university of groningen

faculty of science and engineering

Descent by 3-isogeny on Elliptic Curves

Master Project Mathematics

July 2019

Student: S.R. Groen[1]

First supervisor: Prof.dr. J. Top

Second supervisor: Dr. J.S. Müller

[1] University of Groningen, stevengroen95@gmail.com

Abstract

Descent by a rational isogeny has shown to be a useful tool in computing the rank of elliptic curves. After outlining the general theory, we recall the well-known theory of descent by 2-isogeny. A relatively new approach is descent by a 3-isogeny. In this thesis, we formulate an algorithm that computes the Selmer group of any rational 3-isogeny. We apply these techniques to a family of elliptic curves that allow both types of descent. We force elements into the Selmer group of the 3-isogeny, while we show by 2-descent that the elliptic curves have rank zero. This yields a construction of elements of order 3 in a Tate-Shafarevich group.
Keywords: elliptic curves, descent, 3-isogeny, Selmer groups, Tate-Shafarevich groups, Hasse principle.

Contents

Acknowledgements

I would like to thank my supervisors Prof.dr. J. Top and Dr. J.S. Müller for assisting me more than well in carrying out this research and for helping me launch my scientific career.

1 Introduction

Since ancient times, mathematicians have had an intrinsic interest in the set of rational zeros of (multivariate) polynomials. If such a polynomial defines an elliptic curve, information about this set can be gained by equipping it with a group structure. In 1922, L.J. Mordell proved that the group of rational points on an elliptic curve is finitely generated ([Mor22]). It took A. Weil generalize this result to arbitrary Abelian varieties over arbitrary number fields ([Wei28]). Ever since, this result has been known as the *Mordell-Weil Theorem*. A crucial step in the proof is showing that the factor group $E(K)/mE(K)$ is finite for an integer m. Such a method is called *descent*. This term stems from Fermats technique of showing that a polynomial equation has no integer solution by 'descending' to smaller solutions, effectively showing that a factor group $E(\mathbb{Q})/2E(\mathbb{Q})$ is trivial. If we manage to compute $E(K)/mE(K)$, we can determine the rank of $E(K)$.

Unfortunately, computing this factor group is not always easy. In this thesis, we restrict to the case where multiplication by m splits into two rational isogenies of degree m, namely a rational isogeny $\phi : E \to E'$ and its dual $\hat{\phi} : E' \to E$, with the property that $\hat{\phi} \circ \phi$ equals multiplication by m. We treat the well-known theory for $m = 2$ and formulate the analogous theory for $m = 3$.

We focus on computing $E'(K)/\phi(E(K))$, where $\phi : E \to E'$ is a rational isogeny of degree 2 or 3. By viewing elliptic curves as Galois modules and applying Galois cohomology, we find that the factor group fits in the exact sequence

$$0 \to E'(K)/\phi(E(K)) \to \mathrm{Sel}^{(\phi)}(E/K) \to Ш(E/K)[\phi] \to 0.$$

Of the three groups in this sequence, the so-called *Selmer group* $\mathrm{Sel}^{(\phi)}(E/K)$ is the only one that can be computed straightforwardly. In this thesis, we present two algorithms for computing Selmer groups: one for rational 2-isogenies and one for rational 3-isogenies.

Usually, the map from $E'(K)/\phi(E(K))$ to $\mathrm{Sel}^{(\phi)}(E/K)$ is an isomorphism and we can recover the points on $E'(K)/\phi(E(K))$ from the elements of $\mathrm{Sel}^{(\phi)}(E/K)$. However, it also happens that $\mathrm{Sel}^{(\phi)}(E/K)$ is strictly larger than $E'(K)/\phi(E(K))$. In that case, the 'extra' elements of $\mathrm{Sel}^{(\phi)}(E/K)$ correspond to non-trivial elements of $Ш(E/K)$, the *Tate-Shafarevich group*. In this thesis, we encounter this phenomenon several times. A non-trivial element of a Tate-Shafarevich group can be written as a curve that has a point over every completion of K, but not over K itself, thereby violating the Hasse principle. In this thesis, numerous elements of Tate-Shafarevich groups are presented; some of them have order 2 in $Ш(E/K)$, others have order 3.

Finally, we apply both methods of descent to a family of elliptic curves E_h in order to construct elements of order 3 in their Tate-Shafarevich group. The elliptic curves are arranged to have a 2-isogeny ϕ and a 3-isogeny ψ. We make sure 2-descent does not give an obstruction and hence yields an exact computation of $E_h(\mathbb{Q})/2E_h(\mathbb{Q})$. From this we conclude that the curves have rank zero. We then force elements into the Selmer group $\mathrm{Sel}^{(\psi)}(E_h/\mathbb{Q})$. Since E_h has rank zero, this gives elements of order 3 in $Ш(E/\mathbb{Q})$. Our construction allows us to explicitly write down cubic polynomials that violate the Hasse principle.

2 Elliptic curves

In this chapter, some preliminary knowledge of elliptic curves is provided. Since we are especially interested in rational isogenies, our focus will lie especially on the rational points on elliptic curves and on (rational) isogenies.

2.1 Elliptic curves

Abstractly, an elliptic curve over a field K is a couple (E, O), where E is a smooth, irreducible, projective variety over K of dimension one and genus one, and O is a point on E. However, for the purposes in this thesis, we may just consider curves defined by a *Weierstrass Normal Form*.

Definition 2.1. Let K be a field and let a_1, a_2, a_3, a_4, a_6 be coefficients in K. A *Weierstrass Normal Form* is an equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

If we homogenize a Weierstrass Normal Form, introducing a variable z, we obtain the equation

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

The points $(x : y : z) \in \mathbb{P}^2(\bar{K})$ that satisfy this equality form a projective variety of dimension one. Moreover, if the discriminant Δ of the equation (defined in [Sil86] III.1) is non-zero, this variety is smooth. In that case, the genus of this curve is one. We then choose the point $O := (0 : 1 : 0)$, the so-called *point at infinity* on the curve. Hence the set

$$E := \{(x : y : z) \in \mathbb{P}^2(\bar{K}) \mid y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3\}$$

and the point O form an elliptic curve. Note that we can write every point other than O as $(x : y : 1)$, because of the equivalence relation defining $\mathbb{P}^2(\bar{K})$. We can always divide x and y by z, resulting in the same point in $\mathbb{P}^2(\bar{K})$, except if z is zero. In that case, it follows that x must also be zero, leaving only the possibility $(0 : 1 : 0) = O$. As the coefficients a_i lie in K, we say that E is an *elliptic curve (defined) over* K.

Every elliptic curve over K is isomorphic to a curve over K defined by a Weierstrass Normal Form ([Sil86], III.3.1). Thus in order to study the large class of elliptic curves, we only need to study Weierstrass Normal Forms.

In the context of this thesis, K will be a number field, hence the algebraic closure will be $\bar{\mathbb{Q}}$. We will study the set of rational points on elliptic curves.

Definition 2.2. Let E be an elliptic curve defined by a Weierstrass Normal Form over a field K. We define the *K-rational part* of E as follows:

$$E(K) := \{(x : y : z) \in E \mid x, y, z \in K\}.$$

2.2 Mordell-Weil groups

A very useful property of elliptic curves is that they are equipped with a group structure: one can add and subtract points. The group law on an elliptic curve E can be defined in two ways: algebraically (using the Picard group of E) and geometrically. These two definitions coincide ([Sil86] III.3.4). Since the group law will not be used explicitly, the geometric chord-tangent definition will suffice.

Definition 2.3. ***(Elliptic curve group law)*** Let P and Q be points on an elliptic curve E defined over a field K with $\mathrm{char}(K) \neq 2$. After translating x and y if necessary, we assume that $a_1 = a_3 = 0$. Then every point of E, except for the point at infinity $O = (0 : 1 : 0)$ can be represented in a plane. The point $P + Q$ is constructed as follows.

- Draw the line l on which P and Q lie. If $P = Q$, let l be the tangent line of E at P. If $P = O$, let l be the vertical line through Q and vice versa. If $P = Q = O$, then $P + Q := O$.
- Mark the other intersection point of l with E. If l is vertical, then $P + Q := O$.
- Reflect this intersection point across the x-axis. The point thus obtained is $P + Q$.

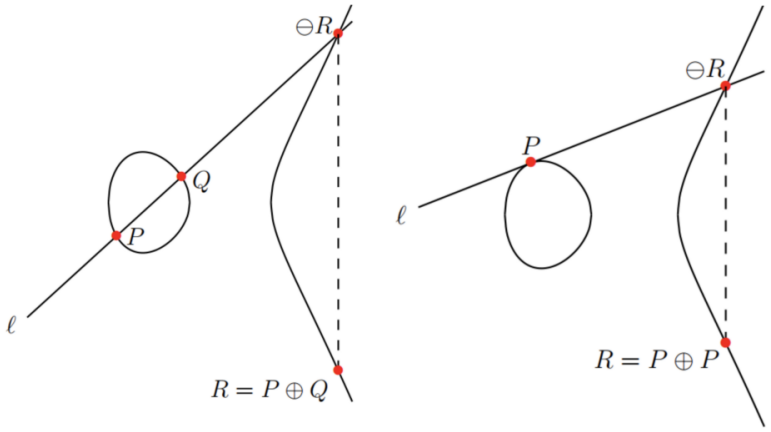


Figure 2.1: A visual representation of addition on an elliptic curve ([Ali18]).

The group law is visualized in figure 2.2. An algorithm for the group law is given in [Sil86], III.2.3.

This *chord-tangent addition* is associative, commutative and invertible ([Sil86], III.2.2). It turns the elliptic curve E into an Abelian group with unit element O. This group operation also gives rise to a morphism $m : E \to E$ for every integer m, mapping a point P to mP, the point obtained by adding P to O m times if m is non-negative, and by adding $-P$ to 0 m times if m is non-positive.

A remarkable property of the chord-tangent addition is that it maps two K-rational points to a K-rational point; the line l will be defined over K, since P and Q have coordinates in K. Similarly, the tangent line at P will be defined over K. It is straightforward to verify that the intersection point, and hence the point $P + Q$ will also be K-rational. This property allows us to define the Mordell-Weil group of an elliptic curve.

Definition 2.4. Let K be a number field and let E be an elliptic curve defined by a Weierstrass Normal Form with coefficients in K. Then the *Mordell-Weil group* of E on K is the abelian group $(E(K), +, O)$, where $E(K)$ is the set of K-rational points of E, $+$ is the chord-tangent addition from Definition 2.3 and O is the point at infinity.

This brings us to the Mordell-Weil Theorem, an essential result in the theory of elliptic curves.

Theorem 2.5. (Mordell-Weil) *Let K be a number field. Then the Mordell-Weil group $E(K)$ is finitely generated ([Mor22], [Wei28]).*

The proof of the Mordell-Weil Theorem is too long and intricate to include in this thesis. However, a crucial part of the proof is showing that the factor group $E(K)/mE(K)$, for some integer $m > 1$, is finite, which is known as the *Weak Mordell-Weil Theorem*. In this thesis, the method of showing this will be central.

The Fundamental Theorem of Finitely Generated Abelian Groups implies that $E(K)$ has the following structure:

$$\begin{aligned} E(K) &\cong \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_m\mathbb{Z} \\ &\cong \mathbb{Z}^r \times \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_t^{e_t}, \end{aligned}$$

where $d_i | d_j$ for $i < j$ and $p_1, \cdots, p_t$ are primes. The non-negative integer r is called the *rank* of $E(K)$ and the finite subgroup of E consisting of points of finite order is called the *torsion* of $E(K)$, denoted $E_{\text{tors}}(K)$.

2.3 Isogenies

So far, we have introduced elliptic curves both as projective varieties and as Abelian groups. A map between elliptic curves should preserve both structures. Such a map is called an *isogeny*.

Definition 2.6. Let (E, O) and (E', O') be two elliptic curves over some field K. An *isogeny* is a morphism of algebraic varieties $\phi : E \to E'$ with the property that $\phi(O) = O'$.

That ϕ is a morphism of algebraic varieties means that ϕ can be written as a quotient of polynomials (since E is irreducible, this can be done globally). If we embed E and E' into projective space with the same point at infinity O, then we can write ϕ as follows:

$$\begin{aligned} \phi : E &\to E' \\ (x : y : 1) &\mapsto \left(\frac{g_1(x,y)}{g_2(x,y)} : \frac{h_1(x,y)}{h_2(x,y)} : 1 \right) \\ O &\mapsto O \end{aligned} \tag{2.1}$$

This restriction ensures that ϕ is a group homomorphism, i.e. $\phi(P+Q) = \phi(P)+\phi(Q)$ for every $P, Q \in E$ ([Sil86], III.4.8). An example of an isogeny from an elliptic curve to itself is multiplication by m.

Apart from the constant isogeny, which maps every point on E to O' and is rather uninteresting, every isogeny is surjective, since all non-constant morphisms between projective curves are surjective.

The kernel of a non-constant isogeny is a finite subgroup of E ([Sil86] III.4.9). The converse also holds: every finite subgroup of E is the kernel of an isogeny to another elliptic curve ([Sil86] III.4.12). A general method for finding the isogeny with a given finite subgroup as its kernel is described in [Vé71].

Definition 2.7. Let $\phi : E \to E'$ be isogeny. The *degree* of ϕ, denoted $\deg \phi$, is the extension degree of function fields $K(E)/\phi^* K(E')$ is ϕ is non-constant. If ϕ is constant, we define $\deg \phi = 0$.

An equivalent and more straightforward definition of the degree can be given if K does not have characteristic 2. In that case, we can write E and E' in the form

$$\begin{aligned} E &: y^2 = x^3 + ax^2 + bx + c \\ E' &: Y^2 = X^3 + AX^2 + BX + C, \end{aligned}$$

such that the inverse of a point (x, y) is $(x, -y)$. The isogeny ϕ is given by (2.1). For any point $P = (x, y) \in E(K)$, the condition that ϕ is a group homomorphism implies that

$$\left(\frac{g_1(x,-y)}{g_2(x,-y)} : \frac{h_1(x,-y)}{h_2(x,-y)} : 1 \right) = \phi(-P) = -\phi(P) = \left(\frac{g_1(x,y)}{g_2(x,y)} : -\frac{h_1(x,y)}{h_2(x,y)} : 1 \right).$$

Hence the polynomials g_1 and g_2 cannot depend on y. We also assume, without loss of generality, that $g_1, g_2 \in K[X]$ are coprime. Then the degree of ϕ becomes the extension degree

$$\left[K(x) : K\left(\frac{g_1(x)}{g_2(x)} \right) \right] = \max\{\deg(g_1), \deg(g_2)\}.$$

Note that the degree of g_2 cannot exceed the degree of g_1, for then, if we write $O = (0, \infty)$, we don't recover $\phi(O) = O$. Thus if $\mathrm{char}(K) \neq 2$, we might as well define $\deg \phi := \deg(g_1)$.

The degree of a separable isogeny is equal to the size of its kernel; $\#\ker \phi = \deg \phi$ ([Sil86] III.4.10.(a)). In our context, the function field will have characteristic 0 and hence ϕ will always be separable, so this equality will always hold.

Lemma 2.8. *Let $\phi : E \to E'$ be an isogeny of degree m. Then there exists a unique isogeny $\hat{\phi} : E' \to E$ such that $\hat{\phi} \circ \phi$ and $\phi \circ \hat{\phi}$ both equal multiplication by m. $\hat{\phi}$ is called the* dual isogeny *of ϕ.*

Proof. See [Sil86] III.4.6.1. □

Throughout this thesis, we will especially interested in *rational isogenies*.

Definition 2.9. Let K be a field, let E and E' be elliptic curves defined over K. An isogeny $\phi : E \to E'$ is called *K-rational* if the polynomials g_1, g_2, h_1 and h_2 in equation (2.1) can be chosen to be in $K[x, y]$.

If $K = \mathbb{Q}$, we will just say that ϕ is a rational isogeny.

Lemma 2.10. *let K be a field and T a finite subgroup of an elliptic curve E defined over K. We write $G_K = \mathrm{Gal}(\bar{K}/K)$ for the absolute Galois group of K. Then T is the kernel of a K-rational isogeny $\phi : E \to E'$ if and only if T is invariant under G_K, i.e. $T^\sigma = T$ for every $\sigma \in G_K$.*

Proof. "Only if": assume such a rational isogeny $\phi : E \to E'$ exists. Let $\sigma \in G_K$ and let P be any point in $T = \ker(\phi)$. We show that $\phi(P^\sigma) = O$. Since ϕ is K-rational, the action of σ on $\phi(P)$ is the same as the action of σ on P: $\phi(P)^\sigma = \phi(P^\sigma)$. This implies that

$$\phi(P^\sigma) = \phi(P)^\sigma = O^\sigma = O,$$

and hence $P^\sigma \in T$

"If": this implication follows (cumbersomely) from the explicit algorithm in [Vé71]. A more insightful proof can be obtained by following the construction in [Sil86] III.4.12. □

Be warned that the subgroup T need not consist of K-rational points in this case; it is just the elliptic curve E' and the isogeny ϕ that are defined over K. The simplest example is multiplication by an integer m. If E is defined over K, then multiplication by m from E to E is defined over K, but this does not imply that the m-torsion is K-rational.

3 Descent by an isogeny

In this chapter, the general theory of descent by an isogeny on elliptic curves is outlined. Applying Galois cohomology to the kernel-cokernel sequence of an isogeny results in a long exact sequence of cohomology groups. The abstract cohomology groups can be substituted by more comprehensible groups. Localizing this sequence allows us to define Selmer groups and Tate-Shafarevich groups. These groups turn out to be useful in bounding the rank from above and yield an exact determination of the rank if the Tate-Shafarevich group is trivial. This chapter serves as a preparation to the investigation of the particular cases where the degree of the isogeny is 2 or 3.

3.1 Galois cohomology

The first step towards applying Galois cohomology to elliptic curves is to view elliptic curves as *Galois modules*. We first introduce the category of G-modules for a group G.

Definition 3.1. Let $(G, *, e)$ be a group. Then a *G-module* M is an Abelian group on which G acts. We denote the action of $\sigma \in G$ on M by $m \mapsto m^\sigma$. Moreover, the following restrictions are satisfied for every $m, n \in M$ and $\sigma \in G$:

$$\begin{aligned} m^e &= m \\ (m+n)^\sigma &= m^\sigma + n^\sigma \\ (m^\sigma)^\tau &= m^{(\sigma * \tau)} \end{aligned}$$

A *morphism of G-modules* is a morphism $f : M \to N$ such that $f(m)^\sigma = f(m^\sigma)$ for every $m \in M$ and $\sigma \in G$.

Throughout this section, we let K be a perfect field and write G_K for $\mathrm{Gal}(\bar{K}/K)$. In practice, K will be a number field and $\bar{K}$ will be $\bar{\mathbb{Q}}$. Since G_K is a profinite group, the inverse limit of finite groups, it is equipped it with the topology indued by the discrete topology on the finite groups $G_K/G_L = \mathrm{Gal}(L/K)$, where L is a finite normal (and hence Galois, since K is perfect) extension of K. The open neighborhoods of the unit element of G_K are the groups G_L, where L is a finite normal extension of K. This topology is called the *profinite topology*.

Definition 3.2. A *Galois module* over G_K, or simply a G_K-module, is an Abelian group M on which every $\sigma \in G_K$ acts continuously, where M is equipped with the discrete topology and G_K with the profinite topology. Equivalently, for every $m \in M$, the subgroup $\{\sigma \in G_K \mid m^\sigma = m\}$, called the *stabilizer* of m, has finite index in G_K.

Easy examples of Galois modules are $\bar{K}^+$ (the additive group of $\bar{K}$), $\bar{K}^*$ (the unit group of $\bar{K}$), and μ_n, the group of n^{th} roots of unity in $\bar{K}$. Elliptic curves defined over K are also G_K-modules; we have seen that they are Abelian groups on which G_K acts, and every point $P \in E$ has coordinates lying in some (minimal) finite extension $L \supseteq K$. Then the stabilizer of P is G_L, which has index

$$[G_K : G_L] = \#(G_K/G_L) = \#\,\mathrm{Gal}(L/K),$$

which is finite because L is a finite extension. By the same argument, subgroups and factor groups of elliptic curves are Galois modules. The theory of Galois modules is thus applicable to elliptic curves. A morphism of G_K-modules is just a K-rational isogeny.

Galois cohomology can be used to turn a short exact sequence of Galois modules into a long exact sequence of groups, starting with the K-rational parts of these Galois modules. This is very useful in arithmetic geometry. We now introduce the groups that enter this long exact sequence.

Definition 3.3. Let K be a perfect field and let M be a Galois module over G_K. The group $H^0(G_K, M)$, called the 0^{th} *cohomology group*, is defined as follows:

$$H^0(G_K, M) = \{m \in M | m^\sigma = m \text{ for all } \sigma \in G_K\}$$

For an elliptic curve E, the group $H^0(G_K, E)$ is the group of points that are fixed by every automorphism of G_K, which are exactly the K-rational points. Thus $H^0(G_K, E) = E(K)$, the Mordell-Weil group of E over K.

Definition 3.4. A *cocycle* is a continuous map $\xi : G_K \to M$, with the property that $\xi(\sigma\tau) = \xi(\sigma)^\tau + \xi(\tau)$. Again, the continuity is with respect to the discrete topology on M and the profinite topology on G_K. The set of cocycles forms a group under pointwise addition.

A *coboundary* is a map from G_K to M that can be written as $\sigma \mapsto m^\sigma - m$. The set of coboundaries forms a normal subgroup of the group of cocycles.

The group $H^1(G_K, M)$, called the 1^{st} *cohomology group*, is defined as the quotient of the aforementioned groups:

$$H^1(G_K, M) := \frac{\{\text{cocycles } G_K \to M\}}{\{\text{coboundaries } G_K \to M\}}$$

Theorem 3.5. *Let* $0 \longrightarrow P \xrightarrow{\psi} M \xrightarrow{\phi} N \longrightarrow 0$ *be an exact sequence of* G_K*-modules. Then there exists a long exact sequence*

$$\begin{array}{l} 0 \longrightarrow H^0(G_K, P) \xrightarrow{\psi} H^0(G_K, M) \xrightarrow{\phi} H^0(G_K, N) \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \xrightarrow{\delta} \\ \qquad\qquad H^1(G_K, P) \xrightarrow{\psi_*} H^1(G_K, M) \xrightarrow{\phi_*} H^1(G_K, P) \end{array}$$

The connecting homomorphism $\delta : H^0(G_K, N) \to H^1(G_K, P)$ *is defined by the diagram chase from the Snake Lemma. Let* $n \in H^0(G_K, N)$ *and let* $m \in M$ *be such that* $\phi(m) = n$*. Then define* $\delta(n)$ *to be the cohomology class in* $H^1(G_K, P)$ *of* $\sigma \mapsto \psi^{-1}(m^\sigma - m)$*.*

Proof. See [Sil86] B.1.2 and B.2.3. □

Such a long exact sequence is called a *cohomology sequence*. In practice, ϕ will be a K-rational isogeny of elliptic curves defined over K. Then the Galois modules become

$$\begin{aligned} P &= E[\phi] := \ker \phi \\ M &= E \\ N &= E' \end{aligned}$$

The morphism ψ will just be inclusion. Note that ϕ is assumed to be non-constant and therefore surjective, making the sequence exact. This exact sequence will eventually yield a method to bound the size of $E(K)/mE(K)$ for integers $m > 1$. We first need to find more explicit descriptions of the cohomology groups and the connecting homomorphism.

3.2 Weil-Châtelet groups

Now, let K be a number field and let $0 \longrightarrow E[\phi] \longrightarrow E \xrightarrow{\phi} E' \longrightarrow 0$ be the kernel-cokernel sequence of a K-rational isogeny ϕ, which is an exact sequence of G_K-modules. By Theorem 3.5, there is a long exact sequence

$$\begin{array}{l} 0 \longrightarrow H^0(G_K, E[\phi]) \longrightarrow H^0(G_K, E) \xrightarrow{\phi} H^0(G_K, E') \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \xrightarrow{\delta} \\ \qquad\qquad H^1(G_K, E[\phi]) \longrightarrow H^1(G_K, E) \xrightarrow{\phi_*} H^1(G_K, E'). \end{array}$$

As noted before, the 0^{th} cohomology group is just the K-rational part. We are not interested in the cohomology group $H^1(G_K, E')$. Thus we obtain the exact sequence

$$0 \longrightarrow E(K)[\phi] \longrightarrow E(K) \xrightarrow{\phi} E'(K) \xrightarrow{\delta} H^1(G_K, E[\phi]) \longrightarrow H^1(G_K, E).$$

We make δ injective by dividing $E'(K)$ by $\ker(\delta) = \phi(E(K))$ (this equality is due to exactness) and we make the final map $H^1(G_K, E[\phi]) \to H^1(G_K, E)$ surjective by noting that its image equals the kernel of $\phi_* : H^1(G_K, E) \to H^1(G_K, E')$ (by exactness). This yields the exact sequence

$$0 \longrightarrow E'(K)/\phi(E(K)) \xrightarrow{\delta} H^1(G_K, E[\phi]) \longrightarrow H^1(G_K, E)[\phi_*] \longrightarrow 0. \tag{3.1}$$

We now characterize the cohomology groups $H^1(G_K, E[\phi])$ and $H^1(G_K, E)$.

Lemma 3.6. *By μ_m we denote the group of m^{th} roots of unity in $\bar{K}^\times$. If $E[\phi]$ is a K-rational cyclic subgroup of order m and $\mu_m \subset K$, then $E[\phi] \cong \mu_m$ as G_K-modules and hence $H^n(G_K, E[\phi]) \cong H^n(G_K, \mu_m)$ for every $n \in \{0, 1\}$.*

Proof. An isomorphism of Abelian groups $f : E[\phi] \to \mu_m$ is obtained by sending a generator of $E[\phi]$ to a primitive m^{th} root of unity in $\bar{K}^\times$. Moreover, the equality $f(P)^\sigma = f(P^\sigma)$ is satisfied for every $P \in E[\phi]$ and every $\sigma \in G_K$, since we assumed that G_K acts trivially on both $E[\phi]$ and μ_m. This means the isomorphism is also a morphism of G_K-modules and hence an isomorphism of G_K-modules. □

The isogenies we work with have a cyclic kernel. If $E[\phi]$ is not K-rational or K does not contain the required roots of unity, then a similar statement holds after replacing K with a finite field extension of K.

Lemma 3.7. *$K^\times / {K^\times}^m \cong H^1(G_K, \mu_m)$. The isomorphism is as follows: for an $\alpha \in K^\times / {K^\times}^m$, let β be an m-th root of α. Then assign to α the class of the cocycle $\sigma \mapsto \frac{\beta^\sigma}{\beta}$ in $H^1(G_K, \mu_m)$. This assignment is the desired isomorphism.*

Proof. View the group $\bar{K}^\times$ as a G_K-module. Then applying Galois cohomology to the short exact sequence $0 \longrightarrow \mu_m \longrightarrow \bar{K}^\times \xrightarrow{z \mapsto z^m} \bar{K}^\times \longrightarrow 0$ yields an exact sequence

$$0 \longrightarrow K^\times[m] \longrightarrow K^\times \xrightarrow{z \mapsto z^m} K^\times \xrightarrow{\delta} H^1(G_K, \mu_m) \longrightarrow H^1(G_K, K^\times).$$

Then we use Hilbert's Theorem 90, stating that $H^1(G_K, K^\times)$ is trivial ([Kum55]), which implies that the connecting homomorphism from $K^\times$ to $H^1(G_K, \mu_m)$ is surjective. By exactness, the kernel of δ is ${K^\times}^m$. Then the Homomorphism Theorem of groups implies that the assignment is an isomorphism. □

These two lemmas give us a useful characterization of $H^1(G_K, E[\phi])$, so now we turn to $H^1(G_K, E)$. The elements of $H^1(G_K, E)$ correspond to so-called *homogeneous spaces* of $E(K)$, which are a special kind of genus one curves that are isomorphic to E over $\bar{K}$.

Definition 3.8. A *homogeneous space* of an elliptic curve E defined over K is a smooth curve C defined over K together with a morphism $\mu : C \times E \to C$. The morphism is a simply transitive group action of E on C, meaning that, given any $p, q \in C$ and $P, Q \in E$, it follows that $\mu(p, O) = p$, $\mu(\mu(p, P), Q) = \mu(p, P + Q)$ and there is a unique $R \in E$ such that $\mu(p, R) = q$.

