COMPUTING THE MORDELL-WEIL GROUP OF ELLIPTIC CURVES

DAKSH AGGARWAL

Contents

1. Introduction

In this exposition, we will study the problem of finding rational solutions to elliptic curves. We will formally discuss elliptic curves in the next section but we begin with a brief introduction to the Diophantine problem of computing rational points on varieties, and why this problem is interesting for elliptic curves.

A familiar Diophantine problem is to compute integer solutions (x, y) to

$$L : ax + by = c,$$

for $a, b, c \in \mathbb{Z}$. We are not interested in only computing a single point but rather, we want to somehow describe or parameterize all possible integer solutions. This problem for L is, of course, fully understood. In general, through linear algebra, we understand a linear Diophantine system in any number of variables as well.

We can say a lot about rational solutions to degree two homogeneous equations, also known as *quadratic forms*, too. For example, consider

$$x^2 + y^2 = z^2.$$

It is equivalent to instead focus on the circle

$$C : X^2 + Y^2 = 1,$$

whose nontrivial rational solutions we know how to parameterize. We can fix a nontrivial rational solution like $P = (3/5, 4/5)$ and let $Q = (x_0, y_0)$ be any other rational solution on C. Then,

joining P and Q, we obtain a line of rational slope. Conversely, if we intersect C with any line through P having rational slope, we recover a rational point on C. In this way, we have provided a parameterization of rational points on C.

The natural next step is to consider homogeneous cubics. But these are already quite difficult to analyze in three variables. For example, take the Fermat equation

$$x^3 + y^3 = z^3,$$

which on dehomogenizing becomes

$$F : X^3 + Y^3 = 1.$$

Like for the circle, we might try to use geometry, but the trouble is that no nontrivial rational solutions are visible upon inspection. Indeed, F has no nontrivial rational solutions, but that is not obvious and requires some work to show. One way is to factor the original equation in $\mathbb{Q}(\zeta_3)$, with ζ_3 a primitive third root of unity, and then use the fact that $\mathbb{Z}[\zeta_3]$ is a UFD along with a Fermat-type descent argument (e.g. [5, Ch. 17, §8]). We will give another proof of this fact in Theorem 8.5, using the method we study of computing rational points on elliptic curves. The situation, however, would have been very different if a single rational point had existed, such as for

$$E : X^3 + Y^3 = 9,$$

that has the nontrivial solution $P = (1, 2)$. Then, by intersecting the tangent at P with E, we find a new rational point $(-17/7, 20/7)$. We can, in fact, continue this process to obtain an infinite number of rational solutions on E (see [5, Ch. 17, §9]). However, unlike the case of the circle, there is no guarantee this process will hit all rational points on E.

The curves F and E are *elliptic curves* and the difficulty of finding a description of the rational points on these curves is characteristic of the problem of describing the rational points on curves that have genus greater than 0. Therefore, to gain insight about the general situation, it is a worthy goal to accumulate as much clarity as possible with the simplest case of elliptic curves, which have genus 1. In fact, elliptic curves being genus 1 curves are special, because we have Falting's Theorem, that says the set of rational points on curves with genus greater 1 is finite. So, elliptic curves sit at a rather exciting cusp.

But it is natural to wonder about why the problem becomes substantially harder in going from quadratic forms to cubics. The fundamental reason we understand quadratic forms well is because they satisfy the *local-to-global principle*. This principle states that given a quadratic form Q over $\mathbb{Q}$, a rational solution to Q exists if a solution to Q exists over $\mathbb{R}$ and $\mathbb{Q}_p$ for every prime p (note that the converse is trivially true). In other words, to determine whether a quadratic form Q has a rational solution, we can instead study it over $\mathbb{Q}_p$, where things become much simpler due to Hensel's Lemma, that allows us to instead work over the finite field $\mathbb{F}_p$. The local-to-global principle, however, can fail for positive genus curves. A famous example due to Selmer [15] is the homogeneous cubic

$$3x^3 + 4y^3 + 5z^3 = 0,$$

which has nontrivial solutions over $\mathbb{R}$ and $\mathbb{Q}_p$ for each prime p, but fails to have a rational solution. We will later on, further emphasize this perspective, since it plays an important role in the computation of rational points on elliptic curves. For now, let us begin by recalling basic facts about elliptic curves.

2. Elliptic Curves

2.1. **Basic terminology.** Though we will assume the basic theory of elliptic curves covered in Silverman's excellent book [16], we set out the basic definitions and notation. Throughout this exposition, K refers to a perfect field (possibly with further constraints).

Definition 2.1. An elliptic curve E/K is a smooth projective curve of genus 1 defined over K with a distinguished point O having coordinates in K.

Let $\bar{K}$ denote the algebraic closure of K. It can be shown that E/K is isomorphic to a projective variety in $\mathbb{P}^2(\bar{K})$ that has the form

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

with $a_1, \ldots, a_6 \in K$. We can dehomogenize this equation to

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

and studied in $\mathbb{A}^2(\bar{K})$, keeping in mind there is a point at infinity $O = [0, 1, 0]$. This is the Weierstrass form of E. An important quantity associated to E/K is its discriminant

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$

where

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{aligned}$$

The assumption that E/K is smooth translates precisely to the fact that $\Delta \neq 0$. It's a fascinating and surprising fact that the points of E form an abelian group under an addition operation with O acting as the identity (see [16, Ch. 3] for how the addition is defined). We denote the subgroup of points $P \in E$ that satisfy $[m]P = O$, $m \in \mathbb{Z}$, as $E[m]$. Throughout this article, we will similarly denote the kernel of any map $\phi : A \to B$ by $A[\phi]$.

The K-rational points $E(K)$ of E is the group of points $(x, y) \in E$ with coordinates $x, y \in K$ and is called the Mordell-Weil group of E. Note that $O \in E(K)$. When K is a number field, the Mordell-Weil Theorem asserts that $E(K)$ is a finitely generated group. The structure theorem for finitely generated $\mathbb{Z}$-modules then implies

$$E(K) \simeq \mathbb{Z}^r \times E_{\text{tors}}(K),$$

where $E_{\text{tors}}(K)$ is the (finite) torsion subgroup of $E(K)$.

The key first step in the proof is the weak Mordell-Weil Theorem, which says $E(K)/mE(K)$ is a finite group for all positive integers m. The subsequent proof of the Mordell-Weil Theorem is almost entirely constructive [16, Ch. 8], except at one step, where we assume we have coset representatives for $E(K)/mE(K)$. Finding these representatives turns out to be a difficult problem and presently no general algorithm is known to solve it. More to the point, the main difficulty is in determining the rank r; we can calculate $E_{\text{tors}}(K)$ easily in most cases. In particular, we can gain global torsion information through local reduction. Let K_v be the completion of K with respect to a discrete valuation v and let k_v be the residue field of K_v.

Proposition 2.2. *Suppose the reduced curve $\tilde{E}/k_v$ is smooth and $m \in \mathbb{Z}_{\geq 2}$ is coprime to* $\text{char}(k_v)$. *Then the natural reduction map*

$$E(K_v)[m] \to \tilde{E}(k_v)$$

is injective.

Proof. This is Proposition 3.1 in Chapter 7 of [16]. □

In other words, $E(K_v)[m]$ is isomorphic to a subgroup of $\tilde{E}(k_v)$. This fact is useful since $K \hookrightarrow K_v$ is injective.

Example 2.3. To illustrate the calculation of $E_{\text{tors}}(K)$, consider

$$E/\mathbb{Q} : y^2 = x^3 - 2.$$

We have $\Delta = -2^6 \cdot 3^3$, and so $E/\mathbb{Q}_p$ has stable reduction for all primes $p \notin \{2, 3\}$. Then reducing mod 5, we compute $\#\tilde{E}(\mathbb{F}_5) = 6$ (for instance, at $x \equiv 0 \pmod 5$, $y^2 \equiv 3 \pmod 5$, which has no solutions by quadratic reciprocity, while at $x \equiv 1 \pmod 5$, we have $y \equiv 2, 3 \pmod 5$). Similarly, $\#\tilde{E}(\mathbb{F}_7) = 7$. Since the orders are coprime, we conclude $E_{\text{tors}}(\mathbb{Q}) = \{O\}$ is trivial.

To calculate torsion, we might have instead used the Nagell-Lutz Theorem [16, Ch. 8, Cor. 7.2] that provides strong necessary conditions for a point to be in $E_{\text{tors}}(K)$. However, Proposition 2.2 illustrates a key idea in the method to compute $E(K)$ - we will ultimately rely on the relative ease of checking if solutions exist to certain equations over finite fields. This strategy is the so-called "method of descent," since we are reducing a difficult Diophantine problem over a global field to several easier problems over a finite field.

There are two kinds of descents at play here. The first one is a descent of base fields and is the kind we will mostly see done in this article since we successively reduce from a global to a local to a finite field. The second kind is, *à la* Fermat, the one the reader might be more familiar with – the delightful fact is that it forms the basis for the theory of heights, which provides the essential foundation for the passage from the weak to the full Mordell-Weil Theorem. So, ultimately, both kinds of descents are being used!

2.2. **Overview of strategy.** Let us give a high-level overview of the strategy to compute $E(K)$ and introduce the main characters of the story. Needless to say, this summary glosses over many details but we hope it motivates why we should care about cohomology or homogeneous spaces.

What we want to do is construct a nice "covering" of E

$$\bigcup_d \psi_d(C_d) = E,$$

where each C_d is some curve over K and $\psi_d : C_d \to E$ is a morphism. Now, a morphism in general *does not* preserve K-rational points, so calculating points in $C_d(K)$ does not necessarily give us points in $E(K)$. But, if C_d is chosen sufficiently nice relative to E, then we can find a different elliptic curve E' such that there exists a nonzero *isogeny* $\phi : E \to E'$ for which $\phi \circ \psi$ is defined over K, i.e., $\phi \circ \psi$ preserves K-rational points:

$$C_d(K) \xrightarrow{\psi_d} E \xrightarrow{\phi} E'(K).$$

To compute K-rational points on E, we can reverse the roles of E and E'. Now, computing $C_d(K)$ is essentially as difficult as computing $E(K)$ (as we will see, C_d is isomorphic to E over $\bar{K}$ and so has genus 1, meaning $C_d(K)$ need not be finite). But, checking whether $C_d(K)$ is non-empty is a slightly more reasonable task. This is also why we need to study multiple C_d's even though a single $C_d(K)$ would be surjective on $E'(K)$ (nonconstant morphisms of curves are surjective).

The first step towards reducing towards this simpler problem is to focus on computing $E(\mathbb{Q})/mE(\mathbb{Q})$ for some $m > 1$. Computing generators for $E(\mathbb{Q})/mE(\mathbb{Q})$ allows us to compute $E(\mathbb{Q})$ by retracing the proof of the Mordell-Weil Theorem. So, we can take $E = E'$ and $\phi = [m]$. Ideally, we want there to be a one-to-one correspondence between these nice curves C_d's and elements of $E(\mathbb{Q})/mE(\mathbb{Q})$ - if C_d has a K-rational point then using the parameter d, we deduce an element of $E(\mathbb{Q})/mE(\mathbb{Q})$.

How does one go about finding these magical C_d? The curves we are looking for are called *homogeneous spaces* of E: they are $\bar{K}$-isomorphic to E and E has a simply transitive action on them. The collection of these homogeneous spaces (up to a nice K-isomorphism) form the *Weil-Châtelet group* $WC(E/K)$. The group $WC(E/K)$ can be quite unwieldy but it is in correspondence with the *first cohomology group* $H^1(G_{\bar{K}/K}, E)$ of E, which allows us to think about homogeneous

spaces concretely. Using Galois cohomology, we will show $E(K)/mE(K)$ embeds into the smaller cohomology group $H^1(G_{\bar{K}/K}, E[m])$. In fact, $E(K)/mE(K)$ embeds into an even smaller *finite* subgroup of $H^1(G_{\bar{K}/K}, E[m])$ called the *Selmer group*.

The Selmer group, via the correspondence between cohomology and homogeneous spaces, helps reduce the large search space of $WC(E/K)$ to a *finite* set of homogeneous spaces C_d's parameterized by a certain set of d's. It turns out, we have to check whether each of these C_d's has a K_v-rational point for each valuation v, and if it does, we obtain an element of the Selmer group. Once we have calculated the Selmer group, to recover $E(K)/mE(K)$, we check which of the homogeneous spaces have a K-rational point. These homogeneous spaces then form the "covering" we were looking for. It be can seen from the theory of heights (not discussed here), and as we will see in practice, there is good reason to think that finding rational points on C_d will be easier. The maps $\phi \circ \psi_d$ with, say, degree n will locally behave like the power map $x \mapsto x^n$, essentially meaning that a K-rational point P on E' will correspond to a K-rational point on C_d whose *height* is scaled down by an order of n. Thus, if C_d has K-rational points, it is often easy to find at least one.

We will be focusing our efforts on elliptic curves over $\mathbb{Q}$ that have at least one rational torsion point of order 2. This is not as restrictive as it might sound. It is a famous theorem of Mazur [10] that $E_{\text{tors}}(\mathbb{Q})$ is isomorphic to one of the following:

- $\mathbb{Z}/n\mathbb{Z}$ for $1 \leq n \leq 10$ or $n = 12$
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ for $1 \leq n \leq 4$.

So, the method we will study does not apply for those elliptic curves with $E_{\text{tors}}(\mathbb{Q})$ equal to $\mathbb{Z}/n\mathbb{Z}$ for $n = 1, 3, 5, 7, 9$. But, the method may be adapted to work for these other cases, as we demonstrate when $n = 3$ in Example 8.5, though the computation becomes more intricate.

We start with an introduction to basic group cohomology because, as we noted above, it provides the basic tools to work with the auxiliary curves that are of interest to us. Further, Example 3.3 provides a more direct glimpse of the relevance of cohomology to parameterizing rational points.

3. Group Cohomology

We mainly need H^0 and H^1 for our purposes (we need H^2 just once, in Example 8.5), and so we explain them with separate definitions. There is, however, a general definition that unifies the two definitions, for which the reader can refer to [1] or [7, Ch. 6].

3.1. **Finite Group Cohomology.** Let G be a finite group and let M be an abelian group acted upon by G. The action of $\sigma \in G$ is denoted $m \mapsto m^\sigma$. In this subsection, a simple example to have in mind is a Galois number field $M = K/\mathbb{Q}$ and $G = \text{Gal}(K/\mathbb{Q})$.

The 0^{th} cohomology group of M, denoted $H^0(G, M)$, is

$$H^0(G, M) = \{m \in M : m^\sigma = m \text{ for all } \sigma \in G\}.$$

So, $H^0(G, M)$ is the part of M on which the action of G is trivial.

