + a_4x + a_6)}}{2}\right)\right)$$

and

$$g_2(x) = F\left(\left(x, \frac{-(a_1x + a_3) - \sqrt{(a_1x + a_3)^2 + 4(x^3 + a_2x^2 + a_4x + a_6)}}{2}\right)\right).$$

Now we just have to perform the simple task of checking the range of the functions $g_1(x)$ and $g_2(x)$ in $\mathbb{R}$. If either function has negative points in its range, then there exists a point $P \in \mathcal{E}(\mathbb{R})$ such that $F_\infty(P) = -1$ so that $F_\infty(\mathcal{E}(\mathbb{R})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{R}))) = \{\pm 1\}$. Otherwise, we see that $F_\infty(\mathcal{E}(\mathbb{R})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{R}))) = \{1\}$.

Example 4. Let $\mathcal{E} : y^2 + xy - 4y = x^3 - 4x^2$ be the elliptic curve from Table 1 where $d = 4$ and $t = -4$. We notice that $\mathcal{E}$ is isogenous to $\widehat{\mathcal{E}} : y^2 + xy - 4y = x^3 - 4x^2 - 60 - 380$ via an isogeny of degree 4. Now Table 3 gives us that

$$F : \mathcal{E}(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q})) \to \mathbb{Q}(S,d)$$

by $F((x,y)) = x^2 - y$. We see that we can solve for y in terms of x in our Weierstrass equation:

$$y = \frac{-(x-4) \pm \sqrt{(x-4)^2 + 4(x^3 - 4x^2)}}{2}.$$

Hence, using the method above, we have

$$g_1(x) = F\left(\left(x, \frac{-(x-4) + \sqrt{(x-4)^2 + 4(x^3 - 4x^2)}}{2}\right)\right) = x^2 - \frac{-(x-4) + \sqrt{(x-4)^2 + 4(x^3 - 4x^2)}}{2}.$$

We see that

$$\begin{aligned} g_1(0) &= 0^2 - \frac{-(0-4) + \sqrt{(0-4)^2 + 4(0^3 - 4(0)^2)}}{2} \\ &= -\frac{4 + \sqrt{16}}{2} \\ &= -4. \end{aligned}$$

That is, $F_\infty(\mathcal{E}(\mathbb{R})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{R}))) = \{\pm 1\}$.

9. Computing $\mathrm{Sel}^{(d)}(\mathcal{E}/\mathbb{Q})$ From $\mathrm{Sel}^{(\phi)}(\mathcal{E}/\mathbb{Q})$

We recall the standard observation that we can compute the rank of $\mathcal{E}(\mathbb{Q})$ by finding $\mathcal{E}(\mathbb{Q})/[d]\mathcal{E}(\mathbb{Q})$ for some integer $d > 1$. Now recall from Lemma 2 that if $\mathcal{E}$ is an elliptic curve defined over $\mathbb{Q}$ and $\phi : \mathcal{E} \to \widehat{\mathcal{E}}$ is a degree-d $\mathbb{Q}$-rational isogeny of elliptic curves, then the following is an exact sequence:

$$0 \to \mathcal{E}(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q})) \to \mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q}) \to Ш(\widehat{\mathcal{E}}/\mathbb{Q})[\widehat{\phi}] \to 0.$$

Hence, if ϕ is the multiplication-by-d map, we can attempt to compute $\mathcal{E}(\mathbb{Q})/[d]\mathcal{E}(\mathbb{Q})$ by noticing that this group injects into $\mathrm{Sel}^{(d)}(\mathcal{E}/\mathbb{Q})$:

$$0 \to \mathcal{E}(\mathbb{Q})/[d]\mathcal{E}(\mathbb{Q}) \to \mathrm{Sel}^{(d)}(\mathcal{E}/\mathbb{Q}) \to Ш(\mathcal{E}/\mathbb{Q})[d] \to 0.$$

However, since $\widehat{\phi}\circ\phi = [d]$ on $\mathcal{E}$, we can actually attempt to find $\mathrm{Sel}^{(d)}(\mathcal{E}/\mathbb{Q})$ from $\mathrm{Sel}^{(\phi)}(\mathcal{E}/\mathbb{Q})$ and $\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})$.

Lemma 7. *Let $\mathcal{E}$ and ϕ be as above. Then the two following sequences are exact:*

$$\begin{aligned} 0 \to \widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]/\phi(\mathcal{E}(\mathbb{Q})[d]) \to Sel^{(\phi)}(\mathcal{E}/\mathbb{Q}) \to Sel^{(d)}(\mathcal{E}/\mathbb{Q}) \\ \to Sel^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q}) \to Ш(\widehat{\mathcal{E}}/\mathbb{Q})[\widehat{\phi}]/\phi(Ш(\mathcal{E}/\mathbb{Q})[d]) \to 0. \end{aligned} \tag{8}$$

and

$$0 \to \widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]/\phi(\mathcal{E}(\mathbb{Q})[d]) \to \widehat{\mathcal{E}}(\mathbb{Q})/\phi(\mathcal{E}(\mathbb{Q})) \xrightarrow{\widehat{\phi}} \mathcal{E}(\mathbb{Q})/[d]\mathcal{E}(\mathbb{Q}) \to \mathcal{E}(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q})) \to 0. \tag{9}$$

Proof: See [28]. □

Lemma 8. *Let $\mathcal{E}$ to be an elliptic curve defined over $\mathbb{Q}_p$ for $p < \infty$. Then we define $\mathcal{E}'_{ns}(\mathbb{F}_p)$ to be the group of nonsingular points in $\mathcal{E}'_p(\mathbb{F}_p)$ under the reduction map*

$$\begin{aligned} R_p : \mathcal{E}(\mathbb{Q}_p) &\to \mathcal{E}'_p(\mathbb{F}_p) \\ P &\mapsto P'. \end{aligned}$$

We define

$$\mathcal{E}_0(\mathbb{Q}_p) = \{P \in \mathcal{E}(\mathbb{Q}_p) : P' \in \mathcal{E}'_{ns}(\mathbb{F}_p)\} \qquad \textit{and} \qquad \mathcal{E}_1(\mathbb{Q}_p) = \{P \in \mathcal{E}(\mathbb{Q}_p) : P' = \mathcal{O}'\}.$$

Then the following is an exact sequence:

$$0 \to \mathcal{E}_1(\mathbb{Q}_p) \to \mathcal{E}_0(\mathbb{Q}_p) \xrightarrow{R_p} \mathcal{E}'_{ns}(\mathbb{F}_p) \to 0.$$

