

**ELLIPTIC CURVES AND DIOPHANTINE STABILITY**

**By**

**MAYAH TEPLITSKIY**

\* \* \* \* \*

Submitted in partial fulfillment of the requirements for  
Honors in the Department of Mathematics

Union College  
March 15, 2024

## ABSTRACT

MAYAH TEPLITSKIY   Elliptic curves and diophantine stability.

Department of Mathematics, March 15, 2024.

ADVISOR: HATLEY, JEFFREY

In [RW23], Ray and Weston define the notion of *diophantine stability at  $\ell$*  for an elliptic curve  $E/K$  defined over a number field  $K$  and a prime  $\ell$ . We provide a brief discussion of Galois theory and algebraic number theory, while building up intuition and implications for possible answers to the following question: For a fixed elliptic curve  $E/K$  and a fixed prime  $\ell > 3$ , what number fields  $K$  allow  $E/K$  to satisfy the property of being diophantine stable at  $\ell$ ?

## ACKNOWLEDGEMENT

Thank you to Jeff Hatley, my advisor, for making this thesis and my math major possible. I can't believe I've had you every term of my undergraduate studies! You continue to push me as a student and to enable me to pursue my mathematical goals and interests. Thank you so much for everything! I couldn't have done it without you.

## NOTATION

We shall use the following notation throughout this thesis. We write  $\mathbb{N}$  for the set of natural numbers,  $\mathbb{Q}$  for the set of rational numbers,  $\mathbb{F}_p$  for the finite field of order  $p$ , and  $\mathrm{GL}_2(\mathbb{F}_p)$  for the general linear group with matrix components in  $\mathbb{F}_p$ . We let  $K$  be an algebraic number field, and  $L/K$  be a Galois field extension over  $K$ . Then we use  $\mathrm{Gal}(L/K)$  to denote the Galois group of the extension  $L/K$ ,  $\bar{\mathbb{Q}}$  to represent the algebraic closure of  $\mathbb{Q}$ , and  $G_{\mathbb{Q}}$  for the absolute Galois group  $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ .

We write  $E/K$  for an elliptic curve  $E$  over a field  $K$ ,  $\mathcal{O}$  for the point at infinity, and  $E[p]$  for the set of all  $p$ -torsion points on  $E$ . Then  $\bar{\rho}_E$  is the mod  $p$  Galois representation  $\bar{\rho}_E : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{F}_p)$  and  $\bar{\rho}'_E : G_{\mathbb{Q}} \rightarrow \frac{\mathrm{GL}_2(\mathbb{F}_p)}{\langle \pm 1 \rangle}$  the composition of  $\bar{\rho}_E$  with the natural quotient map.

We let  $O_K$  be the ring of integers of  $K$ . Then  $D(P_i/p)$  is the decomposition group for  $P_i/p$  where  $P_i$  is a prime that lies over the prime  $p$  in  $O_K$ , and  $I(P_i/p)$  is the inertia group for  $P_i/p$ . Finally,  $\mathrm{Frob}_{\mathcal{P}_i}$  represents the Frobenius element of  $\mathcal{P}_i$ .

## CONTENTS

ABSTRACT	ii
ACKNOWLEDGEMENT	iii
NOTATION	iv
1. INTRODUCTION	1
2. Elliptic Curves	2
3. Diophantine Stability	5
4. Prime Decomposition	8
5. Counting Arguments about Prime Decomposition	14
6. A Concrete Example	18
References	21

## 1. INTRODUCTION

In [RW23], Ray and Weston define the notion of *diophantine stability* for elliptic curves and then proceed to study the following question: Let  $L/K$  be a field extension and  $\ell$  be a prime. How many elliptic curves  $E/K$  are diophantine stable at  $\ell$ ? Mazur and Rubin had partially answered this question in [MR18], where they found that the set of elliptic curves which satisfy the property of being diophantine stable at  $\ell$  has positive density. Ray and Weston showed that the density of this set is in fact 1.

Let  $\mathcal{T}_{K,\ell}$  be the set of elliptic curves  $E/K$  that are diophantine stable at  $\ell$ . Ray and Weston fix an algebraic number field  $K$  and a prime  $\ell$  and calculate the density of  $\mathcal{T}_{K,\ell}$  in the set of all elliptic curves. In this thesis, we look at the inverse problem. We fix an elliptic curve  $E/K$  and a prime  $\ell$  and ask for which number fields  $K$ ,  $E/K$  is an element of  $\mathcal{T}_{K,\ell}$ .

In Section 2, we introduce elliptic curves and Galois representations, providing the necessary background to define diophantine stability. In Section 3, we state Ray and Weston's definition for elliptic curves being diophantine stable at a prime  $\ell$ . In the fourth section, we provide background on prime decomposition in number fields. In Section 5, we discuss results from [DT02] and use them to analyze the main question of this thesis. Finally, in Section 6, we work through a concrete example.

## 2. ELLIPTIC CURVES

The aim of this thesis is to provide intuition for number fields that make elliptic curves diophantine stable. Before we look at the definition of diophantine stability, we will recall some facts about elliptic curves.

**Definition 1.** An *elliptic curve*  $E$  over a field  $K$  is a smooth projective curve of genus 1 defined over  $K$ , together with a specific point  $\mathcal{O} \in E$  which is also defined over  $K$  and is called the point at infinity.

All elliptic curves have a rational point  $\mathcal{O}$ , and can therefore be written in *Weierstrass normal form*, meaning their affine points satisfy equations of the form:

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

It is worth noting that the points on an elliptic curve form a group under an operation called *point addition*, where  $\mathcal{O}$  is the identity. The specifics of this group operation aren't important for the purpose of this thesis. But, the interested reader can look to Chapter 1 of [ST15] for a detailed discussion of point addition.

**Definition 2.** A *torsion point* on an elliptic curve is a point of finite order.

Let  $\ell$  be a prime. If applying the operation of point addition to a point  $\ell$  times produces  $\mathcal{O}$ , then we say the point is an  $\ell$ -torsion point. We denote the set of  $\ell$ -torsion points by  $E[\ell]$ .

