5-2012

Modular Forms, Elliptic Curves and Drinfeld Modules

Catherine Trentacoste
Clemson University, ctrentacoste@gmail.com

Modular Forms, Elliptic Curves and Drinfeld Modules

A Thesis
Presented to
the Graduate School of
Clemson University

In Partial Fulfillment
of the Requirements for the Degree
Ph.D.
Mathematical Science

---

by
Catherine Mary Trentacoste
May 2012

Accepted by:
Dr. Kevin James, Committee Chair
Dr. Hui Xue, Committee Chair
Dr. James Brown
Dr. Hiren Maharaj

Abstract

In this thesis we explore three different subfields in the area of number theory. The first topic we investigate involves modular forms, specifically nearly holomorphic eigenforms. In Chapter 3, we show the product of two nearly holomorphic eigenforms is an eigenform for only a finite list of examples. The second type of problem we analyze is related to the rank of elliptic curves. Specifically in Chapter 5 we give a graph theoretical approach to calculating the size of 3-Selmer groups for a given family of elliptic curves. By calculating the size of the 3-Selmer groups, we give an upper bound for the rank of an elliptic curve. Finally, in Chapter 7, we conclude with an exposition of work from Goss, Thakur and Diaz-Vargas related to Drinfeld modules. We discuss how to build a zeta function for Drinfeld modules and introduce a symmetric group discovered by Thakur and Diaz-Vargas. An element in the symmetric group is essentially a set permutation of the p-adic integers. It is suspected that there is a relationship between this group and the zeros of certain special zeta functions. We give a specific example of this suspected connection and make a conjecture about this action.

Acknowledgments

I would like to sincerly thank my advisors Kevin James and Hui Xue for their support and guidance. I am very grateful for their suggestions, comments and advice mathematically and towards my future career. I am also very thankful to my doctorial committee members Jim Brown and Hiren Maharaj. In addition I would like to thank Rodney Keaton and Justin Peachey for their mathematical advice over the years. I would like to extend special thanks to my co-authors not previously mentioned: Jeff Beyerl, Tony Feng, Carolyn Kim and Eric Ramos. Finally I would like to thank my family and friends for encouraging and supporting me over the years.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

Number theory is a broad branch of mathematics dating back thousands of years. There are numerous subfields which have been developed and studied over the years. The following work is a collection of problems on which I have focused my graduate research. This dissertation is broken down into three sections. We begin with results on nearly holomorphic modular forms, then explore elliptic curves and Selmer groups and finally finish with Zeta functions over function fields. Each section contains a chapter dedicated to background material, which is followed by a chapter on recent results. Here, we give an overview of what the reader will find in each section.

1.1 Introduction to Nearly Holomorphic Modular Forms

It is well known that the modular forms of a specific weight for the full modular group form a complex vector space. The action of the algebra of Hecke operators on these spaces is well understood. For instance, we know that there is a basis for such spaces composed entirely of forms called Hecke eigenforms which are eigenvectors for all of the Hecke operators simultaneously. Since the set of all modular forms (of all weights) for the full modular group

can be viewed as a graded complex algebra, it is quite natural to ask if the special property of being a Hecke eigenform is preserved under multiplication. This problem was studied independently by Ghate [34] and Duke [29] and they found that it is actually quite rare that the product of Hecke eigenforms is again a Hecke eigenform. In fact, they proved that there are only a finite number of examples of this phenomenon. Emmons and Lanphier [30] extended these results to an arbitrary number of Hecke eigenforms. The more general question of preservation of eigenforms through the Rankin-Cohen bracket operator (a bilinear form on the graded algebra of modular forms) was studied by Lanphier and Takloo-Bighash [50, 51] and led to a similar conclusion. One can see [60] or [73] for more on these operators.

The work mentioned above focuses on eigenforms which are "new" everywhere. It seems natural to extend these results to eigenforms which are not new. In Chapter 3, we consider modular forms which are "old" at infinity in the sense that the form comes from a holomorphic form of lower weight. More precisely, we show that the product of two nearly holomorphic eigenforms is an eigenform for only a finite list of examples (see Theorem 21). It would also be interesting to consider the analogous question for forms which are old at one or more finite places.

1.2 Introduction to Selmer Groups

One of the major open problems in number theory involves calculating the rank of an elliptic curve. By calculating the size of the Selmer group, we can give an upper bound for the rank of a given elliptic curve. The goal of Chapter 5 is to bound the size of the 3-Selmer groups for a family of elliptic curves with 3-torsion given by

$$E_{ab} : y^2 = x^3 + (ax + b)^2$$

and its auxiliary curve

$$E'_{ab'} : y^2 = x^3 - 3(ax + b')^2$$

with $b' = \frac{27-4a^3}{9}$ and therefore provide a bound for the rank of E_{ab}. Specifically, we analyze the 3-Selmer groups associated to 3-descent by isogeny of such elliptic curves by relating them to graphs with certain properties, then translate the graph theory into a problem involving matrix analysis. Our methods use an elementary approach involving algebra and combinatorics. These methods have been employed to study 2-Selmer groups which arise from 2-descent for the family of congruent number curves, possessing 2-torsion, but not for curves with 3-torsion or for 3-Selmer groups. Specifically, Feng and Xiong [32] introduce the notion of "odd graphs" in order to study the 2-Selmer groups of congruent number curves and Faulkner and James [31] extend their results to allow a graph theoretical computation of 2-Selmer groups. We extend their methods to the computation of 3-Selmer groups of elliptic curves with 3-torsion. This graph theoretical approach offers a visual and more elementary description of 3-Selmer groups. Significant work has been done using a linear algebraic approach to bound the dimension of 3-Selmer groups. Specifically, using the work of Top [68], DeLong [23] gives a formula for the dimension of 3-Selmer groups using vector spaces and the 3-ranks of quadratic number fields. For additional related work, we refer the reader to [11, 41, 42, 45, 55, 71].

In Chapter 4 we give an overview of 3-descent maps and their relation to the rank of an elliptic curve with rational 3-torsion. Next, we follow the treatment given in [14] and we associate the following homogeneous polynomials of degree 3 to E_{ab} and $E'_{ab'}$ respectively

$$F_u(X, Y, Z) = u_1X^3 + u_2Y^3 + u_3Z^3 - 2aXYZ$$

and

$$\begin{aligned} F_{u'}(X,Y,Z) &= \left(\overline{\gamma}\left(X+Y\sqrt{-3}\right)^3 - \gamma\left(X-Y\sqrt{-3}\right)^3\right)/\sqrt{-3} \\ &\quad +2aZ\left(X+Y\sqrt{-3}\right)\left(X-Y\sqrt{-3}\right) + \left(2b'/N(\gamma)\right)Z^3. \end{aligned}$$

Using these polynomials, we arithmetically define 3-Selmer groups as opposed to the usual definition involving Galois cohomology. For a more general treatment, we refer the reader to [17, 18, 33]. Finding integer solutions to the above equations is difficult, so we relax the condition and define the 3-Selmer groups, $\mathrm{Sel}^{(\phi)}(E_{ab})$ and $\mathrm{Sel}^{(\widehat{\phi})}(E'_{ab'})$, to be the set of $u \in \mathbb{Q}^*/(\mathbb{Q}^*)^3$ (respectively, $u' \in \mathbb{Q}^*(\sqrt{-3})/(\mathbb{Q}^*(\sqrt{-3}))^3$) for which $F_u(X,Y,Z) = 0$ (respectively $F_{u'}(X,Y,Z) = 0$) has local solutions for all places. Once we define Selmer groups in the above manner, it is natural to investigate when we obtain local solutions. We discuss the local solubility of the homogeneous polynomials associated to E_{ab} in Chapter 5, Section 5.1. Many of these conditions involve checking if ratios of the coefficients of the homogeneous polynomials are cubes modulo a given prime.