Proof: See [29] VII.3.2.1. □

Definition 7. Let $\mathcal{E}$ and p be as above. Then we define the *Tamagawa number of* $\mathcal{E}$ *at* p to be the quantity

$$c_p = \#\mathcal{E}(\mathbb{Q}_p)/\mathcal{E}_0(\mathbb{Q}_p).$$

Definition 8. Let $\mathcal{E}$ be an elliptic curve defined over $\mathbb{Q}$ that is described by a Weierstrass equation of the form

$$\mathcal{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Then we let

$$\Omega_{\mathcal{E}} = \int\limits_{\mathcal{E}(\mathbb{R})} \left| \frac{dx}{2y + a_1x + a_3} \right|.$$

Definition 9. Let $\mathcal{E}$ be an elliptic curve defined over $\mathbb{Q}$ and let $\phi : \mathcal{E} \to \widehat{\mathcal{E}}$ be a $\mathbb{Q}$-rational isogeny of elliptic curves where $\mathcal{E}$ and $\widehat{\mathcal{E}}$ are described by Weierstrass equations as follows:

$$\mathcal{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \text{ and } \widehat{\mathcal{E}} : Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4X + A_6.$$

We have Laurent series expansions x, y, X, and Y in terms of local parameters, z and Z, respectively where $z = -x/y$ and $Z = -X/Y$ (see [29], IV.1.1.2):

$$x(z) = \frac{1}{z^2} - \frac{a_1}{z} - a_2 - a_3z - (a_4 + a_1a_3)z^2 + O(z^3) \qquad \text{and} \qquad y(z) = -\frac{1}{z}x(z)$$
$$X(Z) = \frac{1}{Z^2} - \frac{A_1}{Z} - A_2 - A_3Z - (A_4 + A_1A_3)Z^2 + O(Z^3) \qquad \text{and} \qquad Y(Z) = -\frac{1}{Z}X(Z).$$

The notation $O(z^3)$ indicates higher order z-terms with coefficients in $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$, and likewise for $O(Z^3)$.

Now let $\phi((x, y)) = (X, Y)$ be our formula for ϕ. Then we can combine all of this to write

$$Z = -\frac{X}{Y} = f(z) \in \mathbb{Q}[[z]].$$

We define γ_ϕ to be norm of the leading coefficient of $f(z)$. Similarly, we can write

$$z = -\frac{x}{y} = F(Z) \in \mathbb{Q}[[Z]]$$

to find $\gamma_{\widehat{\phi}}$.

Lemma 9. *Let* $\mathcal{E}_t^d$, $\widehat{\mathcal{E}}_t^d$, $\phi : \mathcal{E}_t^d \to \widehat{\mathcal{E}}_t^d$, *and* $\widehat{\phi} : \widehat{\mathcal{E}}_t^d \to \mathcal{E}_t^d$ *be as in Tables 1 and 2. Then* $\gamma_\phi = 1$ *and* $\gamma_{\widehat{\phi}} = d$.

Proof: This follows immediately from [34], Equation 13. □

Lemma 10. *Let $\mathcal{E}$ be an elliptic curve defined over $\mathbb{Q}$ and let $\phi : \mathcal{E} \to \widehat{\mathcal{E}}$ be a degree-d $\mathbb{Q}$-rational isogeny where d is a power of a prime and $\mathcal{E}[\phi] \subseteq \mathbb{Q}$. Let p be a finite prime. Then*

$$\#\mathcal{E}(\mathbb{Q}_p)/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q}_p)) = |\gamma_{\widehat{\phi}}|_p^{-1} \#\widehat{\mathcal{E}}(\mathbb{Q}_p)[\widehat{\phi}] \, \frac{c_{\mathcal{E},p}}{c_{\widehat{\mathcal{E}},p}}.$$

Further, when $p = \infty$, we can use Lemma 6 and Remark 15 to determine $\#\mathcal{E}(\mathbb{R})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{R}))$.

Proof: See [26], 3.8. □

Theorem 6 (Cassels)**.** *Let $\phi : \mathcal{E} \to \widehat{\mathcal{E}}$ be a $\mathbb{Q}$-isogeny of $\mathbb{Q}$-elliptic curves. Then*

$$\frac{\#Sel^{(\phi)}(\mathcal{E}/\mathbb{Q})}{\#Sel^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})} = \frac{\#\mathcal{E}(\mathbb{Q})[\phi] \;\; \Omega_{\widehat{\mathcal{E}}} \;\; \prod_p c_{\widehat{\mathcal{E}},p}}{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}] \;\; \Omega_{\mathcal{E}} \;\; \prod_p c_{\mathcal{E},p}}.$$

Proof: See [4]. In addition, [28] applies this theorem to a descent via isogeny. □

Remark 16. The quantities $\Omega_{\mathcal{E}}$ and $c_{\mathcal{E},p}$ can be easily computed using functions built into Magma [21] or PARI [24]. A general algorithm for computing Tamagawa numbers for elliptic curves can be found in [31]. Finally, determining $\#\widehat{\mathcal{E}}(\mathbb{Q}_p)[\widehat{\phi}]$ is a direct application of Hensel's Lemma.

Now we see that Cassels' ratio theorem gives us a method for trying to compute $\mathcal{E}(\mathbb{Q})/[d]\mathcal{E}(\mathbb{Q})$ (and thus $\mathcal{E}(\mathbb{Q})$) simply by finding $\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})$. Namely, if we have computed $\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})$, then we can use Theorem 6 to find $\#\mathrm{Sel}^{(\phi)}(\mathcal{E}/\mathbb{Q})$. Now Lemma 7 gives us that

$$0 \to \widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]/\phi(\mathcal{E}(\mathbb{Q})[d]) \to \mathrm{Sel}^{(\phi)}(\mathcal{E}/\mathbb{Q}) \to \mathrm{Sel}^{(d)}(\mathcal{E}/\mathbb{Q}) \\ \to \mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q}) \to Ш(\widehat{\mathcal{E}}/\mathbb{Q})[\widehat{\phi}]/\phi(Ш(\mathcal{E}/\mathbb{Q})[d]) \to 0.$$

Hence,

$$\#\mathrm{Sel}^{(d)}(\mathcal{E}/\mathbb{Q}) \leqslant \frac{\#\mathrm{Sel}^{(\phi)}(\mathcal{E}/\mathbb{Q}) \cdot \#\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})}{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]/\phi(\mathcal{E}(\mathbb{Q})[d])} = \frac{\#\mathcal{E}(\mathbb{Q})[\phi] \;\; \Omega_{\widehat{\mathcal{E}}} \;\; \prod_p c_{\widehat{\mathcal{E}},p}}{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}] \;\; \Omega_{\mathcal{E}} \;\; \prod_p c_{\mathcal{E},p}} \cdot \frac{\#\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})}{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]/\phi(\mathcal{E}(\mathbb{Q})[d])}.$$