Elliptic curves are important because they give us a way to transform questions about Galois extensions into linear algebra through a Galois representation. So, what exactly is a Galois representation? Let  $E/\mathbb{Q}$  be an elliptic curve and

let  $G_{\mathbb{Q}}$  denote the Galois group  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ , where  $\bar{\mathbb{Q}}$  is a fixed algebraic closure of  $\mathbb{Q}$ . We call this Galois group the *absolute Galois group* of  $\mathbb{Q}$ . It turns out that  $E[\ell]$  is isomorphic to  $\mathbb{F}_{\ell} \times \mathbb{F}_{\ell}$ , so we can pick a basis  $\{P, Q\}$  for  $E[\ell]$ , meaning  $E[\ell] = \{x_1P + x_2Q \mid x_1, x_2 \in \mathbb{F}_{\ell}\}$ . It is worth noting that, although  $P$  and  $Q$  are likely not defined over  $\mathbb{Q}$ , they are defined over  $\bar{\mathbb{Q}}$ . Let  $\sigma$  be an element of  $G_{\mathbb{Q}}$ . Then  $\sigma(P) = a_{\sigma}P + c_{\sigma}Q$  and  $\sigma(Q) = b_{\sigma}P + d_{\sigma}Q$  for some  $a_{\sigma}, b_{\sigma}, c_{\sigma}, d_{\sigma} \in \mathbb{F}_{\ell}$ . Therefore,  $\sigma$  maps to the matrix

$$\begin{bmatrix} a_{\sigma} & b_{\sigma} \\ c_{\sigma} & d_{\sigma} \end{bmatrix}$$

in  $\text{GL}_2(\mathbb{F}_{\ell})$ .

**Proposition 1.** *The mapping  $\bar{\rho}_E : G_{\mathbb{Q}} \rightarrow \text{GL}_2(\mathbb{F}_{\ell})$  described above is a homomorphism.*

*Proof.* We show that  $\bar{\rho}_E$  satisfies  $\bar{\rho}_E(\sigma \circ \tau) = \bar{\rho}_E(\sigma) \cdot \bar{\rho}_E(\tau)$ . This is the same as matrix multiplication. We know

$$\bar{\rho}_E(\sigma) \cdot \bar{\rho}_E(\tau) = \begin{bmatrix} a_{\sigma} & b_{\sigma} \\ c_{\sigma} & d_{\sigma} \end{bmatrix} \cdot \begin{bmatrix} a_{\tau} & b_{\tau} \\ c_{\tau} & d_{\tau} \end{bmatrix} = \begin{bmatrix} a_{\tau}a_{\sigma} + c_{\tau}b_{\sigma} & b_{\tau}a_{\sigma} + d_{\tau}b_{\sigma} \\ a_{\tau}c_{\sigma} + c_{\tau}d_{\sigma} & b_{\tau}c_{\sigma} + d_{\tau}d_{\sigma} \end{bmatrix}.$$

So, we need to show that this is also equal to  $\bar{\rho}_E(\sigma \circ \tau)$ . We begin by applying  $\tau$  to  $P$  and  $Q$ , which gives  $\tau(P) = a_{\tau}P + c_{\tau}Q$  and  $\tau(Q) = b_{\tau}P + d_{\tau}Q$ . Then, applying  $\sigma$  gives

$$\begin{aligned} \sigma(\tau(P)) &= a_{\tau}\sigma(P) + c_{\tau}\sigma(Q) \\ &= a_{\tau}(a_{\sigma}P + c_{\sigma}Q) + c_{\tau}(b_{\sigma}P + d_{\sigma}Q) \\ &= (a_{\tau}a_{\sigma} + c_{\tau}b_{\sigma})P + (a_{\tau}c_{\sigma} + c_{\tau}d_{\sigma})Q \end{aligned}$$



and, similarly

$$\begin{aligned}
\sigma(\tau(Q)) &= b_\tau\sigma(P) + d_\tau\sigma(Q) \\
&= b_\tau(a_\sigma P + c_\sigma Q) + d_\tau(b_\sigma P + d_\sigma Q) \\
&= (b_\tau a_\sigma + d_\tau b_\sigma)P + (b_\tau c_\sigma + d_\tau d_\sigma)Q
\end{aligned}$$

Therefore,

$$\bar{\rho}_E(\sigma \circ \tau) = \begin{bmatrix} a_\tau a_\sigma + c_\tau b_\sigma & b_\tau a_\sigma + d_\tau b_\sigma \\ a_\tau c_\sigma + c_\tau d_\sigma & b_\tau c_\sigma + d_\tau d_\sigma \end{bmatrix}.$$

So, we can see  $\bar{\rho}_E$  preserves matrix multiplication, i.e.  $\bar{\rho}_E(\sigma \circ \tau) = \bar{\rho}_E(\sigma) \cdot \bar{\rho}_E(\tau)$ .  $\square$

In fact, this homomorphism is what we call a *Galois representation*.

Now, let  $\ker(\bar{\rho}_E)$  be the kernel of  $\bar{\rho}_E$ . Then, by the first isomorphism theorem,  $G_{\mathbb{Q}}/\ker(\bar{\rho}_E)$  is isomorphic to a subgroup of  $\mathrm{GL}_2(\mathbb{F}_\ell)$ . In most cases, though, it turns out that  $\bar{\rho}_E$  is surjective. Since  $\mathrm{GL}_2(\mathbb{F}_\ell)$  is a finite group,  $G_{\mathbb{Q}}/\ker(\bar{\rho}_E)$  is the Galois group for some finite extension of  $\mathbb{Q}$  (particularly, the fixed field of  $\ker(\bar{\rho}_E)$ ), which we will call  $L$ . Then we say  $L$  is the finite extension of  $\mathbb{Q}$  which is *cut out* by  $\bar{\rho}_E$ . In other words, it is the fixed field of  $\ker(\bar{\rho}_E)$ .