A simple example of a homogenous space of E over K is E itself; then μ is just the addition defined in 2.3. We call two homogeneous spaces *equivalent* if they are isomorphic over K and the isomorphism commutes with the morphism μ. Since homogeneous spaces are isomorphic to E over $\bar{K}$, they are genus one curves.

Definition 3.9. Let E be an elliptic curve defined over K. The *Weil-Châtelet group* $\mathrm{WC}(E/K)$ of E over K is the set of homogeneous spaces of E over K modulo the equivalence described above.

Note that it is not at all clear from this definition that the Weil-Châtelet group is in fact a group.

Theorem 3.10. *Let E be an elliptic curve defined over K. Then we construct a natural bijection from $\mathrm{WC}(E/K)$ to $H^1(G_K, E)$ as follows. Given a homogeneous space C/K, choose a point $p_0 \in C$. Map C to the class of the cocycle $\sigma \mapsto p_0^\sigma - p_0$.*

Proof. See [Sil86] X.3.6. □

This theorem implies that $\mathrm{WC}(E/K)$ inherits a group structure from $H^1(G_K, E)$. The unit element of $\mathrm{WC}(E/K)$ is the class of homogeneous spaces that are mapped to a coboundary in $H^1(G_K, E)$. Clearly, the homogeneous space E is in this class, and therefore all homogeneous spaces that are isomorphic to E over K are in this class as well.

Lemma 3.11. *Let C be an element of $\mathrm{WC}(E/K)$ and suppose C has a K-rational point. Then C is equivalent to E.*

Proof. Let $p_0 \in C(K)$ be a rational point. Via Theorem 3.10, this corresponds to the cocycle $\sigma \mapsto p_0^\sigma - p_0 = p_0 - p_0 = O$, which is the trivial cocycle, meaning that C is equivalent to E.

The lemma can also be proven without the use of Theorem 3.10. The isomorphism is given explicitly as follows:

$$\begin{aligned} E &\to C \\ P &\mapsto \mu(p_0, P). \end{aligned}$$

This map is defined over K because p_0 is rational and it is an isomorphism compatible with μ because μ is simply transitive. □

We now assume the antecedent of Lemma 3.6 again. Using Lemma 3.6, Lemma 3.7 and Theorem 3.10, the exact sequence (3.1) becomes

$$0 \longrightarrow E'(K)/\phi(E(K)) \xrightarrow{\delta} K^\times/K^{\times m} \longrightarrow \mathrm{WC}(E/K)[\phi] \longrightarrow 0. \tag{3.2}$$

The key ingredient of the proof of the Weak Mordell-Weil Theorem, is that the image of δ, which equals the kernel of the map to $\mathrm{WC}(E/K)$, is finite. Applying this to both ϕ and the dual isogeny $\hat{\phi}$ yields that both $E'(K)/\phi(E(K))$ and $E(K)/\hat{\phi}(E'(K))$ are finite, rendering $E(K)/mE(K)$ finite by the exact sequence

$$0 \longrightarrow \frac{E'(K)[\hat{\phi}]}{\phi(E(K)[m])} \longrightarrow \frac{E'(K)}{\phi(E(K))} \xrightarrow{\hat{\phi}} \frac{E(K)}{mE(K)} \longrightarrow \frac{E(K)}{\hat{\phi}(E'(K)} \longrightarrow 0. \tag{3.3}$$

Knowing the size of $E(K)/mE(K)$ allows us to compute the rank of the Mordell-Weil group $E(K)$, since

$$E(K)/mE(K) \cong (\mathbb{Z}/m\mathbb{Z})^r \times E(K)[m],$$

in which $E(K)[m]$ is easily computed.

3.3 Selmer groups and Tate-Shafarevich groups

We bound (and aim to compute) the image of δ using localization. If v is a valuation on K, then we extend it to a valuation on $\bar{K}$ and localize (3.1) to obtain

$$0 \longrightarrow E'(K_v)/\phi(E(K_v)) \xrightarrow{\delta_v} H^1(G_v, E[\phi]) \longrightarrow H^1(G_v, E)[\phi_*] \longrightarrow 0\ , \tag{3.4}$$

in which $G_v := \mathrm{Gal}(\bar{K_v}/K_v)$ is the absolute Galois group of the completion K_v.

Taking the product of all the possible localization maps and using Theorem 3.10, we obtain the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E'(K)/\phi(E(K)) & \xrightarrow{\delta} & H^1(G_K, E[\phi]) & \longrightarrow & \mathrm{WC}(E/K)[\phi] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_{v\in M_K} E'(K_v)/\phi(E(K_v)) & \xrightarrow{\delta} & \prod_{v\in M_K} H^1(G_v, E[\phi]) & \longrightarrow & \prod_{v\in M_K} \mathrm{WC}(E/K_v)[\phi] & \longrightarrow & 0. \end{array} \tag{3.5}$$

The vertical arrows are well-defined because of the continuity of cocycles and because of the commutativity of the inclusions

$$\begin{array}{ccc} K & \hookrightarrow & K_v \\ \downarrow & & \downarrow \\ \bar{K} & \hookrightarrow & \bar{K}_v. \end{array}$$

This diagram allows us to define the *ϕ-Selmer group* and the *Tate-Shafarevich group* of E/K.

Definition 3.12. Let $\phi : E/K \to E'/K$ be a K-rational isogeny. The *ϕ-Selmer group* of E over K, denoted $\mathrm{Sel}^{(\phi)}(E/K)$, is defined as the kernel of the composite map

$$H^1(G_K, E[\phi]) \to \prod_{v\in M_K} \mathrm{WC}(E/K_v)$$

in the diagram (3.5).

Definition 3.13. Let E be an elliptic curve defined over K. The *Tate-Shafarevich group* of E over K, denoted $Ш(E/K)$ and pronounced "Sha", is the kernel of the localization map

$$\mathrm{WC}(E/K) \to \prod_{v \in M_K} \mathrm{WC}(E/K_v).$$

These definitions are independent of our choice of extending v to a valuation on $\bar{K}$ ([Sil86] X.4.1.1).

Elements of the Tate-Shafarevich group are homogeneous spaces that have a K_v-rational point for every completion K_v, up to equivalence. If it has a K-rational point, then it is the unit element, since it is equivalent to E by Lemma 3.11. Thus non-trivial elements of the Tate-Shafarevich group correspond to homogeneous spaces that have a point everywhere locally, but not globally. This violates the so-called *Hasse Principle*, which states that a polynomial equation has a global solution if and only if it has one locally at every place.

The ϕ-Selmer group consists of elements of $H^1(G_K, E[\phi])$ that are mapped to a homogeneous space in the Tate-Shafarevich group. Elements of the Selmer group can also be seen as cocycles that are in the image of the connecting homomorphism δ everywhere locally.

Using Definition 3.12 and Definition 3.13, we form the exact sequence

$$0 \longrightarrow E'(K)/\phi(E(K)) \xrightarrow{\delta} \mathrm{Sel}^{(\phi)}(E/K) \longrightarrow Ш(E/K)[\phi] \longrightarrow 0. \tag{3.6}$$

The exactness of this sequence follows straightforwardly from the diagram (3.5).

Definition 3.14. Let $\phi : E/K \to E'/K$ be an isogeny. We define the following set of places:

$$S_{E,\phi} = \{v \in M_K^0 \mid v(\deg \phi) > 0 \text{ or } v(\Delta_E) > 0\} \cup M_K^\infty.$$

This definition allows us to sketch a proof of an important theorem.

Theorem 3.15. *Let $\phi : E/K \to E'/K$ be a K-rational isogeny. Then $\mathrm{Sel}^{(\phi)}(E/K)$ is finite.*

Proof. The proof relies on the fact that cocycles in $\mathrm{Sel}^{(\phi)}(E/K)$ are unramified outside $S_{E,\phi}$ ([Sil86] X.4.1.2.(b)), meaning they become trivial when G_v is replaced by the inertia subgroup I_v. Hence $\mathrm{Sel}^{(\phi)}(E/K)$ is contained in the group

$$H^1(G_K, E[\phi]; S) := \left\{\xi \in H^1(G_k, E[\phi]) \mid \xi \text{ is unramified outside outside } S_{E,\phi}\right\}.$$

As $E[\phi]$ is a finite G_K-module, this cohomology group is finite ([Sil86] X.4.3). □

Corollary 3.16. *Assume $E[\phi]$ is a K-rational cyclic group of order m and that $\mu_m \subset K$. Then*

$$\mathrm{Sel}^{(\phi)}(E/K) \subseteq K(S_{E,\phi}, m) := \left\{d \in K^\times/{K^\times}^m \mid v(d) \equiv 0 \mod m \text{ for every } v \notin S_{E,\phi}\right\}.$$

Proof. In this case, we apply Lemma 3.6 and Lemma 3.7 to obtain

$$H^1(G_K, E[\phi]) \cong K^\times/{K^\times}^m.$$

The elements of this group that are unramified outside $S_{E,\phi}$ are precisely the elements that have valuation zero (up to equivalence) for all valuations outside $S_{E,\phi}$. □

Whereas there is no efficient method known for finding K-rational points (or deciding that there aren't any), deciding whether K_v-rational points exist takes a finite amount of time; we manipulate the equation to make sure that every variable lives in $\mathcal{O}_{K_v}$. Then we can use reduction modulo a sufficient power of the maximal ideal of $\mathcal{O}_{K_v}$ to conclude that there are no solutions or to lift one using Hensel's Lemma.

This gives us an effective way of computing the Selmer group of a K-rational isogeny $\phi : E/K \to E'/K$. We determine the divisors of Δ_E and the divisors of $\deg \phi$ to form the finite group $K(S_{E,\phi}, m)$. For every element $d \in K(S_{E,\phi}, m)$, we check whether the homogeneous space C_d has a K_v-rational point for every $v \in S$. If so, it has a point everywhere locally and we conclude $d \in \mathrm{Sel}^{(\phi)}(E/K)$. Viewing $\mathrm{Sel}^{(\phi)}(E/K)$ in the exact sequence (3.6), we see that d comes from an element in $E'(K)/\phi(E(K))$ if C_d has a K-rational point, and otherwise C_d is an element of $Ш(E/K)$. In general, it is difficult to tell which of these two is the case, which means it is still difficult to compute the rank of an elliptic curve (in fact, no known algorithm is guaranteed to work). At least a computation of $\mathrm{Sel}^{(m)}(E/K)$ provides an upper bound for the rank of $E(K)$. If the following conjecture turns out to be true, then the method of descent by isogenies is guaranteed to result in an exact computation of the rank.

Conjecture 3.17. *Let E/K be an elliptic curve. Then $Ш(E/K)$ is finite.*

If $Ш(E/K)$ is finite, then we can find an integer m such that $Ш(E/K)$ does not contain an element of order m. Then m-descent gives the rank.

4 Descent by 2-isogeny

In this chapter, the method of descent by 2-isogeny is presented. If an elliptic curve admits a rational isogeny of degree 2, we demonstrate how the corresponding Selmer group can be computed. This is illustrated in a few examples.

4.1 Rational 2-isogenies

Let K be a number field and E/K an elliptic curve. Since number fields have characteristic zero, we write E in the form

$$E : y^2 = x^3 + ax^2 + bx + c.$$

Our starting assumption is that we have a K-rational isogeny $\phi : E \to E'$ of degree 2. Then, by lemma 2.10, the kernel $E[\phi]$ is invariant under the action of any $\sigma \in G_K$. Write $E[\phi] = \{O, (\alpha, \beta)\}$ for some $\alpha, \beta \in \bar{K}$. The Galois invariance then implies that $\alpha, \beta \in K$, so $E[\phi]$ is automatically K-rational. Now, by a K-rational translation, we move (α, β) to $(0, 0)$, preserving all properties of the elliptic curve that we're interested in. Thus we have $E[\phi] = \{O, (0, 0)\}$ and the elliptic curve is given by an equation of the form

$$E : y^2 = x^3 + ax^2 + bx.$$

Using the subgroup $\{O, (0, 0)\}$, we compute the isogenous curve E' and the isogeny $\phi : E \to E'$:

$$\begin{aligned} E' &: Y^2 = X^3 - 2aX^2 + (a^2 - 4b)X \\ \phi &: (x, y) \mapsto \left(\frac{y^2}{x^2} \, , \, \frac{y(b - x^2)}{x^2} \right). \end{aligned} \tag{4.1}$$

We introduce the abbreviations $a' := -2a$ and $b' := a^2 - 4b$.

The elliptic curve E' again has a rational 2-isogeny, namely the dual isogeny $\hat{\phi} : E' \to E$. The complete 2-torsion of E is given by

$$E[2] = \phi^{-1}(E'[\hat{\phi}]).$$

4.2 The cohomology sequence

Note that $E[\phi]$ is K-rational and K contains $\mu_2 = \{\pm 1\}$, so we can apply Lemma 3.6 and Lemma 3.7. Thus the 2-isogeny ϕ gives rise to the exact sequence

$$0 \longrightarrow E'(K)/\phi(E(K)) \xrightarrow{\delta} K^\times/{K^\times}^2 \longrightarrow \mathrm{WC}(E/K)[\phi] \longrightarrow 0.$$

By Corollary 3.16, the image of δ is contained in $K(S_{E,\phi}, 2)$, so (possibly losing the surjectivity of the last map), we obtain the exact sequence

$$0 \longrightarrow E'(K)/\phi(E(K)) \xrightarrow{\delta} K(S_{E,\phi}, 2) \longrightarrow \mathrm{WC}(E/K)[\phi]. \tag{4.2}$$

In order to turn this exact sequence into a computation, we determine the connecting homomorphism δ concretely.

Lemma 4.1. *The connecting homomorphism in (4.2) is given as follows:*

$$\begin{aligned} \delta : E'(K)/\phi(E(K)) &\to K(S_{E,\phi}, 2) \\ (X, Y) &\mapsto X \cdot {K^\times}^2 \\ (0, 0) &\mapsto b' \cdot {K^\times}^2 \\ O &\mapsto 1 \cdot {K^\times}^2 \end{aligned}$$

Proof. The map δ comes from the diagram

$$\begin{array}{ccccc} E(K) & \xrightarrow{\phi} & E'(K) & & \\ & & \downarrow{\scriptstyle \delta'} & \searrow^{\delta} & \\ H^1(G_K, E[\phi]) & \xrightarrow{\sim} & H^1(G_K, \mu_2) & \xrightarrow{\sim} & K^\times/{K^\times}^2. \end{array}$$

We recall how the connecting homomorphism was created in Theorem 3.5. Let $P = (X, Y)$ be a point on $E'(K)$. Let $Q = (x, y)$ be a point on E such that $\phi(Q) = P$ (Q is in general not K-rational). Then δ' maps P to the cocycle $\xi : \sigma \mapsto Q^\sigma - Q$ in $H^1(G_K, E[\phi])$, which we plug into the isomorphism to $K^\times/K^{\times 2}$ established in Lemma 3.6 and Lemma 3.7. First, we replace $E[\phi]$ by $\mu_2 = \{\pm 1\}$ by sending ξ to the cocylce

$$\eta : \sigma \mapsto \begin{cases} -1 & \text{if } Q^\sigma - Q = (0,0) \\ 1 & \text{if } Q^\sigma - Q = O \end{cases}$$

in $H^1(G_K, \mu_2)$. Finally, using Lemma 3.7, we must find the unique $d \in K^\times/K^{\times 2}$ such that η can be written as

$$\eta : \sigma \mapsto \frac{\sqrt{d}^\sigma}{\sqrt{d}} = \begin{cases} -1 & \text{if } \sqrt{d}^\sigma = -\sqrt{d} \\ 1 & \text{if } \sqrt{d}^\sigma = \sqrt{d}. \end{cases}$$

Then we are done; $d = \delta(P)$. To make this concrete, we first impose restrictions on $Q = (x, y)$ that follow from $\phi(Q) = P$:

$$X = \frac{y^2}{x^2} \tag{4.3}$$

$$Y = \frac{y(b - x^2)}{x^2}. \tag{4.4}$$

First, let's handle some specific cases for P. If $P \in \phi(E(K))$, and hence $Q \in E(K)$, then δ maps P to 1; P is the unit element in $E'(K)/\phi(E(K))$, so $\delta(P)$ is the unit element of $K^\times/K^{\times 2}$. Alternatively, since Q is K-rational, the cocycle in $H^1(G_K, E[\phi])$ is trivial. This includes the case $P = O$. From now on, we assume that Q is not K-rational.

Second, suppose X is zero, implying that Y is zero and hence $P = (0, 0)$. Then (4.3) implies that y is zero and x is not. Then x is a root of $x^2 + ax + b$. Taking the discriminant of this polynomial yields that $Q = (x, 0)$ lies in the extension $K(\sqrt{a^2 - 4b}) = K(\sqrt{b'})$. An automorphism σ fixes Q if and only if it fixes $\sqrt{b'}$, so $\delta((0, 0)) = b'$, modulo K-squares, as desired. From now on, we assume that X is non-zero.

Substituting $x^2 = \frac{y^2}{X}$ from (4.3) into (4.4) yields

$$\begin{aligned} Y &= \frac{y\left(b - \frac{y^2}{X}\right)}{\frac{y^2}{X}} \\ &= \frac{bXy - y^3}{y^2} \\ &= bXy^{-1} - y \\ \implies Yy &= bX - y^2. \end{aligned}$$

Again, taking the discriminant of $y^2 + Yy - bX$ tells us that y lies in the extension $K(\sqrt{Y^2 + 4bX})$. A closer inspection reveals that

$$Y^2 + 4bX = X^3 - 2aX^2 + (a^2 - 4b)X + 4bX = X(X^2 - 2aX + a^2) = X(X - a)^2,$$

so $y \in K(\sqrt{Y^2 + 4bX}) = K((X - a)\sqrt{X}) = K(\sqrt{X})$. By (4.3), x also lies in the extension $K(\sqrt{X})$. Now, an automorphism σ fixes y (and thereby x) if and only if it fixes $\sqrt{X}$. This means exactly that $\delta(P) = X$, which finishes the proof. □

This explicit description of δ also yields an explicit homomorphism $K(S_{E,\phi}, 2) \to \mathrm{WC}(E/K)$ that makes (4.2) exact. Since our goal is to compute the image of δ, we are predominantly interested in the kernel of the homomorphism $K(S_{E,\phi}, 2) \to \mathrm{WC}(E/K)$, not so much its further behavior. Therefore we determine this homomorphism in a straightforward way, instead of following the diagram

$$K^\times/K^{\times 2} \xrightarrow{\cong} H^1(G_K, E[\phi]) \longrightarrow H^1(G_K, E) \xrightarrow{\cong} \mathrm{WC}(E/K).$$

Lemma 4.2. *Let $\phi : E/K \to E'/K$ be as in (4.1). Then the homomorphism $K(S_{E,\phi}, 2) \to \mathrm{WC}(E/K)[\phi]$ in (4.2) is as follows:*

$$\begin{aligned} K(S_{E,\phi}, 2) &\to \mathrm{WC}(E/K)[\phi] \\ d &\mapsto C_d \\ C_d &: w^2 = d + a'd^2z^2 + b'd^3z^4. \end{aligned}$$

Proof. Note that the kernel of $d \mapsto C_d$ should equal the image of δ for exactness; this means C_d should have a K-rational point if and only if $d = \delta(P)$ for some $P \in E(K)/\phi(E(K))$. We assume that $d = \delta((X, Y))$ so X of the form $X = de^2$ for some $e \in K^\times$. The fact that (X, Y) is a point on $E'(K)$ then means

$$\begin{aligned} Y^2 &= (de^2)^3 + a'(de^2)^2 + b'de^2 \\ \implies \frac{Y^2}{d^2e^6} &= d + \frac{a'}{e^2} + \frac{b'}{de^4}. \end{aligned}$$

Now, setting $w := \frac{Y}{de^3}$ and $z := \frac{1}{de}$ achieves the desired defining equation for the homogeneous space C_d. It is clear that d is in the image of δ if and only if C_d has a K-rational point.

The exceptional cases $\delta : O \mapsto 1$ and $\delta : (0, 0) \mapsto b'$ are also covered by this; for $d = 1$ we always have the solution $(w, z) = (1, 0)$. For $d = b'$ we always have a point at infinity; if we let r homogenize the defining equation of $C_{b'}$ in the weighted projective plane, resulting in

$$C_d : w^2 = b'r^4 + a'(b'z)^2r^2 + (b'z)^4,$$

then $(w : z : r) = (1 : 1 : 0)$ is a point on $C_{b'}$. □

Having obtained an explicit formula for the homogeneous spaces, we first investigate what happens in the archimedean completions. If such a completion is $\mathbb{C}$, there is nothing to check; since $\mathbb{C}$ is algebraically closed, any homogeneous space will have points over $\mathbb{C}$. The following lemma handles the case where the completion is $\mathbb{R}$.

Lemma 4.3. *Let*

$$C_d : w^2 = d + a'd^2z^2 + b'd^3z^4$$

be a homogeneous space coming from a rational 2-isogeny and assume a' and b' are real. Then $C_d(\mathbb{R})$ is non-empty if and only if either $b'd > 0$ or the right-hand side polynomial has a real root.

Proof. The equation defining C_d has a real solution $(w, z) \in \mathbb{R}^2$ if and only if the right-hand side polynomial becomes non-negative for some z. If $b'd$ is positive, then this is bound to happen for sufficiently large $|z|$. On the other hand, if the polynomial has a real root z_0, then $C_d(\mathbb{R})$ has the point $(z_0, 0)$. Conversely, if $b'd$ is negative (it can't be zero), then the right-hand side polynomial attains negative values for sufficiently large $|z|$. If it also attains a non-negative value, then it has a root by the Intermediate Value Property. □

Remark 4.4. Lemma 4.2 also gives rise to a rational map $\zeta : C_d \to E'$. If C_d has a K-rational point (w, z), then C_d comes from a K-rational point on $E'(K)$. From our definition of w and z, we recover the point

$$(X, Y) = \left(\frac{d}{z^2}\ ,\ wd^2z^3\right) =: \zeta((w, z)).$$

Recall that C_d is isomorphic to E over $\bar{K}$. Then ζ is the composition of this isomoprhism with ϕ:

$$C_d \xrightarrow{\sim} E \xrightarrow{\phi} E'.$$
$$\zeta$$

Since ϕ has degree 2, ζ is a two-to-one covering of E'. Provided that rational points exist, searching for them on C_d is more efficient than simply searching for rational points on E'. This is because the quadratic polynomial ζ will (roughly) square the multiplicative height of a point. Thus $P \in C_d(K)$ is encountered faster than $\zeta(P) \in E'(K)$.

Now that the exact sequence (4.2) is entirely explicit, we can compute the ϕ-Selmer groups of some specific isogenies of degree 2. This amounts to finding the representatives in $K(S_{E,\phi}, 2)$ whose corresponding homogeneous space has points everywhere locally.

4.3 Computation of Selmer groups

The procedure of computing the Selmer group of a K-rational 2-isogeny is summarized in this algorithm.

Algorithm 4.5. Input: a number field K, an elliptic curve E/K admitting a K-rational 2-isogeny $\phi : E/K \to E'/K$. Output: the Selmer group $\mathrm{Sel}^{(\phi)}(E/K)$.

1. Write E/K in the form $E : y^2 = x^3 + ax^2 + bx$ with $a, b \in \mathcal{O}_K$.
2. Factor the discriminant $\Delta_E = 16b^2b'$ into prime ideals of $\mathcal{O}_K$.
3. Define:

$$S_{E,\phi} := \{v \in M_K^0 \mid v(\Delta_E) > 0\} \cup M_K^\infty$$
$$K(S_{E,\phi}, 2) := \{d \in K^\times / {K^\times}^2 \mid d \text{ is unramified outside } S_{E,\phi}\}.$$

   The primes that divide 2 are readily included, since these also divide Δ_E. We might have included some primes of good reduction that divide Δ_E (with an exponent divisible by 12). However by Theorem 3.15 this is not a problem. The homogeneous spaces arising from them will not have points everywhere locally and all other homogeneous spaces will have points locally at these primes.

   When choosing representatives of $K(S_{E,\phi}, 2)$, the unit group and class group of $\mathcal{O}_K$ should be taken into account.

4. Let $d \in K(S_{E,\phi}, 2)$. Define

$$C_d : w^2 = d + a'd^2z^2 + b'd^3z^4.$$

   Check whether $C_d(K_v)$ is non-empty for every $v \in S_{E,\phi}$. If so, then $d \in \mathrm{Sel}^{(\phi)}(E/K)$. Do this for every $d \in K(S_{E,\phi}, 2)$.

In order to gain information about the rank of E, we perform this procedure to both ϕ and $\hat{\phi}$. We also need to find the points on $E(K)$ whose order is a power of 2.

Algorithm 4.5 is applied to a few examples. First, we exhibit a proof that an elliptic curve has rank 0 over $\mathbb{Q}$. Thereafter, we do the same but for an elliptic curve over a quadratic number field. Finally, we meet elements of $Ш(E/\mathbb{Q})$, but we do not yet have the tools to classify them as such.

Example 4.6. Let $K = \mathbb{Q}$ and let E_{448} (named after its conductor) be the elliptic curve given by

$$E_{448} : y^2 = x^3 - x^2 - 10913x - 436447.$$

This curve was taken from [LMF13] and it is not immediately visibile that it admits a rational 2-isogeny, i.e. that the polynomial on the right-hand side has a rational root. We apply Algorithm 4.5 to this curve.

1. Factoring the polynomial in x reveals that $x = 121$ is a rational root, implying that $(121, 0)$ is a rational 2-torsion point. We move this point to $(0, 0)$ by the translation $x \mapsto x - 121$. Then the equation of the elliptic curve becomes

$$\begin{aligned} E_{448} : y^2 &= (x + 121)^3 - (x + 121)^2 - 10913(x + 121) - 436447 \\ &= x^3 + 362x^2 + 32768x. \end{aligned}$$

2. We set $a := 362$ and $b := 32768$. Consequently, we have

$$\begin{aligned} a' &= -2a = -724 \\ b' &= a^2 - 4b = -28. \end{aligned}$$

   We factor the discriminant $\Delta_{E_{448}} = 16b^2b'$ to find all the bad primes:

$$\Delta_{E_{448}} = 16b^2b' = 32768 \cdot 28 = 2^{21} \cdot 7.$$

3. The only bad finite primes are 2 and 7. We add ∞, such that we need only look for points in $\mathbb{Q}_2$, $\mathbb{Q}_7$ and $\mathbb{Q}_\infty = \mathbb{R}$:

$$S_{E_{448},\phi} = \{2, 7, \infty\}$$
$$\mathbb{Q}(S_{E_{448},\phi}, 2) = \{\pm 1, \pm 2, \pm 7, \pm 14\}.$$

4. The MAGMA code exhibited in Listing A.1 checks whether the curves C_d have points everywhere locally for all 8 possibilities for d. The only values of d with this property are 1 and -7:

$$\mathrm{Sel}^{(\phi)}(E_{448}/\mathbb{Q}) = \{1, -7\}.$$

This is the image of $E'_{448}(\mathbb{Q})[\hat{\phi}]$:

$$O \mapsto 1$$
$$(0,0) \mapsto b' = -2^2 \cdot 7 \equiv -7$$

In this case, δ is an isomorphism:

$$E'_{448}(\mathbb{Q})/\phi(E_{448}(\mathbb{Q})) = \{O, (0,0)\}.$$

Then (3.6) implies that $Ш(E_{448}/\mathbb{Q})[\phi]$ is trivial.

The first steps of computing $E_{448}(\mathbb{Q})/\hat{\phi}(E'_{448}(\mathbb{Q}))$ are the same, since two isogenous curves have the same set of bad primes. We only replace a' by a and b' by b. Then Listing A.2 tells us that

$$\mathrm{Sel}^{(\hat{\phi})}(E'_{448}/\mathbb{Q}) = \{1, 2\}.$$

Again, we see that the connecting homomorphism is an isomorphism:

$$O \mapsto 1$$
$$(0,0) \mapsto b = 2^1 5 \equiv 2$$

Similarly, $Ш(E'_{448}/\mathbb{Q})[\hat{\phi}]$ is trivial. We now use (3.3) to compute the dimension of $E_{448}(\mathbb{Q})/2E_{448}(\mathbb{Q})$ as an $\mathbb{F}_2$-vector space. It follows from the dimensions of the other vector spaces in this exact sequence (the dimensions are given below the vector spaces)

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & \frac{E'_{448}(\mathbb{Q})[\hat{\phi}]}{\phi(E_{448}(\mathbb{Q})[2])} & \longrightarrow & \frac{E'_{448}(\mathbb{Q})}{\phi(E_{448}(\mathbb{Q}))} & \xrightarrow{\hat{\phi}} & \frac{E_{448}(\mathbb{Q})}{2E_{448}(\mathbb{Q})} & \longrightarrow & \frac{E_{448}(\mathbb{Q})}{\hat{\phi}(E'_{448}(\mathbb{Q})} & \longrightarrow & 0 \\ 0 & & 1 & & 1 & & \dim_{\mathbb{F}_2} \frac{E_{448}(\mathbb{Q})}{2E_{448}(\mathbb{Q})} & & 1 & & 0. \end{array}$$

Since the alternating sum of the dimensions is zero, it follows that $E_{448}(\mathbb{Q})/2E_{448}(\mathbb{Q})$ has dimension 1 as an $\mathbb{F}_2$-vector space. Finally, we conclude from this that

$$E_{448}(\mathbb{Q})/2E_{448}(\mathbb{Q}) = \{O, (0,0)\} \cong E(\mathbb{Q})[2] \times (\mathbb{Z}/2\mathbb{Z})^r.$$

This means that that E_{448} and E'_{448} have rank zero over $\mathbb{Q}$.