Next, the group of 1-cochains $C^1(G, M)$ is the set of all maps from G to M under addition. Within $C^1(G, M)$ we have the subgroup of 1-cocycles $Z^1(G, M)$ defined as the set of all maps $\xi : G \to M$ satisfying

$$\xi_{\sigma\tau} = \xi_\sigma^\tau + \xi_\tau, \text{ for all } \sigma, \tau \in G.$$

(In more conventional function notation, this would read $\xi(\sigma\tau) = \tau(\xi(\sigma)) + \xi(\tau)$.) Note that this condition says ξ is almost a group homomorphism, but not quite because it is being "twisted" by τ (it is a "crossed homomorphism"). Within $C^1(G, M)$ we also have the subgroup of 1-coboundaries $B^1(G, M)$ that is the set of all maps $\xi : G \to M$ for which there exists a point $Q \in M$ such that

$$\xi_\sigma = Q^\sigma - Q, \text{ for all } \sigma \in G.$$

For example, if $Q \in H^0(G, M)$, then $Q^\sigma - Q$ is just the zero map. Note that since M is abelian, $C^1(G, M)$ is abelian too. Further, we can check that every 1-coboundary $\xi : \sigma \mapsto Q^\sigma - Q$ is automatically a 1-cocycle:

$$\xi_{\sigma\tau} = Q^{\sigma\tau} - Q = (Q^\sigma - Q)^\tau + (Q^\tau - Q) = \xi_\sigma^\tau - \xi_\tau.$$

So, we can form the quotient group $H^1(G, M) = Z^1(G, M)/B^1(G, M)$ that is the 1^{st} cohomology group.

Example 3.1. To get some basic intuition, suppose G acts trivially on M. Then, $H^0(G, M) = M$. Further, $Z^1(G, M)$ is just the set of group homomorphisms $\mathrm{Hom}(G, M)$ and $B^1(G, M) = \{0\}$, implying that $H^1(G, M) = \mathrm{Hom}(G, M)$.

Example 3.2. Let us compute with $M = \mathbb{Q}(\sqrt{d})$, where d is a squarefree integer, and $G = \mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$. Since $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ is a Galois extension, $H^0(G, M) = \mathbb{Q}$. What is $Z^1(G, M)$? Note that $G \simeq \mathbb{Z}/2\mathbb{Z}$ has only two elements, the trivial automorphism 1 and the automorphism σ that exchanges $\sqrt{d}$ with $-\sqrt{d}$. So if $\xi \in Z^1$, it satisfies

$$\xi_1 = \xi_{1\cdot 1} = \xi_1^1 + \xi_1 = 2\xi_1,$$

and so $\xi_1 = 0$. Similarly,

$$0 = \xi_1 = \xi_{\sigma\cdot\sigma} = \xi_\sigma^\sigma + \xi_\sigma,$$

and so $\xi_\sigma^\sigma = -\xi_\sigma$, from which we conclude that $\xi_\sigma = q\sqrt{d}$ for some $q \in \mathbb{Q}$. Thus, observe that

$$\xi_\tau = (1 - \frac{q}{2}\sqrt{d})^\tau - (1 - \frac{q}{2}\sqrt{d}),$$

for all $\tau \in G$, meaning that ξ is also a 1-coboundary, and so $H^1(G, M) = 0$.

The result of the previous example is, in fact, a special case of the extremely useful result known as Hilbert's Theorem 90, that says $H^1(\mathrm{Gal}(L/K), L)$ and $H^1(\mathrm{Gal}(L/K), L^\times)$ are both trivial [7, Ch. 6, Thm 10.1].

Example 3.3. Let us see an example that helps motivate why cohomology should be relevant to computing rational points. Returning to our example of the circle in Section 1, suppose we want to find rational solutions to the slightly more general

$$C : x^2 + dy^2 = 1,$$

where $d \in \mathbb{Z}$ is squarefree. Then, working in $L = \mathbb{Q}(\sqrt{-d})$, we can factor C as

$$(x + \sqrt{-d}y)(x - \sqrt{-d}y) = 1.$$

Letting N denote the norm map of $L/\mathbb{Q}$, we notice from this factorisation that each rational point $(x, y) \in C(\mathbb{Q})$ corresponds to the element $\alpha = x + y\sqrt{-d} \in L$ such that $N(\alpha) = 1$. Now, given $\alpha \in L$ with $N(\alpha) = 1$, we can define the 1-cocycle $\hat{\alpha} \in H^1(\mathrm{Gal}(L/\mathbb{Q}), L^\times)$

$$\tau \mapsto \begin{cases} 1 & \tau = 1 \\ \alpha & \tau = \sigma, \end{cases}$$

where 1 is the identity and σ is the nontrivial automorphism on L. We can check that $\hat{\alpha}$ is really a cocycle - the interesting verification is this one:

$$1 = \hat{\alpha}_1 = \hat{\alpha}_{\sigma\cdot\sigma} = \hat{\alpha}_\sigma^\sigma \cdot \hat{\alpha}_\sigma = \alpha^\sigma \cdot \alpha = N(\alpha) = 1.$$

But, by Hilbert's Theorem 90, $H^1(\mathrm{Gal}(L/\mathbb{Q}), L^\times)$ is trivial, so $\hat{\alpha}$ is actually a 1-coboundary, and thus there exists an element $\beta \in L^\times$ such that $\hat{\alpha}_\tau = \beta^\tau/\beta$. Taking $\beta = a - b\sqrt{-d}$ for some $a, b \in \mathbb{Q}$ and $\tau = \sigma$, we get

$$x + y\sqrt{-d} = \alpha = \frac{\beta^\sigma}{\beta} = \frac{a + b\sqrt{-d}}{a - b\sqrt{-d}} = \frac{a^2 - bd^2}{a^2 + bd^2} + \frac{2ab}{a^2 + bd^2}\sqrt{-d}.$$

Thus, we recover the parameterization of rational points on C

$$x = \frac{a^2 - b^2d^2}{a^2 + b^2d^2} \text{ and } y = \frac{2ab}{a^2 + b^2d^2}.$$

This can certainly feel magical at first glance, but it can help to see what is really happening under the hood. Given $\alpha \in L$ with $N(\alpha) = 1$, what we ultimately want to show is $\alpha = \beta/\beta^\sigma$ for some $\beta \in L$ (β can be exchanged with β^σ). But, note that this is the same as requiring 1 to be an eigenvalue of the linear map $T : \lambda \mapsto \alpha \cdot \lambda^\sigma : L \to L$. With the standard $\mathbb{Q}$-basis, T is represented by the matrix

$$T = \begin{bmatrix} x & yd \\ y & -x \end{bmatrix},$$

which can be easily checked to have 1 as an eigenvalue given that $N(\alpha) = x^2 + dy^2 = 1$.

A short exact sequence of G-modules

$$0 \to P \xrightarrow{\phi} M \xrightarrow{\psi} N \to 0,$$

is a diagram in which ϕ and ψ are G-homomorphisms (i.e., they commute with the action of G), ϕ is injective, ψ is surjective, and $\mathrm{im}(\phi) = \ker(\psi)$. Whenever we have an exact sequence of G-modules, we get free information about their cohomology groups. Specifically, the following induced sequence is exact:

$$0 \to H^0(G, P) \to H^0(G, M) \to H^0(G, N) \xrightarrow{\delta} H^1(G, P) \to H^1(G, M) \to H^1(G, N). \tag{3.4}$$

Here the connecting homomorphism δ is defined as follows. It maps $n \in H^0(G, N)$ to the cohomology class $\{\xi\} \in H^1(G, P)$ defined by $\xi_\sigma = m^\sigma - m$ for some $m \in \psi^{-1}(n)$ (ψ is surjective). We should check that $\xi \in Z^1(G, P)$ (after all $m \in M$). First, let us check $m^\sigma - m \in P$ (technically $\phi(P)$, but ϕ is injective) for all $\sigma \in G$. Indeed, since $n \in H^0(G, N)$, we have

$$\psi(m^\sigma - m) = \psi(m)^\sigma - \psi(m) = n^\sigma - n = 0,$$

and so $m^\sigma - m \in \ker(\psi) = \mathrm{im}(\phi) = P$. Next, we have

$$\xi_{\sigma\tau} = m^{\sigma\tau} - m = (m^\sigma - m)^\tau + (m^\tau - m) = \xi_\sigma^\tau + \xi_\tau,$$

and so $\xi \in Z^1(G, P)$, as asserted.

Since the remaining terms can be checked in a similar fashion, here we will only verify that exactness holds in

$$H^1(G, P) \to H^1(G, M) \to H^1(G, N).$$

So, we have to check the kernel of the second map is equal to the image of the first map. Suppose $\xi \in H^1(G, P)$. Then, since $\psi \circ \phi = 0$, we have $\psi \circ \phi \circ \xi = 0 \in B^1(G, N)$. Next, let $\{\xi\} \in H^1(G, M)$ be such that $\psi \circ \xi \in B^1(G, N)$, so that $(\psi\xi)_\sigma = n^\sigma - n$ for some $n \in N$. Fix $m \in M$ such that $\psi(m) = n$. Consider the 1-cocycle $\chi_\sigma = \xi_\sigma + m - m^\sigma \in \{\xi\}$. We have

$$(\psi\xi)_\sigma = (n^\sigma - n) + (n - n^\sigma) = 0,$$

and so $\mathrm{im}(\chi) \subseteq \ker(\psi) = \mathrm{im}(\phi)$. Thus, χ is really a 1-cocycle from G to $\mathrm{im}(\phi)$, as we wanted to show.

Next, suppose H is a subgroup of G. Then, each 1-cochain $G \to M$ can naturally be restricted $H \to M$, preserving cocycles and coboundaries. We obtain the restriction homomorphism

$$\mathrm{Res} : H^1(G, M) \to H^1(H, M).$$

Further, suppose H is normal in G, so that G/H has a well-defined action on $H^0(H, M)$. If $\xi : G/H \to H^0(H, M)$ is a 1-cochain, we obtain we obtain a 1-cochain ξ from G to M by composing with the quotient projection map:

$$\xi : G \to G/H \xrightarrow{\xi} H^0(H, M) \subseteq M.$$

So, we get the inflation homomorphism

$$\mathrm{Inf} : H^1(G/H, H^0(H, M)) \to H^1(G, M).$$

It is a straightforward verification that everything works as we expect when we compose Inf and Res. More precisely, the following sequence is exact:

$$0 \to H^1(G/H, H^0(H, M)) \xrightarrow{\mathrm{Inf}} H^1(G, M) \xrightarrow{\mathrm{Res}} H^1(H, M). \tag{3.5}$$

3.2. **Galois Cohomology.** Let $G_{\bar{K}/K}$ denote the Galois group $\mathrm{Gal}(\bar{K}/K)$ of $\bar{K}$ over K. Recall that $G_{\bar{K}/K}$ has the profinite topology and so the subgroups of finite index form a basis for its topology.

An abelian group M is a discrete $G_{\bar{K}/K}$-module if $G_{\bar{K}/K}$ acts *continuously* on M with respect to the profinite topology on $G_{\bar{K}/K}$ and the discrete topology on M: for each $m \in M$, its stabilizer $\{\sigma \in G_{\bar{K}/K} : m^\sigma = m\}$ is a subgroup of finite index in $G_{\bar{K}/K}$. So, observe that $\bar{K}$ is a $G_{\bar{K}/K}$-module, since for every $\alpha \in \bar{K}$, the index of the stabilizer of α is bounded by the degree of the finite extension $K(\alpha)/K$.

Let M be a discrete $G_{\bar{K}/K}$-module. The 0^{th} cohomology group $H^0(G_{\bar{K}/K}, M)$ is defined exactly as for finite G. The definition of $H^1(G_{\bar{K}/K}, M)$ has some extra restrictions. Particularly, we are interested in only the *continuous* 1-cochains $G_{\bar{K}/K} \to M$: the fiber of each $m \in M$ should be a finite index subgroup in $G_{\bar{K}/K}$. The group of continuous 1-cocycles $G_{\bar{K}/K} \to M$ is denoted $Z^1_{\mathrm{cont}}(G_{\bar{K}/K}, M)$. Note that since M is discrete, the 1-coboundaries $G_{\bar{K}/K} \to M$ are automatically continuous. The 1^{st} cohomology group is then defined as

$$H^1(G_{\bar{K}/K}, M) = Z^1_{\mathrm{cont}}(G_{\bar{K}/K}, M)/B^1(G_{\bar{K}/K}, M).$$

We will soon be reinterpreting this cohomology group as a more interesting object when M is an elliptic curve.

An exact sequence completely analogous to (3.4) holds for the cohomology of discrete $G_{\bar{K}/K}$-modules too. We can also generalize Res and Inf. Let L/K be a finite Galois extension, so that $G_{\bar{K}/L} = \mathrm{Gal}(\bar{K}/L)$ is a normal subgroup of finite index in $G_{\bar{K}/K}$. Since a discrete $G_{\bar{K}/K}$-module is also a discrete $G_{\bar{K}/L}$-module, we obtain

$$\mathrm{Res} : H^1(G_{\bar{K}/K}, M) \to H^1(G_{\bar{k}/L}, M).$$

Next, $H^0(G_{\bar{K}/L}, M)$ has a well-defined action on it by $G_{L/K} = G_{\bar{K}/K}/G_{\bar{K}/L}$, and so we obtain the inflation of a 1-cocycle $\xi : G_{L/K} \to H^0(G_{\bar{K}/L}, M)$ by composing it with the projection map $G_{\bar{K}/K} \to G_{L/K}$. The Galois analogue of (3.5) and Hilbert's Theorem 90 also hold.

Example 3.6. Let us compute $H^1(G_{\bar{K}/K}, \mu_n)$, which will also be useful later on. Let μ_n denote the subgroup of n-th roots of unity in $\bar{K}$. Then we have the short exact sequence of discrete $G_{\bar{K}/K}$-modules

$$1 \to \mu_n \to \bar{K}^\times \xrightarrow{n} \bar{K}^\times \to 1,$$

where n is the power map $\alpha \mapsto \alpha^n$. Applying Galois cohomology (3.4), we obtain

$$1 \to H^0(G_{\bar{K}/K}, \mu_n) \to K^\times \xrightarrow{n} K^\times \xrightarrow{\delta} H^1(G_{\bar{K}/K}, \mu_n) \to H^1(G_{\bar{K}/K}, \bar{K}^\times) \xrightarrow{n} H^1(G_{\bar{K}/K}, \bar{K}^\times).$$

Focusing on $H^1(G_{\bar{K}/K}, \mu_n)$, we see it is surjective on the kernel $H^1(G_{\bar{K}/K}, \bar{K}^\times)[n]$ via the map induced by the inclusion $Z^1_{\text{cont}}(G_{\bar{K}/K}, \mu_n) \hookrightarrow Z^1_{\text{cont}}(G_{\bar{K}/K}, \bar{K}^\times)$. Note that the induced map is not injective because distinct cohomology classes in $H^1(G_{\bar{K}/K}, \mu_n)$ might collapse to a single class in $H^1(G_{\bar{K}/K}, \bar{K}^\times)$ given the new 1-coboundaries that can be formed by the points of $\bar{K}^\times \setminus \mu_n$. Indeed, the kernel of the induced map is the image of δ, which we see is $K^\times/K^{\times n}$. In other words, we obtain a short exact sequence

$$1 \to K^\times/K^{\times n} \xrightarrow{\delta} H^1(G_{\bar{K}/K}, \mu_n) \to H^1(G_{\bar{K}/K}, \bar{K}^\times)[n] \to 1. \tag{3.7}$$

However, by Hilbert's Theorem 90, we know $H^1(G_{\bar{K}/K}, \bar{K}^\times)$ is trivial, and so we obtain an isomorphism of groups

$$H^1(G_{\bar{K}/K}, \mu_n) \simeq K^\times/K^{\times n}. \tag{3.8}$$

Moreover, Galois cohomology also tells us how to calculate the isomorphism δ. It maps each $\{\alpha\} \in K^\times/K^{\times n}$ to the cohomology class $\{\sigma \mapsto \beta^\sigma/\beta\}$, where $\beta \in \bar{K}^\times$ is such that $\beta^n = \alpha$.