The kernel of  $\bar{\rho}_E$  is actually the Galois group of the extension  $\bar{\mathbb{Q}}/L$ . On the other hand,  $\ker(\bar{\rho}_E)$  is the kernel of  $\bar{\rho}_E$ , so it's the collection of elements of  $G_{\mathbb{Q}}$  that get mapped to the identity matrix, or the collection of elements of  $G_{\mathbb{Q}}$  that fix every point in  $E[\ell]$ . In other words,  $L$  is the field obtained by adjoining to  $\mathbb{Q}$  all of the coordinates of the points in  $E[\ell]$ , so we write  $L = \mathbb{Q}(E[\ell])$ . We will come back to this field in Section 3 when we define diophantine stability.

For the purposes of this thesis, we will make the assumption that  $\bar{\rho}_E$  is surjective. We therefore include the following theorem, which shows that this is a mild assumption.

**Theorem 1.** *(Serre, 1972) Let  $E$  be an elliptic curve given by a Weierstrass equation with rational coefficients. Assume that  $E$  does not have complex multiplication. Then for sufficiently large  $\ell$ , the Galois representation*

$$\rho_\ell : \text{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{F}_\ell)$$

*is surjective.*

### 3. DIOPHANTINE STABILITY

Now that we have defined elliptic curves and Galois representations, we are ready to introduce the notion of diophantine stability defined in [RW23], which is really the core idea of this thesis. We let  $\ell$  be a prime greater than 3.

**Definition 3.** Let  $L/K$  be a field extension and let  $E_{/K}$  be an elliptic curve. Then,  $E_{/K}$  is said to be diophantine stable in  $L$  if  $E(L) = E(K)$ . It is said that  $E_{/K}$  is diophantine stable at  $\ell$  if for all  $n \in \mathbb{Z}_{\geq 1}$  and every finite set of primes  $\Sigma$  of  $K$ , there are infinitely many  $\mathbb{Z}/\ell^n\mathbb{Z}$ -extensions  $L/K$  such that

- (1)  $E(L) = E(K)$ ,
- (2) all primes in  $\Sigma$  are completely split in  $L$ .

Given an elliptic curve  $E_{/\mathbb{Q}}$ , we say that  $(E, K, \ell)$  satisfies (DS) if  $E_{/K}$  is diophantine stable at  $\ell$ .

It is worth noting that, generally, if  $L$  is an extension of  $K$ ,  $E(L)$  is not necessarily equal to  $E(K)$ . If  $E(K)$  is the collection of points on an elliptic curve that are defined over the field  $K$ , it's somewhat intuitive that there

would be more of these points on  $E$  that are defined over an extension of  $K$ . And this often happens.

**Example.** For example, take  $E$  to be the elliptic curve with Cremona label 64a4. This curve can be written in Weierstrass form as  $y^2 = x^3 + x$ . Then the only rational point on  $E$  that is defined over  $\mathbb{Q}$  is  $(0, 0)$ . But, if we look at  $E(\mathbb{Q}(i))$  where  $i = \sqrt{-1}$ , we get the point  $(i, 0)$ , which did not exist in  $E(\mathbb{Q})$ . And we can check that this satisfies the elliptic curve equation. Plugging the point into the equation we get  $0^2 = i^3 + i$ , and then we can simplify to  $0 = -i + i$ . So,  $E(\mathbb{Q}) \neq E(\mathbb{Q}(i))$ .

So, elliptic curves  $E/K$  that are diophantine stable at  $\ell$  are special in the sense that they do not pick up points over extensions.

In [RW23], Ray and Weston prove that, density-wise, 100% of elliptic curves  $E/K$  are diophantine stable at  $\ell$  for a fixed number field  $K$  and fixed prime  $\ell$  by defining a set  $\mathcal{T}_{K,\ell}$  of elliptic curves, showing that every elliptic curve in  $\mathcal{T}_{K,\ell}$  is diophantine stable at  $\ell$ , and finally, showing that 100% of elliptic curves are in the set  $\mathcal{T}_{K,\ell}$ . We will define the set  $\mathcal{T}_{K,\ell}$ , but exclude the other results since the definition of  $\mathcal{T}_{K,\ell}$  is particularly important to our analysis.

Before we do this, we first recall the necessary notation for this section. For a number field  $K$ , we write  $G_K$  to denote the Galois group  $\text{Gal}(\bar{K}/K)$ . Letting  $E/\mathbb{Q}$  be an elliptic curve defined over  $\mathbb{Q}$ , we write  $E[\ell]$  to denote the  $\ell$ -torsion group

$$E[\ell] := \ker(E(\bar{\mathbb{Q}}) \xrightarrow{\ell} E(\bar{\mathbb{Q}})).$$

Let  $\bar{\rho}_E : G_{\mathbb{Q}} \rightarrow \text{GL}_2(\mathbb{F}_{\ell})$  denote the Galois representation on  $E[\ell]$ . We will use  $\mathbb{Q}(E[\ell])$  to denote the field cut out by  $E[\ell]$ , or  $\bar{\mathbb{Q}}^{\ker \bar{\rho}_{E,\ell}}$ . Finally,  $\bar{\rho}'_E$  is the

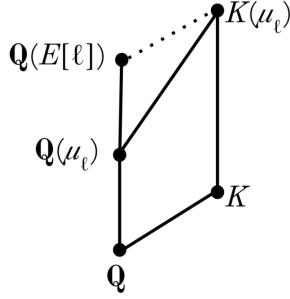


FIGURE 3.1. Field Extension Diagram

Galois representation  $\bar{\rho}'_E : G_{\mathbb{Q}} \rightarrow \frac{\mathrm{GL}_2(\mathbb{F}_\ell)}{\langle \pm 1 \rangle}$ . In other words,  $\bar{\rho}'_E$  is the composite map of  $\bar{\rho}_E$  with the natural quotient map.

We are now ready to define  $\mathcal{T}_{K,\ell}$ .