$Ш(E_{448}/\mathbb{Q})$ does not have elements of order 2 (such elements would show up in either $Ш(E_{448}/\mathbb{Q})[\phi]$ or $Ш(E'_{448}/\mathbb{Q})[\hat{\phi}]$). This renders 2-descent an effective approach for computing the rank of E_{448}.

Example 4.7. To demonstrate the method for $K \neq \mathbb{Q}$, we now consider an elliptic curve defined over the quadratic field $K = \mathbb{Q}(\sqrt{-11})$ with class number 1 ([LMF13]). Since $-11 \equiv 1 \mod 4$, the ring of integers is given by

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right] =: \mathbb{Z}[\alpha],$$

where the minimal polynomial of α is $\alpha^2 - \alpha + 3 = 0$. Since -11 is negative, the unit group of $\mathcal{O}_K$ is just $\{\pm 1\}$. The curve E_{89} is given by

$$E_{89} : y^2 + \alpha xy = x^3 + \alpha x^2 - x.$$

1. We get rid of the coefficient $a_1 = \alpha$, by applying the translation $y \mapsto y + \frac{\alpha x}{2}$. We obtain

$$\begin{aligned} E_{89} : x^3 + \alpha x^2 - x &= \left(y - \frac{\alpha x}{2}\right)^2 + \alpha x(y - \frac{\alpha x}{2}) \\ &= y^2 - \alpha xy + \frac{\alpha^2 x^2}{4} + \alpha xy - \frac{\alpha^2 x^2}{2} \\ &= y^2 - \frac{(\alpha - 3)x^2}{4} \\ E_{89} : y^2 &= x^3 + \frac{5\alpha - 3}{4}x^2 - x. \end{aligned} \tag{4.5}$$

   To make all coefficients integral, multiply the equation with 2^6 and scale $x \mapsto 2^2 x$ and $y \mapsto 2^3 y$ (note that 2 is inert in $\mathbb{Z}[\alpha]$). This results in

$$E_{89} : y^2 = x^3 + (5\alpha - 3)x^2 - 16x,$$

   the desired form.

2. We have $a := (5\alpha - 3)$ and $b := -16$, resulting in

$$\begin{aligned} a' &= -2a = -10\alpha + 6 \\ b' &:= a^2 - 4b = (5\alpha - 3)^2 + 64 = 25\alpha^2 - 30\alpha + 73 = 25(\alpha - 3) - 30\alpha + 73 = -5\alpha - 2. \end{aligned}$$

   Since the element $5\alpha + 2$ has norm 89, it is an irreducible element of $\mathbb{Z}[\alpha]$. As K has class number 1, it is prime. We then factor $\Delta_{E_{89}}$:

$$\Delta_{E_{89}} = 16b^2 b' = -16^3(5\alpha + 2) = -2^{12}(5\alpha + 2).$$

   Note that the factor 2 just comes from the fact that we multiplied a defining equation for E_{89}, which was originally integral, by 2^6; (4.5) is not minimal at 2. We conclude that $5\alpha + 2$ is the only bad prime. However, this is not very relevant since 2 is also the degree of ϕ.

3. The completions we need to consider are K_2, $K_{5\alpha+2}$ and $K_\infty = \mathbb{C}$ (the infinite prime does not split since K has only one pair of complex embeddings and no real embedding). Since $\mathbb{C}$ is algebraically closed, $C_d(\mathbb{C})$ will always be non-empty.

$$\begin{aligned} S_{E_{89},\phi} &= \{2, 5\alpha + 2, \infty\} \\ K(S_{E_{89},\phi}, 2) &= \{\pm 1, \pm 2, \pm(5\alpha + 2), \pm 2(5\alpha + 2)\}. \end{aligned}$$

4. We check for all 8 possible $d \in K(S_{E_{89},\phi}$ whether the curve C_d has points in K_2 and $K_{5\alpha+2}$. Listing A.4 then tells us that

$$\mathrm{Sel}^{(\phi)}(E_{89}/K) = \{1, -5\alpha - 2\}.$$

   These are just the images of O and $(0, 0)$, so δ is an isomorphism:

$$E'_{89}(K)/\phi(E_{89}(K)) = \{O, (0, 0)\}.$$

Similarly, Listing A.5 yields

$$\begin{aligned} \mathrm{Sel}^{(\hat{\phi})}(E'_{89}/K) &= \{1, -1\} \\ \implies E_{89}(K)/\hat{\phi}(E'_{89}(K)) &= \{O, (0, 0)\}. \end{aligned}$$

Finally, this allows us to conclude that

$$\begin{aligned} E_{89}(K)/2E_{89}(K) &= \{O, (0, 0)\} \\ \implies \mathrm{rank}(E_{89}(K)) &= 0. \end{aligned}$$

Since the entire Selmer groups came from points on the curve, it follows that $Ш(E_{89}/K)[2] = 0$.

Example 4.8. In this example, we will encounter non-trivial elements of $Ш(E/K)[2]$, but we cannot conclude this until Example 5.14.

Consider the curve E_{1100} ([LMF13]) defined over $\mathbb{Q}$:

$$E_{1100} : y^2 = x^3 - x^2 - 177508x - 28726488.$$

1. Applying the translation $x \mapsto x + 243$, it is given by

$$\begin{aligned} y^2 &= (x - 243)^3 - (x - 243)^2 - 177508(x - 243) - 28726488 \\ &= x^3 - 730x^2 + 125x. \end{aligned}$$

2. We have $a := -730$ and $b := 125$, resulting in

$$\begin{aligned} a' &= -2a = 1460 \\ b' &= a^2 - 4b = 532400. \end{aligned}$$

   Then we factor the discriminant of E_{1100}:

$$\Delta_E = 16b^2b' = 2^8 \cdot 5^5 \cdot 11^3.$$

3. We define:

$$\begin{aligned} S_{E_{1100},\phi} &= \{2, 5, 11, \infty\} \\ \mathbb{Q}(S_{E_{1100},\phi}, 2) &= \{\pm 1, \pm 2, \pm 5, \pm 11, \pm 10, \pm 22, \pm 55, \pm 110\}. \end{aligned}$$

4. Listing A.6 computes

$$\begin{aligned} \mathrm{Sel}^{(\phi)}(E_{1100}/\mathbb{Q}) &= \{\pm 1, \pm 5, \pm 11, \pm 55\} \\ \mathrm{Sel}^{(\hat{\phi})}(E'_{1100}/\mathbb{Q}) &= \{1, 5\}. \end{aligned}$$

The elements of $\mathrm{Sel}^{(\hat{\phi})}(E'_{1100}/\mathbb{Q})$ come from O and $(0, 0)$, but it is more difficult to classify the elements of $\mathrm{Sel}^{(\phi)}(E_{1100}/\mathbb{Q})$. Only two of them, 1 and 11, come from the known points O and $(0, 0)$. It could still be that the other six elements come from points on $E'_{1100}(\mathbb{Q})/\phi(E_{1100}(\mathbb{Q}))$, but that we haven't found these points yet. Since $a^2 - 4b = b'$ is not a square, we have $E(\mathbb{Q})[2] = \{O, (0, 0)\}$. This means that if the Selmer elements come from points, then these points have infinite order.

In Example 5.14, 3-descent results in a proof that the rank of E_{1100} is zero, implying that the remaining 6 elements of $\mathrm{Sel}^{(\phi)}(E_{1100}/\mathbb{Q})$ give rise to elements of $Ш(E_{1100}/\mathbb{Q})[\phi]$. A consequence of this fact is that the curve

$$C_{-1} : w^2 = -1 + 1460z^2 - 532400z^4$$

has a point in every completion of $\mathbb{Q}$, but not in $\mathbb{Q}$ itself.

An alternative to Algorithm 4.5 is to compute the local image of δ_v in $K_v^\times / {K_v^\times}^2$ directly for every $v \in S_{E,\phi}$, which is essentially equivalent to Algorithm 4.5. We choose this algorithm because we are interested in the homogeneous spaces that violate the Hasse principle.

5 Descent by 3-isogeny

In this chapter, the theory of Galois cohomology is applied to rational isogenies of degree 3. These 3-isogenies do not automatically have a rational kernel like 2-isogenies do. In this case, the connecting homomorphism lands in a quadratic extension. We produce an algorithm to compute the Selmer groups of rational 3-isogenies. Two examples in chapter 4 are revisited in this context.

5.1 Rational 3-isogenies

We follow the introduction in [Top91]. We start out with the assumption that an elliptic curve E/K admits a K-rational isogeny ψ of degree 3. By Lemma 2.10, this means its kernel $E[\psi]$ is invariant under the action of G_K. Let $E[\psi]$ be generated by a point $P = (\alpha, \beta)$ of order 3. We let E be given by the equation

$$E : y^2 = x^3 + ax^2 + bx + c.$$

Then by Algorithm III.2.5 from [Sil86], the assumption $[2]P = -P = (\alpha, -\beta)$ implies that $x(P) = x([2]P)$ and hence $\alpha \in K$. Similarly, $\beta^2 \in K$. The point $(0, \sqrt{d})$ has order 3 if and only if $b^2 = 4ac$. If b is zero, then so is a, and E is given by

$$E : y^2 = x^3 + C. \tag{5.1}$$

Such elliptic curves have j-invariant 0. Capital letters for the parameters are introduced to prevent confusion with 2-descent. We compute the isogenous curve $\bar{E}$ and the isogeny $\psi : E \to \bar{E}$:

$$\begin{aligned} &\bar{E} : \eta^2 = \xi^3 - 27C \\ &\psi : (x, y) \mapsto \left(\frac{y^2 + 3C}{x^2} \ , \ \frac{y(x^3 - 8C)}{x^3} \right). \end{aligned} \tag{5.2}$$

We abbreviate $C' := -27C$. In this case, substituting $x = 0$ yields that the 3-torsion points in the kernel of ψ are $(0, \pm\sqrt{C})$.

On the other hand, if b in non-zero, E can be written as

$$y^2 = x^3 + A(x - B)^2. \tag{5.3}$$

In that case, $\bar{E}$ and ψ are given by

$$\begin{aligned} &\bar{E} : \eta^2 = \xi^3 - 27A(X - 4A - 27B)^2 \\ &\psi : (x, y) \mapsto \left(\frac{3(6y^2 + 6AB^2 - 3x^3 - 2Ax^2)}{x^2} \ , \ \frac{27y(8AB^2 - x^3 - 4ABx)}{x^3} \right). \end{aligned} \tag{5.4}$$

We introduce the abbreviations $A' := -27A$ and $B' := 4A + 27B$. In this case, substituting $x = 0$ yields that the 3-torsion points in the kernel of ψ are given by $(0, \pm B\sqrt{A})$.

It is visible that $\bar{E}$ also admits a K-rational isogeny, which is the dual isogeny $\hat{\psi}$. The 3-torsion of E is given by

$$E[3] = \psi^{-1}(\bar{E}[\hat{\psi}]).$$

5.2 The cohomology sequence

Unfortunately, an approach as general as the approach to 2-descent is not possible here. We would have to distinguish between four different cases, depending on whether K contains the roots of unity μ_3 and whether the kernel $E[\psi]$ is K-rational. Instead, we just analyze the case $K = \mathbb{Q}$. In that case, we cannot use Lemma 3.6. Instead, a similar result holds.

Lemma 5.1. *Let $\psi : E/\mathbb{Q} \to \bar{E}/\mathbb{Q}$ be a rational 3-isogeny. If E is given by (5.1), define*

$$L := \mathbb{Q}\left(\sqrt{-3C}\right).$$

Similarly, if E is given by (5.3), define

$$L := \mathbb{Q}\left(\sqrt{-3A}\right).$$

In both cases, $E[\psi]$ and μ_3 are isomorphic as G_L-modules

Proof. We introduce

$$D := \begin{cases} C & \text{in the case (5.1)} \\ A & \text{in the case (5.3).} \end{cases}$$

Since $E[\psi]$ and μ_3 have 3 elements, they are isomorphic as groups; an isomorphism $f : E[\psi] \to \mu_3$ can be obtained by mapping a generator T of $E[\psi]$ to the root of unity $w = e^{\frac{2\pi i}{3}} = \frac{-1+\sqrt{-3}}{2}$. It still needs to be checked that f is a morphism of G_L-modules, i.e. that $f(P^\sigma) = f(P)^\sigma$ for every $P \in E[\psi]$ and for every $\sigma \in G_L$. For this, recall that $E[\psi]$ lies in the field $\mathbb{Q}\left(\sqrt{D}\right)$ and that μ lies in $\mathbb{Q}\left(\sqrt{-3}\right)$. Now suppose that σ fixes $\sqrt{-3}$. Then it must also fix $\sqrt{D}$, since σ must be the identity on $L = \mathbb{Q}\left(\sqrt{-3D}\right)$. This implies that σ acts trivially on $E[\psi]$. Hence in that case, the requirement is fulfilled:

$$\begin{aligned} f(O^\sigma) = f(O) = 1 = f(O)^\sigma \\ f(T^\sigma) = f(T) = w = f(T)^\sigma \\ f((2T)^\sigma) = f(2T) = \bar{w} = f(2T)^\sigma. \end{aligned}$$

Thus f is an isomorphism of Galois modules. On the other hand, suppose that σ does not fix $\sqrt{-3}$ but maps it to $-\sqrt{-3}$. Since σ acts trivially on $\mathbb{Q}\left(\sqrt{-3D}\right)$, σ must map $\sqrt{D}$ to $-\sqrt{D}$, meaning that it permutes T and $2T$. In that case, the requirement is also fulfilled:

$$\begin{aligned} f(O^\sigma) = f(O) = 1 = f(O)^\sigma \\ f(T^\sigma) = f(2T) = \bar{w} = f(T)^\sigma \\ f((2T)^\sigma) = f(T) = w = f(2T)^\sigma. \end{aligned}$$

We conclude that for all $P \in E[\psi]$ and all possible $\sigma \in G_L$, the equality $f(P^\sigma) = f(P)^\sigma$ holds, meaning that f is the desired isomorphism of Galois modules.

The entire proof works identically if $-3D$ is a square, implying $L = \mathbb{Q}$. In that case, $-3D$ is fixed by every automorphism in $G_\mathbb{Q}$ already, so extending the field is not required to obtain an isomorphism of Galois modules. □

Corollary 5.2. *Let $\psi : E/\mathbb{Q} \to \bar{E}/\mathbb{Q}$ be a rational 3-isogeny. Then*

$$H^1(G_\mathbb{Q}, E[\psi]) \cong H^1(G_L, E[\psi]) \cong L^\times / {L^\times}^3.$$

Proof. The isomorphism $H^1(G_L, E[\psi]) \cong L^\times / {L^\times}^3$ follows from Lemma 5.1 and Lemma 3.7. The isomorphism $H^1(G_\mathbb{Q}, E[\psi]) \cong H^1(G_L, E[\psi])$ is the so-called *restriction homomorphism*: the domain of a cocycle $G_\mathbb{Q} \to E[\psi]$ is restricted to the subgroup $G_L \subset G_\mathbb{Q}$. It is an isomorphism because of the *Inflation-Restriction-Transgression Sequence* ([Sil86] B.1.3, [Ser64] 2.6.b):

$$H^1(\mathrm{Gal}(L/\mathbb{Q}), E(L)[\psi]) \xrightarrow{\text{Inf}} H^1(G_\mathbb{Q}, E[\psi]) \xrightarrow{\text{Res}} H^1(G_L, E[\psi]) \xrightarrow{\text{Tr}} H^2(\mathrm{Gal}(L/\mathbb{Q}), E(L)[\psi]).$$

$H^1(\mathrm{Gal}(L/\mathbb{Q}), E(L)[\psi])$ is trivial, since $\mathrm{Gal}(L/\mathbb{Q})$ has 2 elements and $E(L)[\psi]$ has either 1 or 3 elements. This implies that the restriction morphism is injective. For the same reason, the group $H^2(\mathrm{Gal}(L/\mathbb{Q}), E(L)[\psi])$ is trivial, so restriction is surjective as well. □

In summary, we have the following exact sequence:

$$0 \longrightarrow \bar{E}(\mathbb{Q})/\psi(E(\mathbb{Q})) \xrightarrow{\delta} L(S_{E,\psi}, 3) \longrightarrow \mathrm{WC}(E/\mathbb{Q})[\psi]. \tag{5.5}$$

The infinite primes of L (there are two such primes if D is negative and one otherwise) become trivial in $L^\times / {L^\times}^3$, since -1 is a cube. Moreover, if D is negative (in which case L has two real embeddings and Dirichlet's Unit Theorem implies the existence of a unit of infinite order) or a square (in which case L contains μ_3), then the unit group of $\mathcal{O}_L$ will contribute to $L(S_{E,\psi}, 3)$.

Our goal is again to give an explicit formulation of the homomorphisms in this exact sequence.

Lemma 5.3. *In the case (5.1), the connecting homomorphism δ is as follows:*

$$\begin{aligned} \delta : \bar{E}(\mathbb{Q})/\psi(E(\mathbb{Q})) &\to L(S_{E,\psi}, 3) \\ (\xi, \eta) &\mapsto \left(\eta + \sqrt{C'}\right) {L^\times}^3 = \left(\eta + 3\sqrt{-3C}\right) \cdot {L^\times}^3 \\ O &\mapsto 1 \cdot {L^\times}^3 \end{aligned}$$

If $\xi = 0$ yields a rational point, i.e. a point in the kernel of $\hat{\psi}$, then C' is a square. For these points, we define

$$\delta\left(\left(0, \sqrt{C'}\right)\right) = \frac{1}{4C} \cdot {L^\times}^3$$
$$\delta\left(\left(0, -\sqrt{C'}\right)\right) = 4C \cdot {L^\times}^3$$

Proof. The map δ comes from the diagram

$$\begin{array}{ccccccc} E(\mathbb{Q}) & \xrightarrow{\psi} & \bar{E}(\mathbb{Q}) & & & \xrightarrow{\quad\delta\quad} & \\ & & \downarrow{\scriptstyle \delta'} & & & & \\ H^1(G_\mathbb{Q}, E[\psi]) & \xrightarrow{\sim} & H^1(G_L, E[\psi]) & \xrightarrow{\sim} & H^1(G_L, \mu_3) & \xrightarrow{\sim} & L^\times/{L^\times}^3 \end{array}$$

Let $P = (\xi, \eta)$ be a point on $\bar{E}(\mathbb{Q})$. Let $Q = (x, y)$ be a point on E such that $\psi(Q) = P$ (Q is in general not rational). Then δ' maps P to the cocycle $\kappa : \sigma \mapsto Q^\sigma - Q$ in $H^1(G_\mathbb{Q}, E[\psi])$, which corresponds uniquely to an element of $L^\times/{L^\times}^3$ through the series of isomorphisms. First, we restrict κ to a cocycle with domain G_L, meaning that it now only acts on the automorphisms that fix $\sqrt{C'}$. We now replace $E[\psi]$ by $\mu_3 = \{w, \bar{w}, 1\}$ by sending κ to the cocylce

$$\lambda : \sigma \mapsto \begin{cases} 1 & \text{if } Q^\sigma - Q = O \\ w & \text{if } Q^\sigma - Q = (0, \sqrt{C}) \\ \bar{w} & \text{if } Q^\sigma - Q = (0, -\sqrt{C}) \end{cases}$$

in $H^1(G_L, \mu_3)$. As seen in 5.1, the action of σ on $E[\psi]$ and the action of σ on μ_3 are 'reversed'; when we restrict κ to a cocycle with domain G_L, the automorphisms that fix μ_3 are precisely the ones that invert $E[\psi]$. Finally, using Lemma 3.7, we must find the unique $t \in L^\times/{L^\times}^3$ such that $t = \beta^3$ and λ can be written as

$$\lambda : \sigma \mapsto \frac{\beta}{\beta^\sigma} = \begin{cases} \beta & \text{if } \beta^\sigma = \beta \\ w\beta & \text{if } \beta^\sigma = \bar{w}\beta \\ \bar{w}\beta & \text{if } \beta^\sigma = w\beta. \end{cases}$$

Then we are done; $t = \delta(P)$. To make this concrete, we first impose restrictions on $Q = (x, y)$ that follow from $\psi(Q) = P$:

$$\xi = \frac{y^2 + 3C}{x^2} \tag{5.6}$$
$$\eta = \frac{y(x^3 - 8C)}{x^3}. \tag{5.7}$$

Just like in Lemma 4.1, $P \in \psi(E(\mathbb{Q}))$ implies that $\delta(P) = 1$. From now on, we assume that Q is not rational.

Second, suppose $\xi = 0$ and C' is a square, so $L = \mathbb{Q}$. Equation (5.6) implies that x is non-zero and $y^2 = -3C$, so $y = \pm\frac{\sqrt{C'}}{3}$. Since Q is a point on E, an expression for x follows:

$$\begin{aligned} -3C = y^2 &= x^3 + C \\ \implies x^3 &= -4C \end{aligned}$$

Equation (5.7) then implies that y and η have the same sign. The action of σ on Q is induced by the action of σ on $\sqrt[3]{-4C}$. If σ fixes $\sqrt[3]{-4C}$, then $Q^\sigma - Q = O$. If σ sends $\sqrt[3]{-4C}$ to $w\sqrt[3]{-4C}$, then applying Algorithm III.2.5 from [Sil86] implies that $Q^\sigma - Q = \left(0, -\sqrt{C}\right)$. Thus the α we are looking for is $-\frac{1}{4C}$. Since -1 is a cube, we can leave it out.

Now assume ξ is non-zero. Substituting the fact that Q is a point on E into equation (5.6) and (5.7) yields a cubic equation for x:

$$x^3 - \xi x^2 + 4C = 0.$$

A straightforward computation yields that all zeros of this cubic lie in the Galois extension $\mathbb{Q}(w, \sqrt{C'}, \sqrt[3]{e})$, with

$$\begin{aligned} e &= 6\sqrt{-3C}\sqrt{\xi^3 - 27C} + \xi^3 - 54C \\ &= 6\sqrt{-3C}\eta + \eta^2 - 27C \\ &= 2\sqrt{C'}\eta + \eta^2 + C' \\ &= \left(y + \sqrt{C'}\right)^2. \end{aligned}$$

By equation (5.7), y will lie in this extension as well. Thus the action of σ on Q is determined by the action of σ on $\sqrt[3]{\left(y + \sqrt{C'}\right)^2}$. Again, because of the 'reversal', we obtain

$$\delta(P) = \frac{1}{\left(y + \sqrt{C'}\right)^2} \equiv y + \sqrt{C'}.$$

□

Lemma 5.4. *In the case (5.3), the connecting homomorphism δ is as follows:*

$$\begin{aligned} \delta : \bar{E}(\mathbb{Q})/\psi(E(\mathbb{Q})) &\to L(S_{E,\psi}, 3) \\ (\xi, \eta) &\mapsto (\eta + (\xi - B')\sqrt{A'})L^{\times 3} = (\eta + 3(\xi - 4A - 27B)\sqrt{-3A}) \cdot L^{\times 3} \\ O &\mapsto 1 \cdot L^{\times 3} \end{aligned}$$

If $\xi = 0$ yields a rational point, i.e. a point in the kernel of $\hat{\psi}$, then A' is a square. For these points, we define

$$\begin{aligned} \delta\left(\left(0, \sqrt{A'}B'\right)\right) &= \frac{A}{2B'} \\ \delta\left(\left(0, -\sqrt{A'}B'\right)\right) &= \frac{2B'}{A} \end{aligned}$$

Proof. The proof is similar to the proof of Lemma 5.3. In this case, the restrictions on $Q = (x, y)$ are

$$\xi = \frac{3(6y^2 + 6AB^2 - 3x^3 - 2Ax^2)}{x^2} \tag{5.8}$$

$$\eta = \frac{27y(8AB^2 - x^3 - 4ABx)}{x^3}. \tag{5.9}$$

Substituting $y^2 = x^3 + A(x - B)^2$ into equation (5.8) yields

$$\begin{aligned} \xi x^2 &= 3(6(x^3 + A(X - B)^2) + 6AB^2 - 3x^3 - 2Ax^2) \\ &= 3(3x^3 + 4Ax^2 - 12ABx + 12AB^2) \\ \implies 0 &= 9x^3 + (12A - \xi)x^2 - 36ABx + 36AB^2. \end{aligned}$$

First, if $\xi = 0$ and $A' = -27A$ is a square, then x lies in the extension $\mathbb{Q}(w, \sqrt[3]{f})$, with

$$\begin{aligned} f &= 2\left(-32A^3 - 324A^2B - 729AB^2 + 27\sqrt{16A^4B^2 + 216A^3B^3 + 729A^2B^4}\right) \\ &= 2(-2AB'^2 + 108A^2B + 729AB^2 + 27\sqrt{A^2B^2B'^2}) \\ &= 2(-2AB'^2 + 27ABB' + 27ABB') \\ &= 4AB'(-B' + 27B) \\ &= 4AB'(-4A) \equiv \frac{2B'}{A} \end{aligned}$$

Equation (5.9) reveals that y lies in the same extension. Because of the 'reversal' of Galois action on μ_3 and $E[\psi]$, the point $\left(0, \sqrt{A'}B\right)$ is mapped to $\frac{A}{2B'}$. The point $\left(0, \sqrt{A'}B'\right)$ is mapped to $\frac{2B'}{A}$.

Although this seems different from the image presented in [vT15], namely $\frac{1}{2\sqrt{A'B'}}$, the two images represent the same class of $L^\times/{L^\times}^3$; they differ by the cube $\left(-\frac{\sqrt{A'}}{3}\right)^3$.

Now let ξ be non-zero, the most tedious case. The splitting field of the polynomial

$$9x^3 + (12A - \xi)x^2 - 36ABx + 36AB^2$$

is $\mathbb{Q}\left(\sqrt{A'}, w, \sqrt[3]{g}\right)$, with

$$\begin{aligned}
g &= \xi^3 - 36A\xi^2 + 1458AB\xi + 432A^2\xi - 1728A^3 - 17496A^2B - 39366AB^2 + \\
&\quad 162\sqrt{3}\sqrt{-AB^2\xi^3 + 27A^2B^2\xi^2 - 1458A^2B^3\xi - 216A^3B^2\xi + 432A^4B^2 + 5832A^3B^3 + 19683A^2B^4} \\
&= \xi^3 + A'(\xi - B')^2 - 9A\xi^2 + 216A^2\xi - 1296A^3 - 11664A^2B - 19683AB^2 \\
&\quad + 162\sqrt{-3AB^2(\xi^3 + A'(\xi - B')^2)} \\
&= \eta^2 + 54\sqrt{A'}B\eta - 9A\xi^2 + 216A^2\xi - 1296A^3 - 11664A^2B - 19683AB^2 \\
&= \left(\eta + (\xi - B')\sqrt{A'}\right)^2
\end{aligned}$$

This finishes the proof; again the 'reversal' implies

$$\delta(P) = \frac{1}{\left(\eta + (\xi - B')\sqrt{A'}\right)^2} \equiv \eta + (\xi - B')\sqrt{A'}.$$

□

A more abstract proof of Lemma 5.3 and Lemma 5.4 can be obtained by employing a variant of the method exhibited in [Sch95]. The difference is that we don't extend $\mathbb{Q}$ by the 2-torsion, the roots of $f(x) = 0$, but by the kernel of $\hat{\psi}$, the roots of $\eta^2 = \bar{f}(0)$. However, it is not necessary to invoke this, so we stick with the straightforward proof here.