4. Twisting

As we mentioned in Section 2, homogeneous spaces of an elliptic curve E are fundamentally curves isomorphic to E over $\bar{K}$. In this section, we begin to establish the connection between cohomology and isomorphism classes of an elliptic curve.

Let C_1/K and C_2/K be curves, and let $\bar{K}(C_1)$ denote the function field of C_1. A morphism $\phi : C_1 \to C_2$ is said to be *defined over* K if ϕ has the form $[f_0, f_1, f_2]$ for some regular $f_i \in \bar{K}(C_1)$ such that there exists $\lambda \in \bar{K}^\times$ for which $\lambda f_i \in K(C_1)$ for $i = 0, 1, 2$.

Definition 4.1. A twist of an elliptic curve E/K is a smooth curve C/K isomorphic to E over $\bar{K}$. Further, identify two twists C_1 and C_2 of E if C_1 and C_2 are isomorphic over K. The set of twists of E under this equivalence relation is denoted $\text{Tws}(E/K)$.

The following result gives us a useful characterization for K-isomorphisms.

Lemma 4.2. *Let V_1 and V_2 be projective varieties defined over K embedded in $\mathbb{P}^n(\bar{K})$ and let $\phi : V_1 \to V_2$ be a morphism. Then ϕ is defined over K if and only if $\phi^\sigma = \phi$ for all $\sigma \in G_{\bar{K}/K}$.*

Proof. The forward implication is clear. So, suppose $\phi^\sigma = \phi$ for all $\sigma \in G_{\bar{K}/K}$. Write $\phi = [f_0, \ldots, f_n]$ with $f_i \in \bar{K}(V_1)$. For each $\sigma \in G_{\bar{K}/K}$, we can then fix $\lambda_\sigma \in \bar{K}^\times$ such that $f_i^\sigma = \lambda_\sigma f_i$ for all i. Consider the 1-cochain $\xi : G_{\bar{K}/K} \to \bar{K}^\times$ given by $\sigma \mapsto \lambda_\sigma$. We check that ξ is indeed a 1-cocycle:

$$\lambda_\sigma^\tau \lambda_\tau f_i = \lambda_\sigma^\tau f_i^\tau = (\lambda_\sigma f_i)^\tau = f_i^{\sigma\tau} = \lambda_{\sigma\tau} f_i.$$

However, by Hilbert's Theorem 90, $H^1(G_{\bar{K}/K}, \bar{K}^\times) = 0$, and so there exists $\alpha \in \bar{K}^\times$ such that $\lambda_\sigma = \alpha^\sigma/\alpha$ for all $\sigma \in G_{\bar{K}/K}$. Observe that

$$(\alpha^{-1} f_i)^\sigma = \alpha^{-\sigma} \lambda_\sigma f_i = \alpha^{-1} f_i,$$

for all $\sigma \in G_{\bar{K}/K}$. So, we have reduced the equality in projective space to one in the function field $\bar{K}(V_1)$. The conclusion will then follow once we show if some $f \in \bar{K}[V_1]$ satisfies $f^\sigma = f$ for all $\sigma \in G_{\bar{K}/K}$, then $f \in K[V_1]$. Let $F \in \bar{K}[X] := \bar{K}[x_1, \ldots, x_n]$ be such that $F \equiv f \pmod{I(V_1)}$. Then consider the 1-cochain $\chi : G_{\bar{K}/K} \to I(V_1)$ given by $\sigma \mapsto F^\sigma - F$ (it is indeed into $I(V_1)$ because V_1 is defined over K). Since

$$F^{\sigma\tau} - F = (F^\sigma - F)^\tau + (F^\tau - F),$$

χ is a 1-cocycle. By Hilbert's Theorem 90, $H^1(G_{\bar{K}/K}, I(V_1))$ is trivial, and so there exists $G \in I(V_1)$ such that $F^\sigma - F = G^\sigma - G$ for all $\sigma \in G_{\bar{K}/K}$. Thus, $(F-G)^\sigma = F - G$, and so $F - G \in K[X]$, meaning that $f \in K[V_1]$. □

This lemma gives us a way to "measure" how far an isomorphism $\phi : C \to E$ is from being defined over K. Denote by $\mathrm{Aut}(E)$ the set of isomorphisms $E \to E$. We consider the 1-cochain $\xi : G_{\bar{K}/K} \to \mathrm{Aut}(E)$ given by $\xi_\sigma = \phi^\sigma \phi^{-1}$. Note that ξ is a 1-cocycle. Further, we can show ξ is invariant (up to 1-coboundaries) over the equivalence class of ϕ in $\mathrm{Tws}(E/K)$ so that we get a well-defined map $\mathrm{Tws}(E/K) \to H^1(G_{\bar{K}/K}, \mathrm{Aut}(E))$.

Proposition 4.3. *Let C/K be a twist of E/K and let $\phi : E' \to E$ be an isomorphism. Let $\xi : G_{\bar{K}/K} \to \mathrm{Aut}(E)$ be the 1-cocycle $\xi_\sigma = \phi^\sigma \phi^{-1}$. Then the cohomology class $\{\xi\}$ is determined by the K-isomorphism class of C (and is therefore also independent of the choice of ϕ).*

Proof. Let C'/K be another twist of E such that C' and C are K-isomorphic. Fix an isomorphism $\psi : C' \to E$ and a K-isomorphism $\pi : C \to C'$ (so $\pi^\sigma = \pi$). Let $\alpha = \phi\pi\psi^{-1}$. We have

$$\alpha^\sigma(\psi^\sigma\psi^{-1}) = \phi^\sigma\pi^\sigma\psi^{-1} = \phi^\sigma\pi\psi^{-1} = (\phi^\sigma\phi^{-1})\alpha.$$

So, $\psi^\sigma\psi^{-1}$ and $\phi^\sigma\phi^{-1}$ are off by a 1-coboundary, and thus belong to the same cohomology class. □

Denote this map by $\mathcal{L} : \mathrm{Tws}(E/K) \to H^1(G_{\bar{K}/K}, \mathrm{Aut}(E))$. We have this surprising result:

Theorem 4.4. *The map $\mathcal{L}$ is a bijection.*

Proof. First let us prove injectivity. Suppose C/K and C'/K are twists of E/K with isomorphisms ϕ and ψ respectively, such that $\mathcal{L}(\{C\}) = \mathcal{L}(\{C'\})$. Then there exists $\alpha \in \mathrm{Aut}(E)$ such that

$$\alpha^\sigma\psi^\sigma\psi^{-1} = \phi^\sigma\phi^{-1}\alpha.$$

We then claim the $\bar{K}$-isomorphism $\pi = \phi^{-1}\alpha\psi : C' \to C$ is in fact a K-isomorphism. Indeed, we have

$$\pi^\sigma = (\phi^{-1}\alpha\psi)^\sigma = (\phi^{-1})^\sigma(\alpha^\sigma\psi^\sigma\psi^{-1})\psi = (\phi^{-1})^\sigma(\phi^\sigma\phi^{-1}\alpha)\psi = \phi^{-1}\alpha\psi = \pi,$$

and so π is a K-isomorphism by Lemma 4.2.

Proving surjectivity requires a bit more work, including a few facts from algebraic geometry. Let us fix a 1-cocycle $\xi : G_{\bar{K}/K} \to \mathrm{Aut}(E)$. We have to show there exists a twist C/K of E that is mapped to $\{\xi\}$ by $\mathcal{L}$. The main idea is to define a field $\bar{K}(E)_\xi$ isomorphic to $\bar{K}(E)$ by an isomorphism $Z : \bar{K}(E) \to \bar{K}(E)_\xi$ that it is twisted by σ,

$$Z(f)^\sigma = Z(f^\sigma\xi_\sigma).$$

Note that this allows for a well-defined isomorphism since

$$(Z(f)^\sigma)^\tau = Z(f^\sigma\xi_\sigma)^\tau = Z((f^\sigma\xi_\sigma)^\tau\xi_\tau) = Z(f^{\sigma\tau}(\xi_\sigma^\tau\xi_\tau)) = Z(f^{\sigma\tau}\xi_{\sigma\tau}) = Z(f)^{\sigma\tau}.$$

Let $F = H^0(G_{\bar{K}/K}, \bar{K}(E)_\xi)$ be the fixed field of $\bar{K}(E)_\xi$. We now argue that F is the function field of the required twist C.

First, note that $F \cap \bar{K} = K$. Indeed, suppose $Z(f) \in F \cap \bar{K}$. Then, since an isomorphism of function fields restricts to an automorphism of $\bar{K}$, we have $f \in \bar{K}$ is a constant function. Thus, because $Z(f)$ is fixed by $G_{\bar{K}/K}$,

$$Z(f) = Z(f)^\sigma = Z(f^\sigma\xi_\sigma) = Z(f^\sigma),$$

for all $\sigma \in G_{\bar{K}/K}$, and so $f \in K$.

Next, we argue that the compositum of fields $\bar{K} \cdot F = \bar{K} \otimes_K F$ is $\bar{K}(E)_\xi$. Showing this will allow us to conclude that F has transcendence degree 1 over K (because E has dimension 1 and so $\bar{K}(E) \simeq \bar{K}(E)_\xi$ has transcendence degree 1). So, take an element $v \in \bar{K}(E)_\xi$. We wish to show v

can be written as a $\bar{K}$-linear combination of elements in F. Since $\bar{K}(C)_\xi$ is a discrete $G_{\bar{K}/K}$-module, the stabilizer of v is a finite index subgroup in $G_{\bar{K}/K}$ corresponding to a finite field extension L/K such that $\bar{K}/L$ is Galois. Let L'/K be the Galois closure of L/K. Let $\{e_1, \ldots, e_n\}$ be a K-basis for L' and let $\mathrm{Gal}(L'/K) = \{\sigma_1, \ldots, \sigma_n\}$. Consider the elements $w_i \in \bar{K}(E)_\xi$ defined by

$$w_i = \sum_{j=1}^{n} (e_i v)^{\sigma_j},$$

for $i = 1, \ldots, n$. Note that each w_i is invariant under the action of $\mathrm{Gal}(L'/K)$ (w_i is just the trace of $e_i v$), and we already know $G_{\bar{K}/L'}$ fixes the e_i and v, meaning that $w_i \in F$. Further, note that $(\det(e_i^{\sigma_i}))^2$ is the discriminant of the basis $\{e_1, \ldots, e_n\}$ and so must be nonzero [11, Ch. 1, Prop. 2.8]. Thus, inverting the matrix $(e_i^{\sigma_i})$, we see that v (and the other v^{σ_i}) are $\bar{K}$-linear combinations of the elements $w_i \in F$.

So, from the fact that $F \cap \bar{K} = K$ and F has transcendence degree 1 over K, we conclude there exists a smooth projective curve C/K with function field $K(C) \simeq F$. So, we have

$$\bar{K}(C) \simeq \bar{K} \cdot F = \bar{K}(E)_\xi \simeq \bar{K}(E)$$

and thus C/K is isomorphic over $\bar{K}$ to E/K (see [4, Ch. 1, §6]).

Finally, we need to check that $\mathcal{L}(\{C\}) = \{\xi\}$. Fix an isomorphism $\phi : C \to E$ that gives us the isomorphism $Z : \bar{K}(E) \to \bar{K}(E)_\xi$ via $f \mapsto f \circ \phi$. So, the condition $Z(f)^\sigma = Z(f^\sigma \xi_\sigma)$ reads $f^\sigma \phi^\sigma = f^\sigma \xi_\sigma \phi$, for all $f \in \bar{K}(C)$, implying that $\xi_\sigma = \phi^\sigma \phi^{-1}$, as required. □

5. Homogeneous Spaces

Definition 5.1. Let E/K be an elliptic curve. A homogeneous space for E/K is a smooth projective curve C/K with a morphism $\mu : C \times E \to C$ over K defining a simply transitive group action on C:

(1) (Identity) $\mu(p, O) = p$ for all $p \in C$.
(2) (Associativity) $\mu(\mu(p, P), Q) = \mu(p, P + Q)$ for all $p \in C$ and $P, Q \in E$.
(3) (Transitivity) For all $p, q \in C$ there is a unique $P \in E$ such that $\mu(p, P) = q$.

We will denote the action of μ as an addition. With this interpretation, the second condition reads

$$p + (P + Q) = (p + P) + Q,$$

where we should be aware that on the left side, the first addition is using μ and the second is the usual group law on E. The simple transitivity allows us to define a subtraction map $\nu : C \times C \to E$ sending a pair $(q, p) \in C \times C$ to the unique $P \in E$ such that $p + P = q$. We will similarly denote the action of ν as $q - p = P$. We can easily verify that the intuition afforded by using the notations $+$ and $-$ will not lead us astray. For instance, is it true that, for points $p_0, p, q \in C$,

$$(q - p_0) - (p - p_0) = q - p?$$

Indeed, suppose $Q = \nu(q, p_0)$ and $P = \nu(p, p_0)$. We want to show $\nu(q, p) = Q - P$, i.e., $p + (Q - P) = q$. We have

$$p + (-P + Q) = (p + (-P)) + Q = p_0 + Q = q,$$

as hoped.

We will now show that every homogeneous space is, in fact, a twist and that ν is a morphism defined over K.

Proposition 5.2. *Let E/K be an elliptic curve with a homogenous space C/K. Fix a point $p_0 \in C$, and define the map $\theta : E \to C$ by $P \mapsto p_0 + P$.*

(1) The map θ is an isomorphism defined over $K(p_0)$, and so C/K is a twist of E/K.

(2) For all $p, q \in C$,

$$q - p = \theta^{-1}(q) - \theta^{-1}(p).$$

(3) The subtraction map $\nu : C \times C \to E$ is a morphism defined over K.

Proof. (1) Note that μ is a morphism defined over K by definition. So, letting $L = K(p_0)$, for any $\sigma \in G_{\bar{K}/L}$ we have

$$\theta^\sigma(P^\sigma) = \theta(P)^\sigma = \mu(p_0, P)^\sigma = \mu(p_0^\sigma, P^\sigma) = \mu(p_0, P^\sigma) = \theta(P^\sigma),$$

showing $\theta^\sigma = \theta$. Thus, by Lemma 4.2, θ is defined over $K(p_0)$. That θ is a bijection follows from noting the map $C \to E : q \mapsto q - p_0$ is an inverse for θ. Once we show ν is a morphism below, we will also have established θ is an isomorphism.

(2) We compute

$$\theta^{-1}(q) - \theta^{-1}(p) = (q - p_0) - (p - p_0) = q - p.$$

(3) Since we already know subtraction on E is a morphism [16, Ch. 3, Thm. 3.6], by $\nu(q, p) = \theta^{-1}(q) - \theta^1(p)$, we see ν is a morphism too. To see ν is defined over K, we use that μ subtraction in E are defined over K:

$$\begin{aligned}(q-p)^\sigma &= (\theta^{-1}(q) - \theta^1(p))^\sigma \\ &= \theta^{-1}(q)^\sigma - \theta^{-1}(p)^\sigma \\ &= (q - p_0)^\sigma - (p - p_0)^\sigma \\ &= (q^\sigma - p_0^\sigma) - (p^\sigma - p_0^\sigma) \\ &= q - p.\end{aligned}$$

□

We now define an equivalence relation on the homogeneous spaces of E/K that refines the identification up to K-isomorphism we imposed on the set of all twists. Let C/K and C'/K be homogeneous spaces of an elliptic curve E/K. We identify C and C' if there is a K-isomorphism $\pi : C \to C'$ such that

$$\pi(p + P) = \pi(p) + P,$$

for all $p \in C$ and $P \in E$. The set of equivalence classes of homogeneous spaces of E/K is called the Weil-Châtelet group $WC(E/K)$ for E/K. We will shortly see the group structure on $WC(E/K)$. For example, $\{E/K\}$ is itself an equivalence class of $WC(E/K)$ corresponding to the identity automorphism (or translation by a fixed point $P \in E$) playing the role of the identity, and is called the trivial class.