**Definition 4.** Let  $\mathcal{T}_{K,\ell}$  be the set of elliptic curves  $E/\mathbb{Q}$  such that the following conditions are satisfied:

- (1)  $\bar{\rho}'_E$  is surjective, and
- (2)  $K(\mu_\ell)$  does not contain  $\mathbb{Q}(E[\ell])$ .

After defining  $\mathcal{T}_{K,\ell}$ , Ray and Weston point out that if  $\bar{\rho}'_E$  is surjective, then  $E$  does not have complex multiplication.

Note that if  $\bar{\rho}_E$  is surjective, then  $\bar{\rho}'_E$  is also surjective. So, if an elliptic curve  $E/K$  satisfies  $\bar{\rho}_E$  being surjective and  $K(\mu_\ell)$  does not contain  $\mathbb{Q}(E[\ell])$ , then  $E/K$  is in the set  $\mathcal{T}_{K,\ell}$ . Therefore, for simplicity, we work with  $\bar{\rho}_E$ .

The way that Ray and Weston define  $\mathcal{T}_{K,\ell}$  allows us to state the problem we discuss in this thesis more precisely. We begin by constructing Figure 3.1, the diagram of field extensions pertaining to the definition of  $\mathcal{T}_{K,\ell}$ . In order to satisfy the condition of diophantine stability, we need  $K(\mu_\ell)$  not to contain  $\mathbb{Q}(E[\ell])$ . Therefore, we can rephrase the main question we will analyze in this

thesis in the following way: For a fixed elliptic curve  $E/K$  and a fixed prime  $\ell$ , what number fields  $K$  prevent  $K(\mu_\ell)$  from containing  $\mathbb{Q}(\mu_\ell)$ ?

To understand what's going on in this diagram, we use results from [DT02]. These results allow us to study the prime decomposition of individual primes in these field towers.

#### 4. PRIME DECOMPOSITION

Since our goal for this thesis is to use results from [DT02] to investigate how primes decompose in the field towers from Figure 3.1, we provide a general review of prime decomposition.

Let  $L/K$  be an extension of finite fields that is not necessarily Galois. Suppose the degree of the extension  $L/K$  is  $n$  and let  $p$  be a maximal ideal in  $O_K$ , or the ring of integers of  $K$ . Then, the ideal  $pO_L$  generated in  $O_L$  by  $p$  has a unique decomposition  $pO_L = \prod_{i=1}^g (P_i)^{e(P_i/p)}$  into a product of distinct maximal ideals  $P_i$  with multiplicities  $e(P_i/p)$ .

We note that the maximal ideals  $P_i$  that appear in the expression for  $pO_L$  satisfy the property  $P_i \cap O_K = p$ .

**Definition 5.** If  $P_i$  satisfies the property  $P_i \cap O_K = p$ , we say  $P_i$  lies above  $p$ .

In the following lemma we show that for a prime  $P_i$  in  $L$  that lies above  $p$ ,  $O_L/P_i$  is a finite field and is therefore a finite extension of  $\mathbb{F}_p$ . Since this extension is finite, it has a cyclic Galois group. The proof of the following lemma is taken from Chapter 3 of [Wes99].

**Lemma 1.** *If  $P_i$  is a prime in  $L$  that lies above the prime  $p$  in  $K$ , then the field  $O_L/P_i \cong \mathbb{F}_{p^{f(P_i/p)}}$ , where  $\mathbb{F}_{p^{f(P_i/p)}}$  is a degree  $f(P_i/p)$  extension of  $\mathbb{F}_p$ .*

*Proof.* We first note that  $P_i$  is a maximal ideal in  $O_L$ , and so,  $O_L/P_i$  will be a field. We now need to show this field is finite. Recall that  $O_L \cong \mathbb{Z}[x]/(f(x))$ , where  $f(x)$  is a minimal polynomial with coefficients in  $O_L$ . Then  $O_L/P_i \cong (\mathbb{Z}[x]/f(x))/p \cong \mathbb{Z}[x]/(p, f(x)) \cong \mathbb{F}_p[x]/(\bar{f}(x))$ , where  $\bar{f}(x)$  is  $f(x)$  reduced mod  $p$ . This is a field of order  $p^{f(P_i/p)}$ , and is therefore a finite extension of  $\mathbb{F}_p$ .  $\square$

The degree  $f(P_i/p)$  of this extension is called the *inertia degree* of  $P_i$  over  $p$ .

We note that the proofs of the next few results in this section are taken from Section 5.2 and Section 6.2 of [Sam67].

**Proposition 2.** *The  $P_i$ 's in the expansion of  $pO_L$  are exactly the prime ideals of  $O_L$  that lie above  $p$ .*

*Proof.* For a prime ideal  $R$  of  $O_L$ , since  $R \cap O_K$  is a prime ideal of  $O_K$  and  $p$  is a maximal ideal, it follows that the relation  $R \cap O_K = p$  is equivalent to the relation  $R \supset pO_L$ . We can see that  $pO_L = \prod_{i=1}^g P_i^{e(P_i/p)}$  implies  $pO_L \subset P_i$  for each  $i = 1, \dots, g$ . So,  $P_i$  appears in the product expression for  $pO_L$  if and only if  $P_i \cap O_K = p$ .  $\square$

We call the multiplicity  $e(P_i/p)$  the *ramification index* of  $P_i$  over  $p$ .

**Definition 6.** If  $e(P_i/p) > 1$ , we say  $p$  *ramifies* in  $L$ . When  $e(P_i/p) = 1$ , we say  $p$  is *unramified*.

Note that in any finite extension of  $\mathbb{Q}$ , all but finitely many rational primes are unramified.

We exclude the proof of the following theorem because it is beyond the scope of this thesis. The curious reader may look to Theorem 1 of Section 5.2 in [Sam67] for the proof. It follows immediately after the proof of Proposition 2.