Lemma 5.5. *Assume $L \neq \mathbb{Q}$ and suppose $t \in L(S_{E,\psi}, 3)$ is in the image of δ. Then the norm of t is a rational cube.*

Proof. First, we treat the case (5.1) handled in Lemma 5.3. Write $t = u + v\sqrt{C'}$. Since t is in the image of δ, it comes from some point $(\xi, \eta) \in E'(\mathbb{Q})$:

$$\begin{aligned}
(\xi, \eta) \mapsto \left(\eta + \sqrt{C'}\right) \cdot {L^\times}^3 &= \left(u + v\sqrt{C'}\right) \cdot {L^\times}^3 \\
\implies \left(\eta + \sqrt{C'}\right) &= \left(u + v\sqrt{C'}\right)\left(w + z\sqrt{C'}\right)^3,
\end{aligned}$$

for some $w, z \in \mathbb{Q}$. Now, computing the norm of the right-hand side yields

$$N_{L/\mathbb{Q}}\left(\eta + \sqrt{C'}\right) = \left(\eta + \sqrt{C'}\right)\left(\eta - \sqrt{C'}\right) = \eta^2 - C' = \xi^3.$$

Clearly, the norm of $\left(w + z\sqrt{C'}\right)^3$ is also a cube. Then, by the fact that the norm is a homomorphism, it follows that the norm of $u + v\sqrt{C'}$ is also a cube:

$$N_{L/\mathbb{Q}}\left(u + v\sqrt{C'}\right) = \left(\frac{\xi}{N_{L/\mathbb{Q}}\left(w + z\sqrt{C'}\right)}\right)^3.$$

The proof is similar for the case (5.3) handled in Lemma 5.4. One obtains

$$N_{L/\mathbb{Q}}\left(\eta + (\xi - B')\sqrt{A'}\right) = \left(\eta + (\xi - B')\sqrt{A'}\right)\left(\eta - (\xi - B')\sqrt{A'}\right) = \eta^2 - A'(\xi - B')^2 = \xi^3,$$

which implies that the norm of $u + v\sqrt{A'}$ is also a cube. □

This is not a sudden coincidence; there exists a generalization of this fact, which can be proved in a more abstract way.

Theorem 5.6. *Let K be a perfect field and let $\chi : E/K \to E'/K$ be a K-rational isogeny of degree $m > 2$ with cyclic kernel. Assume that $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) \nmid m$. Moreover, assume that $E'(K)[\hat{\chi}] = \{O\}$ and $K \cap \mu_m = \{1\}$. Let M be the extension of K that contains the kernel of $\hat{\chi}$. If t is in the image of the connecting homomorphism $\delta : E'(K) \to M^\times/{M^\times}^m$, then $N_{M/K}(t) \in {K^\times}^m$.*

Proof. We assume that $t \in M^\times/{M^\times}^m$ comes from a point on $E'(K)$. From this we prove that $N_{M/K}(t)$ corresponds to a coboundary.

Since M is the splitting field of a polynomial and K is perfect, M/K is a Galois extension. Then, like in Lemma 5.1, $E[\chi] \cong \mu_m$ as Galois modules, but in the general setting this follows from the Galois invariance of the Weil pairing ([Sil86], III.8.1). It is clear that $E[\chi]$ and μ_m are isomorphic as Abelian groups; we send a generator of $E[\chi]$ to $w := e^{\frac{2\pi i}{m}}$. We now show that this is a morphism of G_M-modules. Let T be a generator of $E'[\hat{\chi}]$ and let $S \in E'[m]$ be such that $\hat{\chi}(S) \in E[\chi] \setminus \{O\}$. Then $E'[m]$ is generated by T and S. The Weil pairing on $E'[m]$ is given by

$$\begin{aligned} e'_m : E'[m] \times E'[m] &\to \mu_m \\ e'_m : (\langle T\rangle \times \langle S\rangle) \times (\langle T\rangle \times \langle S\rangle) &\to \mu_m \\ e'_m(a_1T + a_2S, b_1T + b_2S) &= e'_m(T,T)^{a_1b_1} e'_m(T,S)^{a_1b_2} e'_m(S,T)^{a_2b_1} e'_m(S,S)^{a_2b_2} \\ &= e'_m(T,S)^{a_1b_2 - a_2b_1} =: e'_m(T,S)^c. \end{aligned}$$

We have used that the Weil pairing is bilinear and alternating. For $\rho \in G_M$, the Galois invariance of e'_m implies

$$\begin{aligned} e'_m\left((a_1T + a_2S)^\rho, (b_1T + b_2S)^\rho\right) &= e'_m(a_1T + a_2S, b_1T + b_2S)^\rho \\ e'_m(T^\rho, S^\rho)^c &= (e'_m(T,S)^c)^\rho \\ e'_m(T, S^\rho)^c &= (e'_m(T,S)^c)^\rho, \end{aligned}$$

where we have used that ρ fixes T. Thus the action of ρ on μ_m equals the action of ρ on $\langle S\rangle$. Since $\hat{\chi}$ is rational, this in turn equals the action of ρ on

$$\hat{\chi}(\langle S\rangle) = E[\chi],$$

which finishes the proof that $E[\chi]$ and μ_3 are isomorhpic as G_M-modules.

Moreover, since we assumed $K \cap \mu_m = \{1\}$ and $E'[\hat{\chi}] = \{O\}$, we obtain

$$\mathrm{Gal}(M/K) \cong \mathrm{Gal}(K(\mu_m)/K) \cong F \subseteq (\mathbb{Z}/m\mathbb{Z})^\times.$$

This gives the following sequence of group homomorphisms:

$$E'(K) \xrightarrow{\delta} H^1(G_K, E[\chi]) \xrightarrow{\mathrm{res}} H^1(G_M, E[\chi]) \xrightarrow{\sim} H^1(G_M, \mu_m) \xrightarrow{\sim} M^\times/{M^\times}^m.$$

We start out with a point $P \in E'(K)$. This point is mapped to the cocycle $\sigma \mapsto Q^\sigma - Q$, where $Q \in E$ is such that $\chi(Q) = P$. This cocycle is restricted to G_M by only allowing automorphisms σ that fix M. Then we write this cocycle as $\sigma \mapsto \frac{\beta^\sigma}{\beta}$ and set $t = \beta^m \in M^\times/{M^\times}^m$. Because of the 'reversal' of Galois action, we actually deal with the cocycle $\sigma \mapsto \frac{\beta}{\beta^\sigma}$, but this does not matter for this proof (we just write β instead of $\frac{1}{\beta}$).

The norm of t is the product of all Galois conjugates of t:

$$N_{M/K}(t) = \prod_{\tau \in \mathrm{Gal}(M/K)} t^\tau.$$

Let τ be an automorphism in $\mathrm{Gal}(M/K)$. We trace the element $t^\tau \in M^\times/{M^\times}^m$ back to the start. Via Hilbert's Theorem 90, t^τ corresponds to a cocycle

$$\sigma \mapsto \frac{\gamma^\sigma}{\gamma},$$

where $\gamma^m = t^\tau$. $\frac{\gamma^\sigma}{\gamma}$ is an m^{th} root of unity, since γ^m is fixed by σ. Moreover, demanding that τ fixes $E[\chi]$ determines, via the Weil pairing, an action of τ on μ_m. We define $\bar{\tau} \in \mathrm{Gal}(K(\mu_m)/K)$ as the automorphism that fixes $E[\chi]$ while acting the same as τ on $E'[\hat{\chi}]$. Then we have

$$\left(\frac{\beta^\sigma}{\beta}\right)^{\bar{\tau}} = \frac{\gamma^\sigma}{\gamma}.$$

Since $E'[\hat{\chi}]$ and $K \cap \mu_m$ were both assumed to be trivial, this establishes an isomorphism

$$\mathrm{Gal}(M/K) \cong \mathrm{Gal}(K(\mu_m)/K).$$

Thus t^τ comes from the cocycle

$$\sigma \mapsto \left(\frac{\beta^\sigma}{\beta}\right)^{\bar{\tau}}$$

in $H^1(G_M, \mu_m)$.

We proceed to the left of the sequence. Let $f : E[\chi] \to \mu_m$ be the isomorphism of Abelian groups we have chosen. Then our cocycle in $H^1(G_M, E[\chi])$ comes from the cocycle

$$\sigma \mapsto f^{-1}\left(\left(\frac{\beta^\sigma}{\beta}\right)^{\bar{\tau}}\right) = f^{-1}\left(f(Q^\sigma - Q)^{\bar{\tau}}\right)$$

in $H^1(G_K, E[\chi])$. Now we use the assumption that P is a rational point: this means precisely that $Q^\sigma - Q$ is in $E[\chi]$ for every $\sigma \in G_K$. Since $N_{M/K}(t)$ is the product of all Galois conjugates of t, it comes from the cocycle

$$\sigma \mapsto \sum_{\tau \in \mathrm{Gal}(M/K)} f^{-1}\left(f(Q^\sigma - Q)^{\bar{\tau}}\right)$$

in $H^1(G_K, E[\chi])$. All terms in this sum are points on $E[\chi]$. If we write $E[\chi] = \langle R \rangle$ and use the structure of $\mathrm{Gal}(M/K)$, then this sum is a multiple of

$$\sum_{k \in F} kR = \left(\sum_{k \in F, 2k < m} k - k\right) R = 0.$$

Here we have used that m is greater than 2; 2 is the greatest value of m such that the sum of the units modulo m is not divisible by m. This means that $N_{M/K}(t)$ comes from a cocycle that is trivial in $H^1(G_K, E[\chi])$. Thus $N_{M/K}(t)$ is trivial in $K^\times / {K^\times}^m$, meaning that it's an m^{th} power. □

We define the subgroup of $L(S_{E,\psi}, 3)$ consisting of elements with cube norm:

$$L(S_{E,\psi}, 3)^* := \ker\left(N_{L/\mathbb{Q}} : L(S_{E,\psi}, 3) \to \mathbb{Q}(S_{E,\psi}, 3)\right).$$

This yields an adaptation of the exact sequence (5.5):

$$0 \longrightarrow \bar{E}(\mathbb{Q})/\psi(E(\mathbb{Q})) \xrightarrow{\delta} L(S_{E,\psi}, 3)^* \longrightarrow \mathrm{WC}(E/\mathbb{Q})[\psi]. \tag{5.10}$$

Lemma 5.7. *Suppose $L \neq \mathbb{Q}$ and let $t \in L(S_{E,\psi}, 3)^*$. Then the factorization of the ideal $t\mathcal{O}_L$ consists solely of split primes and non-principal ramified primes.*

Proof. We prove by contradiction.

Suppose an inert prime $p\mathcal{O}_L$, with $p \in \mathbb{Z}$, occurs in the factorization of (t) with multiplicity e. Then the ideal $(N(t)) = (t)(\bar{t})$ contains a factor $(p)(\bar{p}) = p^{2e}$. Since p is inert, no other prime ideal will contribute to the multiplicity of p in the factorization of $N(t)$. Then the fact that $N(t)$ is a cube implies that 3 divides $2e$ and hence 3 divides e. But then p^e is trivial in $L^\times / {L^\times}^3$, so we can pick a different representative of (t) that does not contain a factor p.

On the other hand, suppose a principal ramified prime $(\alpha) \subset \mathcal{O}_L$ occurs in the factorization of (t) with multiplicity f. Write $\alpha^2 = q$ with $q \in \mathbb{Z}$. Then $N(t)$ contains a factor q^f. But $N(t)$ is a cube, so 3 must divide f. Again, this implies we can pick a representative of (t) that is not divisible by (α). □

Our next goal is to make the final map concrete, that is to define the homogenous spaces that elements of $L(S_{E,\psi}, 3)^*$ are mapped to.

Lemma 5.8. *In the case (5.1), the map $L(S_{E,\psi},3)^* \to \mathrm{WC}(E/\mathbb{Q})[\psi]$ is as follows. Let t be an element of $L(S_{E,\psi},3)^*$. If C' is a square and hence L equals $\mathbb{Q}$, then C_t is the curve in $\mathbb{P}^2(\mathbb{Q})$ defined by the following equation in w and r:*

$$C_t : t^2w^3 - 2t\sqrt{C'} = r^3.$$

If C' is not a square and L is a proper extension of $\mathbb{Q}$, write $t = u + v\sqrt{C'}$. Then C_t is the curve in $\mathbb{P}^2(\mathbb{Q})$ defined by the following equation in the variables w and z:

$$C_t : 3uw^2z + C'uz^3 + vw^3 + 3C'vwz^2 = 1$$

Proof. We first handle the case $L = \mathbb{Q}$. In that case t is in the image of δ if there is a $w \in \mathbb{Q}$ such that

$$tw^3 = \eta + \sqrt{C'}.$$

We substitute this into the equation of $\bar{E}$ to obtain

$$\left(tw^3 - \sqrt{C'}\right)^2 = t^2w^6 - 2tw^3\sqrt{C'} + C' = \xi^3 + C'.$$

Dividing both sides by w^3 and setting $r := \frac{\xi}{w}$ yields the equation for C_t. A rational point $(w,r) \in C_t(\mathbb{Q})$ of this equation comes from a rational point

$$(\xi,\eta) = (rw, tw^3 - \sqrt{C'})$$

on $\bar{E}(\mathbb{Q})$.

The case $\xi = 0$ is also covered by this. Substituting $t = 4C$ gives the solution

$$(w,r) = \left(0, \frac{2\sqrt{C'}}{3}\right).$$

Similarly, $t = \frac{1}{4C}$ results in the point

$$(w,r) = \left(-\frac{2\sqrt{C'}}{3}, 0\right).$$

Moreover, the homogeneous space C_1 coming from the point O always has a point at infinity.

On the other hand, if C' is not a square, then write $t = u + v\sqrt{C'}$ and $N(t) = s^3$ for some $s \in \mathbb{Q}$. If t is in the image of δ, then there is a $w + z\sqrt{C'} \in L^\times$ such that

$$\begin{aligned}
\eta + \sqrt{C'} &= \left(u + v\sqrt{C'}\right)\left(w + z\sqrt{C'}\right)^3 \\
\implies \eta &= uw^3 + 3C'uwz^2 + 3C'vw^2z + C'^2vz^3 && (5.11)\\
1 &= 3uw^2z + C'uz^3 + vw^3 + 3C'vwz^2. && (5.12)
\end{aligned}$$

We show that (5.12) is also sufficient. Suppose $(w,z) \in \mathbb{Q}^2$ solves (5.12). Then (5.11) gives a value for η. A matching value for ξ can be found using $\xi^3 + C' - \eta^2 = 0$:

$$\begin{aligned}
\xi^3 + C' - \eta^2 &= \xi^3 - \left(\eta + \sqrt{C'}\right)\left(\eta - \sqrt{C'}\right) \\
&= \xi^3 - N_{L/\mathbb{Q}}\left(\eta + \sqrt{C'}\right) \\
&= \xi^3 - N_{L/\mathbb{Q}}\left(u + v\sqrt{C'}\right) N_{L/\mathbb{Q}}\left(w + z\sqrt{C'}\right)^3 \\
&= \xi^3 - \left(s(w^2 - C'z^2)\right)^3 \\
&= (\xi - s(w^2 - C'z^2))(\xi^2 + s(w^2 - C'z^2) + s^2(w^2 - C'z^2)^2).
\end{aligned}$$

This polynomial has the rational root $\xi = s(w^2 - C'z^2)$. So a solution (w,z) of (5.12) implies that $u + v\sqrt{A'}$ comes from the point

$$(\xi,\eta) = \left(s(w^2 - C'z^2), uw^3 + 3C'uwz^2 + 3C'vw^2z + C'^2vz^3\right)$$

on $\bar{E}(\mathbb{Q})$. From this we conclude that $u + v\sqrt{C'}$ is in the image of δ if and only if the curve C_t defined by (5.12) has a rational point. □

Lemma 5.9. *In the case (5.3), the map $L(S_{E,\psi},3)^* \to \mathrm{WC}(E/\mathbb{Q})[\psi]$ is as follows. Let t be an element of $L(S_{E,\psi})$. If A' is a square and hence L equals $\mathbb{Q}$, then C_t is the curve in $\mathbb{P}^2(\mathbb{Q})$ defined by the following polynomial in w and r:*

$$C_t : t^2w^3 - 2t(wr - B')\sqrt{A'} = r^3.$$

If A' is not a square, write $t = u + v\sqrt{A'}$ and $N(t) = s^3$. Then C_t is the curve in $\mathbb{P}^2(\mathbb{Q})$ defined by the following equation in w and z:

$$C_t : 3uw^2z + A'uz^3 + vw^3 + 3A'vwz^2 + B' = s(w^2 - A'z^2)$$

Proof. In the case $L = \mathbb{Q}$, we have

$$tw^3 = \eta + (\xi - B')\sqrt{A'}.$$

Since (ξ, η) is a point on $\bar{E}$, one obtains

$$\begin{aligned} \Big(tw^3 - (\xi - B')\sqrt{A'}\Big))^2 &= \xi^3 + A'(\xi - B')^2 \\ \implies t^2w^6 - 2tw^3(\xi - B')\sqrt{A'} &= \xi^3. \end{aligned}$$

Dividing the latter equation by w^3 and introducing $r := \frac{\xi}{w}$ yields the definition for the homogeneous space. A rational point $(w, r) \in C_t(\mathbb{Q})$ comes from a rational point

$$(\xi, \eta) = (wr, tw^3 - (wr - B')\sqrt{A'})$$

on $\bar{E}(\mathbb{Q})$.

Again, it is straightforward to verify that $\bar{E}[\hat{\psi}]$ gives homogeneous spaces with a rational point.

On the other hand, suppose A' is not a square and L is a proper extension of $\mathbb{Q}$. Then the assumption that $t = u + v\sqrt{A'}$ lies in the image of δ implies the following:

$$\begin{aligned} \eta + (\xi - B')\sqrt{A} &= (u + v\sqrt{A'})(w + z\sqrt{A'})^3 \\ \implies \eta &= uw^3 + 3A'uwz^2 + 3A'vw^2z + A'^2vz^3 \\ \xi - B' &= 3uw^2z + A'uz^3 + vw^3 + 3A'vwz^2. \end{aligned} \tag{5.13}$$

Then we demand that (ξ, η) is a point on $\bar{E}$.

$$\begin{aligned} \xi^3 + A'(\xi - B')^2 - \eta^2 &= \xi^3 - (\eta + (\xi - B')\sqrt{A'})(\eta - (\xi - B')\sqrt{A'}) \\ &= \xi^3 - N_{L/\mathbb{Q}}(\eta + (\xi - B')\sqrt{A'}) \\ &= \xi^3 - N_{L/\mathbb{Q}}(u + v\sqrt{A'})N_{L/\mathbb{Q}}(w + z\sqrt{A'})^3 \\ &= \xi^3 - \big(s(w^2 - A'z^2))\big)^3 \\ &= \prod_{i \in \{0,1,2\}} (\xi - q^i s(w^2 - A'z^2)), \end{aligned}$$

where q is a non-trivial third root of unity. This polynomial has precisely the rational root $\xi = s(w^2 - A'z^2)$. Substituting the expression for ξ given in (5.13) gives

$$3uw^2z + A'uz^3 + vw^3 + 3A'vwz^2 + B' = s(w^2 - A'z^2).$$

If (w, z) is a rational solution of this equation, then $u + v\sqrt{A'}$ comes from the point

$$(\xi, \eta) = \big(s(w^2 - A'z^2), uw^3 + 3A'uwz^2 + 3A'vw^2z + A'^2vz^3\big)$$

on $\bar{E}(\mathbb{Q})$. Conversely, if $u + v\sqrt{A'}$ comes from point (ξ, η), then such a solution must exist (w, z). Thus C_t is the homogeneous space we are looking for. □

Contrary to the case of descent by 2-isogeny, it turns out we don't have to check whether the homogeneous spaces have points over the real numbers.

Lemma 5.10. *Let $C_t \in \mathrm{WC}(E/\mathbb{Q})$ be a homogeneous space coming from a rational 3-isogeny. Then $C_t(\mathbb{R})$ is non-empty.*

Proof. In all four cases, we can fix one variable to obtain a cubic polynomial in the other variable. Such a polynomial is surjective as a real function, resulting in a point in $C_t(\mathbb{R})$. □

Remark 5.11. In all cases of Lemma 5.8 and Lemma 5.8, we obtain a rational map

$$\theta : C_t \to \bar{E},$$

which can recover rational points on $\bar{E}$ from rational points on C_t. Recall that C_t is isomorphic to E over $\bar{\mathbb{Q}}$. Then θ is the composition of this isomorphism with ψ:

$$C_t \xrightarrow{\sim} E \xrightarrow{\psi} \bar{E}.$$
$$\theta$$

Since ψ has degree 3, θ is a three-to-one covering of $\bar{E}$. In comparison to descent by 2-isogeny, this yields an even more efficient point search. The multipliciative height of a point of C_t is (roughly) cubed by θ, so a point $P \in C_t(\mathbb{Q})$ will be encountered much faster than $\theta(P) \in \bar{E}(\mathbb{Q})$.

Now that we have made the exact sequence (5.10) entirely explicit in both case (5.1) and (5.3), we can compute Selmer groups of rational isogenies of degree 3.

5.3 Computation of Selmer groups

The procedure of computing the Selmer group of a rational 3-isogeny is summarized in the following algorithm.

Algorithm 5.12. Input: an ellptic curve $E/\mathbb{Q}$ admitting a rational 3-isogeny $\psi : E/\mathbb{Q} \to \bar{E}/\mathbb{Q}$. Output: the Selmer group $\mathrm{Sel}^{(\psi)}(E/\mathbb{Q})$.

1. Write $E/\mathbb{Q}$ in the form $E : y^2 = x^3 + C$ (1) or $y^2 = x^3 + A(x - B)^2$ (2), where A, B and C are integers. If necessary, compute the j-invariant of E to decide which of the two cases applies. An equation for $\bar{E}$ follows in terms of A', B' and C'.

2. Define the extension $L := \mathbb{Q}\left(\sqrt{C'}\right)$ in case (1) and $L := \mathbb{Q}\left(\sqrt{A'}\right)$ in case (2). Determine its ring of integers $\mathcal{O}_L$, the unit group $\mathcal{O}_L^\times$ and the class group $\mathrm{Cl}(\mathcal{O}_L)$.

3. Compute
$$\Delta_E = \begin{cases} -432C^2 & \text{in case (1),} \\ -16A^2B^3B' & \text{in case (2).} \end{cases}$$
Factor the the ideal $(3\Delta_E)$ into prime ideals of $\mathcal{O}_L$.

4. Define:
$$\begin{aligned} S_{E,\psi} &:= \{v \in M_L^0 \mid v(3\Delta_E) > 0\} \\ L(S_{E,\psi}, 3) &:= \{t \in L^\times / {L^\times}^3 \mid t \text{ is unramified outside } S_{E,\psi}\} \\ L(S_{E,\psi}, 3)^* &:= \ker\left(N_{L/\mathbb{Q}} : L(S_{E,\psi}, 3) \to \mathbb{Q}(S_{E,\psi}, 3)\right). \end{aligned}$$

5. Let $t \in L(S_{E,\psi}, 3)^*$, write $t = u + v\sqrt{C'}$ in case (1) and $t = u + v\sqrt{A'}$ in case (2). Then define the homogeneous space
$$C_t : \begin{cases} t^2w^3 - 2t\sqrt{C'} = r^3 & \text{case (1), } L = \mathbb{Q} \\ 3uw^2z + C'uz^3 + vw^3 + 3C'vwz^2 = 1 & \text{case (1), } L \neq \mathbb{Q} \\ t^2w^3 - 2t(wr - B')\sqrt{A'} = r^3 & \text{case (2), } L = \mathbb{Q} \\ uw^2z + A'uz^3 + vw^3 + 3A'vwz^2 + B' = s(w^2 - A'z^2) & \text{case (2), } L \neq \mathbb{Q}. \end{cases}$$
Check whether $C_t(\mathbb{Q}_v)$ is non-empty for every $v \in S_{E,\psi}$. If so, then $t \in \mathrm{Sel}^{(\psi)}(E/\mathbb{Q})$.

In order to gain information about the rank of $E(\mathbb{Q})$, we apply Algorithm 5.12 to both ψ and its dual isogeny.

Algorithm 5.12 is demonstrated in a few examples. Both case (1) and (2) will be treated and we will also encounter non-trivial elements of Tate-Shafarevich groups. We can identify them as such by reusing Example 4.6 and 4.8.

Example 5.13. Consider the elliptic curve $E_{441}/\mathbb{Q}$ from [LMF13]:

$$E_{441} : y^2 + y = x^3 - 331.$$

We apply Algorithm 5.12 to this curve.

1. It is quite easy to see that we are in case (1), but just to be certain we can compute $j_E = 0$. We translate y to $y + \frac{1}{2}$ to obtain

$$\begin{aligned} x^3 - 331 &= (y - \frac{1}{2})^2 + (y - \frac{1}{2}) \\ &= y^2 - \frac{1}{4} \\ \implies y^2 &= x^3 - 331 + \frac{1}{4} \\ &= x^3 - \frac{1323}{4}. \end{aligned}$$

   Multiplying the entire equation by 2^6 and replacing (x, y) by $(2^{-2}x, 2^{-3}y)$ yields the form

$$E_{441} : y^2 = x^3 - 21168.$$

   This gives the parameters

$$\begin{aligned} C &= -21168 = -2^4 \cdot 3^3 \cdot 7^2 \\ C' &= -27C = 571536 = 2^4 \cdot 3^6 \cdot 7^2. \end{aligned}$$

2. Note that $C' = 756^2$ is a square, so the extension L is just $\mathbb{Q}$.

3. The discriminant of E_{441} is given by

$$\Delta_{E_{441}} = -432(C)^2 = -432(-21168)^2 = -193572384768 = -2^{12}3^97^4.$$

   Note that we have multiplied by 2^6, causing the factor 2^{12} in the discriminant. In fact, E_{441} has good reduction at 2 and the equation we work with is not minimal at 2. E_{441} already has bad reduction at 3, so we don't have to add it to $S_{E_{441},\psi}$.

4. We obtain

$$\begin{aligned} S_{E_{441},\psi} &= \{3, 7\} \\ L(S_{E441,\psi})^* &= L(S_{E_{441},\psi}) = \langle 3, 7\rangle \\ &= \{1, 3, 9, 7, 21, 63, 49, 147, 441\}. \end{aligned}$$

5. Using Listing A.10, it is checked whether the homogeneous spaces

$$C_t : t^2w^3 - 2t\sqrt{C'} = r^3$$

   have points locally at the primes 3 and 7. This results in

$$\mathrm{Sel}^{(\phi)}(E_{441}/\mathbb{Q}) = \{1, 7, 49\}.$$

   These elements come from the rational 3-torsion points on $\bar{E}_{441}$:

$$\begin{aligned} \delta((0, 756)) &= \frac{1}{4C} = 2^{-6}3^{-3}7^{-2} \equiv 7 \\ \delta((0, -756)) &= 4C = 2^63^37^2 \equiv 49 \end{aligned}$$

   From the injectivity of δ we conclude that these are all the points in $\bar{E}_{441}(\mathbb{Q})/\psi(E_{441}(\mathbb{Q}))$.

We repeat the last steps of the algorithm to find $E_{441}(\mathbb{Q})/\hat{\psi}(\bar{E}_{441}(\mathbb{Q}))$.

2. We have $L = \mathbb{Q}(\sqrt{-21168}) = L(\sqrt{-3})$. L has class number 1 and ring of integers

$$\mathcal{O}_L = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] =: \mathbb{Z}[\alpha].$$

The minimal polynomial of α is $\alpha^2 - \alpha + 1 = 0$. The unit group of $\mathcal{O}_L$ has rank zero, but $\alpha - 1$ has order 3 in $\mathcal{O}_L^\times$. Furthermore, $N_{L/\mathbb{Q}}(\alpha - 1) = 1$.