After completely characterizing when we obtain local solutions, we begin exploring this question in terms of graph theory. For the elliptic curve, E_{ab}, we construct a directed graph G' with subgraph G. The vertices of G and G' are comprised of the primes dividing $2b$ and the discriminant of the curve. We draw directed edges between primes where local solutions are not guaranteed and label each directed edge with a cubic root of unity. Next we introduce the idea of a "three-balanced" partition, (S_1, S_2, S_3), of the vertices of the subgraph G. We identify each set in the partition with a coefficient associated to the homogeneous polynomial, $F_u(X,Y,Z)$. The general idea is that a partition of a graph is three-balanced if the ratios of the associated coefficients are cubes modulo a given prime. The prime $p = 3$ is slightly more complicated, so we introduce the idea of "three-quasi-balanced" partitions as well. We show that given a three-balanced partition, we can construct an element in the

3-Selmer group, $\mathrm{Sel}^{(\phi)}(E_{ab})$, associated to the elliptic curve E_{ab}.

For example, consider the family of elliptic curves

$$E_n/\mathbb{Q} : y^2 = x^3 + n^2,$$

and its auxiliary family

$$E'_n : y^2 = x^3 - 27n^2.$$

There are isogenies $\phi : E_n \to E'_n$ given by

$$\phi(P) = \phi((x,y)) = \left(\frac{x^3+n^2}{x^2}, \frac{y(x^3-8n)}{x^3}\right).$$

We realize a concrete identification between the associated Selmer group, $\mathrm{Sel}^{(\phi)}(E_n)$, and the subgroup of $\mathbb{Q}^*/(\mathbb{Q}^*)^3$ consisting of equivalence classes $[u]$ with $u = u_1u_2^2$ for which the equation

$$u_1x^3 + u_2y^3 + \frac{2n}{u_1u_2}z^3 = 0$$

has non-trivial solutions over $\mathbb{R}$ and $\mathbb{Q}_p$ for every prime p. Casting this condition into the language of graph theory, we construct a directed graph G' with subgraph G where the vertices of G are exactly the prime divisors of $2n$ and the prime 3. Partitioning the vertices G into 3 possibly empty subsets, (S_1, S_2, S_3), if this partition is three-balanced, then $u = \prod_{p\in S_1} p \prod_{p\in S_2} p^2$ is an element in $\mathrm{Sel}^{(\phi)}(E_n)$. In fact, we have the following theorem.

Theorem 1. *Let $E_n : y^2 = x^3 + n^2$. Suppose that n is odd, square-free, and divisible by 3, and define G to be the associated digraph. Then*

$$\left|\mathrm{Sel}^{(\phi)}(E_n)\right| = \#\{\textit{three-balanced partitions of } G\}.$$

For $E'_{ab'}$, we take a slightly different approach. In this setting we construct a graph G''

with subgraphs G' and G. The vertices of G, G' and G'' are comprised of the primes dividing $2b'$ and the discriminant. However, in this case, we place primes in different subgraphs depending on their classification; split primes, inert primes and ramified primes in $\mathbb{Q}(\zeta_3)$. The subgraph G consists only of split primes which divide $2b'$. Again, we draw directed edges between primes for which local solutions are not guaranteed and label each with a cubic root of unity. Due to complications associated with the local solubility at the primes 2 and 3, we do not require local solutions in $\mathbb{Q}_2$ and $\mathbb{Q}_3$. Hence we introduce the subgroup $\mathrm{Sel}_{\mathcal{S}}^{(\hat{\phi})}(E'_{ab'}) \subset \mathbb{Q}^*(\sqrt{-3})/(\mathbb{Q}^*(\sqrt{-3}))^3$, where we relax the conditions on all primes in $\mathcal{S}$. Once we have constructed the graph, we introduce the notion of a "good" labeling on the vertices of the subgraph G. We label each vertex in G with a 0, 1 or 2 and identify the primes labeled with a 1 or a 2 to the parameters γ and $\overline{\gamma}$ in $F_{u'}(X, Y, Z)$. The idea is that a good labeling will produce an element in the modified 3-Selmer group, $\mathrm{Sel}_{\mathcal{S}}^{(\hat{\phi})}(E'_{ab'})$, associated to the auxiliary curve $E'_{ab'}$. This notion of employing the methods of graph theory to describe the 3-Selmer group gives us a visual interpretation of what these groups look like and we can easily construct examples. Additionally, it gives a definition of the Selmer group, which is completely elementary and could be used, as in [55], to obtain results on the average ranks of 3-Selmer groups of elliptic curves with 3-torsion.

Finally, for completeness, we use the associated graphs to construct a Laplacian matrix. Indexing the rows and columns by primes in the vertex set, we can relate the notion of a three-balanced partition and a good labeling to a Laplacian matrix. The primes associated with the columns will be those primes which are the heads of the directed edges and the primes associated with rows will be the primes which are the tails of the directed edges. The entries of the matrix will consist of cubic roots of unity and zeros. If a prime is associated with both a row and column, this entry will either be the sum of the other entries in the row or the negative of this sum, reduced modulo 3. Looking at the kernel of a submatrix of the Laplacian matrix, we can construct an element of the Selmer group

(or modified Selmer group in the case of the auxiliary curve). Employing the results of the rank-nullity theorem, we can bound the size of the 3-Selmer group. Therefore, combining this result with the fact that the rank of the elliptic curve is bounded by the product of the sizes of the 3-Selmer groups, $\mathrm{Sel}^{(\phi)}(E_{ab})$ and $\mathrm{Sel}^{(\widehat{\phi})}(E'_{ab'})$, we can give an upper bound for the rank of E_{ab}.

1.3 Introduction to Zeta Functions for Drinfeld Modules

Euler computed values of the Riemann zeta function at the positive even integers and the negative integers. By comparing them he found the basic symmetry given by the famous functional equation of $\zeta(s)$.

In classical number theory, mathematicians are interested in studying elliptic curves and their associated L-functions. As stated in Section 1.2, we are interested in calculating the rank of a given elliptic curve. Recall, Mordell's Theorem [63] tells us that given an elliptic curve E of rank r over $\mathbb{Q}$, we can write

$$E(\mathbb{Q}) = \mathbb{Z}^r \oplus E(\mathbb{Q})_{\mathrm{tors}}.$$

Additionally, we are interested in a given elliptic curve's associated Hasse-Weil L-function, $L(E, s)$ and its value at $s = 1$, which is called the 'critical value.' The Birch Swinnerton-Dyer Conjecture relates the arithmetic of a curve to the behavior of its L-function at $s = 1$. More precisely,

Theorem 2 (Weak Birch Swinnerton-Dyer Conjecture)**.** *The rank of an elliptic curve equals the order of vanishing of its associated L-function at $s = 1$.*

We want to attempt to build a zeta function for Drinfeld modules by comparing it to L-series for elliptic curves. In characteristic p, the construction of a zeta function for the

Carlitz module, a dimension one rank one Drinfeld module, is the analogue to the classical zeta function. The zeta function of a rank two Drinfeld module is the analogue to the zeta function of an elliptic curve. In characteristic p, there are results at the positive and negative integers. Recall the classical zeta function satisfies a functional equation relating the values of the Riemann zeta function at s and $1-s$. In characteristic p, however, all attempts to obtain an analogous result have been unsuccessful.