Next, we have the first true indication that all this study of twisting is relevant to computing rational points.

Proposition 5.3. *Let C/K be a homogeneous space for an elliptic curve E/K. Then C/K is in the trivial class if and only if C has at least one K-rational point.*

Proof. Suppose C/K is in the trivial class, so that there exists a K-isomorphism $\pi : E \to C$. Since $O \in E(K)$, we see that $\pi(O)$ is a rational point on C since

$$\pi(O)^\sigma = \pi^\sigma(O^\sigma) = \pi(O),$$

for all $\sigma \in G_{\bar{K}/K}$.

Conversely, suppose $p_0 \in C$ is a K-rational point. By Proposition 5.2, we know $\theta : E \to C$ given by $P \mapsto p_0 + P$ is an isomorphism over $K(p_0) = K$. Further, compatibility with the group action of E

$$\theta(P + Q) = \theta(P) + Q,$$

for all $P, Q \in E$, holds by the associativity of the group action of E on C. □

Example 5.4. Let $\mathbb{F}_q$ be the finite field with q elements and let $E/\mathbb{F}_q$ be an elliptic curve. As an immediate application of Proposition 5.3, we will calculate that $WC(E/\mathbb{F}_q)$ is trivial. Let $C/\mathbb{F}_q$ be a homogeneous space of $E/\mathbb{F}_q$ and we wish to find a $\mathbb{F}_q$-rational point on C . Since C is isomorphic to E over $\bar{\mathbb{F}}_q$, we can make C an elliptic curve over $\bar{\mathbb{F}}_q$ by setting any point $O \in C(\bar{\mathbb{F}}_q)$ to be the distinguished point. Consider the Frobenius morphism $\phi : \mathbb{P}^2(\bar{\mathbb{F}}_q) \to \mathbb{P}^2(\bar{\mathbb{F}}_q)$ that sends a point $[X, Y, Z] \mapsto [X^q, Y^q, Z^q]$. Recall that given a point $P \in \mathbb{P}^2(\bar{\mathbb{F}}_q)$, P belongs to $\mathbb{P}^2(\mathbb{F}_q)$ if and only if $\phi(P) = P$. Since C is defined over $\mathbb{F}_q$, we get the Frobenius morphism $\phi : C \to C$.

Let $P_0 = \phi(O) - O$ and define ψ by letting $\psi(P) = \phi(P) - P_0$, so that we get a morphism $\psi : C \to C$ that preserves O (i.e., ψ is an isogeny of C). If we let λ_{-P_0} denote the translation-by-$(-P_0)$ map, then $\psi = \lambda_{-P_0} \circ \phi$. We claim that ψ is inseparable. Let ω denote the invariant differential of C. Note that since ϕ is inseparable [16, Ch. 2, Prop. 2.11], we have the pullback of ω by ψ is

$$\psi^*\omega = (\lambda_{-P_0} \circ \phi)^*\omega = \lambda^*_{-P_0}(\phi^*\omega) = \lambda^*_{-P_0}(0) = 0,$$

showing ψ is indeed inseparable [16, Ch. 2, Prop. 4.2]. Hence, letting 1 denote the identity map $C \to C$, we have by linearity [16, Ch. 3, Thm. 5.2]

$$(1 - \psi)^*\omega = \omega - \psi^*\omega = \omega \neq 0,$$

and so $1 - \psi$ is separable. Thus, the morphism $1 - \psi$ must be nonzero and hence surjective [4, Ch. 2, Prop. 6.8]. So, there exists a point $Q \in C(\bar{\mathbb{F}}_q)$ such that $(1 - \psi)(Q) = P_0$. This means

$$\phi(Q) = \psi(Q) + P_0 = (Q - P_0) + P_0 = Q,$$

implying that $Q \in C(\mathbb{F}_q)$ and so C is in the trivial class of $WC(E/\mathbb{F}_q)$. A similarly neat result holds for elliptic curves over $\mathbb{R}$ (see [16, Ch. 10, Ex. 10.7]).

We now show $WC(E/K)$ is in bijection with $H^1(G_{\bar{K}/K}, E)$, and as a result also demonstrate the group law on $WC(E/K)$ piggybacking off the group structure of $H^1(G_{\bar{K}/K}, E)$. The following lemma records a useful calculation before we proceed.

Lemma 5.5. *Let C/K and C'/K be equivalent homogeneous spaces via a K-isomorphism $\pi : C \to C'$. Then, for any points $p, q \in C$,*

$$\pi(q) - \pi(p) = q - p.$$

Proof. We have

$$\begin{aligned}
\pi(q) - \pi(p) &= (\pi(q) - \pi(p)) - (q - p) + (q - p) \\
&= [\pi(q) - (\pi(p) + (q - p))] + (q - p) \\
&= [\pi(q) - \pi(p + (q - p))] + (q - p) \\
&= (\pi(q) - \pi(q)) + (q - p) \\
&= O + (q - p) \\
&= q - p.
\end{aligned}$$

□

Theorem 5.6. *Let E/K be an elliptic curve. The sets $WC(E/K)$ and $H^1(G_{\bar{K}/K}, E)$ are in bijection via the map $\mathcal{W}$ sending the class of a homogeneous space C/K to the cohomology class of the 1-cocycle $G_{\bar{K}/K} \to E : \sigma \mapsto p_0^\sigma - p_0$ for any point $p_0 \in C$.*

Proof. First, let us check that $\mathcal{W}$ is well-defined. Suppose C/K and C'/K belong to the same class in $WC(E/K)$, so that there exists a K-isomorphism $\pi : C \to C'$ compatible with the action of E.

Fix a point $q_0 \in C'$. So, using Lemma 5.5,

$$\begin{aligned} p_0^\sigma - p_0 &= \pi(p_0^\sigma) - \pi(p_0) \\ &= (q_0^\sigma - q_0) - (q_0^\sigma - q_0) + (\pi(p_0)^\sigma - \pi(p_0)) \\ &= (q_0^\sigma - q_0) + [(\pi(p_0)^\sigma - q_0^\sigma) - (\pi(p_0) - q_0)] \\ &= (q_0^\sigma - q_0) + [(\pi(p_0) - q_0)^\sigma - (\pi(p_0) - q_0)], \end{aligned}$$

showing that $p_0^\sigma - p_0$ and $q_0^\sigma - q_0$ differ by the 1-coboundary generated by $\pi(p_0) - q_0$, and thus belong to the same cohomology class in $H^1(G_{\bar{K}/K}, E)$. This also shows the choice of p_0 does not affect the image in $\mathcal{W}$.

To show injectivity of $\mathcal{W}$, suppose $p_0 \in C$ and $q_0 \in C'$ are points on homogeneous spaces such that there exists $P_0 \in E$ for which

$$p_0^\sigma - p_0 = (q_0^\sigma - q_0) + (P_0^\sigma - P_0),$$

for all $\sigma \in G_{\bar{K}/K}$. Take the isomorphism $\pi : C \to C'$ given by $p \mapsto q_0 + (p - p_0) + P_0$ (this addition is well-defined by associativity). To show that π is defined over K, we use Lemma 4.2, and compute

$$\begin{aligned} \pi(p)^\sigma &= q_0^\sigma + (p^\sigma - p_0^\sigma) + P_0^\sigma \\ &= q_0^\sigma + (p^\sigma - p_0^\sigma) + (P_0^\sigma - P_0) + P_0 \\ &= q_0 + (q_0^\sigma - q_0) + (p^\sigma - p_0^\sigma) + (P_0^\sigma - P_0) + P_0 \\ &= q_0 + (p^\sigma - p_0^\sigma) + [(q_0^\sigma - q_0) + (P_0^\sigma - P_0)] + P_0 \\ &= q_0 + (p^\sigma - p_0^\sigma) + (p_0^\sigma - p_0) + P_0 \\ &= q_0 + (p^\sigma - p_0) + P_0 \\ &= \pi(p^\sigma). \end{aligned}$$

Thus, C and C' are equivalent homogeneous spaces.

Showing the surjectivity of $\mathcal{W}$ uses a rather beautiful idea and our hard work in proving Theorem 4.4. Fix a 1-cocycle $\xi : G_{\bar{K}/K} \to E$. Note that E can be canonically embedded into $\mathrm{Aut}(E)$ since each point $P \in E$ corresponds to the translation-by-P map λ_P, which is an automorphism [16, Ch. 3, Thm. 3.6]. So, let $\chi : G_{\bar{K}/K} \to \mathrm{Aut}(E)$ be the 1-cochain $\sigma \mapsto \lambda_{-\xi_\sigma}$. We check that χ is a 1-cocycle:

$$\chi_{\sigma\tau} = \lambda_{-\xi_{\sigma\tau}} = \lambda_{-\xi_\sigma^\tau - \xi_\tau} = \lambda_{-\xi_\tau} \circ \lambda_{-\xi_\sigma}^\tau = \lambda_{-\xi_\sigma}^\tau \circ \lambda_{-\xi_\tau} = \chi_\sigma^\tau \chi_\tau.$$

(Taking translation by $-\xi_\sigma$ rather than ξ_σ is a necessary trick in order to end up with ξ as the image in $\mathcal{W}$.) Using Theorem 4.4, we fix a twist of C/K of E/K isomorphic via $\phi : C \to E$ satisfying

$$\phi^\sigma \phi^{-1} = \chi_\sigma$$

for all $\sigma \in G_{\bar{K}/K}$ and show that $\mathcal{W}(\{C\}) = \{\xi\}$. To show C is a homogeneous space of E, we need to specify a simply transitive action defined over K of E on C. We claim this is given by

$$\mu : C \times E \to C, \quad (p, P) \mapsto \phi^{-1}(\phi(p) + P).$$

Let us check the conditions of Definition 5.1. Let $p \in C$ and $P, Q \in E$:

(1) $\mu(p, O) = \phi^{-1}(\phi(p) + O) = \phi^{-1}(\phi(p)) = p$ for all $p \in C$.
(2) $\mu(\mu(p, P), Q) = \mu(\phi^{-1}(\phi(p) + P), Q) = \phi^{-1}(\phi(\phi^{-1}(\phi(p) + P)) + Q) = \phi^{-1}(\phi(p) + P + Q) = \mu(p, P + Q)$.
(3) For $q \in C$, clearly $P = \phi(q) - \phi(p)$ is the unique point in E such that $\mu(p, P) = q$.

We also need to check μ is defined over K, which we do as usual, making good use of $\phi^\sigma\phi^{-1} = \chi_\sigma$:

$$\begin{aligned}
\mu^\sigma(p^\sigma, P^\sigma) &= \mu(p, P)^\sigma \\
&= (\phi^{-1})^\sigma(\phi(p)^\sigma + P^\sigma) \\
&= (\phi^\sigma)^{-1}(\phi^\sigma(p^\sigma) + P^\sigma) \\
&= (\phi^\sigma)^{-1}(\chi_\sigma(\phi(p^\sigma)) + P^\sigma) \\
&= (\phi^\sigma)^{-1}(\phi(p^\sigma) - \xi_\sigma + P^\sigma) \\
&= \phi^{-1}(\chi_\sigma^{-1}(\phi(p^\sigma) - \xi_\sigma + P^\sigma)) \\
&= \phi^{-1}((\phi(p^\sigma) - \xi_\sigma + P^\sigma) + \xi_\sigma) \\
&= \phi^{-1}(\phi(p^\sigma) + P^\sigma) = \mu(p^\sigma, P^\sigma).
\end{aligned}$$

This verifies that C is indeed a homogeneous space of E.

Finally, we need to check that the image of $\{C\}$ under $\mathcal{W}$ is indeed $\{\xi\}$.

We pick the point $p_0 = \phi^{-1}(O)$ and compute

$$\begin{aligned}
p_0^\sigma - p_0 &= \phi^{-1}(O)^\sigma - \phi^{-1}(O) \\
&= (\phi^{-1})^\sigma(O) - \phi^{-1}(O) \\
&= \phi^{-1}(\chi_\sigma^{-1}(O)) - \phi^{-1}(O) \\
&= \phi^{-1}(O + \xi_\sigma) - \phi^{-1}(O) \\
&= \xi_\sigma,
\end{aligned}$$

the last equality following from the very definition of subtraction in C. □

Example 5.7. Let us now pause to see an example of what a homogeneous space looks like. Fix an elliptic curve $E/\mathbb{Q}$ that has a *rational* torsion point of order 2. Since a point T of order 2 has y-coordinate equal to zero, by an appropriate linear change of coordinates, T can be moved to $(0, 0)$. In other, words $E/\mathbb{Q}$ has the form

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

We will be using this Weierstrass form for our computations in Section 8 too. Let us consider the following 1-cocycle $\xi \in H^1(G_{\bar{\mathbb{Q}}/\mathbb{Q}}, E)$. Fix a quadratic extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ with d squarefree. We know that each $\sigma \in G_{\bar{\mathbb{Q}}/\mathbb{Q}}$ restricts to an element of $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$, and thus either fixes $\sqrt{d}$ or sends it to $-\sqrt{d}$. Define ξ_σ to be O if σ fixes $\sqrt{d}$, otherwise $\xi_\sigma = T$. It can be checked easily that this is really a 1-cocycle. Since both O and T are 2-torsion points, observe that $\xi \in H^1(G_{\bar{\mathbb{Q}}/\mathbb{Q}}, E[2])$ − for this reason, this example will be very important in Section 7. Now, we would like to know the homogeneous space C corresponding to ξ. As we saw in the proof above, the required homogeneous space is isomorphic E via a $\phi : C \to E$ satisfying

$$\phi^\sigma\phi^{-1} = \chi_\sigma,$$

where χ_σ is the 1-cocycle corresponding to translation by $-\xi_\sigma$. Since $T = -T$ and $O = -O$, translating by $-\xi_\sigma$ is really the same as translating by ξ_σ. Now, translation by O is trivial and translation by $T = (0, 0)$ can be calculated to be

$$(x_0, y_0) \mapsto (b/x_0, -by_0/x_0^2).$$

So, from the proof of Theorem 4.4, if σ is the nontrivial automorphism on $\mathbb{Q}(\sqrt{d})$, we know the isomorphism of function fields $Z : \bar{\mathbb{Q}}(E) \to \bar{\mathbb{Q}}(E)_\chi$ is twisted in the following manner:

$$Z(x)^\sigma = Z(x^\sigma\chi_\sigma) = b \cdot Z(1/x),$$

and

$$Z(y)^\sigma = Z(y^\sigma \chi_\sigma) = -b \cdot Z(y/x^2).$$

When σ is trivial on $\mathbb{Q}(\sqrt{d})$, we see $Z(x)^\sigma = Z(x)$ and $Z(y)^\sigma = Z(y)$. So, let $X = Z(x)$ and $Y = Z(y)$. Then, note that the functions

$$z = \sqrt{d}X/Y \text{ and } w = \sqrt{d}(X - b/X)(X/Y)^2$$

are invariant under the action of $G_{\bar{\mathbb{Q}}/\mathbb{Q}}$. Indeed, it can be checked that the fixed subfield of $\bar{\mathbb{Q}}(E)_\chi$ is $\mathbb{Q}(\sqrt{d})(z, w)$. In other words, these functions will end up being the coordinate functions for our homogeneous space. The alert reader might complain why not just take $w = \sqrt{d}(X - b/X)$? The (somewhat unsatisfactory) answer is that we eventually want a *hyperelliptic curve* since that allows us to use general facts about such a curve and not worry about things like smoothness. We give an alternate derivation of C_d in Section 7. Indeed, we can eliminate X and Y to obtain the relation between z and w:

$$\begin{aligned} d\left(\frac{w}{z^2}\right)^2 &= \left(X - \frac{b}{X}\right)^2 \\ &= \left(X + \frac{b}{X}\right)^2 - 4b \\ &= \left(\frac{Y^2}{X^2} - a\right)^2 - 4b \\ &= \left(\frac{d}{z^2} - a\right)^2 - 4b, \end{aligned}$$

and we obtain the hyperelliptic curve

$$C : dw^2 = d^2 - 2adz^2 + (a^2 - 4b)z^4.$$

From our construction, we have the morphism

$$\psi : E \to C, (x, y) \mapsto (z, w) = (\sqrt{d}X/Y, \sqrt{d}\,(X - b/X)\,(X/Y)^2).$$

In fact, since we can also compute X and Y in terms of z and w, we can calculate the inverse ψ^{-1} to show ψ is an isomorphism and check that $\psi^{-1} : C \to E$ actually corresponds to our chosen 1-cocycle χ_σ. We omit those verifications here.