**Theorem 2.** *If  $L/K$  is a degree  $n$  extension, then  $\sum_{i=1}^g e_i f_i = [O_L/pO_L : O_K/p] = n$ .*

**Definition 7.** If  $f(P_i/p) = e(P_i/p) = 1$  for every  $i$ , we say  $p$  *splits completely* in  $L$ . If  $f(P_1/p) = g = 1$ , we say  $p$  *totally ramifies* in  $L$ . And, if  $g = e(P_1/p) = 1$ , we say  $p$  *stays inert* in  $L$ .

The following result about the ramification and inertia index is crucial to studying how primes decompose in towers of extensions.

**Proposition 3.** *In a tower of extensions, the ramification index and inertia degree are both multiplicative.*

*Proof.* Let  $L/M/K$  be a tower of field extensions. Let  $p$  be a prime in  $K$ ,  $P$  be a prime in  $M$  that lies over  $p$ , and  $P'$  be a prime in  $L$  that lies over  $P$ . If we factor  $p$  into primes in  $M$ , then in the product expansion of  $pO_M$ ,  $P$  has the exponent  $e(P/p)$ . Then, if we factor in  $L$ , the exponent of  $P'$  will be its exponent in the product expansion of  $PO_L$ ,  $e(P'/P)$ , times the exponent of  $P$  in the product expansion of  $pO_M$ ,  $e(P/p)$ . Therefore  $e(P'/p) = e(P'/P) \cdot e(P/p)$ . The proof for the inertia degree follows from this calculation and from Theorem 2.  $\square$

This means, if we have a tower of extensions  $L/M/K$ ,  $p$  is a prime in  $K$ ,  $P_i$  is one of the primes in  $M$  that lies over  $p$ , and  $P'_i$  is one of the primes in  $L$  that lies over  $P_i$ , then  $e(P'_i/p) = e(P'_i/P_i) \cdot e(P_i/p)$ , where  $e(P'_i/p)$  is the

ramification index of  $P'_i/p$ ,  $e(P'_i/P_i)$  is the ramification index for  $P'_i/P_i$ , and  $e(P_i/p)$  is the ramification index for  $P_i/p$ . The same goes for  $f$  and  $g$ .

We now turn to the case where  $L/K$  is Galois. Here, the ideal  $pO_L$  generated in  $O_L$  by  $p$  once again has a unique decomposition into a product of distinct maximal ideals. But, each of the maximal ideals has the same multiplicity  $e$ .

**Proposition 4.** *If  $p$  is a maximal ideal of  $O_K$ , then the maximal ideals that lie above  $p$ , are all conjugate. They have the same residual degree  $f$  and the same inertia degree  $e$ . Thus,  $pO_L = \prod_{i=1}^g (P_i)^e$ .*

*Proof.* The assertion about the ramification index and the residual degree follows from the fact that an automorphism preserves all algebraic relations. Let  $P$  be one of the  $P_i$ 's and assume that another of the  $P_i$ 's, which we will call  $Q$ , is not conjugate to  $P$ . Since  $Q$  and  $\sigma(P)$ , where  $\sigma$  is an element of  $\text{Gal}(L/K)$ , are maximal and distinct,  $\sigma(P) \not\subseteq Q$ . The prime avoidance lemma tells us that there is an element  $y \in Q$  such that  $y$  is not an element of  $\sigma(P)$  for all  $\sigma$  in  $\text{Gal}(L/K)$ . Consider the norm of  $y$ ,  $N(y) = \prod_{\tau \in \text{Gal}(L/K)} \tau(y)$ . Since  $\tau(y)$  is an element of  $O_L$  for all  $\tau$  in  $\text{Gal}(L/K)$ ,  $N(y)$  is an element of  $Q \cap O_K = p$ . On the other hand,  $y$  is not an element of  $\tau^{-1}(P)$ , so  $\tau(y)$  is not in  $P$  for any  $\tau$  in  $\text{Gal}(L/K)$ . Since  $P$  is prime,  $N(y)$  is not in  $P$ , which contradicts that  $N(y)$  is an element of  $p$ .  $\square$

**Corollary 1.** *If  $L/K$  is a degree  $n$  Galois extension, then  $n = efg$ , where  $f = [O_L/P_i : O_K/p]$  for any of the maximal ideals  $P_i$ .*

*Proof.* This follows directly from Proposition 4 and Theorem 2. Since  $L/K$  is Galois, Proposition 4 tells us that  $e$  and  $f$  are independent of  $P_i$ . Then



this result is just a special case of Theorem 2, where  $e_1 = \cdots = e_g = e$  and  $f_1 = \cdots = f_g = f$ .  $\square$

Note that then  $\frac{n}{ef} = g$ . In other words, the degree of the extension divided by  $ef$  is equal to the number  $g$  of prime factors of  $p$  in  $O_L$ .

If we let  $G = \text{Gal}(L/K)$ , then  $G$  acts on, or permutes, the set of prime ideals in  $O_L$  that lie above  $p$ . More precisely, for all  $\sigma$  in  $G$ ,  $\sigma(P_i) = P_j$  for some  $1 \leq j \leq g$ .

For each one of these primes, we can define what's called the *decomposition group*, which we will denote  $D(P_i/p)$ .

**Definition 8.** The *decomposition group*,  $D(P_i/p)$ , is the set  $D(P_i/p) = \{\sigma \in G \mid \sigma(P_i) = P_i\}$ .

In summary, for each prime  $p$ , there is a set of prime ideals in  $L$  that lie above  $p$ , which we call  $P_i$ . The decomposition group permutes the elements of  $P_i$ , without sending elements of  $P_i$  to elements of  $P_j$  for  $i \neq j$ . Note that  $D(P_i/p)$  is a subgroup of  $G$ . In fact,  $D(P_i/p)$  is the stabilizer of  $p$  in  $G$ . It also turns out that  $g = \frac{|G|}{|D(P_i/p)|}$ , or that for every  $i$ ,  $|D(P_i/p)| = ef$ .

In contrast, we can define the *inertia group*, a subgroup of the decomposition group, which we will denote  $I(P_i/p)$ .

**Definition 9.** The *inertia group*,  $I(P_i/p)$ , is the set  $\{\sigma \in G \mid \sigma|_{P_i} = \text{identity}\}$ .