Through the work of Dinesh Thakur and Javier Diaz-Vargas they discovered a symmetric group which conjecturally allows one to establish certain finiteness results on trivial zeros for characteristic p zeta functions [66, 26]. Further calculations indicate that in the polynomial ring case, this group acts on the zeros of the zeta function. Chapter 7 will give an exposition of work done by Goss, Thakur, Diaz-Vargas as well as others on the action of this symmetric group on zeta zeros. Specifically we will define zeta functions of Drinfeld modules as functions from $\mathbb{C}_\infty$ to $\mathbb{C}_\infty$, which is the analogue of $\mathbb{C}$. There are a few obstacles Goss addresses in his work since exponentiating elements over an extension of a finite field is not the same as in $\mathbb{R}$. We have also included some examples we computed to help solidify the concepts. In addition, we will define the symmetric group Thakur and Dias-Vargas discovered, which seems to act on zeros of the zeta function and give an example of this symmetry. For the unfamiliar reader, a brief introduction to Drinfeld modules can be found in Chapter 6.

Chapter 2

Background on Modular Forms

The purpose of this chapter is to give the reader a brief introduction to modular forms. For further details, we refer the reader to [24, 46, 47, 58].

2.1 Basic Definitions and Notation

Let R be a commutative ring. The **general linear group** is defined as

$$\mathrm{GL}_2(R) := \left\{ g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \det g \in R^* \right\}.$$

The **special linear group** is a subset of the general linear group, defined as

$$\mathrm{SL}_2(R) := \{ g \in \mathrm{GL}_2(R) : \det g = 1 \}.$$

For sake of simplicity, we will specifically examine the cases when $R = \mathbb{R}$ and $R = \mathbb{Z}$. Let $\tilde{\mathbb{C}} := \mathbb{C} \cup \{\infty\}$ where ∞ represents the point at infinity. This is equivalent to the complex projective line $\mathbb{P}^1_{\mathbb{C}}$, which is also known as the "Riemann sphere."

Let $g \in \mathrm{SL}_2(\mathbb{R})$ and $z \in \mathbb{C}$. Define

$$gz := \frac{az+b}{cz+d} \tag{2.1}$$

$$g\infty := \frac{a}{c} = \lim_{z\to\infty} gz \tag{2.2}$$

We define a fractional linear transformation of the Riemann sphere $\tilde{\mathbb{C}}$ by the map $z \mapsto gz$. Equations (2.1) and (2.2) define a group action on $\tilde{\mathbb{C}}$, i.e. $g_1(g_2 z) = (g_1 g_2)z$ and $ez = z$.

Remark 1. Observe that for $g = -I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, then gz is the identify map. However, $\pm I$ are the only matrices which act trivially on $\tilde{\mathbb{C}}$. Therefore, the quotient group, $\mathrm{PSL}_2(R) := \mathrm{SL}_2(\mathbb{R})/\pm I$, acts faithfully on $\mathbb{C}$; meaning every element other than the identity acts non-trivially.

We denote the **upper half plane** by $\mathcal{H} \subset \mathbb{C}$ where

$$\mathcal{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}.$$

Notice that any $g \in \mathrm{SL}_2(\mathbb{R})$ preserves $\mathcal{H}$, since $\mathrm{Im}(z) > 0$ implies $\mathrm{Im}(gz) > 0$. To see this,

observe that

$$\begin{aligned}
\mathrm{Im}(gz) &= \mathrm{Im}\left(\frac{az+b}{cz+d}\right) \\
&= \mathrm{Im}\left(\frac{(az+b)\overline{(cz+d)}}{|cz+d|^2}\right) \\
&= |cz+d|^{-2}\,\mathrm{Im}\,(adz+bc\overline{z}) \\
&= |cz+d|^{-2}\,(ad-bc)\mathrm{Im}(z) \\
&= |cz+d|^{-2}\,\mathrm{Im}(z).
\end{aligned}$$

Note that the last equality follows since $\det(g) = 1$. From this we can see that $\mathrm{SL}_2(\mathbb{R})$ acts on $\mathcal{H}$ by the transformations given in equations (2.1) and (2.2).

An important subgroup of $\mathrm{SL}_2(\mathbb{R})$ is $\mathrm{SL}_2(\mathbb{Z})$, the set of matrices consisting of integer entries. It is known as the **full modular group** and is typically denoted by Γ. Set $\overline{\Gamma} := \Gamma/\pm I$. This group acts faithfully on $\mathcal{H}$ as well and is one of the basic groups which arise in number theory.

Next, we will introduce some special subgroups of Γ. Let $N \in \mathbb{Z}^+$, then we define the **principal congruence subgroup of level** N by

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : a \equiv d \equiv 1 \ (N),\ b \equiv c \equiv 0 \ (N) \right\}.$$

This is a normal subgroup. Also, observe $\Gamma(1) = \Gamma$. Any subgroup of Γ containing $\Gamma(N)$ is

called a **congruence subgroup of level** N. Set

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : c \equiv 0 \ (N) \right\}$$

and

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) : a \equiv 1 \ (N) \right\}.$$

Note that for $\Gamma_1(N)$, $d \equiv 1 \ (N)$. These are the most important congruence subgroups of Γ.

When a group acts on a set, it divides the set into equivalence classes. Let G be a subgroup of Γ and let $z_1, z_2 \in \mathcal{H}$. Then z_1 and z_2 are **G-equivalent** if there exists $g \in G$ such that $z_2 = gz_1$. Let F be a closed region in $\mathcal{H}$. We say that F is the **fundamental domain** for the subgroup G of Γ if every $z \in \mathcal{H}$ is G-equivalent to a point in F, but no two distinct points z_1, z_2 in the interior of F are G-equivalent.

The following proposition defines a fundamental domain for Γ.

Proposition 3 (Chapter 3, Proposition 1, [47])**.** *The region*

$$\mathbf{F} := \left\{ z \in \mathcal{H} : -\frac{1}{2} \leq \mathrm{Re}(z) \leq \frac{1}{2} \ \& \ |z| \geq 1 \right\}$$

is a fundamental domain for Γ.

For a detailed proof, we refer the reader to [47].

As mentioned previously, the group Γ acts on the set $\mathcal{H}$ with fundamental domain $\mathbf{F}$. One can identify the Γ-equivalent points on the boundary of $\mathbf{F}$ and we denote the Γ-equivalence classes in $\mathcal{H}$ by $\Gamma \setminus \mathcal{H}$. Let $\overline{\mathcal{H}}$ denote the set $\mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$. Notice that we adjoin not only ∞, but the rationals, $\mathbb{Q}$, as well. Then we identify adjoined points under Γ-equivalence. A Γ-equivalence class of points in $\mathbb{Q} \cup \{\infty\}$ is called a **cusp** of Γ. Modular forms need to be holomorphic on $\mathcal{H}$ as well as at the cusps in order to keep their associated

vector spaces finite dimensional. With a little work, one can show that Γ permutes the cusps transitively. To see this, consider a fraction $\frac{a}{c}$ with $(a,c)=1$. Then by solving the equation $ad-bc=1$ for b and d, by definition the matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma$ sends ∞ to $\frac{a}{c}$. Therefore all rational numbers are Γ-equivalent to ∞, hence $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ only has one cusp.