3. We don't care about the prime 2 that occurs in the factorization of $\Delta_{\bar{E}_{441}}$ (it is inert in $\mathcal{O}_L$), since $\bar{E}_{441}$ has good reduction at 2. We factor $3\mathcal{O}_L$ and $7\mathcal{O}_L$ into prime ideals of $\mathcal{O}_L$.

$$\begin{aligned} X^2 + X + 1 &\equiv (X+1)^2 \mod 3 \\ \implies 3\mathcal{O}_L &= (3, \alpha+1)^2 = (\alpha+1)^2 \text{ (ramified)} \\ X^2 + X + 1 &\equiv (X+2)(X-3) \mod 7 \\ \implies 7\mathcal{O}_L &= (7, \alpha+2)(7, \alpha-3) = (\alpha+2)(\alpha-3) \text{ (split)} \end{aligned}$$

4. By Lemma 5.7, the ramified prime 3 cannot contribute. We need only check possibilities $(\alpha+2)^i(\alpha-3)^j(\alpha-1)^k$, with $i + j \equiv 0 \mod 3$. This gives

$$L(S_{\bar{E}_{441},\hat{\psi}}, 3)^* = \{(\alpha-1)^k, (\alpha+2)(\alpha-3)^2(\alpha-1)^k, (\alpha+2)^2(\alpha-3)(\alpha-1)^k \mid k \in \{0,1,2\}\}.$$

5. Listing A.11 determines which of the homogeneous spaces

$$C_t : 3uw^2z + Cuz^3 + vw^3 + 3Cvwz^2 = 1$$

coming from $L(S_{\bar{E}_{441},\hat{\psi}}, 3)^*$ have points everywhere locally:

$$\mathrm{Sel}^{(\hat{\psi})}(\bar{E}_{441}/\mathbb{Q}) = \{1, -14 + 21\alpha, -7 + 21\alpha\}.$$

We write the $t = -14 + 21\alpha$ as $t = -\frac{7}{2} + \frac{1}{8}\sqrt{C}$. In fact the curve C_t has a rational point, $(w, z) = (2, 0)$, which can be found through a point search. Plugging this point into our map $\theta : C_t \to E_{441}$ yields the point

$$(x, y) = (28, -28) \in E_{441}(\mathbb{Q}).$$

Indeed, $(-28)^2 = 28^3 - 21168$ is easily verified. Thus we obtain

$$E_{441}(\mathbb{Q})/\hat{\psi}(\bar{E}_{441}) = \langle (28, -28) \rangle = \{O, (28, -28), (28, 28)\}.$$

Then from the exact sequence

$$0 \longrightarrow \frac{\bar{E}_{441}(\mathbb{Q})[\hat{\phi}]}{\psi(E_{441}(\mathbb{Q})[2])} \longrightarrow \frac{\bar{E}_{441}(\mathbb{Q})}{\phi(\bar{E}_{441}(\mathbb{Q}))} \xrightarrow{\hat{\psi}} \frac{E_{441}(\mathbb{Q})}{3E_{441}(\mathbb{Q})} \longrightarrow \frac{E_{441}(\mathbb{Q})}{\hat{\psi}(\bar{E}_{441}(\mathbb{Q})} \longrightarrow 0$$

we conclude that

$$E_{441}(\mathbb{Q})/3E_{441}(\mathbb{Q}) = \langle (28, -28) \rangle = \{O, (28, -28), (28, 28)\}.$$

Now, the order of $(28, -28)$ can be either infinite or a multiple of 3. In the latter case, the order would be divisible by 12, by B.C. Mazur's Classification Theorem ([Maz77]). However, it is straightforward to verify that $[12](28, -28) \neq O$, so $(-28, 28)$ has infinite order.

From this we conclude that $E_{441}(\mathbb{Q})$ and $\bar{E}_{441}(\mathbb{Q})$ have rank one:

$$\begin{aligned} E_{441}(\mathbb{Q}) &\cong \mathbb{Z} \\ \bar{E_{441}}(\mathbb{Q}) &\cong \mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}. \end{aligned}$$

All elements of Selmer groups came from points on the curve, so $Ш(E_{441}/\mathbb{Q})[3]$ is trivial.

Example 5.14. Recall the curve

$$E_{1100} : y^2 = x^3 - x^2 - 177508x - 28726488$$

from Example 4.8. Descent by 2-isogeny resulted in Selmer elements that we were unable to lift to points on $E'_{1100}(\mathbb{Q})$. We now show through descent by 3-isogeny that E_{1100} (and thereby E'_{1100}) has rank zero, implying that the Selmer elements correspond to non-trivial elements of $Ш(E_{1100}/\mathbb{Q})[\phi]$.

1. If there exists a rational 3-isogeny $\psi : E_{1100}/\mathbb{Q} \to \bar{E}_{1100}/\mathbb{Q}$, then E_{1100} has a point of order 3 with rational x-coordinate. To find this point, we use division polynomials ([Sch85]). Translating x gives the form

$$\begin{aligned} E_{1100} : y^2 &= \left(x + \frac{1}{3}\right)^3 - \left(x + \frac{1}{3}\right)^2 - 177508\left(x + \frac{1}{3}\right) - 28726488 \\ &= x^3 - \frac{532525}{3}x - \frac{777212750}{27}. \end{aligned}$$

Using these coefficients, we find that the corresponding division polynomial has the rational root $x = -245$. Translating x by this root gives

$$\begin{aligned} E_{1100} : y^2 &= (x - 245)^3 - \frac{532525}{3}(x - 245) - \frac{777212750}{27} \\ &= x^3 - 735x^2 + \frac{7700}{3}x - \frac{60500}{27} \\ &= x^3 - 735\left(x - \frac{110}{63}\right)^2. \end{aligned}$$

Finally, we want B to be an integer, so we multiply the entire equation by $3^6 \cdot 7^6$ and replace (x, y) by $(3^2 \cdot 7^2 x, 3^3 \cdot 7^3 y)$ to obtain

$$\begin{aligned} E_{1100} : y^2 &= x^3 - 735 \cdot 21^2\left(x - \frac{110}{63} \cdot 21^2\right)^2 \\ &= x^3 - 324135(x - 770)^2. \end{aligned}$$

This is the desired form, with the parameters

$$\begin{aligned} A &= -324135 = -3^3 \cdot 5 \cdot 7^4 \\ B &= 770 = 2 \cdot 5 \cdot 7 \cdot 11 \\ A' &= -27A = 8751645 = 3^6 \cdot 5 \cdot 7^4 \\ B' &= 4A + 27B = -1275750 = -2 \cdot 3^6 \cdot 5^3 \cdot 7. \end{aligned}$$

2. The extension we work with is $L = \mathbb{Q}\left(\sqrt{A'}\right) = \mathbb{Q}\left(\sqrt{5}\right)$. Since $5 \equiv 1 \mod 4$, its ring of integers is

$$\mathcal{O}_L = \mathbb{Z}\left[\frac{1 + \sqrt{5}}{2}\right] = \mathbb{Z}[\varphi],$$

where φ is the golden ratio with minimal polynomial $\varphi^2 - \varphi - 1 = 0$. φ is a unit of infinite order in $\mathcal{O}_L$ (since $\varphi(\varphi - 1) = 1$) with $N_{L/\mathbb{Q}}(\varphi) = -1$. $\mathcal{O}_L$ has class number 1.

3. The bad primes of E_{1100} were determined to be 2, 5 and 11 in Example 4.8. We have to add the prime 3 because it's the degree of our isogeny. We analyze the splitting behavior of these primes to see if they occur in $L(S_{E_{1100},\hat{\psi}}, 3)^*$:

$$\begin{aligned} &X^2 - X - 1 \equiv X^2 + X + 1 \mod 2 \\ &\quad\implies 2\mathcal{O}_L = 2\mathcal{O}_L \text{ (inert)} \\ &X^2 - X - 1 \equiv X^2 + 2X + 2 \mod 3 \\ &\quad\implies 3\mathcal{O}_L = 3\mathcal{O}_L \text{ (inert)} \\ &X^2 - X - 1 \equiv (X + 2)^3 \mod 5 \\ &\quad\implies 5\mathcal{O}_L = (5, \varphi + 2)^2 = (\varphi + 2)^2 \text{ (ramified)} \\ &X^2 - X - 1 \equiv (X + 3)(X + 7) \mod 11 \\ &\implies 11\mathcal{O}_L = (11, \varphi + 3)(11, \varphi + 7) = (\varphi + 3)(\varphi - 4); \text{ (split).} \end{aligned}$$

4. The only primes that can contribute to $L(S_{E_{1100},\hat{\psi}}, 3)^*$ are the ones above 11. The unit φ also contributes:

$$L(S_{E_{1100},\hat{\psi}}, 3)^* = \{\varphi^k, (\varphi + 3)(\varphi - 4)^2\varphi^k, (\varphi + 3)^2(\varphi - 4)\varphi^k \mid k \in \{0, 1, 2\}\}.$$

5. For every $u + v\sqrt{A'}$ of norm s^3, Listing A.8 computes whether the homogeneous space

$$C_t : vw^3 + 3uw^2z + 3Avwz^2 + Auz^3 + B' = s(w^2 - Az^2)$$

has points locally at the primes 2, 3, 5, and 11. We can easily compute s from the fact observation that φ has norm -1, while $\varphi+3$ and $\varphi-4$ both have norm 11. The computation shows

$$\begin{aligned} &\mathrm{Sel}^{(\psi)}(E_{1100}/\mathbb{Q}) = \{1\} \\ \implies &\bar{E}_{1100}(\mathbb{Q})/\psi(E_{1100}(\mathbb{Q})) = \{O\}. \end{aligned}$$

The same process is now applied to the dual isogeny $\hat{\psi} : \bar{E} \to E$.

2. We obtain $L = \mathbb{Q}\left(\sqrt{A}\right) = \mathbb{Q}\left(\sqrt{-15}\right)$. Again, the residue upon division by 4 is one, so we have the ring of integers

$$\mathcal{O}_L = \mathbb{Z}\left[\frac{1+\sqrt{-15}}{2}\right] =: \mathbb{Z}[\alpha].$$

The minimal polynomial of α is $\alpha^2 - \alpha + 4 = 0$. Moreover, $\mathcal{O}_L$ has unit group $\{\pm 1\}$ and class number 2.

3. The splitting behavior in $\mathcal{O}_L$ of the bad primes is as follows:

$$\begin{aligned} X^2 - X + 4 &\equiv X(X+1) \mod 2 \\ \implies 2\mathcal{O}_L &= (2,\alpha)(2,\alpha+1) \text{ (split)} \\ X^2 - X + 4 &\equiv (X+1)^2 \mod 3 \\ \implies 3\mathcal{O}_L &= (3,\alpha+1)^2 \text{ (ramified)} \\ X^2 - X + 4 &\equiv (X+2)^3 \mod 5 \\ \implies 5\mathcal{O}_L &= (5,\alpha+2)^2 \text{ (ramified)} \\ X^2 - X + 4 &\equiv X^2 + 10X + 4 \mod 11 \\ \implies 11\mathcal{O}_L &= 11\mathcal{O}_L \text{ (inert)}. \end{aligned}$$

4. In this case, there are a lot more possible ways to obtain an ideal of cube norm using only bad primes. However, such an ideal has to be a principal ideal, since it can be written as $\left(u + v\sqrt{A}\right)$. We write

$$\left(u + v\sqrt{A}\right) = (2,\alpha)^i(2,\alpha+1)^j(3,\alpha+1)^k(5,\alpha+2)^l.$$

Then, from the assumption that this ideal has cube norm, we obtain the restrictions

$$i + j \equiv k \equiv \lambda \equiv 0 \mod 3.$$

From the assumption that it is a principal ideal, we obtain

$$i + j + k + l \equiv 0 \mod 2,$$

since $\mathcal{O}_L$ has class number 2. Moreover, no multiplicity can exceed 5; in that case $\left(u + v\sqrt{A}\right)$ is divisible by the cube of a principal ideal. The same happens if two multiplicities exceed 2. We dichotomize two cases: $(k,l) = (0,0)$ and $(k,l) \neq (0,0)$. If k and l are both zero, then we have $i \in \{0,1,2,4,5\}$. j is then chosen to be $6 - i$, such that the resulting product is both principal and of cube norm. This accounts for 5 possibilities. If k and l are not both zero, then exactly one of them equals 3 (if both do, then we divide out a principal ideal). Then it follows that $i + j = 3$ with both non-zero, resulting in two more possibilities. In conclusion, this gives us 9 possibilities for $t \in L(S_{E_{1100},\hat{\psi}}, 3)^*$.

5. For every $t = u + v\sqrt{A'}$ of norm s^3, we define the homogeneous space

$$C_t : uw^2z + A'uz^3 + vw^3 + 3A'vwz^2 + B' = s(w^2 - A'z^2)$$

and check whether it has points locally at the bad primes. Listing A.9 yields

$$\begin{aligned} &\mathrm{Sel}^{(\psi)}(\bar{E}_{1100}/\mathbb{Q}) = \{1\} \\ \implies\ &E_{1100}(\mathbb{Q})/\hat{\psi}(\bar{E}_{1100}(\mathbb{Q})) = \{O\}. \end{aligned}$$

Finally, we conclude that the isogeny class of E_{1100} has rank zero over $\mathbb{Q}$. This means that the Selmer elements found in Example 4.8 do not come from points on E'. By the exact sequence (3.6), they correspond to non-trivial elements of $Ш(E_{1100}/\mathbb{Q})[2]$. At last, we conclude that the curve

$$C_{-1} : w^2 = -1 + 1460z^2 - 532400z^4$$

has points everywhere locally, but not globally.

Example 5.15. Recall the elliptic curve

$$E_{448} : y^2 = x^3 - x^2 - 10913x - 436447.$$

In Example 4.6 it was shown through descent by 2-isogeny that E_{448} has rank zero over $\mathbb{Q}$. Descent by 3-isogeny results in Selmer elements, but these cannot come from points, so we immediately conclude we are dealing with elements of $Ш(E_{448}/\mathbb{Q})[3]$.

1. We translate x by $\frac{1}{3}$ to get rid of the quadratic term:

$$\begin{aligned} E_{448} : y^2 &= \left(x + \frac{1}{3}\right)^3 - \left(x + \frac{1}{3}\right)^2 - 10913\left(x + \frac{1}{3}\right) - 436447 \\ &= x^3 - \frac{32740}{3}x - \frac{11882288}{27}. \end{aligned}$$

Factoring the corresponding division polynomial reveals that $x = -50$ is a rational 3-torsion point. Translating by that point yields

$$\begin{aligned} E_{448} : y^2 &= (x - 50)^3 - \frac{32740}{3}(x - 50) - \frac{11882288}{27} \\ y^2 &= x^3 - 150x^2 - \frac{10240}{3}x - \frac{524288}{27} \\ &= x^3 - 150\left(x - \frac{512}{45}\right)^2. \end{aligned}$$

Multiplying the equation by $3^6 \cdot 5^6$ and scaling x and y suitably finally results in

$$E_{448} : y^2 = x^3 - 33750(x + 2560)^2.$$

The parameters A, B, A' and B' are as follows.

$$\begin{aligned} A &= -33750 = -2 \cdot 3^3 \cdot 5^4 \\ B &= -2560 = 2^9 \cdot 5 \\ A' &= -27A = 911250 = 2 \cdot 3^6 \cdot 5^4 \\ B' &= 4A + 27B = -204120 = -2^3 \cdot 3^6 \cdot 5 \cdot 7. \end{aligned}$$

We divide both A' and B' by 3^6, which is an isomorphism of elliptic curves, to obtain more manageable parameters:

$$\begin{aligned} A' &= \frac{A'}{3^6} = 1250 = 2 \cdot 5^4 \\ B' &= \frac{B'}{3^6} = -280 = -2^3 \cdot 5 \cdot 7. \end{aligned}$$

2. We work in the extension $L = \mathbb{Q}\left(\sqrt{A'}\right) = \mathbb{Q}(\sqrt{2})$. L has the ring of integers $\mathcal{O}_L(\sqrt{2})$, which has class number 1 and unit group

$$\mathcal{O}_L^\times = \{\pm 1\} \times \langle 1 + \sqrt{2} \rangle.$$

The fundamental unit $1 + \sqrt{2}$ has norm -1.

3. As observed in Example 4.6, the bad primes are 2 and 7. Since we are dealing with a 3-isogeny, we add 3 to the set of bad primes and analyze the splitting behavior of these primes in $\mathcal{O}_L$:

$$\begin{aligned}
&X^2 - 2 \equiv X^2 \mod 2 \\
\implies &2\mathcal{O}_L = (2, \sqrt{2})^2 = (\sqrt{2})^2 \text{ (ramified)} \\
&X^2 - 2 \equiv X^2 + 1 \mod 3 \\
\implies &3\mathcal{O}_L = 3\mathcal{O}_L \text{ (inert)} \\
&X^2 - 2 \equiv (X + 3)(X - 3) \mod 7 \\
\implies &7\mathcal{O}_L = (7, \sqrt{2} + 3)(7, \sqrt{2} - 3) = (\sqrt{2} + 3)(\sqrt{2} - 3) \text{ (split)}
\end{aligned}$$

4. The building blocks of the group $L(S_{E_{448},\psi}, 3)^*$ are the primes above 7 and the fundamental unit:

$$L(S_{E_{448},\psi}, 3)^* = \{(\sqrt{2}+1)^k, (\sqrt{2}+3)(\sqrt{2}-3)^2(\sqrt{2}+1)^k, (\sqrt{2}+3)^2(\sqrt{2}-3)(\sqrt{2}+1)^k\}.$$

Again, k ranges over the values 0, 1, and 2.

5. Checking the homogeneous spaces for local triviality, by running Listing A.3, shows that all elements of $L(S_{E_{448},\psi}, 3)^*$ are mapped to homogeneous spaces that have points everywhere locally:

$$\mathrm{Sel}^{(\psi)}(E_{448}/\mathbb{Q}) = L(S_{E_{448},\psi}, 3)^*.$$

Since $E_{448}(\mathbb{Q})$ has rank zero and $E[\hat{\psi}]$ does not have non-trivial rational points, the homogeneous spaces coming from $\mathrm{Sel}^{(\psi)}(E_{448}/Q)$ are non-trivial in $Ш(E_{448}/\mathbb{Q})[3]$. The most manageable equation comes from

$$1 + \sqrt{2} = 1 + \frac{1}{25}\sqrt{A'} = 1 + \frac{1}{25}\sqrt{1250}.$$

In order to make both coefficients integral while remaining in the same class of $L^\times/{L^\times}^3$, we multiply this element by 5^3 to obtain $125 + 5\sqrt{1250}$.

Substituting the values of u, v, A', B' and s yields the homogeneous space

$$C_{1+\sqrt{2}} : 375w^2z + 156250z^3 + 5w^3 + 18750wz^2 - 280 = 1250z^2 - w^2.$$

Since this is a non-trivial element of a Tate-Shafarevich group, it has points in every completion of $\mathbb{Q}$, but not in $\mathbb{Q}$ itself. $C_{1+\sqrt{2}}$ has order 3 in $Ш(E_{448}/\mathbb{Q})$. Its inverse in $Ш(E_{448}/\mathbb{Q})$ can be obtained from the inverse of $1 + \sqrt{2}$ in $L^\times/{L^\times}^3$, which is

$$(1 + \sqrt{2})^2 = 2 + 3\sqrt{2} = 2 + \frac{3}{25}\sqrt{1250}.$$

Thus the homogeneous space is given by

$$\left(C_{1+\sqrt{2}}\right)^{-1} = C_{2+3\sqrt{2}} : 750w^2z + 312500z^3 + 15w^3 + 56250wz^2 - 280 = w^2 - 1250z^2.$$

This curve violates the local-global principle as well. The same curve (with a change of coordinates) can be obtained from $-1 + \sqrt{2}$, the mulitplicative inverse of $1 + \sqrt{2}$.

Since the verification of $\mathrm{Sel}^{(\hat{\psi})}(\bar{E}_{448}/\mathbb{Q}) = \{1\}$ does not provide any useful information, we omit it here.

For the elliptic curves E_{1100} and E_{448}, it is useful to be able to apply multiple types of descent; if Tate-Shafarevich elements of order n show up, then it is difficult to decide whether these are actually Tate-Shafarevich elements, since they could also come from rational points that we have not found yet. In such cases, m-descent could result in an exact computation of the rank. Even with the tools acquired in Chapter 4 and Chapter 5, we cannot compute the rank of an elliptic curve if its Tate-Shafarevich group has elements of order 2 and elements of order 3.

If Conjecture 3.17 is true, then it always possible to find such m. Nevertheless, as far as known it is still possible that an elliptic curve has a *divisible* Tate-Shafarevich group, meaning that $m Ш(E/\mathbb{Q}) = Ш(E/\mathbb{Q})$ for every $m \in \mathbb{Z}\backslash\{0\}$. For instance, we could have $Ш(E/\mathbb{Q}) \cong \mathbb{Q}/\mathbb{Z} \times \mathbb{Q}/\mathbb{Z}$. The rank of such an elliptic curve would not be computable by means of our descent methods.

6 Constructing Tate-Shafarevich elements of order 3

Thus far, we have seen some examples of non-trivial elements of Tate-Shafarevich groups. In this chapter, a method of constructing elements of order 3 is presented. We construct a family of elliptic curves E_h which have both a 2-isogeny and a 3-isogeny. We show via 2-descent that these elliptic curves have rank zero. Then the existence of elements of $\mathrm{Sel}^{(\psi)}(E/\mathbb{Q})$ follows from the a theorem of J.W.S. Cassels. Since these elements cannot come from rational points, this construction provides Tate-Shafarevich elements of order 3.

6.1 A useful theorem

Before we can state the theorem of Cassels, we need a few definitions.

Definition 6.1. Let $E/\mathbb{Q}$ be an elliptic curve, defined by a Weierstrass Normal Form in the variables x and y. Assume that the Weierstrass Normal Form is globally minimal, meaning that it is minimal at each prime. Then the *invariant differential* is defined as follows:

$$\omega_E := \frac{dx}{2y}.$$

The *real period* is defined as the integral of the invariant differential:

$$\Omega_E := \int_{E(\mathbb{R})} \omega_E,$$

where the direction of integration is chosen for Ω_E to be positive.

If the 2-torsion of E is not totally real, then $E(\mathbb{R})$ is connected and the real period Ω_E equals the real component of the period lattice of E (see [Sil86], chapter VI). If the 2-torsion is totally real, then $E(\mathbb{R})$ has two components and the real period Ω_E equals twice the real component of the period lattice ([Sil86], C.16.4).

Definition 6.2. Let $E/\mathbb{Q}$ be an elliptic curve and let $p \in \mathbb{Z}$ be prime. We define the group of points of good reduction:

$$E_0(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) \mid \tilde{P} \in E_{ns}(\mathbb{F}_p)\}.$$

Then the *Tamagawa number* of E at p is defined as

$$c_{E,p} := \#\left(E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)\right).$$

Note that the Tamagawa number of E equals 1 at all primes of good reduction, so there are only finitely many to be computed.

We can now state the helpful theorem.

Theorem 6.3. *Let $\psi : E/\mathbb{Q} \to \bar{E}/\mathbb{Q}$ be a rational isogeny and let $\hat{\psi} : \bar{E}/\mathbb{Q} \to E/\mathbb{Q}$ be its dual. Then the following relation between the corresponding Selmer groups holds ([Cas65], Theorem 1.1):*

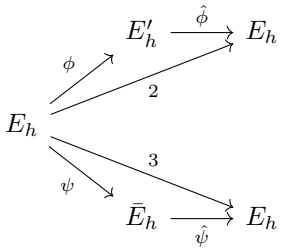
$$\frac{\#\,\mathrm{Sel}^{(\hat{\psi})}(\bar{E}/\mathbb{Q})}{\#\,\mathrm{Sel}^{(\psi)}(E/\mathbb{Q})} = \frac{\#\bar{E}(\mathbb{Q})[\hat{\psi}]\Omega_E \prod_p c_{E,p}}{\#E(\mathbb{Q})[\psi]\Omega_{\bar{E}} \prod_p c_{\bar{E},p}}.$$

By fine-tuning the real period and the Tamagawa numbers of our family of elliptic curves, the Selmer group can be forced to contain elements.

6.2 A family of elliptic curves

The elliptic curves E_h that we construct have both a rational 2-isogeny and a rational 3-isogeny, such that we can apply both types of descent. A quicker way of stating this condition is to say that E_h has a rational 6-isogeny; a subgroup of order 6 is realized as the product of the kernels of

our isogenies. Dividing out this subgroup is a rational 6-isogeny. The situation is summarized in this commutative diagram:



Constructing elliptic curves E_h with a rational 6-isogeny can be done by forcing a rational 2-torsion point upon an elliptic curve of the form (5.3). Otherwise, we could deal with curves of the form (5.1), where C is a cube, but these curves are less interesting. We start out with the equation

$$y^2 = x^3 + A(x-B)^2.$$

A rational 2-torsion point on this curve is a root of $x^3 + A(x-B)^2$. Suppose we want the torsion point to have x-coordinate $c \in \mathbb{Z}$. This gives a restriction on A and B:

$$\begin{aligned} c^3 + A(c-B)^2 &= 0 \\ \implies A &= -\frac{c^3}{(B-c)^2}. \end{aligned}$$

Multiplying through by the denominator and rescaling yields

$$E_{b,c} : y^2 = x^3 - c^3\left(x - B(B-c)^2\right)^2$$

The rescaling also moves the 2-torsion point to $x = c(B-c)^2$. The squarefree part of $-c^3$ determines the extension in which $E[\psi]$ lies. We replace B by the parameter $h \in \mathbb{Z}$. Then the discriminant of E_h is given by

$$\Delta_{E_h} = -16c^6h^3(3h-c)^2(3h-4c)(h-c)^6.$$

Thus any bad prime of E_h is either 2 or a divisor of c, h, $3h-c$, $3h-4c$ or $h-c$. In order to maintain some control over the local computations, we can require all these factors to be plus or minus a prime number. However, if c and h are odd, then h and $h-c$ cannot both be prime. Therefore we let c be ± 2 times a prime number. Since it is convenient that $\bar{E}[\hat{\psi}]$ lies in the extension $\mathbb{Q}(\sqrt{2})$, we let c be 6. This results in a general equation for E_h:

$$E_h : y^2 = x^3 - 216\left(x - h(h-6)^2\right)^2. \tag{6.1}$$

For descent by 2-isogeny, it is more convenient to move the 2-torsion point to $(0,0)$. This yields a different, but equivalent definition:

$$E_h : y^2 = x^3 + \left(18(h-6)^2\right)x^2 + 108(h-2)(h-6)^3x. \tag{6.2}$$

In this definition, h, $h-2$, $h-6$ and $h-8$ are all prime numbers. Note that this is only possible if $h \equiv 1 \mod 3$ and $h \equiv 4 \mod 5$, implying that $h \equiv 4 \mod 15$.

The isogenous curves are given as follows:

$$E'_h : Y^2 = X^3 + \left(432 - 36(h-6)^2\right)X^2 - 108h^3(h-8)X \tag{6.3}$$

$$\bar{E}_h : \eta^2 = \xi^3 + 5832\left(\xi - 27(h-2)^2(h-8)\right)^2. \tag{6.4}$$

All three curves have the same set of bad primes, but the multiplicity differs:

$$\begin{aligned} \Delta_{E_h} &= -16 \cdot 6^6h^3(3h-6)^2(3h-4\cdot 6)(h-6)^6 \\ &= -1259712h^3(h-2)^2(h-6)^6(h-8) \\ &= -2^{10}\cdot 3^9h^3(h-2)^2(h-6)^6(h-8) \\ \Delta_{E'_h} &= 2^{14}\cdot 3^9h^6(h-2)(h-6)^3(h-8)^2 \\ \Delta_{\bar{E}_h} &= -2^{10}\cdot 3^{27}h(h-2)^6(h-6)^2(h-8)^3. \end{aligned} \tag{6.5}$$

The notation E^*_h abbreviates all three isogenous curves E_h, E'_h and $\bar{E}_h$.

6.3 Torsion

It is predominantly important that we find out how many rational points of order 2 and 3 lie on E_h, because these will show up in $E_h(\mathbb{Q})/2E_h(\mathbb{Q})$ or $E_h(\mathbb{Q})/3E_h(\mathbb{Q})$.

Clearly all three curves have a non-trivial 2-torsion point. Moreover, the discriminant of

$$x^2 + \left(18(h-6)^2\right)x + 108(h-2)(h-6)^3$$

is $-108h^3(h-8)$, which is never a square. Similarly,

$$X^2 + \left(432 - 36(h-6)^2\right)X - 108h^3(h-8)$$

has discriminant $1728(h-6)^3(h-2)$. Thus E_h and E'_h only have one non-trivial 2-torsion point.

Furthermore, by our construction neither ψ nor $\hat{\psi}$ has a rational kernel. Thus all $E_h(\mathbb{Q})$ and $\bar{E}_h(\mathbb{Q})$ have trivial 3-torsion.

We can even say a little bit more about the torsion by reducing modulo 5.