The elements of the inertia group act as the identity on each element of  $P_i$ , or they *fix* the elements of  $P_i$ . For every  $i$ , the order of the inertia group is  $e$ .

In [DT02], Duke and Tóth introduce a matrix that calculates the inertia degree of primes in  $\mathbb{Q}(E[\ell])$  that lie above  $p$ . The inertia and decomposition

group play a key role in justifying this calculation. We now provide an important definition and prove a few lemmas related to the decomposition and inertia groups that will allow us to prove the matrix does in fact calculate the inertia index of these primes. The proof of Lemma 2 is taken from [Ste04].

**Definition 10.** The generator of the group  $\frac{D(\mathcal{P}_i/p)}{I(\mathcal{P}_i/p)}$  is called the *Frobenius element* of  $\mathcal{P}_i$ .

Note that we will only be working with unramified  $p$ 's, and so, the order of  $D(\mathcal{P}_i/p)$  is  $f$  and the order of  $I(\mathcal{P}_i/p)$  is 1. Therefore, the Frobenius element is actually an element of  $D(\mathcal{P}_i/p)$ .

**Lemma 2.** *The Frobenius elements for each of the primes  $P_i$  that lie above  $p$  are all conjugate to each other.*

*Proof.* Let  $\tau$  be an element of  $\text{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q})$  and  $\gamma$  be an element of  $D(\mathcal{P}_i/p)$  for some  $i$ . Then  $\tau(\gamma(\tau^{-1}(\mathcal{P}_i))) = \mathcal{P}_i$  if and only if  $\gamma(\tau^{-1}(\mathcal{P}_i)) = \tau^{-1}(\mathcal{P}_i)$ . Therefore,  $\tau \circ \gamma \circ \tau^{-1}$  is an element of  $D(\mathcal{P}_i/p)$  if and only if  $\gamma$  is an element of  $D(\tau^{-1}(\mathcal{P}_i)/p)$ . So,  $\tau^{-1}D(\mathcal{P}_i/p)\tau = D(\tau^{-1}(\mathcal{P}_i)/p)$ . Since  $\text{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q})$  acts transitively on the set of primes lying over  $p$ , it follows that the decomposition groups  $D(\mathcal{P}_i/p)$  are all conjugate in  $\text{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q})$ . But, since the Frobenius element for each of the primes  $P_i$  is an element of  $D(\mathcal{P}_i/p)$ , this implies all the Frobenius elements are conjugate to each other.  $\square$

**Lemma 3.** *Let  $\mathfrak{D}$  be the ring of integers of  $\mathbb{Q}(E[\ell])$ . Then the Galois group  $\text{Gal}((\mathfrak{D}/\mathcal{P}_i)/(\mathbb{Z}/p))$  is isomorphic to  $D(\mathcal{P}_i/p)/I(\mathcal{P}_i/p)$ .*

*Proof.* Th  $\square$

We are now ready to introduce the results from [DT02] and begin our analysis of the main question of this thesis.

## 5. COUNTING ARGUMENTS ABOUT PRIME DECOMPOSITION

At this point we've looked at the question we're trying to answer and built up a lot of theory. So, let's now apply the theory and background we've built up to our actual question. We first note that there are some conditions that are somewhat clear off the bat. If we make  $K$  too small, then we might make  $[K(\mu_\ell) : \mathbb{Q}] < [\mathbb{Q}(E[\ell]) : \mathbb{Q}]$ , in which case it would be impossible for  $K(\mu_\ell) \supset \mathbb{Q}(E[\ell])$ . But, that's not the kind of case we're going to worry about. We're going to be concerned with the case where  $K$  is chosen to be big enough, but the prime decomposition in the extensions  $\mathbb{Q}(E[\ell])/\mathbb{Q}$  and  $K(\mu_\ell)/\mathbb{Q}$  is not compatible in such a way that it would be impossible for  $K(\mu_\ell) \supset \mathbb{Q}(E[\ell])$ .

One approach to making sure the decomposition of primes in  $K(\mu_\ell)$  is inconsistent with the decomposition of primes in  $\mathbb{Q}(E[\ell])$  would be to see how a specific prime  $p$  decomposes in  $\mathbb{Q}(E[\ell])$  and then to pick a  $K$  so that  $p$  decomposes into an incompatible number of primes in  $K(\mu_\ell)$ . But, in order to do this, we need to understand how specific primes decompose in  $\mathbb{Q}(E[\ell])$ . To do this, we look to [DT02].

Let  $p$  be a prime in  $\mathbb{Q}$  that is a prime of good reduction for  $E/K$ . Then, Duke and Tóth define the following matrix:

$$\sigma_p = \begin{bmatrix} \frac{a_p + b_p(\delta_p)}{2} & b_p \\ \frac{b_p(\Delta - \delta_p)}{4} & \frac{a_p - b_p(\delta_p)}{2} \end{bmatrix}$$

where  $|a_p| < 2\sqrt{p}$ ,  $\Delta_p = a_p^2 - 4p$ ,  $\delta_p = 0$  or  $1$  depending on whether  $\Delta \equiv 0, 1 \pmod{4}$ , and  $\Delta_p = b_p^2 \Delta$ , where  $b_p$  is positive.

It turns out that, because of the following proposition, the order of  $\sigma_p$  is important for our understanding of prime decomposition in  $\mathbb{Q}(E[\ell])$ .

**Proposition 5.** *For a prime  $p \in \mathbb{Q}$  that is unramified, the order of the matrix  $\sigma_p$  is equal to the inertial degree of  $p$  in  $\mathbb{Q}(E[\ell])$ .*

*Proof.* Consider the extension  $\mathbb{Q}(E[\ell])/\mathbb{Q}$  and write  $\mathfrak{D}$  for its ring of integers. For any unramified prime  $p \in \mathbb{Q}$ ,  $p\mathfrak{D} = \mathcal{P}_1^e \cdots \mathcal{P}_g^e$ . We know that this extension is Galois, and, more specifically, that it has Galois group  $\mathrm{GL}_2(\mathbb{F}_\ell)$ . Therefore, if we call the degree of this extension  $n$ , we have that  $n = efg$ , where  $e$  is the ramification index and  $f$  is the inertial index. Since  $p$  is unramified,  $e = 1$ , meaning  $n = fg$ .