One can extend the usual topology on $\mathcal{H}$ to the set $\overline{\mathcal{H}}$. We will show how to extend the topology to $\mathcal{H} \cup \{\infty\}$ and refer the interested reader to [47] for details on $\overline{\mathcal{H}}$.

Consider the set of open neighborhoods of ∞ of the form $N_C = \{z \in \mathcal{H} : \mathrm{Im} z > C\} \cup \{\infty\}$ for $C > 0$. By mapping $\mathcal{H}$ to the punctured open unit disk; sending

$$z \mapsto q := e^{2\pi i z} \tag{2.3}$$

and taking the point $\infty \in \overline{\mathcal{H}}$ to the origin, then N_C is the inverse image of the open disc centered at the origin with radius $e^{-2\pi C}$. Hence the map given by (2.3) is continuous and we have a topology on $\mathcal{H} \cup \{\infty\}$.

The change of variables given by (2.3) plays a major role in the theory of modular forms and we use it to define an analytic structure on $\mathcal{H} \cup \{\infty\}$. This leads us to the following definitions.

Definition 1. Let $q = e^{2\pi i z}$ where $z \in \mathcal{H}$. Given a function on $\mathcal{H}$ of period 1, we say it is **meromorphic at** ∞ if it can be expressed as a power series in the variable q having at most finitely many negative terms, i.e. it has a Fourier expansion of the form

$$f(z) = \sum_{n \in \mathbb{Z}} a_n e^{2\pi i n z} = \sum_{n \in \mathbb{Z}} a_n q^n$$

in which $a_n = 0$ for $n \ll 0$.

We say that $f(z)$ is **holomorphic at** ∞ if $a_n = 0$ for all negative n and we say that

$f(z)$ **vanishes at** ∞ if $f(z)$ is holomorphic at ∞ and $a_0 = 0$.

If $f(z)$ has period N, one can use the map $z \mapsto q_N := e^{2\pi iz/N}$ to map $\mathcal{H} \cup \{\infty\}$ to the open disk. So here, one can express $f(z)$ as a series in q_N and we say it's **meromorphic** (respectively **holomorphic, vanishes**) **at** ∞ if $a_n = 0$ for $n \ll 0$ (respectively, for $n < 0$ or for $n \leq 0$).

2.2 Modular forms for the Special Linear Group

Recall a **holomorphic function** is a complex-valued function which is complex differentiable in a neighborhood of every point in its domain. Given an open set D, a **meromorphic function** is a holomorphic function on D except on a set of isolated points, which are called the **poles** of the function. Now we are ready to define a modular form for Γ.

Definition 2. Let $f(z)$ be a meromorphic function on the upper-half plane $\mathcal{H}$ and let k be a non-negative integer. Suppose that $f(z)$ satisfies the relation

$$f(\gamma z) = (cz + d)^k f(z) \tag{2.4}$$

for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. In particular, for the elements $\gamma = T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\gamma = S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, equation (2.4) gives

$$f(z + 1) = f(z) \tag{2.5}$$

and

$$f\left(-\frac{1}{z}\right) = (-z)^k f(z). \tag{2.6}$$

Furthermore, suppose that $f(z)$ is meromorphic at ∞. Then $f(z)$ is called a **modular function of weight** k for $\Gamma = \mathrm{SL}_2(\mathbb{Z})$.

If, in addition, $f(z)$ is holomorphic on $\mathcal{H}$ and at infinity (i.e. $a_n = 0$ for all $n < 0$), then $f(z)$ is called a **modular form of weight** k for Γ. The set of such functions is denoted $M_k(\Gamma)$. Further, if we have $a_0 = 0$, (i.e. the modular form vanishes at infinity), then $f(z)$ is called a **cusp-form of weight** k for Γ. The set of such functions is denoted $S_k(\Gamma)$. The expansion for a modular form $f(z)$ is called its q**-expansion** given by

$$f(z) = \sum_{n \in \mathbb{Z}} a_n q^n \tag{2.7}$$

where $q = e^{2\pi i z}$.

Remark 2.

1. For k odd, there are no non-zero modular functions of weight k for Γ. To see this, let $\gamma = -I$. Then for any z, we have $-Iz = \dfrac{-z+0}{0(z)-1} = z$. And from Definition 2, this implies that $f(-Iz) = f(z) = (-1)^k f(z) = -f(z)$. Hence the only modular form of odd weight is the zero function. So from now on we will assume k is even.

2. Since
$$\frac{d\gamma z}{dz} = \frac{d}{dz}\left(\frac{(az+b)}{(cz+d)}\right) = (cz+d)^{-2},$$
we can rewrite equation (2.4) in the form
$$\left(\frac{d\gamma z}{dz}\right)^{k/2} f(\gamma z) = f(z).$$

3. The set of modular forms, functions and cusp-forms of some fixed weight are complex vector spaces. The set of modular functions of weight zero is a field.

Let's look at some important examples.

Example 1. The following is known as a **general Eisenstein series**. For additional details, see [47]. Let k be an even integer greater than 2. Let $z \in \mathcal{H}$ and define

$$G_k(z) := \sum_{m,n}{}' \frac{1}{(mz+n)^k} \tag{2.8}$$

where we sum over all integer pairs m and n, both not zero. One can show that $G_k(z) \in M_k(\Gamma)$. When computing the q-expansion coefficients for G_k, we find that they are arithmetic functions of n given by

$$\sigma_{k-1}(n) := \sum_{d|n} d^{k-1}. \tag{2.9}$$

Therefore $G_k(z)$ has q-expansion

$$G_k(z) = 2\zeta(k)\left(1 - \frac{2k}{B_k}\sum_{n=1}^{\infty} B_k \frac{x^k}{k!}\right) \tag{2.10}$$

where $q = e^{2\pi i z}$, B_k denotes the kth Bernoulli number and

$$\zeta(k) = \sum_{n=1}^{\infty} \frac{1}{n^k}.$$

Next, it is natural to define the **normalized Eisenstein series**,

$$E_k(z) := \frac{1}{2\zeta(k)} G_k(z), \tag{2.11}$$

which can also be written as

$$\begin{aligned} E_k(z) &= 1 - \frac{2k}{B_k}\sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n \\ &= \frac{1}{2} \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n)=1}} \frac{1}{(mz+n)^k}. \end{aligned}$$

The first few normalized Eisenstein series are

$$\begin{aligned} E_4(z) &= 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n, \\ E_6(z) &= 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n, \\ E_8(z) &= 1 + 480 \sum_{n=1}^{\infty} \sigma_7(n) q^n. \end{aligned}$$

One can define the Eisenstein series E_2, however, it is not a modular form because the absolute convergence of the sum is not guaranteed.