6. The Selmer and Shafarevich-Tate Groups

We can now apply the theory of homogeneous spaces we have developed to the problem of computing rational points. For concreteness, we will work over $K = \mathbb{Q}$, though the arguments apply almost verbatim over any number field. Throughout this section and the next, let $G = G_{\bar{\mathbb{Q}}/\mathbb{Q}}$.

Let $E/\mathbb{Q}$ and $E'/\mathbb{Q}$ be elliptic curves. Recall that an isogeny $\phi : E \to E'$ is a morphism that preserves the point at infinity $\phi(O_E) = O_{E'}$. Fix a nonzero isogeny $\phi : E \to E'$ defined over $\mathbb{Q}$. Then since a nonconstant morphism between curves is surjective [4, Ch. 2, Prop. 6.8], we have the short exact sequence of G-modules

$$0 \to E[\phi] \to E \xrightarrow{\phi} E' \to 0.$$

Applying Galois cohomology (3.4) to this sequence, we obtain the following long exact sequence:

$$0 \to E(\mathbb{Q})[\phi] \to E(\mathbb{Q}) \xrightarrow{\phi} E'(\mathbb{Q}) \xrightarrow{\delta} H^1(G, E[\phi]) \to H^1(G, E) \xrightarrow{\phi} H^1(G, E').$$

Isolating $H^1(G, E[\phi])$, similar to how we deduced (3.7), we then obtain the short exact sequence

$$0 \to E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \xrightarrow{\delta} H^1(G, E[\phi]) \to H^1(G, E)[\phi] \to 0. \tag{6.1}$$

This isomorphism is useful because, by Theorem 5.6, we can replace the last term by $WC(E/\mathbb{Q})[\phi]$, which we saw in Proposition 5.3 encodes whether a rational point exists on a homogeneous space of E. Now, our main aim is to compute $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$, that injects into $H^1(G, E[\phi])$, and so it is enough to compute the kernel of the map $H^1(G, E[\phi]) \to WC(E/\mathbb{Q})[\phi]$. However, the trouble remains that computing this kernel involves at minimum determining the trivial class in $WC(E/\mathbb{Q})$, a problem that is in some sense at least as hard as determining $E(\mathbb{Q})$! The central insight is that the same exact sequence holds for a completion $\mathbb{Q}_p$ of $\mathbb{Q}$, where by applying the useful Hensel's Lemma [11, Ch. 2, Lem. 4.6], the problem reduces to a computation over $\mathbb{F}_p$. Indeed, since this is such a key idea, let us quote Neukirch here:

> The *raison d'être* of valuation theory, however, is not to reformulate ideal-theoretic knowledge, but rather, as has been stressed earlier, to provide the possibility of passing from the extension L/K to the various completions L_w/K_v where much simpler arithmetic laws apply. Let us also emphasize once more that completions may always be replaced with henselizations. [11, Ch. 2, §8, pp. 165]

So, we do the first step of descent, by considering the analogue of (6.1) for a completion $\mathbb{Q}_p$. For each prime p, fix an extension of $|\cdot|_p$ to $\bar{\mathbb{Q}}$ and let $G_p \subseteq G$ be the decomposition group of the extension (fixing a different extension of p will only replace G_p by a conjugate). The important fact about G_p is that $G_p \simeq \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ [11, Ch. 2, Prop. 9.6] and so by exactly the same argument as above, we obtain the exact sequence

$$0 \to E'(\mathbb{Q}_p)/\phi(E(\mathbb{Q}_p)) \xrightarrow{\delta} H^1(G_p, E[\phi]) \to H^1(G_p, E)[\phi] \to 0. \tag{6.2}$$

Before proceeding further, let us first identify the main objects that will play a central role in the descent.

Because $G_p \subseteq G$ and $E(\bar{\mathbb{Q}}) \subseteq E(\bar{\mathbb{Q}}_p)$, by restricting cohomology we obtain the map

$$H^1(G, E[\phi]) \to H^1(G, E)[\phi] \to H^1(G_p, E)[\phi].$$

Using the identification $\mathcal{W}$ of Theorem 5.6, we then have the map

$$H^1(G, E[\phi]) \to WC(E/\mathbb{Q})[\phi] \to WC(E/\mathbb{Q}_p)[\phi].$$

Since a rational solution $P \in C(\mathbb{Q})$ of a curve C trivially gives a $\mathbb{Q}_p$-rational solution for each p, an obvious obstruction to the existence of a rational solution of C is the nonexistence of a $\mathbb{Q}_p$-rational solution for even a *single* p. Thus, intuitively, we want to study all the $WC(E/\mathbb{Q}_p)[\phi]$ simultaneously, and so we extend the map to

$$H^1(G, E[\phi]) \to WC(E/\mathbb{Q})[\phi] \to WC(E/\mathbb{Q}_p)[\phi] \to \prod_p WC(E/\mathbb{Q}_p)[\phi], \tag{6.3}$$

where the product runs over the primes (over an arbitrary number field, we would take the product over all non-archimedean absolute values, which for $\mathbb{Q}$ are just the p-adic absolute values for primes p by Ostrowski's Theorem [11, Ch. 2, Thm. 4.2]).

Definition 6.4. The subgroup of $H^1(G, E[\phi])$ that is the kernel of the map in (6.3) is called the ϕ-Selmer group of $E/\mathbb{Q}$ and is denoted $S^{(\phi)}(E/\mathbb{Q})$.

As we noted earlier, the fundamental reason why determining rational points on elliptic curves is a hard problem is the failure of the local-global principle. In particular, we can have a homogeneous space that has a $\mathbb{Q}_p$-rational solution over each completion $\bar{\mathbb{Q}}_p$ but fails to have a $\mathbb{Q}$-rational solution.

One example of such a homogeneous space due to Lind [8] and Reichardt [13] is the innocent-looking curve

$$2w^2 = 1 - 17z^4.$$

By Proposition 5.3, we know a homogeneous space maps to the trivial class in some $WC(E/\mathbb{Q}_p)$ if and only if it has a $\bar{\mathbb{Q}}_p$-rational solution. Thus, observe that we can detect the failure of the local-global principle via the kernel of the natural map

$$WC(E/\mathbb{Q}) \to WC(E/\mathbb{Q}_p) \to \prod_p WC(E/\mathbb{Q}_p). \tag{6.5}$$

Definition 6.6. The subgroup of $WC(E/\mathbb{Q})$ that is the kernel of the map in (6.5) is called the Shafarevich-Tate group of $E/\mathbb{Q}$ and is denoted $Ш(E/\mathbb{Q})$[1].

The following lemma explains the relationship between the Selmer and Shafarevich-Tate groups.

Lemma 6.7. *Let $E/\mathbb{Q}$ and $E'/\mathbb{Q}$ be elliptic curves and let $\phi : E/\mathbb{Q} \to E'/\mathbb{Q}$ be an isogeny defined over $\mathbb{Q}$. We have the following short exact sequence:*

$$0 \to E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \xrightarrow{\delta} S^{(\phi)}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[\phi] \to 0.$$

Proof. The proof is mainly unwinding the definitions and applying the sequence (6.1). (Of course, one should also verify that these induced maps are well-defined but that is straightforward.)

The injectivity of $E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \xrightarrow{\delta} S^{(\phi)}(E/\mathbb{Q})$ follows directly from the injectivity of $E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \xrightarrow{\delta} H^1(G, E[\phi])$.

Suppose that $\{C\} \in Ш(E/\mathbb{Q})[\phi]$, so that $\{C\}$ becomes trivial in each completion $\mathbb{Q}_p$. Since $H^1(G, E[\phi]) \to WC(E/\mathbb{Q})[\phi]$ is surjective (6.1), fix a cohomology class $\{\xi_C\} \in H^1(G, E[\phi])$ mapping to $\{C\}$. But then under the mapping (6.3) we have

$$\{\xi_C\} \mapsto \{C\} \mapsto \prod_p \textit{trivial class},$$

and so $\xi \in S^{(\phi)}(E/\mathbb{Q})$. Thus, we have the surjectivity of $S^{(\phi)}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[\phi]$.

Next, suppose $\{\xi\}$ is in the image of $E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \xrightarrow{\delta} S^{(\phi)}(E/\mathbb{Q})$. Then, by (6.1), we know $\{\xi\}$ belongs to the kernel of the map $S^{(\phi)}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[\phi]$. Conversely, suppose $\{\xi\}$ is in the kernel of this map. But then, $\{\xi\}$ is also in the kernel of the map $H^1(G, E[\phi]) \to WC(E/\mathbb{Q})$, which means, by (6.1), that $\{\xi\}$ is in the image of $E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \xrightarrow{\delta} S^{(\phi)}(E/\mathbb{Q})$. □

Now, we are interested in computing $S^{(\phi)}(E/\mathbb{Q})$ (see our discussion following (6.1)). Suppose $E' = E$ and $\phi = [m]$ is the multiplication-by-m map. The weak Mordell-Weil Theorem tells us that $E(\mathbb{Q})/mE(\mathbb{Q})$ is a finite order subgroup of $S^{(m)}(E/\mathbb{Q})$. As we will now see, in fact, $S^{(\phi)}(E/\mathbb{Q})$ for any isogeny ϕ is a finite group (which also implies the weak Mordell-Weil Theorem). This proof is important because it hints at how to compute the Selmer group.

Theorem 6.8. *Let $E/\mathbb{Q}$ and $E'/\mathbb{Q}$ be elliptic curves and let $\phi : E/\mathbb{Q} \to E'/\mathbb{Q}$ be an isogeny defined over $\mathbb{Q}$. The ϕ-Selmer group $S^{(\phi)}(E/\mathbb{Q})$ is finite.*

Proof. Let $I_p \subseteq G_p$ be the inertia subgroup corresponding to the extension $\bar{\mathbb{Q}}_p/\mathbb{Q}_p$. A cohomology class $\{\xi\} \in H^1(G, E[\phi])$ is said to be unramified at p if it becomes trivial in $H^1(I_p, E[\phi])$ (via the restriction map). The strategy is to show that all elements of $S^{(\phi)}(E/\mathbb{Q})$ are unramified at each

[1]It is worth mentioning here the following cultural factoid due to Cassels [2, Ch. 23, Footnote 29]: "This [the notation Ш] is the author's [Cassels'] most lasting contribution to the subject. The original notation was TS, which, Tate tells me, was intended to continue the lavatorial allusion of WC. The Americanism "tough shit" indicates the part that is difficult to eliminate."

prime p (specifically those at which E has stable reduction) and then show that any such cohomology group must be finite. We will not argue the latter part here as it is essentially a result of basic class field theory and thus it would take us too far afield (an alternate argument is in [16, Ch. 10, Lemma 4.3]).

So, fix a cohomology class $\{\xi\} \in S^{(\phi)}(E/\mathbb{Q})$ and let p be any prime not dividing $m := \deg(\phi)$ and for which $E/\mathbb{Q}$ has stable reduction. Then, by the definition of $S^{(\phi)}(E/\mathbb{Q})$, $\{\xi\}$ becomes the trivial class in $WC(E/\mathbb{Q}_p)$, which is equivalent to saying $\{\xi\}$ becomes the trivial cohomology class in $H^1(G_p, E)$. Thus, we can fix a point $P \in E(\bar{\mathbb{Q}}_p)$ such that

$$\xi_\sigma = P^\sigma - P,$$

for all $\sigma \in G_p$. Moreover, by (6.2), we can assume $P^\sigma - P \in E[\phi]$ for all $\sigma \in G_p$. We want to argue that ξ is in the trivial class in $H^1(I_p, E[\phi])$ too. Consider the reduction map

$$E(\bar{\mathbb{Q}}) \hookrightarrow E(\bar{\mathbb{Q}}_p) \to \tilde{E}(\bar{\mathbb{F}}_p),$$

where $\tilde{E}$ is the curve obtained after reducing the coefficients of E in $\bar{\mathbb{F}}_p$ (remember a point on an elliptic curve lives in projective space and so we can clear denominators such that the point's projective coordinates land inside the ring of integers of $\bar{\mathbb{Q}}_p$, allowing for reduction modulo the maximal ideal). Since the elements of I_p (by definition) fix the elements of $\bar{\mathbb{F}}_p$, we have

$$P^\sigma - P \equiv O \pmod{\bar{\mathbb{F}}_p},$$

for all $\sigma \in I_p$.

Now, consider the dual isogeny of $\hat{\phi} : E' \to E$, which has the property that $\hat{\phi} \circ \phi = [m]$ [16, Ch. 3, Thm. 6.1]. Since $P^\sigma - P \in E[\phi]$, for all $\sigma \in G_p$, and $\hat{\phi}(O) = O$, we see that $P^\sigma - P \in E[m]$ for all $\sigma \in I_p \subseteq G_p$. Now, since $E(\bar{\mathbb{Q}})[m]$ is finite (it has size exactly m^2 since we are in zero characteristic), we can fix a finite extension $L/\mathbb{Q}$ that contains the coordinates of points in $E[m]$. Because E has stable reduction for p, by Proposition 2.2, we know the reduction map

$$E(L)[m] \hookrightarrow E[L_p][m] \to \tilde{E}(\mathbb{F}_p)$$

is injective. However, we know $P^\sigma - P \in E(L)[m]$ for each $\sigma \in I_p$ reduces to O, and so we must have $P^\sigma - P = O$ for all $\sigma \in I_p$. Thus, $\{\xi\}$ does indeed become the trivial cohomology class in $H^1(I_p, E[\phi])$, and so all elements of $S^{(\phi)}(E/\mathbb{Q})$ are unramified at all primes with stable reduction. As we noted above, this can be used to then show that $S^{(\phi)}(E/\mathbb{Q})$ is finite. □

Let us denote by $B(\phi)$ the set of "bad" primes: those at which E has bad reduction or those that divide $\deg(\phi)$. Further, for any G-module M, let $H^1(G, M; B(\phi))$ be the set of elements of $H^1(G, M)$ that are unramified at all primes except possibly those in $B(\phi)$. Then we proved just now that $S^{(\phi)}(E/\mathbb{Q}) \subseteq H^1(G, E[\phi]; B(\phi))$ and this gives at least a start on our quest to compute the Selmer group.