For each prime  $\mathcal{P}_i$ , we know that we have the extension  $(\mathfrak{D}/\mathcal{P}_i)/(\mathbb{Z}/p)$ . Then, by Lemma 1,  $\mathfrak{D}/\mathcal{P}_i \cong \mathbb{F}_{p^f}$  and the Galois group of this extension is cyclic. By Lemma 3, we know that  $\mathrm{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p) \cong D(\mathcal{P}_i/p)/I(\mathcal{P}_i/p)$ , which is generated by the Frobenius element. By Lemma 2, the Frobenius elements for all of these primes  $\mathcal{P}_i$  are conjugate to one another.

In [DT02], the  $\sigma_p$  matrix is defined to be a representation of the conjugacy class of the Frobenius elements for each of the  $\mathcal{P}_i$ 's, i.e. the  $\sigma_p$  matrix is a stand-in for any of the Frobenius elements of the  $\mathcal{P}_i$ 's. So,  $\mathrm{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p)$  is also generated by  $\sigma_p$ . Then,  $\langle \sigma_p \rangle$  is isomorphic to  $\langle \mathrm{Frob}_{\mathcal{P}_i} \rangle$ , where  $\mathrm{Frob}_{\mathcal{P}_i}$  is the Frobenius element of  $\mathcal{P}_i$ . So, the order of the  $\sigma_p$  matrix in  $\mathrm{GL}_2(\mathbb{F}_\ell)$  is the degree of the extension  $D(\mathcal{P}_i/p)/I(\mathcal{P}_i/p)$ , which is  $f$ .  $\square$

**Example.** We will now work through an example. Let  $p = 2$  and  $\ell = 5$ . Then we can make a table of possibilities for  $a_p$  and  $\Delta_p$ .

$a_2$	$\Delta_2 = (a_2)^2 - 4(2)$	square-free?	possible $b_p$	possible $\Delta = \frac{\Delta_p}{b_p^2}$
$\pm 2$	-4	No	1	-4
$\pm 1$	-7	Yes	1	-7
0	-8	No	1, 2	-8, -2

Taking into account that  $\Delta$  must be 0 or 1 mod 4, we can produce the following five triples  $(a_p, b_p, \Delta)$ :

$$(i) (1, 1, -7), \quad (ii) (-1, 1, -7), \quad (iii) (2, 1, -4), \quad (iv) (-2, 1, -4), \quad (v) (0, 1, -8).$$

For each of these triples, we can calculate the  $\sigma_2$  matrix to get:

$$(i) \begin{bmatrix} 1 & 1 \\ -2 & 0 \end{bmatrix}, \quad (ii) \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}, \quad (iii) \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}, \quad (iv) \begin{bmatrix} -1 & 1 \\ -1 & -1 \end{bmatrix}, \quad (v) \begin{bmatrix} 0 & 1 \\ -2 & 0 \end{bmatrix}.$$

By Proposition 5, the order of  $\sigma_p$  in  $\mathrm{GL}_2(\mathbb{F}_\ell)$  is equal to the inertial degree of the primes in  $\mathbb{Q}(E[\ell])$  that lie above  $p$ . But, we know that  $|\mathrm{GL}_2(\mathbb{F}_5)| = efg$ , and by assumptions made in [DT02], all of the primes we can compute  $\sigma_p$  for must be primes of good reduction, which implies that  $e = 1$ . So, we can also use the order of  $\sigma_p$  to calculate how many primes  $p$  splits into in  $\mathbb{Q}(E[\ell])$ . We now list the order of each of these matrices in  $\mathrm{GL}_2(\mathbb{F}_5)$  and the information it provides about how the prime 2 splits in  $\mathbb{Q}(E[5])$ :

- The order of matrix (i) in  $\mathrm{GL}_2(\mathbb{F}_5)$  is 24. Therefore, if  $E$  is an elliptic curve and 2 is a prime of good reduction for  $E$ , with  $a_2(E) = 1$ , then, in  $\mathbb{Q}(E[5])$ , 2 splits into 20 primes, each with inertial degree 24.
- The order of matrix (ii) in  $\mathrm{GL}_2(\mathbb{F}_5)$  is also 24. Therefore, if  $E$  is an elliptic curve and 2 is a prime of good reduction for  $E$ , with  $a_2(E) = -1$ , then in  $\mathbb{Q}(E[5])$ , 2 splits into 20 primes, each with inertial degree 24.

- The order of matrix (iii) in  $\mathrm{GL}_2(\mathbb{F}_5)$  is 4. Therefore, if  $E$  is an elliptic curve and 2 is a prime of good reduction for  $E$ , with  $a_2(E) = 2$ , then, in  $\mathbb{Q}(E[5])$ , 2 splits into 120, each with inertial degree 4.
- The order of matrix (iv) in  $\mathrm{GL}_2(\mathbb{F}_5)$  is also 4. Therefore, if  $E$  is an elliptic curve and 2 is a prime of good reduction for  $E$ , with  $a_2(E) = -2$ , then, in  $\mathbb{Q}(E[5])$ , 2 splits into 120 primes, each with inertial degree 4.
- The order of matrix (v) in  $\mathrm{GL}_2(\mathbb{F}_5)$  is 8. Therefore, if  $E$  is an elliptic curve and 2 is a prime of good reduction for  $E$ , with  $a_2(E) = 0$ , then, in  $\mathbb{Q}(E[5])$ , 2 splits into 60 primes, each with inertial degree 8.