Example 2. The following is known as the **discriminant modular form**:

$$\Delta(z) = \frac{(2\pi)^{12}}{1728} \left(E_4(z)^3 - E_6(z)^2 \right). \tag{2.12}$$

We can see that $\Delta(z)$ is a modular form of weight 12 for Γ. Additionally, since $E_4(z)$ and $E_6(z)$ both have constant term $a_0 = 1$; $\Delta(z)$ is a cusp form. One can show $\Delta(z)$ is the cusp form of lowest possible weight for Γ. The interested reader should consult [24, 47] for additional details and examples.

Let ω denote a primitive cube root of unity and i denote a primitive fourth root of unity. The next result will assist in determining the spaces $M_k(\Gamma)$ and $S_k(\Gamma)$ of a given weight k.

Proposition 4 (Chapter 3, Proposition 8, [47])**.** *Let $f(z)$ be a non-zero modular function of weight k for Γ. For $P \in \mathcal{H}$, let $v_P(f)$ denote the order of the zero (or minus the order of pole) of $f(z)$ at the point P. Let $v_\infty(f)$ denote the index of the first non-vanishing term in the q-expansion of $f(z)$. Then*

$$v_\infty(f) + \frac{1}{2} v_i(f) + \frac{1}{3} v_\omega(f) + \sum_{\substack{P \in \Gamma \backslash \mathcal{H}, \\ P \neq i, \omega}} v_P(f) = \frac{k}{12}. \tag{2.13}$$

For a proof, we refer the reader to [47].

To conclude this Chapter, we now state and prove important properties of $M_k(\Gamma)$ and $S_k(\Gamma)$.

Proposition 5 (Chapter 3, Proposition 9, [47]). *Let k be an even integer, $\Gamma = \mathrm{SL}_2(\mathbb{Z})$.*

(a) The only modular forms of weight 0 for Γ are constants, i.e. $M_0(\Gamma) = \mathbb{C}$.

(b) $M_k(\Gamma) = 0$ if k is negative or $k = 2$.

(c) $M_k(\Gamma)$ is one-dimensional, generated by E_k, if $k = 4, 6, 8, 10$ or 14; in other words, $M_k(\Gamma) = \mathbb{C}E_k$ for those values of k.

(d) $S_k(\Gamma) = 0$ if $k < 12$ or $k = 14$; $S_{12}(\Gamma) = \mathbb{C}\Delta$; and for $k > 14$ $S_k(\Gamma) = \Delta M_{k-12}(\Gamma)$ (i.e. the cusp forms of weight k are obtained by multiplying modular forms of weight $k - 12$ by the function $\Delta(z)$).

(e) $M_k(\Gamma) = S_k(\Gamma) \oplus \mathbb{C}E_k$ for $k > 2$.

Proof. We begin by observing that all terms on the left hand side of equation (2.13) are non-negative.

(a) Let $f \in M_0(\Gamma)$. Suppose $f(z)$ takes on the value c. Then $f(z) - c \in M_0(\Gamma)$ and it has a zero. Observe

$$v_\infty(f(z) - c) + \frac{1}{2}v_i(f(z) - c) + \frac{1}{3}v_\omega(f(z) - c) + \sum_{P \in \Gamma\backslash\mathcal{H}, P \neq i, \omega} v_P(f(z) - c) = 0.$$

Since $f(z) - c$ has a zero, one of the terms on the left hand side must be positive. However, since the right hand side is identically zero, this only occurs when $f(z) - c$ is the zero function. Hence $f(z)$ is constant.

(b) From equation (2.13), if $k < 0$, then the right hand side of the equation is negative. However, every term on the left hand side is positive. So $M_k(\Gamma) = 0$ for $k < 0$. Additionally, when $k = 2$, the right hand side equals $\frac{1}{6}$, which is not a possible value for the left hand side.

(c) Assume $k \in \{4, 6, 8, 10, 14\}$. Then $v_p(f)$ must be chosen in the following ways in order to satisfy equation (2.13).

When $k = 4$, $v_\omega(f) = 1$ and $v_p(f) = 0$ for all $p \neq \omega$.

When $k = 6$, $v_i(f) = 1$ and $v_p(f) = 0$ for all $p \neq i$.

When $k = 8$, $v_\omega(f) = 2$ and $v_p(f) = 0$ for all $p \neq \omega$.

When $k = 10$, $v_\omega(f) = v_i(f) = 1$ and $v_p(f) = 0$ for all $p \neq i, \omega$.

Finally, when $k = 14$, $v_\omega(f) = 2$, $v_i(f) = 1$ and $v_p(f) = 0$ for all $p \neq i, \omega$.

Consider two non-zero modular forms of the same weight. From above, we know that $f_1(z)$ and $f_2(z)$ must have the same zeros. Hence $\dfrac{f_1(z)}{f_2(z)}$, the weight zero modular function, is actually a modular form. From part (a), we can conclude that $f_1(z) = cf_2(z)$ for some constant c. So we may choose $f_2(z) = E_k(z)$ and thus obtaining the result.

(d) For $f \in S_k(\Gamma)$, we know $v_\infty(f) > 0$. When $k = 12$ and $f = \Delta$, as defined in Example 2, equation (2.13) tells us that the only zero of $\Delta(z)$ is at infinity. Therefore, given any k and any $f \in S_k(\Gamma)$, the modular function $\dfrac{f}{\Delta}$ is a modular form. So $\dfrac{f}{\Delta} \in M_{k-12}(\Gamma)$. From this, one can obtain the result.

(e) We know E_k does not vanish at ∞. Given any $f \in M_k(\Gamma)$, there exists a multiple of E_k such that $f - cE_k$ vanishes at ∞. So $f - cE_k \in S_k(\Gamma)$.

□

Chapter 3

Nearly Holomorphic Eigenforms

In this chapter, we prove that the product of two nearly holomorphic Hecke eigenforms is again a Hecke eigenform for only finitely many choices of factors. This is joint work with Jeff Beyerl, Kevin James and Hui Xue. I would like to thank them for allowing the republication of these results. For related work, we refer the reader to [29, 30, 34, 50, 51, 53] and a more concise version of this work can be found in [2].

3.1 Nearly Holomorphic Modular Forms

Let $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ be the full modular group and let $M_k(\Gamma)$ represent the space of level Γ modular forms of even weight k. Let $f \in M_k(\Gamma)$ and $g \in M_l(\Gamma)$. Throughout k, l will be positive even integers and r, s will be non-negative integers.

Definition 3. We define the Maass-Shimura operator δ_k on $f \in M_k(\Gamma)$ by

$$\delta_k(f) = \left(\frac{1}{2\pi i}\left(\frac{k}{2i\mathrm{Im}z} + \frac{\partial}{\partial z}\right) f\right)(z).$$

Write $\delta_k^{(r)} := \delta_{k+2r-2} \circ \cdots \circ \delta_{k+2} \circ \delta_k$, with $\delta_k^{(0)} = id$. A function of the form $\delta_k^{(r)}(f)$ is called a **nearly holomorphic modular form of weight** $k + 2r$ as in [50]. Let $\widetilde{M}_k(\Gamma)$ denote the

space generated by nearly holomorphic forms of weight k and level Γ.

Note that the image of δ_k is contained in $\widetilde{M}_{k+2}(\Gamma)$. Also, the notation $\delta_k^{(r)}(f)$ will only be used when f is in fact a holomorphic modular form.