Example 6.9. Indeed, to see this is actually significant progress, let us take $E' = E$ and $\phi = [2]$. Further, let $E[2] \subseteq E(\mathbb{Q})$. Now, $E[2]$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ [16, Ch. 3, Cor. 6.4] and thus can be identified as a group with $\mu_2 \times \mu_2$, where μ_2 is the subgroup of second roots of unity. Since $E[2] \subseteq E(\mathbb{Q})$ and $\mu_2 \subseteq \mathbb{Q}$, the identification holds as a G-module too. Using the isomorphism (3.8), we know that

$$H^1(G, E[2]) \simeq H^1(G, \mu_2 \times \mu_2) \simeq H^1(G, \mu_2) \times H^1(G, \mu_2) \simeq \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \times \mathbb{Q}^\times/\mathbb{Q}^{\times 2}. \tag{6.10}$$

Take $\{\alpha\} \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, which is sent by the isomorphism δ to the cohomology class of $\xi_\sigma = \beta^\sigma/\beta$ for some $\beta \in \bar{\mathbb{Q}}^\times$ such that $\beta^2 = \alpha$. Suppose that $\{\xi\} \in H^1(G, \mu_2; B(2))$. So, if we let p be a prime

not in $B(2)$, then ξ becomes trivial in $H^1(I_p, \mu_2)$, allowing us to fix an element $\zeta \in \mu_2$ such that $\xi_\sigma = \zeta^\sigma/\zeta$ for all $\sigma \in I_p$. Then we have

$$(\beta/\zeta)^\sigma = \beta/\zeta,$$

for all $\sigma \in I_p$, implying that the action of I_p on the extension $\mathbb{Q}_p(\beta\zeta^{-1})$ is trivial and so $\mathbb{Q}_p(\beta\zeta^{-1})/\mathbb{Q}_p$ is an unramified extension (recall that the fixed subfield of I_p in $\bar{\mathbb{Q}}_p$ is the largest unramified extension of $\mathbb{Q}_p$). Write $\alpha = p^n u$ for some $n \in \mathbb{Z}$ and unit $u \in \mathbb{Z}_p^\times$. We claim that $2 \mid n$. Since multiplying or dividing α by p^2 leaves the extension $\mathbb{Q}_p(\beta\zeta^{-1})/\mathbb{Q}_p$ unchanged, we can assume $0 \leq n < 2$ and we are claiming $n = 0$ in order for $\mathbb{Q}_p(\beta\zeta^{-1})/\mathbb{Q}_p$ to be unramified. But, indeed, if $n > 0$, then the equation $x^2 - \alpha$ (the minimal polynomial of $\beta\zeta^{-1}$) reduces to $x^2 \pmod p$, which is not separable over $\mathbb{F}_p$, contradicting that the extension is unramified. Indeed, the converse is also true. Let $n = 0$, so that $\alpha \in \mathbb{Z}_p^\times$ is a unit, then the equation $x^2 - \alpha \pmod p$ is separable over $\mathbb{F}_p$ since it is coprime to its formal derivative

$$x \cdot 2x - 2 \cdot (x^2 - \alpha) = 2\alpha,$$

where 2α is a unit because $p \nmid 2$. Thus, by Hensel's Lemma, the degree of the residue field extension matches that of $\mathbb{Q}_p(\beta\zeta^{-1})/\mathbb{Q}_p$, and so $\mathbb{Q}_p(\beta\zeta^{-1})/\mathbb{Q}_p$ is unramified. We have thus proved that $H^1(G, \mu_2; B(2))$ can be identified with the elements $\{\alpha\}$ of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ for which $2 \mid \mathrm{ord}_p(\alpha)$ whenever $p \notin B(2)$. Denote this set of classes in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ by $\mathbb{Q}(B(2), 2)$.

So, continuing from (6.10), we can identify $H^1(G, E[2]; B(2))$ with $\mathbb{Q}(B(2), 2) \times \mathbb{Q}(B(2), 2)$. Observe that $\mathbb{Q}(B(2), 2)$ is finite because $B(2)$ is finite. For example, suppose $B(2) = \{2, 3\}$. Then $\{\pm 1, \pm 2, \pm 3, \pm 6\}$ is a complete set of unique class representatives for $\mathbb{Q}(B(2), 2)$. Thus, we need to only examine a finite number of homogeneous spaces (those corresponding to the points of $\mathbb{Q}(B(2), 2) \times \mathbb{Q}(B(2), 2)$) to determine $S^{(2)}(E/\mathbb{Q})$. This method can be developed further to calculate the weak Mordell-Weil group because all that remains is to calculate the homogeneous spaces corresponding to each element of $H^1(G, E[2])$. We will not pursue that line of attack here, but see [16, Ch. 10, Prop. 1.4] for a derivation of this method without cohomology. Rather, we will assume only a single rational torsion point of order 2 and take ϕ to be an isogeny that has the rational torsion point in its kernel.

7. Descent via Degree-2 Isogenies

Let $E/\mathbb{Q}$ be an elliptic curve that has rational torsion point T of order 2, so that after moving T to $(0, 0)$, we can assume a Weierstrass form

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

We take E' to be the elliptic curve

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

and $\phi : E \to E'$ to be the isogeny

$$(x, y) \mapsto (y^2/x^2, y(b - x^2)/x^2).$$

Note that $E[\phi] = \{O, (0, 0)\}$ and so ϕ has degree 2. Further, the dual isogeny $\hat{\phi} : E' \to E$ is given by

$$(X, Y) \mapsto (Y^2/4X^2, Y((a^2 - 4b) - X^2)/8X^2),$$

which too has degree 2 and satisfies $\hat{\phi} \circ \phi = [2]$. We need to find a characterization (more useful than the definition) for when an element of $H^1(G, E[\phi])$ is in $S^{(\phi)}(E/\mathbb{Q})$. In Theorem 6.7, we showed that $S^{(\phi)}(E/\mathbb{Q}) \subseteq H^1(G, E[\phi]; B(\phi))$. Note that here $B(\phi)$ consists of 2 ($= \deg(\phi)$) and any other prime that divides the discriminant $\Delta(E)$. It can be calculated that

$$\Delta(E) = 16b^2(a^2 - 4b),$$

and so $B(\phi)$ consists of the primes dividing $2b(a^2-4b)$. What is $H^1(G, E[\phi]; B(\phi))$? We discussed this for $E[2]$ and in this case it is even simpler. We know $E[\phi] = \{O, (0,0)\}$, and so $E[\phi] \simeq \mu_2$ as G-modules. Thus, using 3.8, we have

$$H^1(G, E[\phi]) \simeq H^1(G, \mu_2) \simeq \mathbb{Q}^\times/\mathbb{Q}^{\times 2}. \tag{7.1}$$

Then, as we showed in Example 6.9, $H^1(G, E[\phi]; B(\phi))$ can be identified with $\mathbb{Q}(B(\phi), 2)$, which consists of those classes $\{\alpha\}$ of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ for which α has even valuation at the primes *not* in $B(\phi)$, i.e., those not dividing $2b(a^2-4b)$. All in all, this means we need only be concerned with the classes of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ represented by a squarefree d sharing a prime factor with $2b(a^2-4b)$. So, we need to determine which elements of $\mathbb{Q}(B(\phi), 2)$ end up being in $S^{(\phi)}(E/\mathbb{Q})$. Let us fix $\{d\} \in \mathbb{Q}(B(\phi), 2)$ with d squarefree. What element does $\{d\}$ correspond to in $H^1(G, E[\phi]; B(\phi))$? Walking back the last isomorphism of 7.1, in $H^1(G, \mu_2)$, $\{d\}$ corresponds to the cohomology class of

$$\sigma \mapsto \sqrt{d}^\sigma/\sqrt{d} = \begin{cases} 1 & \sigma \text{ is trivial on } \mathbb{Q}(\sqrt{d}) \\ -1 & \sigma \text{ is nontrivial on } \mathbb{Q}(\sqrt{d}), \end{cases}$$

where $\sqrt{d} \in \bar{\mathbb{Q}}$ is a fixed squareroot of d. Then, going back the first isomorphism, we see $\{d\}$ corresponds to the cohomology class $\{\xi\} \in H^1(G, E[\phi])$ of

$$\xi : \sigma \mapsto \begin{cases} O & \sigma \text{ is trivial on } \mathbb{Q}(\sqrt{d}) \\ (0,0) & \sigma \text{ is nontrivial on } \mathbb{Q}(\sqrt{d}). \end{cases}$$

Note that ξ is precisely the 1-cocycle we considered in Example 5.7, so we know the corresponding homogeneous space $C_d \in WC(E/\mathbb{Q})$ is

$$C_d : dw^2 = d^2 - 2adz^2 + (a^2-4b)z^4.$$

Thus, by definition, $\{d\} \in S^{(\phi)}(E/\mathbb{Q})$ if and only if C_d becomes trivial in $\prod_p WC(E/\mathbb{Q}_p)$ i.e., C_d has a $\mathbb{Q}_p$-rational point for each prime p.

Let us see an example of this correspondence. We have the point $T = (0,0) \in E'(\mathbb{Q})$. According to Lemma 6.7, $\{T\}$ is mapped to some $\{\xi\} \in S^{(\phi)}(E/\mathbb{Q})$ by the connecting homomorphism δ. More specifically, ξ is a 1-cocycle given by $\xi_\sigma = P^\sigma - P$, where $P \in E$ is such that $\phi(P) = T$. Looking at the formula for ϕ, we see $y(P) = 0$ and so $x(P)$ is one of the roots

$$\frac{-a \pm \sqrt{a^2-4b}}{2}.$$

Let us take the $+$ sign (taking the $-$ sign will simply result in a cohomologous 1-cocycle). So, if σ is trivial on the extension $\mathbb{Q}(\sqrt{a^2-4b})$, we get

$$\xi_\sigma = P^\sigma - P = P - P = O.$$

Otherwise, σ acts nontrivially on $\mathbb{Q}(\sqrt{a^2-4b})$, and therefore

$$\begin{aligned} P^\sigma - P &= \left(\frac{-a+\sqrt{a^2-4b}}{2}, 0\right)^\sigma - \left(\frac{-a+\sqrt{a^2-4b}}{2}, 0\right) \\ &= \left(\frac{-a-\sqrt{a^2-4b}}{2}, 0\right) + \left(\frac{-a+\sqrt{a^2-4b}}{2}, 0\right) \\ &= (0,0). \end{aligned}$$

So, $\{(0,0)\} \in E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ corresponds to the class of $d = a^2-4b$ in $\mathbb{Q}(B(\phi), 2)$, and as a result we always know a^2-4b is there in $S^{(\phi)}(E/\mathbb{Q})$. Similarly, the point $O \in E'(\mathbb{Q})$ gives us the class of 1 (which we knew should be case because $S^{(\phi)}(E/\mathbb{Q})$ is a subgroup of $\mathbb{Q}(B(\phi), 2)$ or just by examining C_1, we see $(1,0)$ is always a solution).

Viewing things in light of this characterization, we also have a more satisfactory explanation for the equation of C_d. This also connects to strategy of "coverings" we had explained in Section 2. Note that $d \mapsto C_d$ is a map $K(B(\phi), 2) \to WC(E/\mathbb{Q})[\phi]$. By the short exact sequence 6.1, we know the kernel of this map is precisely the image of $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ under δ, and so C_d is trivial in $WC(E/\mathbb{Q})$ if and only if there exists a point $P' \in E'(\mathbb{Q})$ such that $\delta(P') = d$. In other words, a rational point exists on C_d if and only if d corresponds to a rational point on $E'(\mathbb{Q})$. Taking an arbitrary rational point $P' \in E'(\mathbb{Q})$, we saw it corresponds to a 1-cocycle $\sigma : P^\sigma - P$, where $P \in E$ is such that $\phi(P) = P'$. Letting $P = (x, y)$ and $P' = (X, Y) \neq (0, 0)$, we see

$$X = y^2/x^2 \text{ and } Y = y(b - x^2)/x^2,$$

and so substituting $x^2 = y^2/X$ into second relation, we get

$$y^2 + Yy - bX = 0.$$

Then, since $X, Y \in \mathbb{Q}$, P' corresponds to $\sqrt{d} = \sqrt{Y^2 + 4bX}$. But, using the equation of E', we have

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

Thus, $P' = (X, Y)$ corresponds to $d = X(X - a)^2 \equiv X \pmod{\mathbb{Q}^{\times 2}}$.

Now, suppose C_d (with $d \neq 1$) is trivial in $WC(E/\mathbb{Q})$. Then, there exists a point $P' = (X, Y) \in E'(\mathbb{Q})$ such that $d = Xq^2$, for some $q \in \mathbb{Q}^\times$. Substituting $X = d/q^2$ into E', we obtain

$$Y^2 = \frac{d^3}{q^6} - 2a\frac{d^2}{q^4} + (a^2 - 4b)\frac{d}{q^2},$$

and so

$$\frac{q^6 Y^2}{d} = d^2 - 2adq^2 + (a^2 - 4b)q^4.$$

Taking $w = q^3 Y/d$ and $z = q$, we recover the form of C_d we had derived earlier! This method of derivation also directly tells us how to compute a rational point (X, Y) on $E'(\mathbb{Q})$, given a rational solution (z, w) on C_d :

$$(X, Y) = (d/z^2, dw/z^3). \tag{7.2}$$

We saw the Tate-Shafarevich group $Ш(E/\mathbb{Q})$ detects the failure of the global-local principle. Suppose $Ш(E/\mathbb{Q})$ was infinite. This would mean the existence of an infinite number of nonequivalent homogeneous spaces of E that have a $\mathbb{Q}_p$-rational point for each prime p but have no rational point. Consequently, there would be nothing stopping the ϕ-torsion in $Ш(E/\mathbb{Q})$ from being infinite, effectively destroying any hopes of using Lemma 6.7 (at least in an easy manner) to compute $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ from $S^{(\phi)}(E/\mathbb{Q})$! However, it is conjectured that in general $Ш(E/\mathbb{Q})$ is finite and strong evidence for this has been collected. The most direct evidence comes from, for example, Kolyvagin's [6] and Rubin's [14] work showing the finiteness of Ш for certain families of elliptic curves. In fact, as we will see in Section 8, it can be the case that $Ш(E/\mathbb{Q})[\phi] = 0$, which, in light of Lemma 6.7, implies

$$E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \simeq S^{(\phi)}(E/\mathbb{Q}),$$

and so no additional work is required to compute $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ from $S^{(\phi)}(E/\mathbb{Q})$. But we have ignored one question completely: how exactly does computing $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ help us compute $E'(\mathbb{Q})/2E(\mathbb{Q})$? After all, we had earlier motivated the Selmer group with the promise that it will help us compute $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ when we take $\phi = [2]$, but we have taken ϕ to be a different isogeny. Here is where the dual isogeny comes into play. Observe that since $\hat{\phi} \circ \phi = [2]$, we have the natural surjective map

$$E(\mathbb{Q})/2E(\mathbb{Q}) \to E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q})).$$

So, it suffices to compute the kernel of this map, which is simply the image of the map

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

(Note that this map is which is well-defined because $\hat{\phi} \circ \phi = [2]$ and $\hat{\phi}$ is an isogeny defined over $\mathbb{Q}$.) The kernel of $\hat{\phi}$, in turn, is $E'(\mathbb{Q})[\hat{\phi}]/(E'(\mathbb{Q})[\hat{\phi}] \cap \phi(E(\mathbb{Q})))$. We claim that

$$E'(\mathbb{Q})[\hat{\phi}] \cap \phi(E(\mathbb{Q})) = \phi(E(\mathbb{Q})[2]).$$

Suppose $P' \in \phi(E(\mathbb{Q})[2])$. Then, obviously $P' \in \phi(E(\mathbb{Q}))$ but also, fixing a point $P \in E(\mathbb{Q})[2]$ such that $\phi(P) = P'$, we have

$$\hat{\phi}(P') = \hat{\phi}(\phi(P)) = [2]P = O.$$

Conversely, suppose $P' \in E'(\mathbb{Q})[\hat{\phi}] \cap \phi(E(\mathbb{Q})$. Then, there exists a point $P \in E(\mathbb{Q})$ such that $\phi(P) = P'$. But then we have

$$[2]P = \hat{\phi} \circ \phi(P) = \hat{\phi}(P') = O.$$

Taken together, we have argued that the following sequence is exact:

$$0 \to E'(\mathbb{Q})[\hat{\phi}]/\phi(E(\mathbb{Q})[2]) \to E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \to E(\mathbb{Q})/2E(\mathbb{Q}) \to E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q})) \to 0. \tag{7.3}$$

Thus, to compute $E(\mathbb{Q})/2E(\mathbb{Q})$, we compute both $S^{(\phi)}(E/\mathbb{Q})$ and $S^{(\hat{\phi})}(E'/\mathbb{Q})$, and then use the sequence.