In addition, as long as $Ш(\widehat{\mathcal{E}}/\mathbb{Q})[\widehat{\phi}]/\phi(Ш(\mathcal{E}/\mathbb{Q})[d])$ is trivial, this will be an equality. Now from Lemma 2, we have the following exact sequence:

$$0 \to \mathcal{E}(\mathbb{Q})/[d]\mathcal{E}(\mathbb{Q}) \to \mathrm{Sel}^{(d)}(\mathcal{E}/\mathbb{Q}) \to Ш(\mathcal{E}/\mathbb{Q})[d] \to 0.$$

So this implies that

$$\#\mathcal{E}(\mathbb{Q})/[d]\mathcal{E}(\mathbb{Q}) \leqslant \#\mathrm{Sel}^{(d)}(\mathcal{E}/\mathbb{Q}) \leqslant \frac{\#\mathcal{E}(\mathbb{Q})[\phi] \;\; \Omega_{\widehat{\mathcal{E}}} \;\; \prod_p c_{\widehat{\mathcal{E}},p}}{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}] \;\; \Omega_{\mathcal{E}} \;\; \prod_p c_{\mathcal{E},p}} \cdot \frac{\#\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})}{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]/\phi(\mathcal{E}(\mathbb{Q})[d])}, \tag{10}$$

where everything becomes an equality when $Ш(\widehat{\mathcal{E}}/\mathbb{Q})[\widehat{\phi}]/\phi(Ш(\mathcal{E}/\mathbb{Q})[d])$ and $Ш(\mathcal{E}/\mathbb{Q})[d]$ are trivial. So we see that when this is the case, we can completely determine $\#\mathcal{E}(\mathbb{Q})/[d]\mathcal{E}(\mathbb{Q})$ (and thus $\mathcal{E}(\mathbb{Q})$) simply by computing $\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})$ and some other values that can be easily calculated in Magma [21] or PARI [24].

Application 1. While we will use Theorem 6 mainly for the purpose of finding the order of $\mathrm{Sel}^{(\phi)}(\mathcal{E}/\mathbb{Q})$ from the order of $\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})$, it has another use that does not seem to have been previously exploited. Namely, given two isogenous curves, $\mathcal{E}$ and $\widehat{\mathcal{E}}$, where the rank of $\mathcal{E}(\mathbb{Q})$ can be computed by a complete 2-descent, we can sometimes quickly demonstrate the existence of nontrivial elements in the d-part of the Tate-Shafarevich group, while avoiding the difficult portion of the isogeny computation, as follows.

Let $\phi : \mathcal{E} \to \widehat{\mathcal{E}}$ be a degree-d $\mathbb{Q}$-rational isogeny of $\mathbb{Q}$-rational elliptic curves, where d is a prime power. Suppose that $Ш(\mathcal{E}/\mathbb{Q})[2]$ is trivial so that a complete 2-descent on $\mathcal{E}$ yields that the rank of $\mathcal{E}(\mathbb{Q})$ is some $r \in \mathbb{Z}^+$. By also computing $\mathcal{E}_{\text{tors}}(\mathbb{Q})$, we can immediately find $\#\mathcal{E}(\mathbb{Q})/[d]\mathcal{E}(\mathbb{Q}) \subseteq \text{Sel}^{(d)}(\mathcal{E}/\mathbb{Q})$. It is similarly an easy task to find $\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]/\phi(\mathcal{E}(\mathbb{Q})[d])$. Now if we use Cassels formula from Theorem 6 to compute the ratio of the sizes of our Selmer groups, we get

$$\frac{\#\text{Sel}^{(\phi)}(\mathcal{E}/\mathbb{Q})}{\#\text{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})} = \frac{\#\mathcal{E}(\mathbb{Q})[\phi] \ \ \Omega_{\widehat{\mathcal{E}}} \ \ \prod_p c_{\widehat{\mathcal{E}},p}}{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}] \ \ \Omega_{\mathcal{E}} \ \ \prod_p c_{\mathcal{E},p}} = q^k$$

where $q|d$ and $k \in \mathbb{Z}$. Without loss of generality, we may assume that $k \geqslant 0$ (if k is negative, then relabel $\widehat{\phi} : \widehat{\mathcal{E}} \to \mathcal{E}$ as $\phi : \mathcal{E} \to \widehat{\mathcal{E}}$ and start over). Now since $\#\text{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q}) \geqslant 1$, we see that this ratio gives us a lower bound on the size of $\text{Sel}^{(\phi)}(\mathcal{E}/\mathbb{Q})$. Further, the exact sequence from Lemma 7,

$$0 \to \widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]/\phi(\mathcal{E}(\mathbb{Q})[d]) \to \text{Sel}^{(\phi)}(\mathcal{E}/\mathbb{Q}) \to \text{Sel}^{(d)}(\mathcal{E}/\mathbb{Q}) \to$$
$$\text{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q}) \to Ш(\widehat{\mathcal{E}}/\mathbb{Q})[\widehat{\phi}]/\phi(Ш(\mathcal{E}/\mathbb{Q})[d]) \to 0,$$

can be used to extend this to a lower bound on the order of $\text{Sel}^{(d)}(\mathcal{E}/\mathbb{Q})$:

$$\begin{aligned}
\#\text{Sel}^{(d)}(\mathcal{E}/\mathbb{Q}) &\geqslant \frac{\#\text{Sel}^{(\phi)}(\mathcal{E}/\mathbb{Q})}{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]/\phi(\mathcal{E}(\mathbb{Q})[d])} \\
&\geqslant \left(\frac{\#\text{Sel}^{(\phi)}(\mathcal{E}/\mathbb{Q})}{\#\text{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})}\right)\left(\frac{1}{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]/\phi(\mathcal{E}(\mathbb{Q})[d])}\right) \\
&= \left(\frac{\#\mathcal{E}(\mathbb{Q})[\phi] \ \ \Omega_{\widehat{\mathcal{E}}} \ \ \prod_p c_{\widehat{\mathcal{E}},p}}{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}] \ \ \Omega_{\mathcal{E}} \ \ \prod_p c_{\mathcal{E},p}}\right)\left(\frac{1}{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]/\phi(\mathcal{E}(\mathbb{Q})[d])}\right).
\end{aligned}$$

Now if it happens that our lower bound on the order of $\text{Sel}^{(d)}(\mathcal{E}/\mathbb{Q})$ exceeds the value we computed for $\#\mathcal{E}(\mathbb{Q})/[d]\mathcal{E}(\mathbb{Q})$, then we have verified that $Ш(\mathcal{E}/\mathbb{Q})[d]$ is nontrivial. Further, the exact sequence from Lemma 2 allows us to put a lower bound on the order of the d-part of Sha:

$$\#Ш(\mathcal{E}/\mathbb{Q})[d] \geqslant \left(\frac{\#\mathcal{E}(\mathbb{Q})[\phi] \ \ \Omega_{\widehat{\mathcal{E}}} \ \ \prod_p c_{\widehat{\mathcal{E}},p}}{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}] \ \ \Omega_{\mathcal{E}} \ \ \prod_p c_{\mathcal{E},p}}\right)\left(\frac{1}{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]/\phi(\mathcal{E}(\mathbb{Q})[d])}\right)\left(\frac{1}{\#\mathcal{E}(\mathbb{Q})/[d]\mathcal{E}(\mathbb{Q})}\right).$$

We summarize this result in the following proposition, which does not seem to have been written down elsewhere in this form in the other descent literature, and which will prove useful in our subsequent examples.