We define the Hecke operator $T_n : \widetilde{M}_k(\Gamma) \to \widetilde{M}_k(\Gamma)$ following [49], as

$$\left(T_n\left(f\right)\right)(z) = n^{k-1} \sum_{d|n} d^{-k} \sum_{b=0}^{d-1} f\left(\frac{nz+bd}{d^2}\right).$$

A modular form (or nearly holomorphic modular form) $f \in \widetilde{M}_k(\Gamma)$ is said to be an **eigenform** if it is an eigenvector for all the Hecke operators $\{T_n\}_{n\in\mathbb{N}}$.

The Rankin-Cohen bracket operator $[f,g]_j : M_k(\Gamma) \times M_l(\Gamma) \to M_{k+l+2j}(\Gamma)$ is given by

$$[f,g]_j := \frac{1}{(2\pi i)^j} \sum_{a+b=j} (-1)^a \binom{j+k-1}{b} \binom{j+l-1}{a} f^{(a)}(z) g^{(b)}(z)$$

where $f^{(a)}$ denotes the a^{th} derivative of f.

Proposition 6 (Proposition 2.2, [2])**.** *Let $f \in M_k(\Gamma)$, $g \in M_l(\Gamma)$. Then*

$$\delta_k^{(r)}(f)\delta_l^{(s)}(g) = \sum_{j=0}^{s} (-1)^j \binom{s}{j} \delta_{k+l+2r+2j}^{(s-j)} \left(\delta_k^{(r+j)}(f) g\right).$$

Before we prove this result, we will prove a simpler result first.

Lemma 7. *Let $f \in M_k(\Gamma)$, $g \in M_l(\Gamma)$. Then*

$$\delta_{k+l}^{(1)}(fg) = \delta_k^{(1)}(f)g + f\delta_l^{(1)}(g).$$

Proof. Assume that $f \in M_k(\Gamma)$ and $g \in M_l(\Gamma)$. Then

$$\begin{aligned}\delta_{k+l}^{(1)}(fg) &= \left(\frac{1}{2\pi i}\right)\left(\frac{k+l}{2iy} + \frac{\partial}{\partial z}\right)(fg) \\ &= \left(\frac{1}{2\pi i}\right)\left(\frac{(k+l)fg}{2iy} + \frac{\partial f}{\partial z}g + f\frac{\partial g}{\partial z}\right).\end{aligned}$$

Also,

$$\begin{aligned}\delta_k^{(1)}(f)g &= \left[\left(\frac{1}{2\pi i}\right)\left(\frac{k}{2iy} + \frac{\partial}{\partial z}\right)(f)\right]g \\ &= \left(\frac{1}{2\pi i}\right)\left(\frac{fgk}{2iy} + \frac{\partial f}{\partial z}g\right)\end{aligned}$$

and

$$\begin{aligned}f\delta_l^{(1)}(g) &= f\left(\frac{1}{2\pi i}\right)\left(\frac{l}{2iy} + \frac{\partial}{\partial z}\right)(g) \\ &= \left(\frac{1}{2\pi i}\right)\left(\frac{fgl}{2iy} + f\frac{\partial g}{\partial z}\right).\end{aligned}$$

Therefore combining these we obtain the result.

□

With some additional work we can prove a more general result of this lemma.

Lemma 8.

$$\delta_{k+l+2r}^{(1)}\left(\delta_k^{(r)}(f)g\right) = \delta_k^{(r+1)}(f)g + \delta_k^{(r)}(f)\delta_l^{(1)}(g)$$

The proof of this lemma is identical to Lemma 7 by replacing f by $\delta_k^{(r)}f$.

Now we are able to easily prove Proposition 6.

Proof. (of Proposition 6)

Let f and g be as above. We will proceed by induction on s. By Lemma 8, we know that

for any r,

$$\begin{aligned}\delta_k^{(r)}(f)\delta_l^{(1)}(g) &= \delta_{k+l+2}^{(1)}\left(\delta_k^{(r)}(f)g\right) - \delta^{(r+1)}(f)g \\ &= (-1)^0\binom{1}{0}\delta_{k+l+2r}^{(1)}\left(\delta_k^{(r)}(f)g\right) + (-1)\binom{1}{1}\delta_{k+l+2r+2}^{(0)}\left(\delta_k^{(r+1)}(f)g\right).\end{aligned}$$

So the formula holds for the base case of $s = 1$.

Assume the formula holds for all $i \leq s$. Then for any r the standard product rule, Lemma 7, gives,

$$\delta_{k+l+2s+2r}^{(1)}\left(\delta_k^{(r)}(f)\delta_l^{(s)}(g)\right) = \delta_k^{(r+1)}(f)\delta_l^{(s)}(g) + \delta_k^{(r)}(f)\delta_l^{(s+1)}(g).$$

Thus,

$$\begin{aligned}\delta_k^{(r)}(f)\delta_l^{(s+1)}(g) = & \quad \delta_{k+l+2s+2r}^{(1)}\left(\delta_k^{(r)}(f)\delta_l^{(s)}(g)\right) - \delta_k^{(r+1)}(f)\delta_l^{(s)}(g) \\ = & \quad \delta_{k+l+2s+2r}^{(1)}\left(\sum_{j=0}^{s}(-1)^j\binom{s}{j}\delta_{k+l+2r+2j}^{(s-j)}\left(\delta_k^{(r+j)}(f)g\right)\right) \\ & \quad - \sum_{j=0}^{s}(-1)^j\binom{s}{j}\delta_{k+l+2r+2j+2}^{(s-j)}\left(\delta_k^{(r+j+1)}(f)g\right) \\ = & \quad \sum_{j=0}^{s}(-1)^j\binom{s}{j}\delta_{k+l+2r+2j}^{(s+1-j)}\left(\delta_k^{(r+j)}(f)g\right) \\ & \quad + \sum_{j=0}^{s}(-1)^{j+1}\binom{s}{j}\delta_{k+l+2r+2j+2}^{(s-j)}\left(\delta_k^{(r+j+1)}(f)g\right).\end{aligned}$$

Since,

$$\binom{s}{j} + \binom{s}{j-1} = \binom{s+1}{j}$$

and

$$1 = \binom{s}{0} = \binom{s+1}{0} = \binom{s}{s} = \binom{s+1}{s+1}$$

it follows by reindexing the second sum with $j \mapsto j-1$ that

$$\delta_k^{(r)}(f)\delta_l^{(s+1)}(g) = \sum_{j=0}^{s+1}(-1)^j \binom{s+1}{j} \delta_{k+l+2r+2j}^{(s+1-j)} \left(\delta_k^{(r+j)}(f)g\right).$$

Thus we have proven the formula holds for any r and any s. □

Combining Proposition 6 and the Rankin-Cohen bracket operator gives us the following expansion of a product of nearly holomorphic modular forms.