8. Computational Examples

8.1. **Descent via a degree-2 isogeny.** We will illustrate with two concrete examples how descent via a degree-2 isogeny is used to calculate the Mordell-Weil group of an elliptic curve. Before we proceed, we prove the following lemma that will come in handy in showing that certain homogeneous spaces do not have a $\mathbb{Q}_p$-rational solution for some prime p (and hence don't belong to $S^{(\phi)}(E/\mathbb{Q})$). The lemma may be strengthened in different directions but it will suffice for our purposes.

Lemma 8.1. *Let $d \in \mathbb{Z}$ be squarefree and consider the hyperelliptic curve*

$$C : dw^2 = d^2 + adz^2 + bz^4,$$

for some $a, b \in \mathbb{Z}$. Let $p \mid d$ be a prime such that either

- $\mathrm{ord}_p(b) = 0$ *or,*
- $\mathrm{ord}_p(b) \neq 0$ *is even and* $4 \leq \mathrm{ord}_p(b) \leq \mathrm{ord}_p(a) + 2$.

Then $C(\mathbb{Q}_p) = \varnothing$.

Proof. Let p be such a prime. For the sake of contradiction, let (z, w) be a $\mathbb{Q}_p$-rational solution to C. Note that $\mathrm{ord}_p(dw^2)$ is odd since d is squarefree while $\mathrm{ord}_p(bz^4)$ is even in either case. We consider the two cases:

- $\mathrm{ord}_p(b) = 0$. We claim that $z \in \mathbb{Z}_p$ and thus $w \in \mathbb{Z}_p$ (since d is squarefree). Suppose not, so that we can rewrite C as

  $$\frac{u}{p^{2k-1}} = p^2 v_1 + \frac{a v_2}{p^{2l-1}} + \frac{v_3}{p^{4l}},$$

  with $l, k > 0$ (we are ignoring the case $k \leq 0$ here because it can be handled similarly) and $u, v_i \in \mathbb{Z}_p^\times$. Then either $2k-1 < 4l$ or $2k-1 > 4l$. Take the first possibility, so that clearing denominators and rearranging, we get

  $$v_3 = u p^{4l-2k+1} - p^{2l+2} v_1 - p^{2l+1} a v_2,$$

  which is a clear contradiction since the right side has positive valuation. The other possibility yields a similar contradiction. So, we must have $z, w \in \mathbb{Z}_p$ and we can reduce C over $\mathbb{F}_p$. Looking at C mod p, we see that $z \equiv 0 \pmod{d}$. Consequently, looking mod p^2, we have

$w \equiv 0 \pmod{p}$. But then we obtain $0 \equiv d^2 \pmod{p^3}$, a contradiction since d was assumed to be squarefree.

- $\mathrm{ord}_p(b) \neq 0$ is even and $4 \leq \mathrm{ord}_p(b) \leq \mathrm{ord}_p(a) + 2$. By an argument very similar to the previous case, we must have $z, w \in \mathbb{Z}_p$ (the inequality $\mathrm{ord}_p(b) - \mathrm{ord}_p(a) \leq 2$ is used here). Then, looking mod p^2, since $\mathrm{ord}_p(b) \geq 4$ and $\mathrm{ord}_p(a) \geq 2$, we conclude that $w \equiv 0 \pmod{p}$. But then reducing mod p^3, we again get $0 \equiv d^2 \pmod{p^3}$.

Thus, in either case we see that $C(\mathbb{Q}_p) = \varnothing$. □

Example 8.2. Let us now compute the Mordell-Weil group of

$$E : y^2 = x^3 + 6x^2 + x.$$

This elliptic curve has a degree-2 rational isogeny to

$$E' : y^2 = x^3 - 12x^2 + 32x.$$

We calculate the discriminant of E to be $\Delta = 2^9$. So, $B(2) = \{2\}$ and $\mathbb{Q}(B(2), 2) = \{\pm 1, \pm 2\}$. Note that,

$$(0, 0) \mapsto 6^2 - 4 \cdot 1 = 32 \equiv 2 \pmod{\mathbb{Q}^{\times 2}}.$$

We also know $O \mapsto 1 \pmod{\mathbb{Q}^{\times 2}}$. So, $1, 2 \in S^{(\phi)}(E/\mathbb{Q})$. We have to now analyze the homogeneous space C_d corresponding to each remaining $d \in \mathbb{Q}(B(2), 2)$ given by

$$C_d : dw^2 = d^2 - 12dz^2 + 32z^4.$$

Let us first analyze $d = -1$. The curve is

$$C_{-1} : -w^2 = 1 + 12z^2 + 32z^4.$$

Suppose $(z, w) \in \mathbb{Q}_2$ is a solution of C_{-1}. Then, since $\mathrm{ord}_2(-w^2)$ is even while $\mathrm{ord}_2(32z^4)$ is odd, by an argument very similar to the one in Lemma 8.1, we must have $z, w \in \mathbb{Z}_2$. However, we then have

$$w^2 \equiv -1 \equiv 3 \pmod{4},$$

a contradiction. Therefore, $-1 \notin S^{(\phi)}(E/\mathbb{Q})$. Since $S^{(\phi)}(E/\mathbb{Q})$ is a subgroup of $\mathbb{Q}(B(2), 2)$, and we know $2 \in S^{(\phi)}(E/\mathbb{Q})$, we also deduce that $-2 \notin S^{(\phi)}(E/\mathbb{Q})$.

Thus, $S^{(\phi)}(E/\mathbb{Q}) = \{1, 2\}$ and since we have shown each locally trivial homogeneous space also has a rational solution, we have $Ш(E/\mathbb{Q})[2] = 0$. So, we conclude from Lemma 6.7 that

$$E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \simeq S^{(\phi)}(E/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}.$$

Next, we have to repeat the same computation with the dual isogeny $\hat{\phi} : E' \to E$ to calculate $E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q}))$. It is easily checked that the discriminant of E' will involve the same primes as that of E and so $\mathbb{Q}(B(2), 2)$ remains the same. We have $O \mapsto 1 \pmod{\mathbb{Q}^{\times 2}}$ and

$$(0, 0) \mapsto 16 \equiv 1 \pmod{\mathbb{Q}^{\times 2}}.$$

So, here we don't get one point for free in $S^{(\phi)}(E'/\mathbb{Q})$. For each $d \in \mathbb{Q}(B(2), 2)$, the corresponding homogeneous space is

$$C'_d : dw^2 = d^2 + 24dz^2 + 16z^4.$$

Observe that we can then use Lemma 8.1 to rule out $d = \pm 2$. It remains to check $d = -1$, which is the curve

$$C'_{-1} : -w^2 = 1 - 24z^2 + 16z^4.$$

First, let us somewhat simplify the form of this curve by substituting $Z = 2z$ to get

$$-w^2 = 1 - 6Z^2 + Z^4.$$

Then, we notice the rational solution $(Z,w)=(1,2)\mapsto(z,w)=(1/2,2)$ and so $-1\in S^{(\hat{\phi})}(E'/\mathbb{Q})$. Thus, we have computed $S^{(\hat{\phi})}(E'/\mathbb{Q})=\{\pm 1\}$, and so

$$E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q}))\simeq S^{(\hat{\phi})}(E'/\mathbb{Q})\simeq\mathbb{Z}/2\mathbb{Z}.$$

Since $E'(\mathbb{Q})[\hat{\phi}]=\{O,(0,0)\}$ and $\phi(E(\mathbb{Q})[2])=\{O\}$, we have

$$E'(\mathbb{Q})[\hat{\phi}]/\phi(E(\mathbb{Q})[2])\simeq\mathbb{Z}/2\mathbb{Z}.$$

Then, the exact sequence 7.3 reads

$$0\to\mathbb{Z}/2\mathbb{Z}\to\mathbb{Z}/2\mathbb{Z}\to E(\mathbb{Q})/2E(\mathbb{Q})\to\mathbb{Z}/2\mathbb{Z}\to 0,$$

and so $E(\mathbb{Q})/2E(\mathbb{Q})\simeq\mathbb{Z}/2\mathbb{Z}$. The Mordell-Weil Theorem then implies that $E(\mathbb{Q})$ is either $\mathbb{Z}$ or $\mathbb{Z}/2m\mathbb{Z}$, but since E does have a nontrivial point of torsion $(0,0)$, we rule out the first possibility. So, E has rank 0 and we need to determine the torsion $E_{\text{tors}}(\mathbb{Q})$, which we could do using Proposition 2.2, but in this case the Nagell-Lutz Theorem is quicker (because we already know all rational points must be torsion). A nonzero point $(x,y)\neq(0,0)\in E_{\text{tors}}(\mathbb{Q})$ has integer coordinates and further $y^2\mid\Delta=2^9$, i.e., $y^2\in\{1,2^2,2^4,2^6,2^8\}$. We have

$$y^2=x(x^2+6x+1),$$

and so we see $y^2=1$ is not possible. For $y^2=2^{2k}$ with $k>0$, we must have $x=\pm 1$ (otherwise x^2+6x+1 is odd and different from ± 1). From this, we thus get $y^2=4$ corresponding to $x=1$ as the only possibility. Therefore, $E_{\text{tors}}(\mathbb{Q})=\{O,(0,0),(-1,\pm 2)\}$ and Mordell-Weil group of E has rank 0 and is isomorphic to $\mathbb{Z}/4\mathbb{Z}$. Indeed, we can confirm this result is correct by searching the LMFDB database [9] using the j-invariant 287496 of E. Then comparing Weierstrass forms, the elliptic curve in the LMFDB that is isomorphic over $\mathbb{Q}$ to our curve E is 32.a2, where the reader can find plenty more fascinating information about it. (Note that their Weierstrass form differs ours and can be obtained by the transformation $x\mapsto x-2$.)

But why stop there? Through this computation, we have also determined

$$E'(\mathbb{Q})/2E'(\mathbb{Q})\simeq\mathbb{Z}/2\mathbb{Z},$$

and then calculating the torsion, we get $E'(\mathbb{Q})\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. In fact, E' is rather special because it has j-invariant 1728 and can be represented by the Weierstrass form

$$E':y^2=x^3-x,$$

corresponding to 32.a3 in the LMFDB.

Example 8.3. Let us next look at the slightly more interesting elliptic curve

$$E:y^2=x^3+9x^2-x,$$

with

$$E':y^2=x^3-18x^2+85x,$$

and discriminant $\Delta=2^4\cdot 5\cdot 17$. So, we have 16 possibilities in

$$\mathbb{Q}(B(2),2)=\{\pm 1,\pm 2,\pm 5,\pm 17,\pm 10,\pm 34,\pm 85,\pm 170\}.$$

Note that $(0,0)\in E'(\mathbb{Q})$ is mapped to 85 (mod $\mathbb{Q}^{\times 2}$). Corresponding to each remaining $d\in\mathbb{Q}(B(2),2)$ is the homogeneous space

$$C_d:dw^2=d^2-18dz^2+85z^4.$$

Then, we immediately know that $\pm 2,\pm 10,\pm 34,\pm 170\notin S^{(\phi)}(E/\mathbb{Q})$ using Lemma 8.1. Let us next check $d=5$,

$$C_5:5w^2=25-90z^2+85z^4,$$

in which we can cancel 5 to obtain

$$w^2 = 5 - 18z^2 + 17z^4.$$

By inspection, we see this has the rational solution $(z, w) = (1, 2)$, and so $5 \in S^{(\phi)}(E/\mathbb{Q})$. By our discussion in the preceding section (7.2), we also recover the rational point $(5/1^2, 5 \cdot 2/1^3) = (5, 10)$ on E'.

Since $85 \in S^{(\phi)}(E/\mathbb{Q})$, we have $17 = 85/5 \in S^{(\phi)}(E/\mathbb{Q})$. So far we have $\{1, 5, 17, 85\} \subseteq S^{(\phi)}(E/\mathbb{Q})$. Since $S^{(\phi)}(E/\mathbb{Q})$ is a subgroup of $\mathbb{Q}(B(2), 2)$, $S^{(\phi)}(E/\mathbb{Q})$ must be either contain or be disjoint from $\{-1, -5, -17, -85\}$. We observe that if $d < 0$, then C_d has no solutions over $\mathbb{R}$, so like in the previous example, we should be praying that the elements of $\{-1, -5, -17, -85\}$ are not nontrivial in Ш. This is indeed the case! Consider

$$C_{-85} : -85w^2 = 85^2 + 18 \cdot 85z^2 + 85z^4,$$

which after cancelling 85 and completing the square becomes

$$\left(\frac{z^2 + 9}{2}\right)^2 + \left(\frac{w}{2}\right)^2 = -1.$$

Note that a $\mathbb{Q}_p$-rational solution for this equation implies one for

$$a^2 + b^2 = -1.$$

Suppose we have a solution (a, b) over $\mathbb{Q}_2$. Then for large enough $k \in \mathbb{Z}_{\geq 0}$, we can write this last equation as

$$u^2 + v^2 = -2^{2k},$$

with $u, v \in \mathbb{Z}_2$, where we can assume without loss of generality that $\mathrm{ord}_2(v) = 0$. Suppose $k = 0$. Then, $u^2 + v^2 \equiv 3 \pmod 4$, which is impossible. Alternatively, if $k > 0$, then $u^2 + v^2 \equiv 0 \pmod 4$, implying that $u, v \equiv 0 \pmod 2$, contradicting our assumption that $\mathrm{ord}_2(v) = 0$. Thus, $C_{-85}(\mathbb{Q}_2) = \varnothing$ and $-85 \notin S^{(\hat{\phi})}(E'/\mathbb{Q})$.