Proposition 3. *Let $\phi : \mathcal{E} \to \widehat{\mathcal{E}}$ be a $\mathbb{Q}$-rational isogeny of $\mathbb{Q}$-rational elliptic curves such that $\deg(\phi)$ is a prime power. Then*

$$\#Ш(\mathcal{E}/\mathbb{Q})[d] \geqslant \left(\frac{\#\mathcal{E}(\mathbb{Q})[\phi] \ \ \Omega_{\widehat{\mathcal{E}}} \ \ \prod_p c_{\widehat{\mathcal{E}},p}}{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}] \ \ \Omega_{\mathcal{E}} \ \ \prod_p c_{\mathcal{E},p}}\right)\left(\frac{1}{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]/\phi(\mathcal{E}(\mathbb{Q})[d])}\right)\left(\frac{1}{\#\mathcal{E}(\mathbb{Q})/[d]\mathcal{E}(\mathbb{Q})}\right)$$

and

$$\#Ш(\widehat{\mathcal{E}}/\mathbb{Q})[d] \geqslant \left(\frac{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}] \ \ \Omega_{\mathcal{E}} \ \ \prod_p c_{\mathcal{E},p}}{\#\mathcal{E}(\mathbb{Q})[\phi] \ \ \Omega_{\widehat{\mathcal{E}}} \ \ \prod_p c_{\widehat{\mathcal{E}},p}}\right)\left(\frac{1}{\#\mathcal{E}(\mathbb{Q})[\phi]/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q})[d])}\right)\left(\frac{1}{\#\widehat{\mathcal{E}}(\mathbb{Q})/[d]\widehat{\mathcal{E}}(\mathbb{Q})}\right).$$

Example 5. Consider

$$\mathcal{E} : y^2 + xy + y = x^3 - x^2 - 1005630x + 571521997$$

and

$$\widehat{\mathcal{E}} : y^2 + xy + y = x^3 - x^2 - 911138880x - 10586098442003.$$

We notice that there exists a $\mathbb{Q}$-rational isogeny of degree 13 such that $\phi : \mathcal{E} \to \widehat{\mathcal{E}}$. Using Magma [21] to perform a complete 2-descent on $\mathcal{E}$, we see that $\mathrm{rank}(\mathcal{E}(\mathbb{Q})) = \mathrm{rank}(\widehat{\mathcal{E}}(\mathbb{Q})) = 0$. Further, recall that elliptic curves cannot have rational torsion points of order 13. Hence, we have that

$$\begin{aligned} Ш(\widehat{\mathcal{E}}/\mathbb{Q})[13] &\geqslant \left(\frac{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]\ \ \Omega_{\mathcal{E}}\ \ \prod_p c_{\mathcal{E},p}}{\#\mathcal{E}(\mathbb{Q})[\phi]\ \ \Omega_{\widehat{\mathcal{E}}}\ \ \prod_p c_{\widehat{\mathcal{E}},p}}\right)\left(\frac{1}{\#\mathcal{E}(\mathbb{Q})[\phi]/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q})[13])}\right)\left(\frac{1}{\#\widehat{\mathcal{E}}(\mathbb{Q})/[13]\widehat{\mathcal{E}}(\mathbb{Q})}\right) \\ &= \left(\frac{\Omega_{\mathcal{E}}\ \ \prod_p c_{\mathcal{E},p}}{\Omega_{\widehat{\mathcal{E}}}\ \ \prod_p c_{\widehat{\mathcal{E}},p}}\right) \\ &= 13^2. \end{aligned}$$

So we have found an elliptic curve with nontrivial 13-part of Sha. However, to find the actual size of $Ш(\widehat{\mathcal{E}}/\mathbb{Q})[13]$, we would need to actually compute $\mathrm{Sel}^{(13)}(\widehat{\mathcal{E}}/\mathbb{Q})$. As a point of interest, note that we can use Magma [21] to see that the Birch and Swinnerton-Dyer conjecture (see [35]) predicts that $\#Ш(\widehat{\mathcal{E}}/\mathbb{Q}) = 13^2$, which coincides with the lower bound that we computed for $\#Ш(\widehat{\mathcal{E}}/\mathbb{Q})[13]$.

10. A Sketch of the Algorithm

In this section, we combine all of the above discussion to outline our specific descent process. See [27] for the more general algorithm on which this is based. This same approach is used for descents on elliptic curves in, for example, [12] and [28].

Input: $d \in \{4,5,7,8,9\}$ and $t \in \mathbb{Q}$ corresponding to the elliptic curve $\mathcal{E}_t^d$ from Table 1.

Output: $\dfrac{\#\mathrm{Sel}^{(\phi)}(\mathcal{E}/\mathbb{Q}) \cdot \#\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})}{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]/\phi(\mathcal{E}(\mathbb{Q})[d])}$, which serves as an upper bound for $\#\mathcal{E}_t^d(\mathbb{Q})/[d]\mathcal{E}_t^d(\mathbb{Q})$.

Step 1: Pick $d \in \{4,5,7,8,9\}$ and $t \in \mathbb{Q}^*$ such that $\mathcal{E}_t^d = \mathcal{E}$ is an elliptic curve (see Table 1).

Step 2: Use Lemma 1 to find the isogeny $\phi : \mathcal{E} \to \widehat{\mathcal{E}}$ such that $\mathcal{E}[\phi] = \langle(0,0)\rangle \subseteq \mathcal{E}(\mathbb{Q})$. In addition, use Table 2 to find the Weierstrass equation for $\widehat{\mathcal{E}}$.

Step 3: Find the set of primes S of (5) where $\mathcal{E}$ has bad reduction (the prime at ∞, and the primes p such that $p|d$) minus any primes p such that $\gcd(d, c_{\mathcal{E},p}) = \gcd(d, c_{\widehat{\mathcal{E}},p}) = 1$. If d is odd, then Corollary 1 implies that we can let S be $S - \{\infty\}$.

Step 4: Refer to Table 3 to find a suitable map $F : \mathcal{E}(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q})) \to \mathbb{Q}(S,d)$ as in Proposition 2. In addition, let F_p be the natural extension of F to $F_p : \mathcal{E}(\mathbb{Q}_p)/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q}_p)) \to \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^d$.