Proposition 9 (Proposition 2.3, [2]). *Let $f \in M_k(\Gamma)$, $g \in M_l(\Gamma)$. Then*

$$\delta_k^{(r)}(f)\delta_l^{(s)}(g) = \sum_{j=0}^{r+s} \frac{1}{\binom{k+l+2j-2}{j}} \left(\sum_{m=\max(j-r,0)}^{s} (-1)^{j+m} \frac{\binom{s}{m}\binom{r+m}{j}\binom{k+r+m-1}{r+m-j}}{\binom{k+l+r+m+j-1}{r+m-j}} \right) \delta_{k+l+2j}^{(r+s-j)}\left([f,g]_j(z)\right).$$

Proof. Lanphier [51] gives the following formula:

$$\delta_k^{(n)}(f(z)) \cdot g(z) = \sum_{j=0}^{n} \frac{(-1)^j \binom{n}{j}\binom{k+n-1}{n-j}}{\binom{k+l+2j-2}{j}\binom{k+l+n+j-1}{n-j}} \delta_{k+l+2j}^{(n-j)}\left([f,g]_j(z)\right).$$

Substituting this into the equation in Proposition 6, we obtain

$$\delta_k^{(r)}(f)\delta_l^{(s)}(g) = \sum_{m=0}^{s}(-1)^m \binom{s}{m} \delta_{k+l+2r+2m}^{(s-m)} \left[\sum_{j=0}^{r+m} \frac{(-1)^j \binom{r+m}{j}\binom{k+r+m-1}{r+m-j}}{\binom{k+l+2j-2}{j}\binom{k+l+r+m+j-1}{r+m-j}} \delta_{k+l+2j}^{(r+m-j)}\left([f,g]_j(z)\right) \right].$$

Therefore,

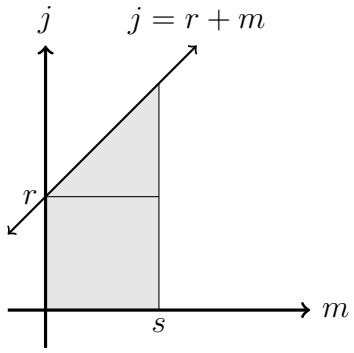
$$\delta_k^{(r)}(f)\delta_l^{(s)}(g) = \sum_{m=0}^{s}(-1)^m\binom{s}{m}\delta_{k+l+2r+2m}^{(s-m)}\left[\sum_{j=0}^{r+m}\frac{(-1)^j\binom{r+m}{j}\binom{k+r+m-1}{r+m-j}}{\binom{k+l+2j-2}{j}\binom{k+l+r+m+j-1}{r+m-j}}\delta_{k+l+2j}^{(r+m-j)}[f,g]_j(z)\right]$$

$$= \sum_{m=0}^{s}\sum_{j=0}^{r+m}(-1)^m\binom{s}{m}\delta_{k+l+2r+2m}^{(s-m)}\frac{(-1)^j\binom{r+m}{j}\binom{k+r+m-1}{r+m-j}}{\binom{k+l+2j-2}{j}\binom{k+l+r+m+j-1}{r+m-j}}\delta_{k+l+2j}^{(r+m-j)}[f,g]_j(z)$$

$$= \sum_{j=0}^{r}\sum_{m=0}^{s}(-1)^m\binom{s}{m}\delta_{k+l+2r+2m}^{(s-m)}\frac{(-1)^j\binom{r+m}{j}\binom{k+r+m-1}{r+m-j}}{\binom{k+l+2j-2}{j}\binom{k+l+r+m+j-1}{r+m-j}}\delta_{k+l+2j}^{(r+m-j)}[f,g]_j(z)$$
$$+ \sum_{j=r+1}^{r+s}\sum_{m=j-r}^{s}(-1)^m\binom{s}{m}\delta_{k+l+2r+2m}^{(s-m)}\frac{(-1)^j\binom{r+m}{j}\binom{k+r+m-1}{r+m-j}}{\binom{k+l+2j-2}{j}\binom{k+l+r+m+j-1}{r+m-j}}\delta_{k+l+2j}^{(r+m-j)}[f,g]_j(z)$$

$$= \sum_{j=0}^{r+s}\frac{\delta_{k+l+2j}^{(r+s-j)}[f,g]_j(z)}{\binom{k+l+2j-2}{j}}\left(\sum_{m=\max(j-r,0)}^{s}(-1)^{j+m}\frac{\binom{s}{m}\binom{r+m}{j}\binom{k+r+m-1}{r+m-j}}{\binom{k+l+r+m+j-1}{r+m-j}}\right)$$

where we interchanged summations by noting that we are summing over the integer points in the following region.



□

Note that by the fact that $\binom{s}{m} = 0$ for integral $m < 0$ we may rewrite the equation

given in Proposition 9 as

$$\delta_k^{(r)}(f)\delta_l^{(s)}(g) = \sum_{j=0}^{r+s} \frac{\delta_{k+l+2j}^{(r+s-j)}[f,g]_j(z)}{\binom{k+l+2j-2}{j}} \left(\sum_{m=j-r}^{s} (-1)^{j+m} \frac{\binom{s}{m}\binom{r+m}{j}\binom{k+r+m-1}{r+m-j}}{\binom{k+l+r+m+j-1}{r+m-j}} \right).$$

Next we state a simple result relating Hecke operators and the Maass-Shimura operator.

Proposition 10. *Assume $f \in M_k$. Then*

$$(\delta_k (T_n f))(z) = \frac{1}{n} (T_n (\delta_k f))(z)$$

where T_n is the Hecke operator and δ_k is the Maass-Shimura operator.

Proof. By Theorem 6.1 of [46], we know we can write

$$(T_n (f))(z) = n^{k-1} \sum_{d|n} d^{-k} \sum_{b=0}^{d-1} f\left(\frac{nz+bd}{d^2}\right).$$

By definition of the Maass-Shimura operator, we have

$$\delta_k (f(z)) = \left(\frac{1}{2\pi i}\right)\left(\frac{kf(z)}{2i\mathrm{Im}(z)} + \frac{\partial f}{\partial z}(z)\right).$$

First note that

$$\mathrm{Im}\left(\frac{nz+bd}{d^2}\right) = \frac{n\mathrm{Im}(z)}{d^2}.$$

Then combining the above two results, we have that

$$\begin{aligned} T_n\left(\delta_k f\right)(z) &= n^{k+1}\sum_{d|n} d^{-(k+2)}\sum_{b=0}^{d-1}\left(\frac{1}{2\pi i}\right)\left(\frac{k}{2i\mathrm{Im}\left(\frac{nz+bd}{d^2}\right)}f\left(\frac{nz+bd}{d^2}\right)+\frac{\partial f}{\partial z}\left(\frac{nz+bd}{d^2}\right)\right) \\ &= n^{k+1}\sum_{d|n} d^{-(k+2)}\sum_{b=0}^{d-1}\left(\frac{1}{2\pi i}\right)\left(\frac{kd^2}{2in\mathrm{Im}(z)}f\left(\frac{nz+bd}{d^2}\right)+\frac{\partial f}{\partial z}\left(\frac{nz+bd}{d^2}\right)\right) \\ &= n\left[n^{k-1}\sum_{d|n} d^{-k}\sum_{b=0}^{d-1}\left(\frac{1}{2\pi i}\right)\left(\frac{k}{2i\mathrm{Im}(z)}f\left(\frac{nz+bd}{d^2}\right)+\frac{n}{d^2}\frac{\partial f}{\partial z}\left(\frac{nz+bd}{d^2}\right)\right)\right]. \end{aligned}$$