Theorem 6.4. *Let E_h be given by (6.1), E'_h by (6.3) and $\bar{E}_h$ by (6.4), with h, $h-2$, $h-6$ and $h-8$ prime numbers. Then all three curves have a torsion subgroup over $\mathbb{Q}$ that is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.*

Proof. Observe that 5 cannot be one of the primes of bad reduction. This implies that reduction from $E^*_{h,tors}(\mathbb{Q})$ to $E(\mathbb{F}_5)$ is injective ([Sil86], VII.3.1).

Reducing equation (6.1) modulo 5 and using $h \equiv -1 \mod 5$ gives

$$\begin{aligned} E_h/\mathbb{F}_5 : y^2 &= x^3 - 1\left(x - (-1)(-1-1)^2\right)^2 \\ &= x^3 - (x-1)^2. \end{aligned}$$

One straightforwardly computes

$$E_h(\mathbb{F}_5) = \{O, (1,1), (1,4), (4,0), (5,2), (5,3)\}.$$

Since $E_{h,\text{tors}}(\mathbb{Q})$ can be injected into a group of order 6, but does not contain non-trivial 3-torsion points, it must be that

$$E_{h,\text{tors}}(\mathbb{Q}) = \left\{O, \left(6(h-6)^2, 0\right)\right\}.$$

Similarly, reducing equation (6.3) modulo 5 yields

$$\begin{aligned} E'_h/\mathbb{F}_5 : Y^2 &= X^3 + \left(2 - 1(4-1)^2\right)X^2 - 3\cdot 4^3(4-3)X \\ &= X^3 + 3X^2 + 3. \end{aligned}$$

In this case, we have

$$E'_h(\mathbb{F}_5) = \{O, (0,0), (2,1), (2,4), (4,2), (4,3)\}.$$

E'_h cannot have a point of order 3, for $\hat{\phi}$ would map this point to a point of order 3 on E_h, but such a point doesn't exist. We conclude

$$E'_{h,\text{tors}}(\mathbb{Q}) = \{O, (0,0)\}.$$

Finally, reducing equation (6.4) modulo 5 yields

$$\begin{aligned} \bar{E}_h/\mathbb{F}_5 : \eta^2 &= \xi^3 + 2\left(\xi - 2(4-3)(4-2)^2\right)^2 \\ &= \xi^3 + 2(\xi+2)^2 \\ \bar{E}_h(\mathbb{F}_5) &= \{O, (1,2), (1,3), (2,0), (4,1), (4,4)\}. \end{aligned}$$

Again, since $\bar{E}(\mathbb{Q})$ does not have non-trivial 3-torsion points, this implies that

$$\bar{E}_{h,\text{tors}}(\mathbb{Q}) = \left\{O, \left(-162(h-2)^2, 0\right)\right\}.$$

□

All the curves have a 3-torsion point over $\mathbb{F}_5$, which is just because -6 is a square in $\mathbb{F}_5$, so the kernel of $\hat{\psi}$ lies in $\mathbb{F}_5$. This results in a 3-torsion point on all three curves.

6.4 Local properties

By demanding that all factors occuring in the discriminant of E_h are prime numbers, the set of bad primes is $\{2, 3, h-8, h-6, h-2, h\}$. We determine the reduction type at these primes, which allows us to compute the Tamagawa numbers.

Since a rational isogeny sends nonsingular points to nonsingular points, it preserves good reduction. Moreover, it sends cusps to cusps, thereby preserving additive reduction. Finally, since it sends rational tangents to rational tangents, thereby preserving split multiplicative reduction. An isogeny always comes with a dual isogeny, so the preservation works both ways. This observation reduces the amount of work that needs to be done.

The following lemma will be useful when determining whether some tangents are defined over finite fields.

Lemma 6.5. *Let $p \neq 2, 3$ be a prime number. Then the following equivalences hold:*

$$\left(\frac{2}{p}\right) = 1 \iff p \equiv \pm 1 \mod 8$$
$$\left(\frac{-3}{p}\right) = 1 \iff p \equiv 1 \mod 3$$

Proof. For the first equivalence, let $\beta^2 = 2 \in \mathbb{F}_p$. We show that β lies in $\mathbb{F}_p$ if and only if $p \equiv \pm 1 \mod 8$. Let α be a primitive eighth root of unity. Then we write $\pm\beta = \alpha + \alpha^7 = \alpha - \alpha^3$. Now β lies in $\mathbb{F}_p$ if and only if it is fixed by the Frobenius automorphism:

$$(\pm\beta)^p = \left(\alpha + \alpha^7\right)^p = \alpha^p + \alpha^{7p} = \alpha^p + \alpha^{-p}.$$

This equals $\pm\beta$ if and only if $p \equiv \pm 1 \mod 8$.

The second equivalence is more straightforward. $\mathbb{F}_p$ contains a square root of -3 if and only if it contains the third roots of unity, which happens precisely if the order of the multiplicative group $\mathbb{F}_p^\times$ is divisible by 3. □

Lemma 6.6. *The reduction of E_h^* at h is multiplicative. It is split multiplicative if and only if $h \equiv \pm 1 \mod 8$.*

Proof. Reducing the equation (6.3) to one over $\mathbb{F}_h$ yields

$$\begin{aligned} E_h'/\mathbb{F}_h : Y^2 &= X^3 + \left(432 - 36(-6)^2\right) X^2 \\ &= X^2(X - 864). \end{aligned}$$

This means the reduction is multiplicative ($c_4 = -864$). The reduction at h is split multiplicative if and only if $-864 = -2^5 \cdot 3^3$ is a square modulo h, whence -6 is a square modulo h. Since $h \equiv 1 \mod 3$ followed from the assumption that $h - 2$ is prime, we obtain

$$\left(\frac{-6}{h}\right) = \left(\frac{-3}{h}\right)\left(\frac{2}{h}\right) = \left(\frac{2}{h}\right).$$

Thus the reduction is split multiplicative if and only if $h \equiv \pm 1 \mod 8$. □

Lemma 6.7. *The reduction of E_h^* at $h - 2$ is multiplicative. It is split multiplicative if and only if $h \equiv 1 \mod 8$ or $h \equiv 3 \mod 8$*

Proof. Reducing the equation (6.2) to one over $\mathbb{F}_{h-2}$ yields

$$\begin{aligned} E_h/\mathbb{F}_{h-2} : y^2 &= x^3 + \left(18(-4)^2 - 216\right) x^2 \\ &= x^2(x + 72). \end{aligned}$$

The reduction is split multiplicative if and only if $72 = 2^3 \cdot 3^2$ is a square, which happens when $h - 2 \equiv \pm 1 \mod 8$. □

Lemma 6.8. *The reduction of E_h^* at $h - 6$ is multiplicative. It is split multiplicative if and only if $h \equiv 5 \mod 8$ or $h \equiv 7 \mod 8$.*

Proof. Reducing the equation (6.2) to one over $\mathbb{F}_{h-6}$ yields

$$\begin{aligned} E_h/\mathbb{F}_{h-6} : y^2 &= x^3 + (0 - 216)\, x^2 \\ &= x^2(x - 216). \end{aligned}$$

The reduction is split multiplicative if and only if $-216 = -2^3 \cdot 3^3$ is a square. By assumption, $h - 6 \equiv 1 \mod 3$, so -6 is a square if and only if 2 is:

$$\left(\frac{-6}{h-6}\right) = \left(\frac{-3}{h-6}\right)\left(\frac{2}{h-6}\right) = \left(\frac{2}{h-6}\right).$$

This is a square if and only if $h - 6 \equiv \pm 1 \mod 8$. □

Lemma 6.9. *The reduction of E_h^* at $h - 8$ is multiplicative. It is split multiplicative if and only if $h \equiv \pm 1 \mod 8$.*

Proof. Reducing the equation (6.3) to one over $\mathbb{F}_{h-8}$ yields

$$\begin{aligned} E_h'/\mathbb{F}_{h-8} : Y^2 &= X^3 + \left(432 - 36(2)^2\right) X^2 \\ &= X^2(X + 288). \end{aligned}$$

The reduction is split multiplicative if $288 = 2^5 \cdot 3^2$ is a square, which happens if and only if $h - 8 \equiv \pm 1 \mod 8$. □

The reduction types at 2 and 3 are a bit more difficult.

Lemma 6.10. *The reduction of E_h^* at 2 is additive. E_h and $\bar{E}_h$ have reduction type I_0^*, E_h' has reduction type I_4^*. In any case, $c_{E_h^*,2} = 2$.*

Proof. Reducing modulo 2 immediately makes it visible that the reduction is additive. We have to distinguish between several types of additive reduction, with varying Tamagawa numbers.

We use J.T. Tate's algorithm ([Tat75]). When applied to the curve E_h with $p = 2$, the algorithm halts at the sixth step: the polynomial

$$P(T) = T^3 + a_{2,1}T^2 + a_{4,2}T + a_{6,3} \equiv T^3 + T^2 + T$$

has distinct roots, of which one lies in the residue field $\mathbb{F}_2$. This implies that the reduction type is I_0^* and $c_{E_h,2} = 2$. Since ψ has degree 3, it preserves the reduction type at 2 ([DD15]). Hence the reduction of $\bar{E}_h$ is also I_0^*. E_h' requires special attention. In this case, the polynomial becomes $P(T) = T^3 + T^2$, which has a double root and a simple root. The subalgorithm of the seventh step is repeated (four times) until $P(T)$ has distinct roots, of which exactly one lies in $\mathbb{F}_2$. We get reduction type I_4^* with $c_{E_h',2} = 2$. □

Lemma 6.11. *The reduction of E_h^* at 3 is additive. E_h and E_h' have reduction type III^*, $\bar{E}_h$ has reduction type III. In any case $c_{E_h^*,3} = 2$.*

Proof. We apply Tate's algorithm to E_h. The polynomial $P(T) = T^3$ has a triple root. Then the polynomial

$$Y^2 + a_{3,2}Y - a_{6,4} \equiv Y^2$$

has a double root. The algorithm halts at the ninth step, since a_4 is not divisible by 3^4. This results in reduction type III^*. This reduction type is preserved by ϕ, so E_h' will also have reduction type III^*. In order to find the reduction of $\bar{E}_h$ at 3, we first make its defining equation minimal at 3 by dividing by 3^{12} and rescaling. This results in the equation

$$\bar{E}_h : \eta^2 = \xi^3 + 8\left(3\xi - (h-8)(h-2)^2\right)^2 \tag{6.6}$$

Then Tate's algorithm halts at the fourth step already, since 3^3 does not divide

$$b_8 = 4a_2a_6 - a_4^2 = 4 \cdot 72 \cdot 8(h-8)^2(h-2)^4 - 144(h-8)(h-2)^2 \equiv 3^2(1+1).$$

This yields the reduction type III. □

	$h \equiv 1 \mod 8$	$h \equiv 3 \mod 8$	$h \equiv 5 \mod 8$	$h \equiv 7 \mod 8$
$p = 2$	Additive	Additive	Additive	Additive
$p = 3$	Additive	Additive	Additive	Additive
$p = h - 8$	Split mult.	Non-split mult.	Non-split mult.	Split mult.
$p = h - 6$	Non-split mult.	Non-split mult.	Split mult.	Split mult.
$p = h - 2$	Split mult.	Split mult.	Non-split mult.	Non-split mult.
$p = h$	Split mult.	Non-split mult.	Non-split mult.	Split mult.
$\prod_p c_{E_h,p}$	48	16	48	144
$\prod_p c_{E'_h,p}$	48	16	48	144
$\prod_p c_{\bar{E}_h,p}$	144	48	16	48

Table 6.1: A table representing the local properties of E_h^*.

Computing the Tamagawa numbers goes as follows: if the reduction is split multiplicative, the Tamagawa number equals the exponent of the prime in the discriminant. If the reduction is non-split multiplicative, then the Tamagawa number is either 1, if the exponent in the discriminant is odd, or 2, if the exponent in the discriminant is even. The local properties at all bad primes of E_h^* are summarized in Table 6.4.

In view of Theorem 6.3, we want $\prod_p c_{\bar{E}_h,p} > \prod_p c_{E_h,p}$ in order to force elements into the Selmer group $\mathrm{Sel}^{(\psi)}(E_h/\mathbb{Q})$. Then the suitable residues are $h \equiv 1 \mod 8$ and $h \equiv 3 \mod 8$. However $h \equiv 3 \mod 8$ is more attractive; this case gives smaller factor groups $E_h(\mathbb{Q}_p)/E_{h,0}(\mathbb{Q}_p)$, which makes 2-descent more feasible.

From now on, we assume $h \equiv 3 \mod 8$. Recall that $h \equiv 4 \mod 15$ follows from the assumption that h, $h-2$, $h-6$ and $h-8$ are prime. Applying the Chinese Remainder Theorem gives

$$h \equiv 19 \mod 120.$$

6.5 2-descent

Using the rational isogeny ϕ of degree 2, we show that

$$E'_h(\mathbb{Q})/\phi(E_h(\mathbb{Q})) = \{O, (0,0)\}$$
$$E_h(\mathbb{Q})/\hat{\phi}(E'_h(\mathbb{Q})) = \{O, (0,0)\}.$$

This means that all curves E_h^* have rank zero. In order to distinguish between 2-descent and 3-descent, and to accord with the notation of [ST92], we introduce α for the connecting homomorphism of ϕ and δ for the connecting homomorphism of ψ.

Lemma 6.12. *Let h, $h-2$, $h-6$ and $h-8$ be prime numbers and assume $h \equiv 3 \mod 8$. Then ϕ-descent yields*

$$\mathrm{Sel}^{(\phi)}(E_h/\mathbb{Q}) = \{1, -3h(h-8)\}$$
$$\implies E'_h(\mathbb{Q})/\phi(E_h(\mathbb{Q})) = \{O, (0,0)\}.$$

Proof. We apply Lemma 4.1 and Lemma 4.2 with the parameters

$$a' = 432 - 36(h-6)^2$$
$$b' = -108h^3(h-8)$$

We determine the image of

$$\alpha : E'_h(\mathbb{Q})/\phi(E_h(\mathbb{Q})) \to \mathbb{Q}^\times/{\mathbb{Q}^\times}^2.$$

First of all, $E'_h(\mathbb{Q})/\phi(E(\mathbb{Q}))$ contains the point $(0,0)$. By Lemma 4.1, α maps this point to

$$-108h^3(h-8) \equiv -3h(h-8) \in \mathbb{Q}^\times/{\mathbb{Q}^\times}^2,$$

making the inclusion "$\supseteq$" clear.

In order to show the other inclusion, we bound $\mathrm{im}(\alpha)$ from above by computing local images. First, by Theorem 3.15, the image of α is ramified only at 2, ∞ and the primes of bad reduction, resulting in the bound

$$\mathrm{im}(\alpha) \subseteq \langle -1, 2, 3, h-8, h-6, h-2, h \rangle.$$

Recall from Lemma 4.2 that $d \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ lies in the image of α if and only if the homogeneous space

$$C_d : w^2 = d + a'd^2z^2 + b'd^3z^4$$

has a rational point. We show that d must divide b'. Let the variable r homogenize the equation:

$$C_d : w^2 = dr^4 + a'd^2z^2r^2 + b'd^3z^4.$$

By rescaling if necessary, we may assume that w, z and r are integers with $\gcd(w, z, r) = 1$. Since d represents a class of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, we can restrict to the case where d is a squarefree integer. Clearly d divides the right-hand side. Therefore d divides the left-hand side w^2. Since d is squarefree, this implies that d divides w. Then a similar argument provides that d^2 divides dr^4 and hence $d|r$. Finally, every term except $b'd^3z^4$ is divisible by d^4, so this term must be divisible by d^4 as well. But $\gcd(d, z) = 1$, since d already divides w and r. Thus it must be that b' is divisible by d. This gives the bound

$$\mathrm{im}(\alpha) \subseteq \langle -1, 2, 3, h-8, h\rangle.$$

In order to compute the ϕ-Selmer group, we compute the images of the local maps α_p, defined by the diagram

$$\begin{array}{ccc} E'_h(\mathbb{Q})/\phi(E_h(\mathbb{Q})) & \xrightarrow{\alpha} & \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \\ \downarrow & & \downarrow \\ E'_h(\mathbb{Q}_p)/\phi(E_h(\mathbb{Q}_p)) & \xrightarrow[\alpha_p]{} & \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}. \end{array}$$

The Selmer group $\mathrm{Sel}^{(\phi)}(E/\mathbb{Q})$ is the subgroup of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ that reduces to an element of the image of α_p for every p.

We start with $p = 2$. The local homomorphism is given by

$$\begin{aligned} \alpha_2 : E'_h(\mathbb{Q}_2)/\phi(E_h(\mathbb{Q}_2)) &\to \mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2} = \langle 2, -1, 5\rangle \\ (X, Y) &\mapsto X \cdot \mathbb{Q}_2^{\times 2} \\ (0, 0) &\mapsto b' \cdot \mathbb{Q}_2^{\times 2} = -3h(h-8) \cdot \mathbb{Q}_2^{\times 2} = 5 \cdot \mathbb{Q}_2^{\times 2} \\ O &\mapsto 1 \cdot \mathbb{Q}_2^{\times 2}. \end{aligned}$$

It follows from Lemma 6.10 that

$$E'_h(\mathbb{Q}_2)/E'_{h,0}(\mathbb{Q}_2) = \{O, (0, 0)\}.$$

Hence any point $P \in E'_h(\mathbb{Q}_2)$ can be written as $k(0, 0) + Q$, where $k \in \{0, 1\}$ and Q has good reduction. Moreover, observe that

$$E'_{h,ns}(\mathbb{F}_2) = \{O, (1, 1)\},$$

so Q reduces to O or to $(1, 1)$. Since the reduction is surjective (by Hensel's Lemma), some point $R \in E'_{h,0}(\mathbb{Q}_2)$ reduces to $(1, 1)$. Now, suppose $Q = (X : Y : Z)$ reduces to $(1, 1)$. Then Q corresponds to a solution

$$Y^2Z = X^3 + a'X^2Z + b'XZ^2$$

with X, Y and Z odd integers. Reducing modulo 8 yields

$$Z \equiv X + a'Z + b'X \mod 8 = X \mod 8,$$

since a' and b' are both divisible by 4, but not by 8. We obtain

$$\begin{aligned} \alpha_2(Q) = \alpha_2\left(\left(\frac{X}{Z} : \frac{Y}{Z} : 1\right)\right) &= 1 \cdot \mathbb{Q}_2^{\times 2} \\ \implies \alpha_2(P) = \alpha_2((0, 0))^k\alpha_2(Q) &= 5^k \in \langle 5\rangle. \end{aligned}$$

On the other hand, suppose Q reduces to O. Then write $Q = (Q - R) + R$. $Q - R$ and R both reduce to $(1, 1)$. We obtain

$$\alpha_2(P) = \alpha_2((0, 0))^k\alpha_2(Q - R)\alpha_2(R) \in \langle 5\rangle.$$

Thus every element of $\mathrm{im}(\alpha)$ is $1 \mod 4$:

$$\mathrm{im}(\alpha) \subseteq \langle -3, -h, -(h-8) \rangle.$$

Next, we consider $p = 3$, with the local homomorphism

$$\begin{aligned} \alpha_3 : E'_h(\mathbb{Q}_3)/\phi(E_h(\mathbb{Q}_3)) &\to \mathbb{Q}_3^\times/{\mathbb{Q}_3^\times}^2 = \langle 3, 2 \rangle \\ (X, Y) &\mapsto X \cdot {\mathbb{Q}_3^\times}^2 \\ (0,0) &\mapsto b' \cdot {\mathbb{Q}_3^\times}^2 = -3h(h-8) \cdot {\mathbb{Q}_3^\times}^2 = 3 \cdot 2 \cdot {\mathbb{Q}_3^\times}^2 \\ O &\mapsto 1 \cdot {\mathbb{Q}_3^\times}^2. \end{aligned}$$

Since

$$E'_h(\mathbb{Q}_3)/E'_{h,0}(\mathbb{Q}_3) = \{O, (0,0)\},$$

we can write any point $P \in E'_h(\mathbb{Q}_3)$ as $P = k(0,0) + Q$, where $k \in \{0, 1\}$ and Q has good reduction. Observe that

$$E'_{h,ns}(\mathbb{F}_2) = \{O, (1,1), (1,2)\}$$

and let $R \in E'_{h,0}(\mathbb{Q}_3)$ reduce to $(1,1)$. Then either Q, $Q - 2R$ or $Q + 2R$ reduces to $(1,1)$, so we write $P = k(0,0) + (Q - 2lR) + 2lR$, where $l \in \{0, 1, 2\}$ and $Q - 2lR$ reduces to $(1,1)$ Furthermore, R is a point $(X : Y : Z)$ with $X, Y, Z \equiv 1 \mod 3$. Thus we compute

$$\begin{aligned} \alpha_3(R) = \alpha_3\left(\left(\frac{X}{Z} : \frac{Y}{Z} : 1\right)\right) &= 1 \cdot {\mathbb{Q}_3^\times}^2 \\ \implies \alpha_3(P) = \alpha_3((0,0))^k \alpha_3(Q - 2lR)\alpha_3(R)^{2l} &= 3^k \cdot 2^k \cdot 1 \in \langle 3 \cdot 2 \rangle. \end{aligned}$$

Thus every element in the image of α must reduce to the subgroup $\langle 6 \rangle$ of $\mathbb{Q}_3^\times/{\mathbb{Q}_3^\times}^2$. This gives the restriction

$$\mathrm{im}(\alpha) \subseteq \langle 3h, -(h-8) \rangle.$$

Finally, we consider $p = h - 2$. The local homomorphism is given by

$$\begin{aligned} \alpha_3 : E'_h(\mathbb{Q}_{h-2})/\phi(E_h(\mathbb{Q}_3)) &\to \mathbb{Q}_{h-2}^\times/{\mathbb{Q}_{h-2}^\times}^2 = \langle h-2, -3 \rangle \\ (X, Y) &\mapsto X \cdot {\mathbb{Q}_{h-2}^\times}^2 \\ (0,0) &\mapsto b' \cdot {\mathbb{Q}_{h-2}^\times}^2 = -3h(h-8) \cdot {\mathbb{Q}_{h-2}^\times}^2 = 36 \cdot {\mathbb{Q}_{h-2}^\times}^2 = 1 \cdot {\mathbb{Q}_{h-2}^\times}^2 \\ O &\mapsto 1 \cdot {\mathbb{Q}_{h-2}^\times}^2. \end{aligned}$$

Note that -3 is not a square in $\mathbb{F}_{h-2}$ because $h - 2 \equiv 2 \mod 3$. Since $E_h(\mathbb{Q}_{h-2}) = E_{h,0}(\mathbb{Q}_{h-2})$, we only need to check how α_{h-2} acts on a point P of good reduction. The reduction at $h - 2$ is split multiplicative:

$$\begin{aligned} E'_h/\mathbb{F}_{h-2} : Y^2 &= X(X - 72)^2 \\ &= \bar{X}^2(\bar{X} + 72), \end{aligned}$$

where we introduce $\bar{X} = X - 72$. The tangent lines at the node, which we moved to $(0,0)$, are given by $Y = \pm\gamma\bar{X}$, with $\gamma^2 = 72$. The fact that the reduction is split multiplicative means precisely that γ is an element of $\mathbb{F}_{h-2}$. It then follows from [Sil86], III.2.5, that

$$\begin{aligned} E'_{h,ns}(\mathbb{F}_{h-2}) &\cong \mathbb{F}_{h-2}^\times \\ (X, Y) &\mapsto \frac{Y + \gamma\bar{X}}{Y - \gamma\bar{X}}. \end{aligned}$$

We wish to find an point $(X, Y) \in E'_{h,ns}(\mathbb{F}_{h-2})$ that is not a multiple of 2. We construct this point

from an element of $\mathbb{F}_{h-2}^{\times}$ that is not a square, namely -3.

$$\begin{aligned} & \frac{Y+\gamma\bar{X}}{Y-\gamma\bar{X}} = -3 \\ \implies & Y+\gamma\bar{X} = -3(Y-\gamma\bar{X}) \\ \implies & Y = \frac{\gamma\bar{X}}{2} \\ \implies & \left(\frac{\gamma\bar{X}}{2}\right)^2 = \bar{X}^2(\bar{X}+72) \\ \implies & 18 = \bar{X}+72 = X \end{aligned}$$

Let $R \in E'_{h,0}(\mathbb{Q}_{h-2})$ reduce to this point. We compute

$$\alpha_{h-2}(R) = 18 \cdot {\mathbb{Q}_{h-2}^{\times}}^2 = 2 \cdot {\mathbb{Q}_{h-2}^{\times}}^2 = 1 \cdot {\mathbb{Q}_{h-2}^{\times}}^2,$$

since $h-2 \equiv 1 \mod 8$. As $(18,*)$ is not a multiple of 2 and reduction is a homomorphism, it follows that every point reduces to a point of which the X-coordinate is a square. Thus

$$\alpha_{h-2}(E'_h(\mathbb{Q}_{h-2})) = \{1\}.$$

This finally gives the restriction that every element of $\mathrm{im}(\alpha)$ is a square mod $h-2$. We conclude that $\mathrm{im}(\alpha) = \{1, -3(h-8)\}$. From the exactness of (4.2) follows that

$$E'_h(\mathbb{Q})/\phi(E_h(\mathbb{Q})) = \{O, (0,0)\}.$$

□

Lemma 6.13. *Let h, $h-2$, $h-6$ and $h-8$ be prime numbers and assume $h \equiv 3 \mod 8$. Then $\hat{\phi}$-descent yields*

$$\begin{aligned} & \mathrm{Sel}^{(\hat{\phi})}(E'_h/\mathbb{Q}) = \{1, 3(h-2)(h-6)\} \\ \implies & E_h(\mathbb{Q})/\hat{\phi}(E'_h(\mathbb{Q})) = \{O, (0,0)\}. \end{aligned}$$

Proof. The machinery from Lemma 6.12 is used. It is convenient to use definition (6.2) of E_h. We determine the image of

$$\alpha' : E_h(\mathbb{Q})/\hat{\phi}(E(\mathbb{Q})) \to \mathbb{Q}^{\times}/{\mathbb{Q}^{\times}}^2.$$

First off, the point $(0,0)$ is mapped to the class

$$108(h-6)^3(h-2) \equiv 3(h-6)(h-2)$$

in $\mathbb{Q}^{\times}/{\mathbb{Q}^{\times}}^2$, which shows the inclusion "$\supseteq$". We now boud $\mathrm{im}(\alpha')$ from above. The image must consist of squarefree divisors of b:

$$\mathrm{im}(\alpha') \subseteq \langle -1, 2, 3, h-6, h-2 \rangle.$$

We start with $p=2$ and determine the image of the local homomorphism

$$\begin{aligned} \alpha'_2 : E_h(\mathbb{Q}_2)/\hat{\phi}(E'_h(\mathbb{Q}_2)) \to \mathbb{Q}_2^{\times}/{\mathbb{Q}_2^{\times}}^2 &= \langle 2, -1, 5 \rangle \\ (x,y) &\mapsto X \cdot {\mathbb{Q}_2^{\times}}^2 \\ (0,0) &\mapsto b' \cdot {\mathbb{Q}_2^{\times}}^2 = 3(h-6)(h-2) \cdot {\mathbb{Q}_2^{\times}}^2 = -1 \cdot {\mathbb{Q}_2^{\times}}^2 \\ O &\mapsto 1 \cdot {\mathbb{Q}_2^{\times}}^2. \end{aligned}$$

We have have

$$E_{h,ns}(\mathbb{F}_2) = \{O, (1,1)\},$$

which is generated by $(1,1)$. Let $R \in E_{h,0}(\mathbb{Q}_2)$ reduce to $(1,1)$. Then $\alpha'_2(R) \in \langle -1, 5 \rangle$. Combining this with the fact $E_h(\mathbb{Q}_2)/E_{h,0}(\mathbb{Q}_2) = \{O, (0,0)\}$ yields

$$\mathrm{im}(\alpha'_2) \subseteq \langle -1, 5 \rangle.$$

This excludes even possibilities of d:

$$\mathrm{im}(\alpha') \subseteq \langle -1, 3, h-6, h-2 \rangle.$$

A further restriction can be obtained from considering $p = 3$:

$$\begin{aligned} \alpha'_3 : E_h(\mathbb{Q}_3)/\hat{\phi}(E'_h(\mathbb{Q}_3)) &\to \mathbb{Q}_3^\times/{\mathbb{Q}_3^\times}^2 = \langle 3, 2 \rangle \\ (x, y) &\mapsto X \cdot {\mathbb{Q}_3^\times}^2 \\ (0, 0) &\mapsto b' \cdot {\mathbb{Q}_3^\times}^2 = 3(h-6)(h-2) \cdot {\mathbb{Q}_3^\times}^2 = 3 \cdot 2 \cdot {\mathbb{Q}_3^\times}^2 \\ O &\mapsto 1 \cdot {\mathbb{Q}_3^\times}^2. \end{aligned}$$