Step 5: For each $p \in S$, find generators for $\mathcal{E}(\mathbb{Q}_p)/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q}_p))$ by using the method outlined in Remark 12. Note that we continue our search until the number of generators we find implies that $\#\mathcal{E}(\mathbb{Q}_p)/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q}_p))$ coincides with Lemma 10:

$$\#\mathcal{E}(\mathbb{Q}_p)/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q}_p)) = |\gamma_{\widehat{\phi}}|_p^{-1} \#\widehat{\mathcal{E}}(\mathbb{Q}_p)[\widehat{\phi}]\, \frac{c_{\mathcal{E},p}}{c_{\widehat{\mathcal{E}},p}}.$$

Step 6: Compute $\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})$ by finding

$$\bigcap_{p \in S} \beta_p^{-1}\Big(F_p\Big(\mathcal{E}(\mathbb{Q}_p)/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q}_p))\Big)\Big).$$

Step 7: Use Theorem 6 to compute the size of $\mathrm{Sel}^{(\phi)}(\mathcal{E}/\mathbb{Q})$:

$$\frac{\#\mathrm{Sel}^{(\phi)}(\mathcal{E}/\mathbb{Q})}{\#\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})} = \frac{\#\mathcal{E}(\mathbb{Q})[\phi]\ \ \Omega_{\widehat{\mathcal{E}}}\ \ \prod_p c_{\widehat{\mathcal{E}},p}}{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]\ \ \Omega_{\mathcal{E}}\ \ \prod_p c_{\mathcal{E},p}}.$$

Step 8: Use the inequality in (10),

$$\#\mathcal{E}(\mathbb{Q})/[d]\mathcal{E}(\mathbb{Q}) \leqslant \#\mathrm{Sel}^{(d)}(\mathcal{E}/\mathbb{Q}) \leqslant \frac{\#\mathrm{Sel}^{(\phi)}(\mathcal{E}/\mathbb{Q}) \cdot \#\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})}{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]/\phi(\mathcal{E}(\mathbb{Q})[d])},$$

to find an upper bound for the order of $\mathrm{Sel}^{(d)}(\mathcal{E}/\mathbb{Q})$. Recall that as long as

$$Ш(\widehat{\mathcal{E}}/\mathbb{Q})[\widehat{\phi}]/\phi(Ш(\mathcal{E}/\mathbb{Q})[d]) \text{ and } Ш(\mathcal{E}/\mathbb{Q})[d]$$

are both trivial, then our upper bound is actually an equality. Now we can try to find the rank of $\mathcal{E}(\mathbb{Q})$ by finding enough independent points on $\mathcal{E}(\mathbb{Q})$ to imply that, indeed,

$$\#\mathcal{E}(\mathbb{Q})/[d]\mathcal{E}(\mathbb{Q}) = \frac{\#\mathrm{Sel}^{(\phi)}(\mathcal{E}/\mathbb{Q}) \cdot \#\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})}{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]/\phi(\mathcal{E}(\mathbb{Q})[d])}.$$

So in this step, we initiate a search on $\mathcal{E}(\mathbb{Q})$ to try to find these independent points. Note that we need a criterion for determining whether two rational points on an elliptic curve are independent from one another in $\mathcal{E}(\mathbb{Q})$. While we can use our F-map to determine this in $\mathcal{E}(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q}))$, this is not sufficient for $\mathcal{E}(\mathbb{Q})$ or $\mathcal{E}(\mathbb{Q})/[d]\mathcal{E}(\mathbb{Q})$. Luckily, this is not considered to be a difficult problem. See [36] for a PARI function that does precisely this by using height pairing matrices. Once we have found enough points to verify that the above bound is an equality, we terminate the algorithm and return the rank of $\mathcal{E}(\mathbb{Q})$. Of course, if we encounter nontrivial Sha, then this step will never terminate.

Remark 17. We have made available at [17] the PARI function SelmerBound(d, t), which implements the above algorithm for $\mathcal{E}_t^d$. For example, SelmerBound(5, 4) returns 5, which implies that the rank of $\mathcal{E}_4^5 : y^2 + 5xy + 4y = x^3 + 4x^2$ is 0 and $\mathcal{E}_4^5(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z}$.

11. An Example of a Descent Via 9-Isogeny on a Curve of Rank 1

Let $d = 9$ and $t = 2$ in the algorithm from Section 10. Then our curves $\mathcal{E}_t^d$ and $\widehat{\mathcal{E}}_t^d$ are:

$$\mathcal{E} : y^2 + 13xy + 84y = x^3 + 84x^2 \qquad \text{and} \qquad \widehat{\mathcal{E}} : y^2 + 13xy + 84y = x^3 + 84x^2 - 154410 - 41506050.$$

Further, $S = \{2, 3, 7, 37\}$. From Table 3, we have that

$$\begin{aligned} F : \mathcal{E}(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q})) &\to \mathbb{Q}(S, 9) \\ (x, y) &\mapsto -6x^4 + (y - 49)x^3 + (15y - 196)x^2 + 77yx + 196y. \end{aligned}$$

Now a few simple calculations can be combined with Lemma 10 to yield the following:

p	$\lvert\gamma_{\widehat{\phi}}\rvert_p^{-1}$	$\#\widehat{\mathcal{E}}(\mathbb{Q}_p)[\widehat{\phi}]$	$c_{\mathcal{E},p}$	$c_{\widehat{\mathcal{E}},p}$	$\#\mathcal{E}(\mathbb{Q}_p)/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q}_p))$
2	1	1	9	1	9
3	9	1	9	1	81
7	1	3	3	3	3
37	1	9	1	9	1

Using the techniques from Section 8, we have the following information about our local quotient groups, $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^9$:

p	Generators for $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^9$	$\beta_p(2)$	$\beta_p(3)$	$\beta_p(7)$	$\beta_p(37)$
2	$\langle 2\rangle$	2	1	1	1
3	$\langle 2,3\rangle$	2	3	2^7	2^6
7	$\langle 2,7 : 2^3=1\rangle$	2	2^2	7	2
37	$\langle 2,37\rangle$	2	2^8	2^5	37

We notice that, since $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^9=\langle 2\rangle$ and $\#\mathcal{E}(\mathbb{Q}_2)/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q}_2))=9$, it must be the case that

$$\beta_2^{-1}\Big(F_2\Big(\mathcal{E}(\mathbb{Q}_2)/\widehat{\phi}\big(\widehat{\mathcal{E}}(\mathbb{Q}_2)\big)\Big)\Big)=\langle 2,3,7,37\rangle.$$

Similarly, since $\#\mathbb{Q}_3^*/(\mathbb{Q}_3)^9=\#\langle 2,3\rangle=81$ and $\#\mathcal{E}(\mathbb{Q}_3)/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q}_3))=81$, we have that

$$\beta_3^{-1}\Big(F_3\Big(\mathcal{E}(\mathbb{Q}_3)/\widehat{\phi}\big(\widehat{\mathcal{E}}(\mathbb{Q}_3)\big)\Big)\Big)=\langle 2,3,7,37\rangle.$$

In addition, since $\#\mathcal{E}(\mathbb{Q}_{37})/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q}_{37}))=1$, we see that

$$\begin{aligned}\beta_{37}^{-1}\Big(F_{37}\Big(\mathcal{E}(\mathbb{Q}_{37})/\widehat{\phi}\big(\widehat{\mathcal{E}}(\mathbb{Q}_{37})\big)\Big)\Big) &= \ker(\beta_{37})\\ &= \{2^{k_2}\cdot 3^{k_3}\cdot 7^{k_7} : 0\leqslant k_i\leqslant 8 \text{ and } k_2+8k_3+5k_7\equiv 0 \bmod 9\}\\ &= \langle 2^1\cdot 3^1, 3^5\cdot 7^1\rangle.\end{aligned}$$

Now all we have left to do is consider the case when $p=7$.