We will now finish the example by showing what the implications of these calculations are for the number field  $K$  we would like to produce. Before we do this, we make the assumption that 2 is a prime of good reduction for  $E/K$ . If 2 is not a prime of good reduction for  $E/K$ , then we can find another prime that is and perform the same calculations to find the splitting behavior for that prime. So, finishing the example, if we wanted to produce a number field  $K$  that would make  $E/K$  diophantine stable, we would need one of the following things to happen:

- If  $a_2(E) = \pm 1$ , then 2 splits into  $x$  primes in  $K(\mu_5)$ , where  $x$  is not a multiple of 20.
- If  $a_2(E) = \pm 1$  and 2 splits into 20 primes in  $K(\mu_5)$ , then the inertial degree for those 20 primes is not a multiple of 24.
- If  $a_2(E) = \pm 2$ , then 2 splits into  $x$  primes in  $K(\mu_5)$ , where  $x$  is not a multiple of 120.

- If  $a_2(E) = \pm 2$  and 2 splits into 120 primes in  $K(\mu_5)$ , then the inertial degree for those 120 primes is not a multiple of 4.
- If  $a_2(E) = 0$ , then 2 splits into  $x$  primes in  $K(\mu_5)$ , where  $x$  is not a multiple of 60.
- If  $a_2(E) = 0$  and 2 splits into 60 primes in  $K(\mu_5)$ , then the inertial degree for those 60 primes is not a multiple of 8.

## 6. A CONCRETE EXAMPLE

We will now work through a similar example to that in the previous section, but with a specific elliptic curve  $E$  and prime  $\ell$ . We choose  $E$  to be the elliptic curve with Cremona label 11a1 and  $\ell = 7$ .

**Theorem 3.** *If  $[K : \mathbb{Q}] < 2016$ , or one of the following occurs,*

- *In  $K(\mu_7)$ , the number of primes 2 splits into is not a multiple of 84, the number of primes 3 splits into is not a multiple of 42, or the number of primes 5 splits into is not a multiple of 336.*
- *In  $K(\mu_7)$ , the 84 primes 2 splits into have inertial degree that is not divisible by 24, the 42 primes 3 splits into have inertial degree that is not divisible by 48, or the 336 primes 5 splits into have inertial degree that is not divisible by 6.*

*then,  $(E, K, 7)$  is diophantine stable.*

*Proof.* We know  $|\mathrm{GL}_2(\mathbb{F}_7)| = 2016$ . So, if  $[K : \mathbb{Q}] < 2016$ , then  $(E, K, 7)$  is diophantine stable.

Just like before, we want to look at more interesting cases of  $(E, K, 7)$  being diophantine stable, which are related to prime decomposition in  $\mathbb{Q}(E[7])$ . We

will study how the primes 2, 3, and 5 decompose in this field. From the LMFDB (linked), we find that  $a_2(E) = -2$ ,  $a_3(E) = -1$ , and  $a_5(E) = 1$ .

So, we get the following three triples  $(a_p, b_p, \Delta)$ :

$$(-2, 1, -4), (-1, 1, -11), (1, 1, -19).$$

For each of these triples, we can form the  $\sigma_p$  matrix to get:

$$\sigma_2 = \begin{bmatrix} -1 & 1 \\ -1 & -1 \end{bmatrix}, \quad \sigma_3 = \begin{bmatrix} 0 & 1 \\ -3 & -1 \end{bmatrix}, \quad \sigma_5 = \begin{bmatrix} 1 & 1 \\ -5 & 0 \end{bmatrix}.$$

We can calculate that  $\sigma_2$  has order 24 in  $\text{GL}_2(\mathbb{F}_7)$ ,  $\sigma_3$  has order 48 in  $\text{GL}_2(\mathbb{F}_7)$ , and  $\sigma_5$  has order 6 in  $\text{GL}_2(\mathbb{F}_7)$ .

So, in  $\mathbb{Q}(E[7])$ , 2 splits into 84 primes, each with inertial degree 24, 3 splits into 42 primes, each with inertial degree 48, and 5 splits into 336 primes, each with inertial degree 6. So, if  $K(\mu_7) \supseteq \mathbb{Q}(E[7])$ , then the inertial degrees and the number of primes 2, 3, and 5 split into in  $K(\mu_7)$  must be multiples of these values. Therefore, for  $(E, K, 7)$  to be diophantine stable, we need one of the following things to happen:

- In  $K(\mu_7)$ , the number of primes 2 splits into is not a multiple of 84, the number of primes 3 splits into is not a multiple of 42, or the number of primes 5 splits into is not a multiple of 336.
- In  $K(\mu_7)$ , the 84 primes 2 splits into have inertial degree that is not divisible by 24, the 42 primes 3 splits into have inertial degree that is not divisible by 48, or the 336 primes 5 splits into have inertial degree that is not divisible by 6.

Note that for the second condition, it suffices to just have one prime that  $p$  splits into have inertial degree in  $K(\mu_7)$  that is not divisible by its inertial



degree in  $\mathbb{Q}(E[7])$  because we are making the assumption that  $K$  is a Galois extension of  $\mathbb{Q}$ , so  $K(\mu_7)$  is as well. Therefore, all the primes  $P_i$  in  $K(\mu_7)$  that lay above a specific prime of good reduction in  $\mathbb{Q}$  have the same inertial degree. □

## REFERENCES

- [DT02] W. Duke and Á. Tóth, The splitting of primes in division fields of elliptic curves, Experiment. Math. **11** (2002), no. 4, 555–565. MR 1969646
- [MR18] Barry Mazur and Karl Rubin, Diophantine stability, Amer. J. Math. **140** (2018), no. 3, 571–616, With an appendix by Michael Larsen. MR 3805014
- [RW23] Anwesh Ray and Tom Weston, Diophantine stability for elliptic curves on average, 2023.
- [Sam67] Pierre Samuel, Théorie algébrique des nombres, Hermann, Paris, 1967. MR 215808
- [ST15] Joseph H. Silverman and John T. Tate, Rational points on elliptic curves, second ed., Undergraduate Texts in Mathematics, Springer, Cham, 2015. MR 3363545
- [Ste04] William Stein, The decomposition group.
- [Wes99] Tom Weston, Algebraic number theory.