Observe that

$$E_{h,ns}(\mathbb{F}_3) = \{O, (1,1), (1,2)\},$$

which is generated by $(1, 1)$. Let $R \in E_{h,0}(\mathbb{Q}_3)$ reduce to $(1, 1)$. This entails that

$$\begin{aligned} \alpha'_3(R) &= 1 \cdot {\mathbb{Q}_3^\times}^2 \\ \implies \mathrm{im}(\alpha_3) &\subseteq \langle 3 \cdot 2 \rangle \end{aligned}$$

This provides a restriction on $\mathrm{im}(\alpha')$:

$$\mathrm{im}(\alpha') \subseteq \langle -3, h-6, -(h-2) \rangle.$$

Next, we deal with $p = h - 8$:

$$\begin{aligned} \alpha'_{h-8} : E_h(\mathbb{Q}_{h-8})/\hat{\phi}(E'_h(\mathbb{Q}_{h-8})) &\to \mathbb{Q}_{h-8}^\times/{\mathbb{Q}_{h-8}^\times}^2 = \langle h-8, 2 \rangle \\ (x, y) &\mapsto X \cdot {\mathbb{Q}_{h-8}^\times}^2 \\ (0, 0) &\mapsto b' \cdot {\mathbb{Q}_{h-8}^\times}^2 = 3(h-6)(h-2) \cdot {\mathbb{Q}_{h-8}^\times}^2 = 1 \cdot {\mathbb{Q}_{h-8}^\times}^2 \\ O &\mapsto 1 \cdot {\mathbb{Q}_{h-8}^\times}^2. \end{aligned}$$

Since $E_h(\mathbb{Q}_{h-8}) = E_{h,0}(\mathbb{Q}_{h-8})$, we check how α' acts on the points of good reduction by determining how it acts on a point of $E_h(\mathbb{F}_{h-8})$ that is not a multiple of 2. The reduction at $h - 8$ is non-split multiplicative:

$$\begin{aligned} E_h/\mathbb{F}_{h-8} : y^2 &= x(x-72)^2 \\ &= \bar{x}^2(\bar{x}+72). \end{aligned}$$

The tangent lines at the node $(\bar{x}, y) = (0, 0)$ are given by $y = \pm\gamma\bar{x}$, where $\gamma^2 = 72$. Because of the residue of $h - 8$ modulo 8, γ is not an element of $\mathbb{F}_{h-8}$ (meaning precisely that the reduction is non-split). Then we have the following isomorphism ([Sil86], Ex.3.5):

$$\begin{aligned} E_h(\mathbb{F}_{h-8}) &\cong \ker\left(N : \mathbb{F}_{(h-8)^2}^\times \to \mathbb{F}_{h-8}^\times\right) \\ (x, y) &\mapsto \frac{y + \gamma\bar{x}}{y - \gamma\bar{x}} \end{aligned}$$

The norm on $\mathbb{F}_{(h-8)^2}$ is the product of all Galois automorphisms of $F_{(h-8)^2}$, which are the identity and the Frobenius automorphism; $N(\beta) = \beta \cdot \beta^{h-8} = \beta^{h-7}$. Since the multiplicative group $\mathbb{F}_{(h-8)^2}^\times$ is cyclic, the kernel of the norm map is a cyclic group of $h - 7$ elements. A non-square element of this group is i (where $i^2 = -1$); $i^{h-7} = i^4 = 1$, so $i \in \ker(N)$, and i cannot be a square in $\ker(N)$, for this would imply that $\ker(N)$ has an element of order 8 while its order is not divisible by 8. We recover the point $(x, y) \in E_h(\mathbb{F}_{h-8})$ that is mapped to i:

$$\begin{aligned} \frac{y + \gamma\bar{x}}{y - \gamma\bar{x}} &= i \\ \implies y &= -i\gamma\bar{x} \\ \implies (-i\gamma\bar{x})^2 &= \bar{x}^2(\bar{x}+72) \\ \implies -72 &= \bar{x} + 72 = x. \end{aligned}$$

Now, observe that since $h-8 \equiv 3 \mod 8$, -72 is a square in $\mathbb{F}_{h-2}$:

$$\left(\frac{-72}{h-8}\right) = \left(\frac{-2}{h-8}\right) = \left(\frac{-1}{h-8}\right)\left(\frac{2}{h-8}\right) = (-1)\cdot(-1) = 1.$$

This means that every point on $E_{h,0}(\mathbb{Q}_{h-8})$ reduces to a point with a square as x-coordinate, giving the restriction

$$\begin{aligned} &\operatorname{im}(\alpha'_{h-8}) = \{1\} \\ \implies &\operatorname{im}(\alpha') \subseteq \langle -3(h-6), -(h-2)\rangle. \end{aligned}$$

Finally, consider $p = h$:

$$\begin{aligned} \alpha'_h : E_h(\mathbb{Q}_h)/\hat{\phi}(E'_h(\mathbb{Q}_h)) &\to \mathbb{Q}_h^\times/{\mathbb{Q}_h^\times}^2 = \langle h, 2\rangle \\ (x,y) &\mapsto X \cdot {\mathbb{Q}_h^\times}^2 \\ (0,0) &\mapsto b' \cdot {\mathbb{Q}_h^\times}^2 = 3(h-6)(h-2)\cdot {\mathbb{Q}_h^\times}^2 = 1\cdot {\mathbb{Q}_h^\times}^2 \\ O &\mapsto 1\cdot {\mathbb{Q}_h^\times}^2. \end{aligned}$$

The reduction at h is also non-split multiplicative:

$$\begin{aligned} E_h/\mathbb{F}_h : y^2 &= x(x+216)^2 \\ &= \bar{x}^2(\bar{x}-216). \end{aligned}$$

The tangent lines at the node are given by $y = \pm\gamma\bar{x}$, where $\gamma^2 = -216$. We obtain the isomorphism

$$\begin{aligned} E_h(\mathbb{F}_h) &\cong \ker\left(N : \mathbb{F}_{h^2}^\times \to \mathbb{F}_h^\times\right) \\ (x,y) &\mapsto \frac{y+\gamma\bar{x}}{y-\gamma\bar{x}}. \end{aligned}$$

The kernel of the norm map has $h+1$ elements, imlying that i is again a suitable choice for an element that is not a multiple of 2. We compute

$$\begin{aligned} &\frac{y+\gamma\bar{x}}{y-\gamma\bar{x}} = i \\ \implies &(-i\gamma\bar{x})^2 = \bar{x}^2(\bar{x}-216) \\ \implies &216 = \bar{x} - 216 = x. \end{aligned}$$

Finally, we compute the Legendre symbol

$$\left(\frac{216}{h}\right) = \left(\frac{6}{h}\right) = \left(\frac{-1}{h}\right)\left(\frac{2}{h}\right)\left(\frac{-3}{h}\right) = (-1)\cdot(-1)\cdot 1 = 1.$$

Thus we conclude

$$\begin{aligned} &\operatorname{im}(\alpha'_h) = \{1\} \\ \implies &\operatorname{im}(\alpha') \subseteq \langle 3(h-6)(h-2)\rangle. \end{aligned}$$

This finishes the proof; the $E_h(\mathbb{Q})/\hat{\phi}(E'_h(\mathbb{Q}))$ is represented only by the elements in $E_h(\mathbb{Q})[2]$. □

Theorem 6.14. *Let h, $h-2$, $h-6$ and $h-8$ be prime numbers and assume $h \equiv 3 \mod 8$. Then the elliptic curves E_h^* have rank zero over $\mathbb{Q}$.*

Proof. Consider the exact sequence

$$0 \longrightarrow \frac{E'_h(\mathbb{Q})[\hat{\phi}]}{\phi(E_h(\mathbb{Q})[2])} \longrightarrow \frac{E'_h(\mathbb{Q})}{\phi(E_h(\mathbb{Q}))} \xrightarrow{\hat{\phi}} \frac{E_h(\mathbb{Q})}{2E_h(\mathbb{Q})} \longrightarrow \frac{E_h(\mathbb{Q})}{\hat{\phi}(E'_h(\mathbb{Q})} \longrightarrow 0.$$

In Lemma 6.12 and Lemma 6.13, the groups $\frac{E'_h(\mathbb{Q})}{\phi(E_h(\mathbb{Q}))}$ and $\frac{E_h(\mathbb{Q})}{\hat{\phi}(E'_h(\mathbb{Q})}$ were computed. Furthermore, one straightforwardly computes

$$\frac{E'_h(\mathbb{Q})[\hat{\phi}]}{\phi(E_h(\mathbb{Q})[2])} = \frac{\langle(0,0)\rangle}{\{O\}} = \langle(0,0)\rangle.$$

Thus the last unknown group in the exact sequence is given by

$$\frac{E_h(\mathbb{Q})}{2E_h(\mathbb{Q})} = \{O, (0,0)\}.$$

We conclude that $E_h(\mathbb{Q})$ does not have elements of infinite order; its rank is zero.

Since isogeny preserves rank, E'_h and $\bar{E}_h$ also have rank zero. □

6.6 Real periods

Recall the useful formula in Theorem 6.3:

$$\frac{\#\text{Sel}^{(\hat{\psi})}(\bar{E}/\mathbb{Q})}{\#\text{Sel}^{(\psi)}(E/\mathbb{Q})} = \frac{\#\bar{E}(\mathbb{Q})[\hat{\psi}]\Omega_E \prod_p c_{E,p}}{\#E(\mathbb{Q})[\psi]\Omega_{\bar{E}} \prod_p c_{\bar{E},p}}.$$

Before we can conclude anything about the ratio between the sizes of the Selmer groups, we compute the ratio between the real periods.

Lemma 6.15. *Let h, $h-2$, $h-6$ and $h-8$ be prime numbers and assume $h \equiv 3 \mod 8$. Then the real periods of E and $\bar{E}$ are related:*

$$\Omega_{\bar{E}} = 3\Omega_E.$$

Proof. We use Lemma 7.4 in [DD15], with $\mathcal{K} = \mathbb{R}$:

$$\frac{\Omega_{E_h}}{\Omega_{\bar{E}_h}} = \frac{\#\ker\left(\psi : E_h(\mathbb{R}) \to \bar{E}_h(\mathbb{R})\right)}{\#\operatorname{coker}\left(\psi : E_h(\mathbb{R}) \to \bar{E}_h(\mathbb{R})\right)} \cdot \left|\frac{\omega_{E_h}}{\psi^*\omega_{\bar{E}_h}}\right|. \tag{6.7}$$

Since the degree of ψ is odd, the cokernel is trivial. We constructed ψ such that its kernel lies in $\mathbb{Q}(\sqrt{-6})$, which is a purely imaginary extension. Hence the kernel is also trivial.

Note that we should use the minimal equation (6.6) for $\bar{E}_h$:

$$\eta^2 = \xi^3 + 8\left(3\xi - (h-8)(h-2)^2\right)^2.$$

Then ψ is given by

$$\begin{aligned}\psi : E_h &\to \bar{E}_h \\ (x,y) &\mapsto \left(3^{-4} \cdot \frac{3(6y^2 + 6AB^2 - 3x^3 - 2Ax^2)}{x^2},\ 3^{-6} \cdot \frac{27y(8AB^2 - x^3 - 4ABx)}{x^3}\right).\end{aligned}$$

It is not necessary to substitute values of A and B. Using this, we compute the pullback of $\omega_{\bar{E}_h}$ under ψ:

$$\begin{aligned}\psi^*\omega_{\bar{E}_h} &= \psi^*\left(\frac{d\xi}{2\eta}\right) \\ &= \frac{d\left(3^{-3}(6y^2 + 6AB^2 - 3x^3 - 2Ax^2)x^{-2}\right)}{2 \cdot 3^{-3}(8AB^2 - x^3 - 4ABx)x^{-3}} \\ &= \frac{x^3 d\left((6\left(x^3 + A(x-B)^2\right) + 6AB^2 - 3x^3 - 2Ax^2)x^{-2}\right)}{2(8AB^2 - x^3 - 4ABx)} \\ &= \frac{x^3 d(3x + 4A - 12ABx^{-1} + 12AB^2x^{-2})}{2(8AB^2 - x^3 - 4ABx)} \\ &= \frac{x^3(3 + 12ABx^{-2} - 24AB^2x^{-3})dx}{2(8AB^2 - x^3 - 4ABx)} \\ &= \frac{-3dx}{2y} = -3\omega_{E_h}.\end{aligned}$$

Substituting this into (6.7) yields

$$\frac{\Omega_{E_h}}{\Omega_{\bar{E}_h}} = \frac{\#\ker\left(\psi : E_h(\mathbb{R}) \to \bar{E}_h(\mathbb{R})\right)}{\#\operatorname{coker}\left(\psi : E_h(\mathbb{R}) \to \bar{E}_h(\mathbb{R})\right)} \cdot \left|\frac{\omega_{E_h}}{\psi^*\omega_{\bar{E}_h}}\right| = \frac{1}{1} \cdot \left|\frac{-1}{3}\right| = \frac{1}{3}.$$

□

We have now gathered sufficient information about the elliptic curves E_h to make use of Theorem 6.3.

Theorem 6.16. *Let h, $h-2$, $h-6$ and $h-8$ be prime numbers and assume $h \equiv 3 \mod 8$. Then $\mathrm{Sel}^{(\psi)}(E_h/\mathbb{Q})$ contains 9 times as many elements as $\mathrm{Sel}^{(\hat{\psi})}(\bar{E}_h/\mathbb{Q})$*

Proof. All values required for Theorem 6.3 are now known. Both ψ and $\hat{\psi}$ have a kernel with trivial rational part. Moreover, the products of the Tamagawa numbers can be read off Table 6.4. Finally, Lemma 6.15 provides the ratio between the real periods. We complete the computation:

$$\frac{\#\,\mathrm{Sel}^{(\hat{\psi})}(\bar{E}_h/\mathbb{Q})}{\#\,\mathrm{Sel}^{(\psi)}(E_h/\mathbb{Q})} = \frac{\#\bar{E}_h(\mathbb{Q})[\hat{\psi}]\Omega_{E_h}\prod_p c_{E_h,p}}{\#E_j(\mathbb{Q})[\psi]\Omega_{\bar{E}_h}\prod_p c_{\bar{E}_h,p}} = \frac{1\cdot 1\cdot 16}{1\cdot 3\cdot 48} = \frac{1}{9}.$$

□

6.7 3-descent

We now perform descent by the 3-isogeny $\psi : E \to E'$. By Theorem 6.16, we will find at least 9 elements in $\mathrm{Sel}^{(\psi)}(E_h/\mathbb{Q})$. A closer inspection of the possible elements of $\mathrm{Sel}^{(\psi)}(E_h/\mathbb{Q})$ also gives a bound from above.

Theorem 6.17. *Let h, $h-2$, $h-6$ and $h-8$ be prime numbers and assume $h \equiv 3 \mod 8$. Then $Selpsi(E_h/\mathbb{Q})$ contains precisely 9 elements. All of these elements, except for the element 1, give non-trivial element of $Ш(E_h/\mathbb{Q})[3]$.*

Proof. This is an application of Algorithm 5.12. We have manufactured E_h to make sure our extension is $L = \mathbb{Q}(\sqrt{2})$. When factoring the discriminant of E_h into prime ideals (or rather into irreducible elements, since L has class number 1), we find that $2\mathcal{O}_L$ ramifies and $(h-2)\mathcal{O}_L$ splits, while all other bad primes stay inert. This can be concluded from their residue modulo 8. Furthermore, the free part $\mathcal{O}_L^\times$ is generated by $1+\sqrt{2}$. Hence we have

$$L(S_{E_{448},\psi},3)^* = \{(1+\sqrt{2})^k, (k+l\sqrt{2})(k-l\sqrt{2})^2(1+\sqrt{2})^k, (k+l\sqrt{2})^2(k-l\sqrt{2})(1+\sqrt{2})^k\},$$

Where

$$h-2 = \left(k+l\sqrt{2}\right)\left(k-l\sqrt{2}\right) = k^2-2l^2.$$

Observe that $L(S_{E_h,3})^*$ has 9 elements and contains $\mathrm{Sel}^{(\psi)}(E/\mathbb{Q})$, which has at least 9 elements by Theorem 6.16. Thus we have

$$\mathrm{Sel}^{(\psi)}(E_h/\mathbb{Q}) = L(S_{E_h,3})^*.$$

Theorem 6.16 then also implies that $\mathrm{Sel}^{(\hat{\psi})}(E'_h(\mathbb{Q})) = \{1\}$. Unfortunately it's not possible to write down explicit formulae for k and l, that is to give a general account of how $h-2$ splits in $\mathbb{Q}(\sqrt{2})$.

By Theorem 6.14, E_h has rank 0. Moreover, by our construction $E'_h(\mathbb{Q})$ does not have non-trivial elements of order 3. Thus the group $E'_h(\mathbb{Q})/\psi(E_h(\mathbb{Q}))$ is trivial. It follows from the exact sequence

$$0 \longrightarrow E'_h(\mathbb{Q})/\phi(E_h(\mathbb{Q})) \xrightarrow{\delta} \mathrm{Sel}^{(\psi)}(E_h/\mathbb{Q}) \longrightarrow Ш(E_h/\mathbb{Q})[\psi]$$

that all 9 elements of $\mathrm{Sel}^{(\psi)}(E_h/\mathbb{Q})$ correspond to distinct homogeneous spaces in $Ш(E_h/\mathbb{Q})[\psi]$. □

Corollary 6.18. *Let h, $h-2$, $h-6$ and $h-8$ be prime numbers and assume $h \equiv 3 \mod 8$. Then the curves*

$$C_h : 18w^2z + 432z^3 + w^3 + 216wz^2 + 2(h-2)^2(h-8) = 432z^2 - 6w^2$$
$$D_h : 27w^2z + 648z^3 + w^3 + 216wz^2 + (h-2)^2(h-8) = 3w^2 - 216z^2$$

Have points in every completion of $\mathbb{Q}$, but not in $\mathbb{Q}$ itself. For instance, the curves

$$C_{19} : 18w^2z + 432z^3 + w^3 + 216wz^2 + 6358 = 432z^2 - 6w^2$$
$$D_{19} : 27w^2z + 648z^3 + w^3 + 216wz^2 + 3179 = 3w^2 - 216z^2$$

have points everywhere locally, but not globally.

Proof. This is a straightforward application of Lemma 5.9. When letting the equation of $\bar{E}_h$ be minimal, we have

$$A' = 72$$
$$B' = \frac{1}{3}(h-2)^2(h-8).$$

Since $1+\sqrt{2}$ is an element of $\mathrm{Sel}^{(\psi)}(E_h/\mathbb{Q})$, we construct the corresponding homogeneous space. We write

$$1+\sqrt{2} = 1 + \frac{1}{6}\sqrt{72}$$

and recall $N_{L/\mathbb{Q}}\left(1+\sqrt{2}\right) = -1$. Using our values for A', B', u, v and s, the equation for the homogeneous space becomes

$$C_h : 3w^2z + 72z^3 + \frac{1}{6}w^3 + 72wz^2 + \frac{1}{3}(h-2)^2(h-8) = 72z^2 - w^2.$$

Multiplying by 6 to make the coefficients integral yields the equation given. The equation for D_h is constructed analogously, except that we start with the element $\left(1+\sqrt{2}\right)^2 = 3+2\sqrt{2}$ of $\mathrm{Sel}^{(\psi)}(E_h/\mathbb{Q})$.

Finally, note that $h = 19$ satisfies all conditions; $19 \equiv 3 \mod 8$ and 19, 17, 13 and 11 are all prime. Substituting $h = 19$ gives the equations for C_{19} and D_{19}. □

Remark 6.19. It is not clear how many examples were constructed in this chapter. If we write $h = 8n+3$, then we are interested in the values attained by the polynomial

$$F(n) := (8n+3)(8n+1)(8n-3)(8n-5) = h(h-2)(h-6)(h-8).$$

Shinzel's Hypothesis (H) in [SS58] states that if all values of $F(n)$ do not share a prime factor, then it happens infinitely often that all factors are prime. The question whether Shinzel's Hypothesis (H) is true remains open. In fact, the only verified case is when F consists of one linear factor, whence you recover Dirichlet's Theorem on Arithmetic Progressions.

In our case, the condition is satisfied; $F(0)$ and $F(2)$ are coprime. Thus a proof of Shinzel's Hypothesis (H) would imply that the family $\{E_h\}$ consists of infinitely many elliptic curves. Then Theorem 6.17 provides infinitely many elliptic curves E with $\#Ш(E/\mathbb{Q})[3] = 9$.

7 Discussion and further research

In this section, several aspects of the results in this thesis are placed in the context of other work that has been done. Besides, some ideas for future research are discussed.

7.1 Explicit descent

The method of descent by 2-isogeny has been known at least since Tate's Haverford lectures in 1961. Ever since, more methods of descent on elliptic curves have been devised. The method of 3-descent was introduced in [Top91]. Later, general p-descent was made explicit in [Dok00]. In the series of papers [CFO+08] [CFO+09] [CFO+15], a procedure for explicit n-descent, where n may be composite, is outlined. In [CFO+15], a specific example of $Ш(E/\mathbb{Q})[3]$ is dealt with. However, a general formula for the homogeneous spaces, like the ones in Lemma 5.8 and Lemma 5.9, is not provided. I think it would be interesting to give an explicit account of the homogeneous spaces coming from different isogenies and construct Tate-Shafarevich elements of several orders. Elements of order 5 and 7 are constructed in [Fis01] and of course other orders are also possible. For instance, the construction of Tate-Shafarevich elements of order 13 could be explored.

7.2 Large Selmer groups

In chapter 6, we used Theorem 6.3 to force elements into the Selmer group. This procedure can be extended. In [KS03], the Tamagawa numbers are arranged to make the corresponding Selmer groups arbitrarily large, for 3-isogenies among others. However, the approach is not constructive; it doesn't allow one to write down an elliptic curve with $\dim_{\mathbb{F}_3} \mathrm{Sel}^{(\psi)}(E/\mathbb{Q})[3] \geq m$ given a positive integer m. That is still a difficult problem. A step in this direction is to make $L(S_{E,\psi}, 3)^*$ large. In our context, if we let E be given by

$$E : y^2 = x^3 - c^3\left(x - B(B-c)^2\right)^2,$$

Then we would have to increase the number of prime divisors of c in order to at least achieve $\dim_{\mathbb{F}_3} L(S_{E,\psi}, 3)^* \geq m$. Of course this does not guarantee that these elements are everywhere locally in the image of the connecting homomorphism.

7.3 Large Tate-Shafarevich groups

Recalling the exact sequence

$$0 \to E'(K)/\phi(E(K)) \to \mathrm{Sel}^{(\phi)}(E/K) \to Ш(E/K)[\phi] \to 0,$$

we realize that

$$\dim \mathrm{Sel}^{(\phi)}(E/K) = \mathrm{rank}(E'(K)) + \dim E'(K)[\hat{\phi}] + \dim Ш(E/K)[\phi].$$

Hence large Selmer groups come with high rank elliptic curves or with large Tate-Shafarevich groups. It is not known whether the rank of elliptic curves over $\mathbb{Q}$ can be arbitrarily large. In [PPCW10], it is argued, using argument based on random matrices, that there are only finitely many ellitpic curves with rank exceeding 21, even though an infinite family of elliptic curves has been constructed with rank at least 19. If the rank of elliptic curves is uniformly bounded, then arbitrarily large Selmer groups entail arbitrarily large Tate-Shafarevich groups. Indeed, it is shown in [Fis01] that the 5-primary part of $Ш(E/\mathbb{Q})$ is unbounded. The same is done for the 3-primary part in [Aok04], but it was already shown in [Cas64] that $Ш(E/\mathbb{Q})[3]$ can be arbitrarily large. Again, these proofs are not constructive. We could pose the same problem as for Selmer groups: given integers m and n, write down an elliptic curve E such that $Ш(E/\mathbb{Q})[n]$ has rank at least m as $\mathbb{Z}/n\mathbb{Z}$-module. That problem remains unsolved. In this thesis, we constructed a family of elliptic curves with $\dim_{\mathbb{F}_3} Ш(E/\mathbb{Q})[3] = 2$. The advantage of our approach is that the elements, genus one curves that are soluble everywhere locally but not globally, can be written down explicitly.

The existence of arbitrarily large Selmer groups implies at least that the rank of elliptic curves and the size of Tate-Shafarevich groups cannot both be uniformly bounded. If one could prove that the Selmer group $\mathrm{Sel}^{(p)}(E/\mathbb{Q})$ becomes arbitrarily large for infinitely many prime numbers p simultaneously, then the statement becomes stronger; either the rank of elliptic curves is unbounded or infinitely large Tate-Shafarevich groups exist, rendering Conjecture 3.17 false.

7.4 The Hasse principle

The Hasse principle states that a (multivariate) polynomial F has a global solution if and only if it has one everywhere locally. If the degree of F is at most 2, this is a theorem. The smallest degree for which the principle may fail is 3, so in a sense the irreducible cubics that can be found in $Ш(E_h/\mathbb{Q})[\psi]$ are 'minimal' counterexamples. I consider it valuable that chapter 6 provides a very explicit and direct way to construct counterexamples to the Hasse Principle; the only requirements to be tested are primality and residue modulo 8, and a counterexample to the Hasse principle can be written down immediately from Corollary 6.18.

7.5 The converse of Chapter 6

One might attempt to achieve a similar result as Theorem 6.17, but with 2 and 3 reversed; one shows by explicit 3-descent that a family of elliptic curves with a 6-isogeny has rank 0 and uses the formula in Theorem 6.3 to force elements in the Selmer group of the 2-isogeny. Then these elements belong to the Tate-Shafarevich group. Unfortunately, this procedure turns out to be more difficult. The problem is that forcing a difference in the Tamagawa product is not feasible. In other words, if we start out with an elliptic curve of the form

$$E_t : y^2 = x^3 - c^3(x - t(t-c)^2)^2,$$

then we have

$$\prod_p c_{E,p} = \prod_p c_{E',p}.$$

In Chapter 6, we let the residue modulo 24 determine whether there is split or non-split multiplicative reduction at certain primes. If the valuation of the discriminant at this prime is 3, then non-split multiplicative reduction yields the Tamagawa number 1, while split multiplicative reduction yields the Tamagawa number 3. The same happens if the valuation is 6; then the possible Tamagawa numbers are 2 and 6. Finetuning this introduces a factor 3 difference between $\prod_p c_{E,p}$ and $\prod_p c_{\bar{E},p}$, allowing us to benefit from Theorem 6.3. On the other hand, in order to obtain a factor 2 difference between $\prod_p c_{E,p}$ and $\prod_p c_{E',p}$, the only factor difference that can occur, we would need a prime of multiplicative reduction that divides the discriminant 4 times (or a higher power of 2). As seen in equation (6.5), this does not happen in such a family of elliptic curves. Thus we would need a somewhat different family of curves; perhaps the elliptic curve E_{1100} from Example 4.8 and Example 5.14 lies in such a family. In any case, this would be an interesting topic for a future research project.

7.6 The rank of elliptic curves with a rational 3-isogeny

An interesting challenge is to construct elliptic curves with a rational 3-isogeny and a high rank. Consider the elliptic curve

$$E : y^2 = x^3 + A(x - B)^2.$$

We can use the freedom we have in choosing A and B to increase the rank of $E(\mathbb{Q})$. A very basic approach is the following: suppose we want a rational point $(1, D)$; this yields

$$\begin{aligned} D^2 &= 1 + A(B-1)^2 \\ \implies A &= \frac{D^2 - 1}{(B-1)^2}. \end{aligned}$$

Such a point $(1, D)$ on the elliptic curve

$$E : y^2 = x^3 + \frac{D^2 - 1}{(B-1)^2}(x - B)^2$$

generically has infinite order, so this construction yields infinitely many elliptic curves with a 3-isogeny and positive rank. If we work carefully, we can even impose more points of infinite order, as done in [vT15], but we generally do not achieve an extraordinarily high rank.

In [vT15], a more sophisticated approach, using elliptic curves over $\mathbb{Q}(t)$, results in the example

$$E : y^2 = x^3 - 753247(x - 8100)^2$$

with rank 7.