We start by mapping our torsion points:

$P\in\mathcal{E}(\mathbb{Q})[\phi]$	$F(P)$	$F_7(P)$
$(0,0)$	$2^5\cdot 3^8\cdot 7^6$	$2^3\cdot 7^6$
$2(0,0)$	$2^1\cdot 3^7\cdot 7^3$	$2^6\cdot 7^3$
$3(0,0)$	$2^6\cdot 3^6$	1
$4(0,0)$	$2^2\cdot 3^5\cdot 7^6$	$2^3\cdot 7^3$
$5(0,0)$	$2^7\cdot 3^4\cdot 7^3$	$2^6\cdot 7^6$
$6(0,0)$	$2^3\cdot 3^3$	1
$7(0,0)$	$2^8\cdot 3^2\cdot 7^6$	$2^3\cdot 7^3$
$8(0,0)$	$2^4\cdot 3^1\cdot 7^3$	$2^6\cdot 7^6$
$\mathcal{O}$	1	1

Hence, we see that

$$\begin{aligned}\beta_7^{-1}\Big(F_7\Big(\mathcal{E}(\mathbb{Q}_7)/\widehat{\phi}\big(\widehat{\mathcal{E}}(\mathbb{Q}_7)\big)\Big)\Big) &= \langle 2^3\cdot 7^3\rangle\{2^{k_2}\cdot 3^{k_3} : 0\leqslant k_i\leqslant 8 \text{ and } k_2+2k_3\equiv 0 \bmod 3\}\\ &= \langle 2^1\cdot 3^1, 2^3\cdot 7^3, 3^3\cdot 7^3\rangle.\end{aligned}$$

When we take our intersection, we get

$$\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q}) = \langle 2^1\cdot 3^1, 2^3\cdot 7^3, 3^3\cdot 7^3\rangle \bigcap \langle 2^1\cdot 3^1, 3^5\cdot 7^1\rangle = \langle 2^1\cdot 3^1, 2^3\cdot 7^3\rangle \cong \mathbb{Z}/9\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}.$$

Using our formula from Theorem 6, we see that this implies $\#\mathrm{Sel}^{(\phi)}(\mathcal{E}/\mathbb{Q}) = 3$. Now recall the following exact sequence from Lemma 7:

$$0 \to \mathcal{E}(\mathbb{Q})[\phi]/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q})[9]) \to \mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q}) \to \mathrm{Sel}^{(9)}(\widehat{\mathcal{E}}/\mathbb{Q}) \to \mathrm{Sel}^{(\phi)}(\mathcal{E}/\mathbb{Q}) \to \dots .$$

Since $\#\mathrm{Sel}^{(\phi)}(\mathcal{E}/\mathbb{Q}) = 3$, $\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}] = 1$, and $\#\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q}) = 27$, we see that

$$\#\mathrm{Sel}^{(9)}(\mathcal{E}/\mathbb{Q}) \leqslant \frac{\#\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q})\cdot\#\mathrm{Sel}^{(\phi)}(\mathcal{E}/\mathbb{Q})}{\#\mathcal{E}(\mathbb{Q})[\phi]} = 9^2.$$

A short search for independent rational points on $\mathcal{E}(\mathbb{Q})$ yields the point $(-21/4, 315/8)$ of infinite order. Since $\#\mathcal{E}_{\mathrm{tors}}(\mathbb{Q}) = 9$, this gives us that $\#\mathcal{E}(\mathbb{Q})/[9]\mathcal{E}(\mathbb{Q}) \geqslant 9^2$. Hence,

$$9^2 \leqslant \#\mathcal{E}(\mathbb{Q})/[9]\mathcal{E}(\mathbb{Q}) \leqslant \#\mathrm{Sel}^{(9)}(\mathcal{E}/\mathbb{Q}) \leqslant 9^2,$$

which implies that the rank of $\mathcal{E}(\mathbb{Q})$ is 1 and

$$\mathcal{E}(\mathbb{Q}) = \langle (0,0), (-21/4, 315/8)\rangle \cong \mathbb{Z}/9\mathbb{Z}\times\mathbb{Z}^1.$$

12. An Elliptic Curve with Non-Trivial 9-part of Sha

Let $d = 9$ and $t = 1/2$ in the algorithm from Section 10. Then

$$\mathcal{E}: y^2 + \frac{11}{8}xy + \frac{21}{32}y = x^3 + \frac{21}{32}x^2 \qquad \text{and} \qquad \widehat{\mathcal{E}}: y^2 + \frac{11}{8}xy + \frac{21}{32}y = x^3 + \frac{21}{32}x^2 - \frac{190905}{2048}x - \frac{49989225}{131072}.$$

We recall from Proposition 3 that

$$\#Ш(\widehat{\mathcal{E}}/\mathbb{Q})[d] \geqslant \left(\frac{\#\widehat{\mathcal{E}}(\mathbb{Q})[\widehat{\phi}]\ \ \Omega_{\mathcal{E}}\ \ \prod_p c_{\mathcal{E},p}}{\#\mathcal{E}(\mathbb{Q})[\phi]\ \ \Omega_{\widehat{\mathcal{E}}}\ \ \prod_p c_{\widehat{\mathcal{E}},p}}\right)\left(\frac{1}{\#\mathcal{E}(\mathbb{Q})[\phi]/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q})[d])}\right)\left(\frac{1}{\#\widehat{\mathcal{E}}(\mathbb{Q})/[d]\widehat{\mathcal{E}}(\mathbb{Q})}\right).$$

Now by computing all of these values with a computer algebra package such as Magma [21], we see that

$$\#Ш(\widehat{\mathcal{E}}/\mathbb{Q})[9] \geqslant \left(\frac{1\cdot(9\Omega_{\widehat{\mathcal{E}}})\cdot 243}{9\cdot(\Omega_{\widehat{\mathcal{E}}})\cdot 3}\right)\left(\frac{1}{9}\right)\left(\frac{1}{1}\right) = 9.$$