We have then calculated

$$E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \simeq S^{(\phi)}(E/\mathbb{Q}) = \{1, 5, 17, 85\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Let us now analyze

$$C'_d : dw^2 = d^2 + 36dz^2 - 16z^4.$$

But, by Lemma 8.1, we can rule out any d which has at least one prime divisor. Further, note that $(0, 0)$ maps to $-16 \equiv -1 \pmod{\mathbb{Q}^{\times 2}}$. Thus,

$$E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q})) \simeq S^{(\hat{\phi})}(E'/\mathbb{Q}) = \{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z}.$$

Therefore, the sequence 7.3 is

$$0 \to \mathbb{Z}/2\mathbb{Z} \to (\mathbb{Z}/2\mathbb{Z})^2 \to E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathbb{Z}/2\mathbb{Z} \to 0,$$

and so $E(\mathbb{Q})/2E(\mathbb{Q})$ is either $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. But it is easy to see that the former is not possible because elements of $E(\mathbb{Q})/2E(\mathbb{Q})$ have order at most 2 (therefore, in general it is $(\mathbb{Z}/2\mathbb{Z})^n, n \in \mathbb{Z}_{\geq 0}$). Finally, using the Nagell-Lutz Theorem we check that $E_{\mathrm{tors}}(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$, and thus $E(\mathbb{Q}) \simeq \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, meaning that E has rank 1. This elliptic curve E corresponds to 340.a1 in the LMFDB. Similarly, $E'(\mathbb{Q}) \simeq \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and E' is 340.a2.

8.2. **Descent via a degree-3 isogeny.** We now attempt to mimic the technique of descent by a degree-2 isogeny with a degree-3 isogeny. Because $\mathbb{Q}$ does not contain μ_3, the transition to a degree-3 isogeny introduces complications. See Top [17] for a discussion on elliptic curves that admit a rational 3-isogeny.

Example 8.4. Let us consider

$$E : y^2 = x^3 + 16.$$

This curve can be calculated to have rational torsion $E_{\text{tors}}(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$ corresponding to the points $\{O, (0, \pm 4)\}$. Thus, it does not have a rational point of order 2, and the degree-2 isogeny we have been using does not exist for this curve. To begin trying to adapt the descent by 2-isogeny for this curve, we need a degree-3 isogeny with kernel $E_{\text{tors}}(\mathbb{Q})$. Vèlu [18] has shown how to construct such isogenies and the method is implemented in Sage as `EllipticCurveIsogeny`. Using Sage, we find the following degree-3 rational isogeny $\phi : E \to E'$

$$\phi : (x, y) \mapsto \left((x^3 + 64)/x^2, y(x^3 - 128)/x^3\right),$$

where E' is the elliptic curve

$$E' : y^2 = x^3 - 432.$$

Here $E[\phi] \simeq \mu_3$ as groups. But the identification does not extend as $G = G_{\bar{\mathbb{Q}}/\mathbb{Q}}$-modules since μ_3 is not contained within $\mathbb{Q}$, and so some care needs to be taken in how we identify cohomology. This can be fixed in the following way. Let $K = \mathbb{Q}(\zeta_3)$, where ζ_3 is a primitive third root of unity. Then, we *can* identify $E[\phi]$ with μ_3 as a $G_{\bar{\mathbb{Q}}/K}$-module. By exactly the same argument as in Example 6.9, we then have

$$H^1(G_{\bar{\mathbb{Q}}/K}, E[\phi]) \simeq H^1(G_{\bar{\mathbb{Q}}/K}, \mu_3) \simeq K^\times / K^{\times 3},$$

and

$$H^1(G_{\bar{\mathbb{Q}}/K}, E[\phi]; S) \simeq K(B(\phi), 3).$$

The cohomology group $H^1(G_{\bar{\mathbb{Q}}/K}, E[\phi])$, however, does not fit well into our sequence 6.1, since we are still interested in computing rational points rather than K-rational points on E. This is a good example of the kind of situtation the restriction-inflation sequence 3.5 comes in handy. In particular, since $G_{\bar{\mathbb{Q}}/K}$ is normal in G, the restriction-inflation sequence reads

$$0 \to H^1(G/G_{\bar{\mathbb{Q}}/K}, H^0(G_{\bar{\mathbb{Q}}/K}, E[\phi])) \to H^1(G, E[\phi]) \to H^1(G_{\bar{\mathbb{Q}}/K}, E[\phi]).$$

As $E[\phi] \subseteq \mathbb{Q}$, we have $H^0(G_{\bar{\mathbb{Q}}/K}, E[\phi]) = E[\phi]$. We claim that $H^1(G/G_{\bar{\mathbb{Q}}/K}, E[\phi]) = 0$. Indeed, $G/G_{\bar{\mathbb{Q}}/K}$ is isomorphic to $\text{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q}) \simeq (\mathbb{Z}/3\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}$. If 1 is the trivial automorphism, σ is the nontrivial automorphism, and $\xi \in H^1(G/G_{\bar{\mathbb{Q}}/K}, E[\phi])$, then

$$(0, 0) = \xi_1 = \xi_{\sigma\cdot\sigma} = \xi_\sigma^\sigma + \xi_\sigma = 2\xi_\sigma,$$

meaning that $\xi_\sigma = (0, 0)$ since the other points of $E[\phi]$ have order 3. So, $H^0(G_{\bar{\mathbb{Q}}/K}, E[\phi])$ is trivial and $H^1(G, E[\phi]) \to H^1(G_{\bar{\mathbb{Q}}/K}, E[\phi])$ is injective. In fact, it is also surjective and the quickest way to see this is appeal to the full restriction-inflation sequence, which tells us the term on the right of $H^1(G_{\bar{\mathbb{Q}}/K}, E[\phi])$ is $H^2(G/G_{\bar{\mathbb{Q}}/K}, E[\phi])$. It can be checked that $H^2(G/G_{\bar{\mathbb{Q}}/K}, E[\phi]) = 0$ too, but we don't do that here since we have not formally introduced H^2 (but see [1]). Therefore, we have the isomorphism

$$H^1(G, E[\phi]) \simeq H^1(G_{\bar{\mathbb{Q}}/K}, E[\phi]),$$

that is essentially saying each 1-cocycle $G_{\bar{\mathbb{Q}}/K} \to E[\phi]$ can be extended uniquely to a 1-cocycle $G \to E[\phi]$. Thus, we have, similar to the 2-isogeny case, that

$$H^1(G, E[\phi]; B(\phi)) \simeq K(B(\phi), 3).$$

What is $K(B(\phi),3)$? We have $\Delta(E) = -2^{12}\cdot 3^3$ and $\deg(\phi) = 3$. Over $\mathbb{Q}$, the bad primes would have been 2 and 3, but since we are now working in $K = \mathbb{Q}(\zeta_3)$, we have to work with the valuations induced by the prime ideals of $\mathbb{Z}[\zeta_3]$, the ring of integers of K. So, we have to determine how 2 and 3 factor in $\mathbb{Z}[\zeta_3]$. The minimal polynomial of ζ_3 over $\mathbb{Q}$ is $f(x) = x^2 + x + 1$. Therefore, by the Dedekind-Kummer Theorem [11, Ch. 1, Prop. 8.3]

- $f(x)$ is irreducible over $\mathbb{Z}/2\mathbb{Z}$ and so 2 remains prime in $\mathbb{Z}[\zeta_3]$.
- $f(x) \equiv (x-1)^2 \pmod 3$ and so 3 ramifies with
$$\langle 3\rangle = \langle 3, \zeta_3 - 1\rangle^2 = \langle \zeta_3 - 1\rangle^2,$$
since $3 = -(\zeta_3 - 1)(\zeta_3 + 2)$.

Since $\mathbb{Z}[\zeta_3]^\times = \{\pm 1, \pm\zeta_3, \pm\zeta_3^2\}$ and $\mathbb{Z}[\zeta_3]$ is a UFD, a complete set of unique representatives for $K(B(\phi),3)$ is
$$\{\zeta_3^r \cdot 2^s \cdot (\zeta_3 - 1)^t : r, s, t \in \{0,1,2\}\}.$$
It remains to consider the homogeneous space corresponding to each class $\{d\} \in K(B(\phi),3)$. Each $\{d\} \in K(B(\phi),3)$ corresponds to the 1-cocycle
$$\sigma \mapsto \begin{cases} 1 & \sqrt[3]{d}^\sigma = \sqrt[3]{d} \\ (0,4) & \sqrt[3]{d}^\sigma = \zeta_3\sqrt[3]{d} \\ (0,-4) & \sqrt[3]{d}^\sigma = \zeta_3^2\sqrt[3]{d}. \end{cases}$$
Then, for each $d \in K(B(\phi),3)$, similar to how we re-derived C_d in Section 7, we find the following homogeneous space for each $d = a + b\zeta_3 \in K(B(\phi),3)$:
$$C_d : bw^3 + 6(2a-b)w^2z + 36bwz^2 - 24(2a-b)z^3 = 24.$$
Besides the fact that this is more complicated than the case of 2-isogenies, note the asymmetry in a and b that arises from the fact that $d = a + b\zeta_3$ has real part $a - b/2$ and complex part $b\sqrt{3}/2$. Studying such spaces for each of the 27 classes in $K(B(\phi),3)$ would obviously be quite painstaking. The saving grace is the following fact: the elements of $K(B(\phi),3)$ that end up being in $S^{(\phi)}(E/\mathbb{Q})$ must necessarily have norm (in the extension $K/\mathbb{Q}$) that is a rational cube; we will take this result for granted here but see [17, §4]. This observation drastically cuts down the values of d we have to consider to $\{1, \zeta_3, \zeta_3^2\}$. We know $O \in E'(\mathbb{Q})$ maps to $d = 1$. We can also check $\zeta_3, \zeta_3^2 \in S^{(\phi)}(E/\mathbb{Q})$, for example because the point $(z,w) = (0,1)$ is on both C_{ζ_3} and $C_{\zeta_3^2}$. Thus,
$$E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \simeq S^{(\phi)}(E/\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}.$$
From the points on C_{ζ_3} and $C_{\zeta_3^2}$, we also find the non-obvious points $(12, \pm 36) \in E'(\mathbb{Q})$.

We next repeat the computation with $S^{(\hat\phi)}(E'\mathbb{Q})$. Since $\Delta(E') = -2^{12}\cdot 3^9$, $K(B(\phi),3)$ remains the same (and we have to only check $d = \zeta_3$ and ζ_3^2). The corresponding homogeneous spaces are
$$C'_d : bw^3 + (2a-b)w^2z + 27bwz^2 + 3(2a-b)z^3 = 24.$$
We again find that
$$E(\mathbb{Q})/\hat\phi(E'(\mathbb{Q})) \simeq S^{(\hat\phi)}(E'/\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}.$$
Finally, using the sequence (7.3), we compute
$$E(\mathbb{Q})/3E(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z} \simeq E'(\mathbb{Q})/3E'(\mathbb{Q}).$$
Checking torsion, we conclude that
$$E(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z} \simeq E'(\mathbb{Q}).$$
Thus, $E(\mathbb{Q}) = \{O, (0,\pm 4)\}$ and $E'(\mathbb{Q}) = \{O, (12, \pm 36)\}$. The elliptic curves E and E' are 27.a4 and 27.a3 respectively in the LMFDB.

The LMFDB entry 27.a3 tells us that E' is a Weierstrass model for the Fermat cubic curve. We end by using this fact to prove the following. It is fascinating that this proof ultimately still requires a full understanding of arithmetic in $\mathbb{Q}(\zeta_3)$ and uses descent, albeit dressed up quite differently.

Theorem 8.5. *The equation*

$$X^3 + Y^3 = Z^3$$

has no nontrivial integer solutions.

Proof. Suppose we had an integer solution (X, Y, Z) with $XYZ \neq 0$. Then, we obtain a rational solution different from O to

$$y^2 = x^3 - 432,$$

by letting $(x, y) = (-12X/(Y - Z), 36(Y + Z)/(Y - Z))$. By the previous example, we must then have $(Y + Z)/(Y - Z) = \pm 1$, from which we obtain either $Y = 0$ or $Z = 0$, a contradiction. □

Acknowledgments

I would like to thank Professor Joe Mileti for giving me the opportunity to study this topic and for his valuable feedback. Thanks also to Professor Jen Paulhus for inspiring my interest in elliptic curves and for helping me find references that were useful in writing this exposition.

References

[1] M.F. Atiyah and C. Wall. "Algebraic Number Theory". In: ed. by J.W.S Cassels and A. Fröhlich. Academic Press, 1967. Chap. Cohomology of groups, pp. 94–115.

[2] J.W.S Cassels. *Lectures on Elliptic Curves*. Cambridge University Press, 1991.

[3] J.W.S Cassels and E.V. Flynn. *Prolegomena to Middlebrow Artihmetic of Curves of Genus 2*. Cambridge University Press, 1996.

[4] R. Hartshorne. *Algebraic Geometry*. Springer, 1977.

[5] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory*. Springer, 1982.

[6] V.A. Kolyvagin. "Finiteness of $E(\mathbb{Q})$ and $Ш(E, \mathbb{Q})$ for a Subclass of Weil Curves". In: *Izv. Akad. Nauk SSSR Ser. Mat.* 52.3 (1988), pp. 522–540.

[7] S. Lang. *Algebra*. 2nd. Addison-Wesley Publishing Company, 1984.

[8] C-E. Lind. "Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins". PhD thesis. University of Uppsala, 1940.

[9] The LMFDB Collaboration. *The L-functions and Modular Forms Database*. `http://www.lmfdb.org`. May 2021.

[10] B. Mazur. "Rational isogenies of prime degree (appendix by D. Goldfeld)". In: *Invent. Math.* 44.2 (1978), pp. 129–162.

[11] J. Neukirch. *Algebraic Number Theory*. Springer, 1991.

[12] B. Poonen. *Computing Rational Points on Curves*. URL: `http://www-math.mit.edu/~poonen/papers/millennial.pdf`.

[13] H. Reichardt. "Einige im Kleinen überall lösbare, im Grossen unlösbare diophantische Gleichungen". In: *J. Reine Angew. Math.* 184 (1942), pp. 12–18.

[14] K. Rubin. "Tate-Shafarevich group and L-functions of Elliptic Curves with Complex Multiplication". In: *Invent. Math.* 89.3 (1987), pp. 527–560.

[15] E.S. Selmer. "The Diophantine Equation $ax^3 + by^3 + cz^3 = 0$". In: *Acta Math.* 85 (1951), pp. 203–362.

[16] J.H. Silverman. *The Arithmetic of Elliptic Curves*. 1st ed. Springer, 1985.

[17] J. Top. "Descent by 3-isogeny and 3-rank of quadratic fields". In: *Advances in number theory : the Proceedings of the Third Conference of the Canadian Number Theory Association*. Vol. Oxford University Press. 1993, pp. 303–317.

[18] J. Vélu. “Isogénies entre courbes elliptiques”. In: *C.R. Acad. Sc. Paris* 273 (1971), pp. 238–241.