Another method for constructing elliptic curves with high rank is given in [Mes91]. Given 10 distinct numbers $a_1, \cdots, a_{10}$, define the polynomial

$$p(x) := \prod_{i=1}^{10}(x - a_i).$$

Then define $q(x) := x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$. The parameters b_i can be chosen such that q^2 and p have the same coefficients for $x^5, \cdots, x^{10}$. Then we have $p = q^2 - r$, where r has degree at most 4. Then $E : y^2 = r(x)$ is a curve of genus one with 10 rational points $(a_i, q_i(a_i))$. Moving one of them to infinity yields an elliptic curve which generically has rank at least 9. If we also request that $r(x)$ can be written as (5.1) or (5.3), this would yield elliptic curves with a 3-isogeny and rank at least 9. Unfortunately, there was no time to include an elaborate investigation of this in this thesis. However, I have tried a modest variant, with only 4 points $a_1, \cdots, a_4$. In this case, we have

$$p(x) = x^4 - \left(\sum_{i=1}^{4} a_i\right)x^3 + \left(\sum_{1\leq i<j\leq 4} a_ia_j\right)x^2 - \left(\sum_{i=1}^{4}\prod_{j\neq i} a_j\right)x + a_1a_2a_3a_4.$$

Furthermore, we expand

$$q^2 = (x^2 + b_1x + b_0)^2 = x^4 + 2b_1x^3 + \left(b_1^2 + 2b_0\right) + 2b_1b_0x + b_0^2.$$

We impose the restrictions

$$b_1^2 + 2b_0 = \sum_{1\leq i<j\leq 4} a_ia_j$$
$$2b_1b_0 = \sum_{i=1}^{4}\prod_{j\neq i} a_j,$$

which entail that the polynomial $r = q^2 - p$ is of the form $cx^3 + C$. This means, I hoped, that the elliptic curve $E : y^2 = r(x)$ has a rational 3-isogeny and, generically, rank at least 3. But there is one problem; the polynomial q is uniquely given by

$$q(x) = x^2 - \left(\sum_{i=1}^{4} a_i\right)x + \left(\sum_{i=1}^{4} a_i\right).$$

Then the cubic term in r always vanishes as well, so $y^2 = r(x)$ does not define an elliptic curve. Perhaps other variants of Mestre's method are more fruitful.

Unfortunately, Dujella's archive of high rank elliptic curves does not contain a category of elliptic curves with prescribed isogeny order. Nevertheless, it contains rank records of elliptic curves with prescribed torsion. Clearly a curve with rational 3-torsion has a rational 3-isogeny. Recently, a new record in this category was discovered by N.D. Elkies ([Elk18]): an elliptic curve with a point of order 3 and rank 14. One shows that its rank is at most 14 through descent by 3-sogeny. In [Elk07], Elkies also constructs an infinite family family of elliptic curves with a point of order 3 and rank at least 7.

8 Conclusion

In this thesis, two types of descent were introduced, analyzed and implemented.

First, a general account was given of the theory of descent by a (rational) isogeny on elliptic curves. For this, some Galois cohomology was required. This provided an introduction to Weil-Châtelet groups, Selmer groups and Tate-Shafarevich groups.

As an application, we recovered this theory to rational isogenies of degree 2, a well-known procedure. We made the connecting homomorphism and the homogeneous spaces completely explicit. These explicit descriptions yield an algorithm for computing the Selmer groups of rational isogenies of degree 2. This algorithm was applied to a few examples. Both possible outcomes of the computation of Selmer groups have been demonstrated: in some examples it led to an exact computation of the rank, in other examples it gave rise to non-trivial elements of Tate-Shafarevich groups. These elements were respresented as hyperelliptic curves that violate the Hasse principle.

We then presented the analog for rational isogenies of degree 3. Using an explicit formulation of the connecting homomorphism and the homogeneous spaces, we devised an algorithm that computes the Selmer group of any given rational isogeny of degree 3. By reusing some examples with both a 2-isogeny and a 3-isogeny, we proved that certain homogeneous spaces belong to the Tate-Shafarevich group. In the case of a 3-isogeny, these homogeneous spaces are defined by irreducible cubic polynomials. We also demonstrate how to recover a rational point on the elliptic curve $\bar{E}$ from a point on the homogeneous space C_t, allowing for a much more efficient point search.

We illustrated the combined power of both methods by applying them to a family of elliptic curves E_h. We designed E_h to have precisely 9 Tate-Shafarevich elements of order 3. E_h admits both a rational 2-isogeny and a rational 3-isogeny, rendering it suitable for both descent procedures. We applied both presented algorithms. Descent by 2-isogeny provided that the elliptic curves have rank zero, while we forced elements elements into the Selmer group $\mathrm{Sel}^{(\psi)}(E_h/\mathbb{Q})$. These elements cannot come from rational points on $\bar{E}_h$, and hence they belong to a Tate-Shafarevich group. Ultimately, this yields a way to generate explicit counterexamples to the Hasse principle. The first one produced is given by

$$C_{19} : 18w^2z + 432z^3 + w^3 + 216wz^2 + 6358 = 432z^2 - 6w^2.$$

The technique of descent could in the future be applied to isogenies of a different degree. Another possible goal for future research is to write down abitrarily large Selmer groups explicitely. This can be used for two purposes: to formulate elliptic curves with a 3-isogeny and high rank or to construct arbitrarily large Tate-Shafarevich groups. It is safe to say that there is still a lot of interesting research to be done in this rich and elegant subject.

References

[Ali18] Alina. Elliptic-curve cryptography, iot security, and cryptocurrencies. https://forum.iotex.io/thread/5c20df58520d9500139615d4, 2018.

[Aok04] Noboru Aoki. On the tate–shafarevich group of semistable elliptic curves with a rational 3-torsion. *Acta Arithmetica*, pages 209–227, 2004.

[Cas64] J.W.S. Cassels. Arithmetic on curves of genus 1. vi. the tate-safarevic group can be arbitrarily large. *Journal für die reine und angewandte Mathematik*, 0214_0215:65–70, 1964.

[Cas65] J.W.S. Cassels. Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer. *Journal für di reine und angewandte Mathematik*, pages 180–199, 1965.

[CFO+08] John Cremona, Tom Fisher, Cathy O'Neil, Denis Simon, and Michael Stoll. Explicit n-descent on elliptic curves i. algebra. *Journal für die reine und angewandte Mathematik*, pages 121–155, 2008.

[CFO+09] John Cremona, Tom Fisher, Cathy O'Neil, Denis Simon, and Michael Stoll. Explicit n-descent on elliptic curves ii. geometry. *Journal für die reine und angewandte Mathematik*, pages 63–84, 2009.

[CFO+15] John Cremona, Tom Fisher, Cathy O'Neil, Denis Simon, and Michael Stoll. Explicit n-descent on elliptic curves iii. algorithms. *Mathematics of Computation*, pages 895–922, 2015.

[DD15] Tim Dokchitser and Vladimir Dokchitser. Local invariants of isogenous elliptic curves. *Transactions of the American Mathematical Society*, pages 4339–4358, 2015.

[Dok00] Tim Dokchitser. *Deformations of p-divisible groups and p-descent on elliptic curves*. PhD thesis, University of Utrecht, 2000.

[Elk07] Noam D. Elkies. Three lectures on elliptic surfaces and curves of high rank, 2007.

[Elk18] Noam D. Elkies. Torsion group z/3z, rank = 14, 2018.

[Fis01] Tom Fisher. Some examples of 5 and 7 descent for elliptic curves over q. *Journal of the European Mathematical Society*, page 169–201, 3 2001.

[KS03] Remke Kloosterman and Edward F. Schaefer. Selmer groups of elliptic curves that can be arbitrarily large. *Journal of Number Theory*, 99:148–163, 3 2003.

[Kum55] Ernst F. Kummer. Über eine besondere Art, aus complexen Einheiten gebildeter Ausdrücke. *Journal für reine und angewandte Mathematik*, pages 212–232, 1855.

[LMF13] The LMFDB Collaboration. The L-functions and Modular Forms Database. http://www.lmfdb.org, 2013. [Online; accessed 16 September 2013].

[Maz77] Barry Mazur. Modular curves and the eisenstein ideal. *Publications Mathématiques de l'IHÉS*, 47:33–186, 1977.

[Mes91] Jean-Franćois Mestre. Courbes elliptiques de rang ≥ 11 sur q(t). *Comptes rendus de l'Académie des sciences*, pages 139–142, 1991.

[Mor22] Louis J. Mordell. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proceedings of the Cambridge Philosophical Society*, pages 179–192, 1922.

[PPCW10] Jennifer Park, Bjorn Poonen, John Coight, and Melanie Matchett Wood. A heuristic for boundedness of ranks of elliptic curves. *Mathematics Subject Classification*, 2010.

[Sch85] René Schoof. Elliptic Curves over Finite Fields and the Computation of Square Roots mod p. *Mathematics of Computation*, pages 483–494, 1985.

[Sch95] Edward F. Schaefer. 2-descent on the Jacobians of Hyperelliptic Curves. *Journal of Number Theory*, pages 219–232, 1995.

[Ser64] Jean-Pierre Serre. *Galois Cohomology.* Springer-Verlag, Berlin Heidelberg, 1964.

[Sil86] Jospeh H. Silverman. *The Arithmetic of Elliptic Curves.* Springer, Dordrecht Heidelberg London New York, 1986.

[SS58] Andrzei Schinzel and Waclaw Sierpiński. Sur certaines hypothèses concernant les nombres premiers. *Acta Arithmetica*, pages 185–208, 1958.

[ST92] Joseph H. Silverman and John T. Tate. *Rational points on elliptic curves.* Springer, Heidelberg New York Dordrecht London, 1992.

[Tat75] John T. Tate. Algorithm for determining the type of a singular fiber in an elliptic pencil. In Bryan Birch and Willem Kuyk, editors, *Modular Functions of One Variable IV*, pages 33–52, Berlin Heidelberg, 1975. Springer-Verlag.

[Top91] Jaap Top. Descent by 3-isogeny and the 3-rank of quadratic fields. *Advances in number theory*, 05 1991.

[vT15] Lianne van Timmeren. The rank of elliptic curves of the form $E_{A,B} : y^2 = x^3 + A(x-B)^2$. Master's thesis, University of Groningen, 2015.

[Vé71] Jacques Vélu. Isogénies entre courbes elliptiques. *Comptes Rendus de l'Académie des Sciences Paris*, pages 238–241, 1971.

[Wei28] André Weil. *L'arithmétique sur les courbes algébriques.* PhD thesis, University of Uppsala, 1928.

A MAGMA code

All the MAGMA code used for this thesis is presented in this section. We exhibit and explain the MAGMA programs per examplary elliptic curve, in order of appearance.

A.1 The example E_{448}

In Example 4.6, we computed the Selmer group $\text{Sel}^{(\phi)}(E_{448}/\mathbb{Q})$ by means of the following code.

```
1  Selphi:={Rationals()|1};
2  P<z>:=PolynomialRing(Rationals());
3  a:=-724;
4  b:=-28;
5  for i in [0,1] do
6      for j in [0,1] do
7          for k in [0,1] do
8              d:=(-1)^i*2^j*7^k;
9              if HasPointsEverywhereLocally(d+a*d^2*z^2+b*d^3*z^4,2) and (HasRoot(d+a
       *d^2*z^2+b*d^3*z^4,RealField()) or b*d gt 0) then
10                 Include(~Selphi,d);
11             end if;
12 end for; end for; end for;
13 print "Selphi is ", Selphi;
```

Listing A.1: The code used to compute $\text{Sel}^{(\phi)}(E_{448}/\mathbb{Q})$.

Line 1: the Selmer group is created; it will always contain the element 1.
Line 2: the appropriate polynomial ring is created.
Line 3-4: the parameters of E'_{448} are implemented.
Line 5-8: the possible elements d of $\text{Sel}^{(\phi)}(E_{448}/\mathbb{Q})$ are constructed.
Line 9-11: it is checked whether the homogeneous space corresponding to d has points everywhere locally. If so, d is added to the Selmer group.

A similar program computes $\text{Sel}^{(\hat{\phi})}(E'_{448}/\mathbb{Q})$, the Selmer group of the dual isogeny.

```
1  Selphih:={Rationals()|1};
2  P<z>:=PolynomialRing(Rationals());
3  a:=362;
4  b:=32768;
5  for i in [0,1] do
6      for j in [0,1] do
7          for k in [0,1] do
8              d:=(-1)^i*2^j*7^k;
9              if HasPointsEverywhereLocally(d+a*d^2*z^2+b*d^3*z^4,2) and (HasRoot(d+a
       *d^2*z^2+b*d^3*z^4,RealField()) or b*d gt 0) then
10                 Include(~Selphih,d);
11             end if;
12 end for; end for; end for;
13 print "Selphih is ", Selphih;
```

Listing A.2: The code used to compute $\text{Sel}^{(\hat{\phi})}(E'_{448}/\mathbb{Q})$.

The only differences with Listing A.1 are the values of a and b.

In Example 5.15, we compute the Selmer group $\text{Sel}^{(\psi)}(E_{448}/\mathbb{Q})$ with this MAGMA.

```
1  Q:=Rationals();
2  P2<w,z,homgen>:=ProjectiveSpace(Q,2);
3  A:=1250;
4  B:=-280;
5  Asquarepart:=25;
6  K<sq2>:=QuadraticField(A);
7  O<sq2>:=RingOfIntegers(K);
8  Selpsi:={O|1};
9  squarerootofA:=O!(sq2*Asquarepart);
10 for i in [0,1,2] do
11     for k in [0,1,2] do
12         if IsZero(i) then
13             t:=(1+sq2)^k;
14             cuberootofnormt:=(-1)^k;
15         else
```

```
16              t:=(sq2+3)^i*(sq2-3)^(3-i)*(1+sq2)^k;
17              cuberootofnormt:=7*(-1)^k;
18          end if;
19          u:=Trace(t)/2;
20          v:=Q!((t-u)/squarerootofA);
21          Ft:=3*u*w^2*z+A*u*z^3+v*w^3+3*A*v*w*z^2+B*homgen^3-cuberootofnormt*(w^2-A*z
    ^2)*homgen;
22          Ct:=Curve(P2,Ft);
23          if IsLocallySoluble(Ct,2) and IsLocallySoluble(Ct,3) and IsLocallySoluble(
    Ct,7) then
24              Include(~Selpsi,t);
25              print t;
26              print "u= ", u, ", v= ", v;
27              print PointSearch(Ct,999);
28          end if;
29 end for; end for;
30 print "Selpsi is ", Selpsi;
```

Listing A.3: The code used to compute $\mathrm{Sel}^{(\psi)}(E_{448}/\mathbb{Q})$.

Line 1-2: the projective space in which the homogeneous spaces will live is created.
Line 3-9: the parameters A and B are implemented. Accordingly, the suitable field extension and its ring of integers, of which $\mathrm{Sel}^{(\psi)}(E_{448}/\mathbb{Q})$ is a subset, are created.
Line 10-20: the possibilities for $t = u + v\sqrt{A'}$ are constructed.
Line 21-26: it is checked whether the homogeneous space C_t has points everywhere locally. If so, t belongs in the Selmer group.
Line 27: if a homogeneous space has a point everywhere locally, we try to find a global point.

A.2 The example E_{89}

In Example 4.7, the Selmer group $\mathrm{Sel}^{(\phi)}(E_{89}/K)$ is computed by means of this MAGMA code.

```
1  K<wortelminelf>:=QuadraticField(-11);
2  O<al>:=RingOfIntegers(K);
3  Selphi:={O|1};
4  R<z>:=PolynomialRing(K);
5  a:=-10*al+6;
6  b:=-5*al-2;
7  p2:=ideal<O|2>;
8  pal:=ideal<O|5*al+2>;
9  for i in [0,1] do
10     for j in [0,1] do
11         for k in [0,1] do
12             d:=(-1)^i*2^j*(5*al+2)^k;
13             F:=d+a*d^2*z^2+b*d^3*z^4;
14             Cd:=HyperellipticCurve(F);
15             if IsLocallySolvable(Cd,p2) and IsLocallySolvable(Cd,pal) then
16                 Include(~Selphi,d);
17             end if;
18 end for; end for; end for;
19 print "Selphi is ", Selphi;
```

Listing A.4: The code used to compute $\mathrm{Sel}^{(\phi)}(E_{89}/K)$.

Line 1-4: The quadratic field K, its ring of integers, the (still trivial) Selmer group, and a polynomial ring over K are created.
Line 5-6: the parameters of E'_{89} are implemented.
Line 7-8: the primes $S_{E_{89},\phi}$ are really prime ideals in this case.
Line 9-12: the possible values d of $\mathrm{Sel}^{(\phi)}(E_{89}/K)$ are constructed.
Line 13-17: For every such d, it is checked whether the homogeneous space C_d is everywhere locally trivial.

A similar program was used to compute the Selmer group of the dual isogeny.

```
1  K<wortelminelf>:=QuadraticField(-11);
2  O<al>:=RingOfIntegers(K);
3  Selphih:={O|1};
4  R<z>:=PolynomialRing(K);
5  a:=5*al-3;
6  b:=-16;
```

```
p2:=ideal<O|2>;
pal:=ideal<O|5*al+2>;
for i in [0,1] do
    for j in [0,1] do
        for k in [0,1] do
            d:=(-1)^i*2^j*(5*al+2)^k;
            F:=d+a*d^2*z^2+b*d^3*z^4;
            Cd:=HyperellipticCurve(F);
            if IsLocallySolvable(Cd,p2) and IsLocallySolvable(Cd,pal) then
                Include(~Selphih,d);
            end if;
end for; end for; end for;
print "Selphih is ", Selphih;
```

Listing A.5: The code used to compute $\mathrm{Sel}^{(\hat{\phi})}(E'_{89}/K)$.

This is just Listing A.4 but with altered values of a and b.

A.3 The example E_{1100}

In Example 4.8, the Selmer group $\mathrm{Sel}^{(\phi)}(E_{1100}/\mathbb{Q})$ is computed as follows.

```
Selphi:={Rationals()|1};
P<z>:=PolynomialRing(Rationals());
a:=1460;
b:=532400;
for i in [0,1] do
    for j in [0,1] do
        for k in [0,1] do
            for l in [0,1] do
                d:=(-1)^i*2^j*5^k*11^l;
                if HasPointsEverywhereLocally(d+a*d^2*z^2+b*d^3*z^4,2) and (HasRoot
    (d+a*d^2*z^2+b*d^3*z^4,RealField()) or b*d gt 0) then
                    Include(~Selphi,d);
                end if;
end for; end for; end for; end for;
print "Selphi is ", Selphi;
```

Listing A.6: The code used to compute $\mathrm{Sel}^{(\phi)}(E_{1100}/\mathbb{Q})$.

For an explanation of the code, see the explanation of Listing A.1.

The Selmer group of the dual isogeny is computed as follows.

```
Selphih:={Rationals()|1};
P<z>:=PolynomialRing(Rationals());
a:=-730;
b:=125;
for i in [0,1] do
    for j in [0,1] do
        for k in [0,1] do
            for l in [0,1] do
                d:=(-1)^i*2^j*5^k*11^l;
                if HasPointsEverywhereLocally(d+a*d^2*z^2+b*d^3*z^4,2) and (HasRoot
    (d+a*d^2*z^2+b*d^3*z^4,RealField()) or b*d gt 0) then
                    Include(~Selphih,d);
                end if ;
end for; end for; end for; end for;
print "Selphih is ", Selphih;
```

Listing A.7: The code used to compute $\mathrm{Sel}^{(\hat{\phi})}(E'_{1100}/\mathbb{Q})$.

It works the same as Listing A.6.

In Example 5.14, we compute $\mathrm{Sel}^{(\psi)}(E_{1100}/\mathbb{Q})$ as follows.

```
Q:=Rationals();
P2<w,z,homgen>:=ProjectiveSpace(Q,2);
A:=8751645;
B:=-1275750;
Asquarepart:=3^3*7^2;
K<squarerootoffive>:=QuadraticField(A);
O<ph>:=RingOfIntegers(K);
Selpsi:={O|1};
```

```
squarerootofA:=O!(squarerootoffive*Asquarepart);
for i in [0,1,2] do
    for k in [0,1,2] do
        if IsZero(i) then
            t:=ph^k;
            cuberootofnormt:=(-1)^k;
        else
            t:=(ph+3)^i*(ph-4)^(3-i)*ph^k;
            cuberootofnormt:=11*(-1)^k;
        end if;
        u:=Trace(t)/2;
        v:=Q!((t-u)/squarerootofA);
        Ft:=3*u*w^2*z+A*u*z^3+v*w^3+3*A*v*w*z^2+B*homgen^3-cuberootofnormt*(w^2-A*z
    ^2)*homgen;
        Ct:=Curve(P2,Ft);
        if IsLocallySoluble(Ct,2) and IsLocallySoluble(Ct,3) and IsLocallySoluble(
    Ct,5) and IsLocallySoluble(Ct,11) then
            Include(~Selpsi,t);
            print t;
            print "u= ", u, ", v= ", v;
            print PointSearch(Ct,9999);
        end if;
end for; end for;
print "Selpsi is ", Selpsi;
```

Listing A.8: The code used to compute $\mathrm{Sel}^{(\psi)}(E_{1100}/\mathbb{Q})$.

Line 1-2: the projective space in which the homogeneous spaces will live is created.
Line 3-9: the parameters A and B are implemented. Accordingly, the suitable field extension and its ring of integers, of which $\mathrm{Sel}^{(\psi)}(E_{1100}/\mathbb{Q})$ is a subset, are created.
Line 10-20: the possibilities for $t = u + v\sqrt{A'}$ are constructed.
Line 21-26: it is checked whether the homogeneous space C_t has points everywhere locally. If so, t belongs in the Selmer group.
Line 27: if a homogeneous space has a point everywhere locally, we try to find a global point.

Later on, the Selmer group of the dual isogeny was computed as follows.

```
Q:=Rationals();
P2<w,z,homgen>:=ProjectiveSpace(Q,2);
A:=-324135;
B:=770;
Asquarepart:=3*7^2;
K<squarerootofminusfifteen>:=QuadraticField(A);
O<al>:=RingOfIntegers(K);
Selpsih:={O|1};
squarerootofA:=O!(squarerootofminusfifteen*Asquarepart);
p2:=ideal<O | 2, al>;
q2:=ideal<O | 2, al+1>;
p3:=ideal<O | 3, al+1>;
p5:=ideal<O | 5, al+2>;
for k in [0,3] do
    for l in [0,3] do
        if IsZero(k) or IsZero(l) then
            if IsZero(k) and IsZero(l) then
                for i in [1,2,4,5] do
                    yesitisprincipal,t:=IsPrincipal(p2^i*q2^(6-i));
                    cuberootofnormt:=4;
                    u:=Trace(t)/2;
                    v:=Q!((t-u)/squarerootofA);
                    Ft:=3*u*w^2*z+A*u*z^3+v*w^3+3*A*v*w*z^2+B*homgen^3-
    cuberootofnormt*(w^2-A*z^2)*homgen;
                    Ct:=Curve(P2,Ft);
                    if IsLocallySoluble(Ct,2) and IsLocallySoluble(Ct,3) and
    IsLocallySoluble(Ct,5) and IsLocallySoluble(Ct,11) then
                        Include(~Selpsih,t);
                        print t;
                        print "u= ", u, ", v= ", v;
                        print PointSearch(Ct,9999);
                    end if;
                end for;
            else
                for i in [1,2] do
                    yesitisprincipal,t:=IsPrincipal(p2^i*q2^(3-i)*p3^k*p5^l);
```

```
35                      cuberootofnormt:=Integers()!(2*3^(k/3)*5^(l/3));
36                      u:=Trace(t)/2;
37                      v:=Q!((t-u)/squarerootofA);
38                      Ft:=3*u*w^2*z+A*u*z^3+v*w^3+3*A*v*w*z^2+B*homgen^3-
    cuberootofnormt*(w^2-A*z^2)*homgen;
39                      Ct:=Curve(P2,Ft);
40                      if IsLocallySoluble(Ct,2) and IsLocallySoluble(Ct,3) and
    IsLocallySoluble(Ct,5) and IsLocallySoluble(Ct,11) then
41                          Include(~Selpsih,t);
42                          print t;
43                          print "u= ", u, ", v= ", v;
44                          print PointSearch(Ct,9999);
45                      end if;
46                  end for;
47          end if; end if;
48  end for; end for;
49  print "Selpsih is ", Selpsih;
```

Listing A.9: The code used to compute $\mathrm{Sel}^{(\hat{\psi})}(\bar{E}_{1100}/\mathbb{Q})$.

Line 1-2: the projective space in which the homogeneous spaces will live is created.
Line 3-9: the parameters A and B are implemented. Accordingly, the suitable field extension and its ring of integers, of which $\mathrm{Sel}^{(\hat{\psi})}(\bar{E}_{1100}/\mathbb{Q})$ is a subset, are created.
Line 10-13: we define the prime ideals that will serve as building blocks for the possible values of t.
Line 14-30 some possibilities for $t = u + v\sqrt{A}$ are constructed. It is immediately checked whether the corresponding homogeneous spaces are locally trivial. If so, t is added to the Selmer group and we search for rational points.
Line 35-66: the same is done for the remaining possibilities of t. The possibilities for t were more difficult to program because of the class group of K.

A.4 The example E_{441}

In Example 5.13, we compute the Selmer group $\mathrm{Sel}^{(\psi)}(E_{441}/\mathbb{Q})$ as follows.

```
1  Q:=Rationals();
2  Selpsi:={Q|1};
3  P2<w,r,homgen>:=ProjectiveSpace(Q,2);
4  C:=571536;
5  sqrtC:=756;
6  for i in [0,1,2] do
7      for j in [0,1,2] do
8          t:=3^i*7^j;
9          Ft:=t^2*w^3-2*t*sqrtC*homgen^3-r^3;
10         Ct:=Curve(P2,Ft);
11         if IsLocallySoluble(Ct,3) and IsLocallySoluble(Ct,7) then
12             Include(~Selpsi,t);
13         end if;
14 end for; end for;
15 print "Selpsi is ", Selpsi;
```

Listing A.10: The code used to compute $\mathrm{Sel}^{(\psi)}(E_{441}/\mathbb{Q})$.

Line 1-3: the Selmer group and the projective space are created.
Line 4-5: C and its square root are implemented.
Line 6-8: the possibilities for t are produced.
Line 10-14: for all such t, it is determined whether the homogeneous space has points locally everywhere. If so, t is included in the Selmer group.

Thereafter, we computed $\mathrm{Sel}^{(\hat{\psi})}(\bar{E}_{441}/\mathbb{Q})$ via these lines of MAGMA code.

```
1  Q:=Rationals();
2  P2<w,z,homgen>:=ProjectiveSpace(Q,2);
3  C:=-21168;
4  Csquarepart:=84;
5  K<squarerootofminusthree>:=QuadraticField(C);
6  O<al>:=RingOfIntegers(K);
7  Selpsih:={O|1};
8  squarerootofC:=O!(squarerootofminusthree*Csquarepart);
```

```
9  for i in [0,1,2] do
10 for k in [0,1,2] do
11 if IsZero(i) then
12 t:=(al-1)^k;
13 else
14 t:=(al+2)^i*(al-3)^(3-i)*(al-1)^k;
15 end if;
16 u:=Trace(t)/2;
17 v:=Q!((t-u)/squarerootofC);
18 Ft:=3*u*w^2*z+C*u*z^3+v*w^3+3*C*v*w*z^2-homgen^3;
19 Ct:=Curve(P2,Ft);
20 if IsLocallySoluble(Ct,3) and IsLocallySoluble(Ct,7) then
21 Include(~Selpsih,t);
22 print t;
23 print "u= ", u, ", v= ", v;
24 print PointSearch(Ct,999);
25 end if;
26 end for; end for;
27 print "Selpsih is ", Selpsih;
```

Listing A.11: The code used to compute $\mathrm{Sel}^{(\hat{\psi})}(\bar{E}_{441}/\mathbb{Q})$.

Line 1-2: the projective space in which the homogeneous spaces will live is created.
Line 3-8: the parameter C is implemented. Accordingly, the suitable field extension and its ring of integers, of which $\mathrm{Sel}^{(\hat{\psi})}(\bar{E}_{441}/\mathbb{Q})$ is a subset, are created.
Line 9-17: the possibilities for $t = u + v\sqrt{C}$ are constructed.
Line 18-23: it is checked whether the homogeneous space C_t has points everywhere locally. If so, t belongs in the Selmer group.
Line 24: if a homogeneous space has a point everywhere locally, we try to find a global point. This is the only case where this step is useful; it allows us to find a point on $\bar{E}_{441}(\mathbb{Q})$ of infinite order via the rational three-to-one covering $C_t \to \bar{E}$.