We claim that, in fact, $\#Ш(\widehat{\mathcal{E}}/\mathbb{Q})[9] = 9$, as follows. The same method of descent via isogeny as above yields that

$$\begin{aligned}\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q}) &= \beta_7^{-1}\Big(F_7\big(\mathcal{E}(\mathbb{Q}_7)/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q}_7))\big)\Big)\bigcap\langle 2,3,7\rangle \\ &= \langle 7^3\rangle\{2^{k_2}\cdot 3^{k_3}\cdot 17^{k_{17}} : 0\leqslant k_i\leqslant 8 \text{ and } k_2 + 2\cdot k_3 \equiv 0 \bmod 3\}.\end{aligned}$$

A quick calculation gives us that $\#\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q}) = 9^2$. Using our formula from Theorem 6, we see that this implies $\#\mathrm{Sel}^{(\phi)}(\mathcal{E}/\mathbb{Q}) = 1$. Now recall the following exact sequence from Lemma 7:

$$\begin{aligned}0 \to \mathcal{E}(\mathbb{Q})[\phi]/\widehat{\phi}(\widehat{\mathcal{E}}(\mathbb{Q})[9]) \to \mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q}) \to \mathrm{Sel}^{(9)}(\widehat{\mathcal{E}}/\mathbb{Q}) \\ \to \mathrm{Sel}^{(\phi)}(\mathcal{E}/\mathbb{Q}) \to Ш(\mathcal{E}/\mathbb{Q})[\phi]/\widehat{\phi}(Ш(\widehat{\mathcal{E}}/\mathbb{Q})[9]) \to 0.\end{aligned}$$

Since $\#\mathrm{Sel}^{(\phi)}(\mathcal{E}/\mathbb{Q}) = 1$, $\#\widehat{\mathcal{E}}(\mathbb{Q})[9] = 1$, $\#\mathcal{E}(\mathbb{Q})[\phi] = 9$, $\#\mathrm{Sel}^{(\widehat{\phi})}(\widehat{\mathcal{E}}/\mathbb{Q}) = 9^2$, we see that $\#\mathrm{Sel}^{(9)}(\widehat{\mathcal{E}}/\mathbb{Q}) = 9$. Hence, we have that

$$\mathrm{Sel}^{(9)}(\widehat{\mathcal{E}}/\mathbb{Q}) \cong Ш(\widehat{\mathcal{E}}/\mathbb{Q})[9]$$

and $\#Ш(\widehat{\mathcal{E}}/\mathbb{Q})[9] = 9$, as claimed.

Note that based on the above calculations, we can only *bound* the order of the 9-Selmer group of $\mathcal{E}$:

$$\#\mathrm{Sel}^{(9)}(\mathcal{E}/\mathbb{Q}) \leqslant 9^2.$$

However, if the well-known conjecture that the order of $Ш(\mathcal{E}/K)$ is finite for any elliptic curve $\mathcal{E}$ defined over a number field K is someday proved, then we will be able to say a bit more about $\#\mathrm{Sel}^{(9)}(\mathcal{E}/\mathbb{Q})$. Namely, if we knew that $\#Ш(\mathcal{E}/\mathbb{Q}) < \infty$, then this would imply that the order of $Ш(\mathcal{E}/\mathbb{Q})[d]$ is a perfect square for any $d \geqslant 2$ (see, for example, [16], 5.5). This follows from results of Cassels and Tate, which imply that if $Ш(\mathcal{E}/\mathbb{Q})$ is finite, then its order is a perfect square. They do this by constructing a pairing

$$Ш(\mathcal{E}/\mathbb{Q}) \times Ш(\mathcal{E}/\mathbb{Q}) \to \mathbb{Q}/\mathbb{Z}$$

with certain properties (see [3],[32]). So if we suppose that $\#Ш(\mathcal{E}/\mathbb{Q}) < \infty$ for our particular $\mathcal{E}$, then we would be able to determine that either $\#\mathrm{Sel}^{(9)}(\mathcal{E}/\mathbb{Q}) = 9$ and $\#Ш(\mathcal{E}/\mathbb{Q})[9] = 1$ or $\#\mathrm{Sel}^{(9)}(\mathcal{E}/\mathbb{Q}) = 9^2$ and $\#Ш(\mathcal{E}/\mathbb{Q})[9] = 9$. Note that using Magma [21], we can see that the Birch Swinnerton-Dyer conjecture [35] predicts that $\#Ш(\mathcal{E}/\mathbb{Q}) = 1$ and $\#Ш(\widehat{\mathcal{E}}/\mathbb{Q}) = 9$, so the next logical step (which we have not been able to complete, as the computations become unwieldy) would be to perform a complete 9-descent on $\mathcal{E}$ to verify that the order of $Ш(\mathcal{E}/\mathbb{Q})[9]$ really is 1.

13. Conclusion

While the standard method of computing the rank of an elliptic curves and finding a set of generators for the free part of the group is the well-described method of complete 2-descent, we have seen that our higher descents can still be of considerable interest. First of all, when $\mathcal{E}$ has a rational torsion point of order $\geqslant 3$ and $Ш(\mathcal{E}/\mathbb{Q})[2]$ is nontrivial, then a descent via d-isogeny can be a useful method for finding the rank of the curve. Further, we have shown that it is possible to compare the results of a complete 2-descent to a descent via d-isogeny to find the order of $Ш(\mathcal{E}/\mathbb{Q})[d]$, which is of particular interest when the d-part of the Tate-Shafarevich group is nontrivial. Finally, one of the main benefits of our method for descent via isogeny is that fact that all of our calculations are performed over $\mathbb{Q}$, which makes it easier to implement, in these cases, than a complete descent. We should also note that our restriction that d is a prime power was merely for computational convenience, and minor modifications of the above should also deal with elliptic curves with rational points of order $d = 10, 12$, while still working over $\mathbb{Q}$.

But while it is convenient that the method we used to perform descent via isogeny involves arithmetic only over $\mathbb{Q}$, it is not essential. One way to extend the results in this article is to apply the method to curves that may require arithmetic over a higher degree number field. Namely, if $\mathcal{E}$ admits a K-rational isogeny of degree k where k is a prime power but $\mathcal{E}[\phi] \not\subset \mathcal{E}(\mathbb{Q})$, then we can attempt a descent via isogeny using the same general method used earlier, with the slight modification that we do all of our arithmetic over a number field K such that $\mathcal{E}[\phi] \subseteq \mathcal{E}(K)$. Often, the degree of this number field will still be low enough that the computation will be feasible. In essence, if d is a prime power, the method described in this article is for elliptic curves parametrized by the modular curve $X_1(d)$ where $X_1(d)$ is of genus 0, but we could extend it, for example, to elliptic curves parametrized by the modular curve $X_0(d)$, where $X_0(d)$ is of genus 0.

The obvious benefit of this generalization is that we have a larger body of curves on which to perform descents: For $X_1(d)$, our method (when d is a prime power) can only be applied when $d \in \{2, 3, 4, 5, 7, 8, 9\}$, but for $X_0(d)$, it could be modified to accommodate $d \in \{2, 3, 4, 5, 7, 8, 9, 13, 16, 25\}$. Further, there exist sporadically occurring curves with rational isogenies of prime power degree $d \in \{11, 17, 19, 27, 37, 43, 67, 163\}$ on which we could perform descents. This gives us a whole class of curves for which we can find the rank, with a method other than a complete 2-descent, and a means of finding interesting orders of the Tate-Shafarevich group.

References

[1] C.D. Beaver. 5-Torsion in the Shafarevich-Tate Group of a Family of Elliptic Curves. *J. Number Theory*, **82** (2000), 25–46.
[2] J.W.S. Cassels. Arithmetic on curves of genus 1. I. On a conjecture of Selmer. *J. reine angew. Math.* **202** (1959), 52-99.
[3] J.W.S. Cassels. Arithmetic on curves of genus 1, IV. Proof of the Hauptvermutung. *J. reine angew. Math.* **211** (1962), 95–112.
[4] J.W.S. Cassels. Arithmetic on curves of genus 1, VIII. On conjectures of Birch and Swinnerton-Dyer. *J. reine angew. Math.* **217** (1965), 180–199.
[5] J.W.S. Cassels and E.V. Flynn. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*. London Mathematical Society Lecture Note Series **230** (1996), Cambridge University Press.
[6] J. Coates, P. Schneider, and R. Sujatha. Links between cyclotomic and GL_2 Iwasawa Theory. *Documenta Mathematica*. Extra Volume: Kazuya Kato's Fiftieth Birthday (2003), 187–215.
[7] *Arithmetic Algebraic Geometry*, B. Conrad and K. Rubin, eds. American Mathematical Society (2001).
[8] *Modular Forms and Fermat's Last Theorem*, G. Cornell, G. Stevens. and J.H. Silverman, eds. Springer (2000).
[9] J.E. Cremona, T.A. Fisher, C. O'Neil, D. Simon, and M. Stoll. Explicit n-Descent on Elliptic Curves: I. Algebra. http://www.arxiv.org/abs/math.NT/0606580
[10] J.E. Cremona and P. Serf. Computing the rank of elliptic curves over real quadratic number fields of class number 1. *Math. Comp.* **68**:227 (1999), 1187–1200.
[11] M. Delong. A formula for the Selmer group of a rational three-isogeny. *Acta Arith.* **105** (2002), 119–131.
[12] Z. Djabri, E.F. Schaefer and N.P. Smart. Computing the p-Selmer group of an elliptic curve. *Trans. Amer. Math. Soc.* **352**:1 (2000), 5583–5597.
[13] N. Elkies and N.F. Rogers. Elliptic Curves $x^3 + y^3 = k$ of High Rank. *Lecture Notes in Computer Science*. Proceedings of ANTS-VI; D.Buell, ed. **3076** (2004), 184–193.
[14] T. Fisher. *On 5 and 7 Descents for Elliptic Curves*. PhD Thesis, Cambridge (2000).
[15] T. Fisher. Some examples of 5 and 7 descent for elliptic curves over $\mathbb{Q}$. *J. European Math. Soc.* **3** (2001), 169–201.
[16] T. Fisher. A counterexample to a conjecture of Selmer. *Number Theory and Algebraic Geometry*, London Mathematical Society Lecture Note Series **303** (2004), Cambridge University Press.
[17] E.V. Flynn and C. Grattoni. PARI Programs and more detailed descriptions of the algorithms, made available at: http://www.maths.ox.ac.uk/~flynn/genus2/flynngrattoni/
[18] E.H. Goins. Explicit Descent Via 4-Isogeny on an Elliptic Curve. http://arxiv.org/abs/math.NT/0411215
[19] R. Hartshorne. *Algebraic Geometry*. Springer (1977).
[20] D. Husemöller. *Elliptic Curves*. Springer (2003).
[21] The Magma Computational Algebra System. Available from: http://magma.maths.usyd.edu.au/magma/
[22] B. Mazur. Rational Isogenies of Prime Degree. *Invent. Math.* **44** (1978), 129–162.
[23] J.R. Merriman, S. Siksek and N. Smart. Explicit 4-descents on an elliptic curve. *Acta Arith.* **77** (1996), 385–404.
[24] PARI Computer Algebra Package. C. Batut, K. Belabas, D. Bernardi, H. Cohen and M. Olivier, Université Bordeaux I. Available at: http://pari.math.u-bordeaux.fr/
[25] A. Robert. *A Course in p-adic Analysis*. Springer (2000).
[26] E.F. Schaefer. Class Groups and Selmer Groups. *J. Number Theory* **56** (1996), 79–114.
[27] E.F. Schaefer. Computing a Selmer group of a Jacobian using functions on the curve. *Math. Ann.* **310** (1998), 447–471.
[28] E.F. Schaefer and M. Stoll. How to do a p-descent on an elliptic curve. *Trans. Amer. Math. Soc.* **356** (2004), 1209–1231.
[29] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Springer (1986).
[30] S. Stamminger. *Explicit 8-Descent on Elliptic Curves*. PhD Thesis, International University Bremen (2005).
[31] J. Tate. Algorithm for determining the type of a singular fiber in an elliptic pencil. *Modular functions of one variable IV*, Lecture Notes in Mathematics **476** (1975), Springer.
[32] J. Tate. Duality theorems in Galois cohomology over number fields. *Proc. Intern. Cong. Math. Stockholm* (1962), 288–295.
[33] J. Top. Descent by 3-isogeny and 3-rank of quadratic fields. *Advances in Number Theory* (1993), 303–317.
[34] J. Vélu. Isogénies entre courbes elliptiques. *Comptes Rendus hebdomadaires des séances de l'Académie des sciences*, Série A, **273** (1971), 238–241.

[35] A. Wiles. The Birch and Swinnerton-Dyer Conjecture. Clay Math Institute Problem Description. http://www.claymath.org/millennium/Birch_and_Swinnerton-Dyer_Conjecture/BSD.pdf
[36] T. Womack. A Mestre-style search for high-rank curves of small conductor. http://www.tom.womack.net/maths/mestre.gp

Mathematical Institute, University of Oxford, 24–29 St. Giles', Oxford OX1 3LB, United Kingdom
E-mail address: flynn@maths.ox.ac.uk

Mathematical Institute, University of Oxford, 24–29 St. Giles', Oxford OX1 3LB, United Kingdom
E-mail address: grattoni@gmail.com