Now let's compute $\delta_k\left(T_n f\right)(z)$. Let $F(z)=f\left(\frac{nz+bd}{d^2}\right)$. Then

$$\begin{aligned} \frac{\partial}{\partial z}\left(F(z)\right) &= \frac{\partial}{\partial z}\left(f\left(\frac{nz+bd}{d^2}\right)\right) \\ &= \frac{\partial f}{\partial z}\left(\frac{nz+bd}{d^2}\right)\frac{\partial}{\partial z}\left(\frac{nz+bd}{d^2}\right) \\ &= \frac{n}{d^2}\frac{\partial f}{\partial z}\left(\frac{nz+bd}{d^2}\right). \end{aligned}$$

So,

$$\begin{aligned}
\delta_k \left(T_n f\right)(z) &= \delta_k \left(n^{k-1} \sum_{d|n} d^{-k} \sum_{b=0}^{d-1} f\left(\frac{nz+bd}{d^2}\right)\right) \\
&= n^{k-1} \sum_{d|n} d^{-k} \sum_{b=0}^{d-1} \delta_k \left(f(z)\right) \\
&= n^{k-1} \sum_{d|n} d^{-k} \sum_{b=0}^{d-1} \left(\frac{1}{2\pi i}\right) \left[\frac{k}{2i\mathrm{Im}(z)} f(z) + \frac{\partial}{\partial z}\left(f(z)\right)\right] \\
&= n^{k-1} \sum_{d|n} d^{-k} \sum_{b=0}^{d-1} \left(\frac{1}{2\pi i}\right) \left[\frac{k}{2i\mathrm{Im}(z)} f\left(\frac{nz+bd}{d^2}\right) + \frac{n}{d^2}\frac{\partial f}{\partial z}\left(\frac{nz+bd}{d^2}\right)\right].
\end{aligned}$$

Therefore we obtain the result. □

From Proposition 10, we obtain the following corollary.

Corollary 11 (Proposition 2.4, [2]). *Let $f \in M_k(\Gamma)$. Then*

$$\left(\delta_k^{(m)}\left(T_n f\right)\right)(z) = \frac{1}{n^m}\left(T_n\left(\delta_k^{(m)}(f)\right)\right)(z)$$

where $m \geq 0$.

Proof. We will proceed by induction. From Proposition 10, we know that the case $m = 1$ is

true. So assume for all $l \leq m$, the formula holds. Then

$$\begin{aligned}
\delta_k^{(m+1)}\left(T_n f\right)(z) &= \delta_{k+2m}\left(\delta_k^{(m)}\left(T_n f\right)\right)(z) \\
&= \delta_{k+2m}\left(\frac{1}{n^m}\left(T_n\left(\delta_k^{(m)} f\right)\right)(z)\right) \\
&= \frac{1}{n^m}\delta_{k+2m}\left(T_n\left(\delta_k^{(m)} f\right)\right)(z) \\
&= \frac{1}{n^m}\left(\frac{1}{n}T_n\left(\delta_{k+2m}\left(\delta_k^{(m)} f\right)\right)(z)\right) \\
&= \frac{1}{n^{m+1}}T_n\left(\delta_k^{(m+1)} f\right)(z).
\end{aligned}$$

□

In order to prove the next result, we need the following lemma.

Lemma 12. *The Maass-Shimura operator, δ, is injective.*

Proof. We begin by noticing that

$$\begin{aligned}
\left(\delta_k f\right)(z) &= \frac{1}{2\pi i}\left(\frac{k}{2i\mathrm{Im}(z)}f(z) + \frac{\partial f}{\partial z}(z)\right) \\
&= \left(\frac{1}{2\pi i}\right)\left(\frac{kf(z)}{2i\mathrm{Im}(z)}\right) + \left(\frac{1}{2\pi i}\right)\frac{\partial f}{\partial z}
\end{aligned}$$

We observe that the holomorphic part of $\left(\delta_k f\right)(z)$ is $\left(\frac{1}{2\pi i}\right)\frac{\partial f}{\partial z}$, and the non-holomorphic part is $\left(\frac{1}{2\pi i}\right)\left(\frac{kf(z)}{2i\mathrm{Im}(z)}\right)$. It is easy to see that the non-holomorphic part is zero if and only if $f(z)$ is identically zero. Then $\left(\delta_k f\right)(z) \equiv 0$ if and only if both the non-holomorphic part and the holomorphic part are zero. This occurs if and only if the non-holomorphic part

is zero, which occurs if and only if $f(z) \equiv 0$. Therefore if $(\delta_k f)(z) = 0$, then we have that $f(z) = 0$. Hence δ_k is injective. □

We would like to show that a sum of eigenforms of distinct weights can only be an eigenform if each form has the same set of eigenvalues. In order to prove this, we need to know the relationship between eigenforms and nearly holomorphic eigenforms.

Proposition 13 (Proposition 2.5, [2]). *Let $f \in M_k(\Gamma)$. Then $\delta_k^{(r)}(f)$ is an eigenform for T_n if and only if f is. In this case, if λ_n denotes the eigenvalue of T_n associated to f, then the eigenvalue of T_n associated to $\delta_k^{(r)}(f)$ is $n^r\lambda_n$.*

Proof. Assume f is an eigenform. So $(T_n f)(z) = \lambda_n f(z)$. Then applying $\delta_k^{(r)}$ to both sides and applying Proposition 11 we obtain the following:

$$T_n\left(\delta_k^{(r)}(f)\right)(z) = n^r\lambda_n\left(\delta_k^{(r)}(f)\right)(z).$$

So $\delta_k^{(r)}(f)$ is an eigenform.

Now assume that $\delta_k^{(r)}(f)$ is an eigenform. Then $T_n\left(\delta_k^{(r)}(f)\right)(z) = \lambda_n\left(\delta_k^{(r)}(f)\right)(z)$. Using Proposition 11, we obtain

$$\begin{aligned}\delta_k^{(r)}(T_n f)(z) &= \frac{\lambda_n}{n^r}\delta_k^{(r)}(f)(z) \\ &= \delta_k^{(r)}\left(\frac{\lambda_n}{n^r}f\right)(z).\end{aligned}$$

Since $\delta_k^{(r)}$ is injective,

$$(T_n f)(z) = \frac{\lambda_n}{n^r}f(z).$$

Hence f is an eigenform.

□

Finally, before we state the result on a sum of eigenforms, it is important to note the spaces the Maass-Shimura operator acts between.

Lemma 14. *The Maass-Shimura operator, δ_k, is an operator from $\widetilde{M}_k(\Gamma)$ to $\widetilde{M}_{k+2}(\Gamma)$.*

Proof. Let $h \in \widetilde{M}_k(\Gamma)$. First note that

$$\frac{\partial}{\partial z}\left(h(\gamma z)\right) = \frac{\partial h}{\partial z}(\gamma z)\frac{\partial \gamma z}{\partial z} = \frac{\partial h}{\partial z}(\gamma z)\frac{1}{(cz+d)^2}$$

where $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Hence we have:

$$\begin{aligned}
(2\pi i)(\delta_k h)(\gamma z) &= \left(\frac{k}{2i\mathrm{Im}\cdot} + \frac{\partial}{\partial z}\right)(h)(\gamma z) \\
&= \frac{kh(\gamma z)}{2i\mathrm{Im}\gamma z} + \left(\frac{\partial h}{\partial z}\right)(\gamma z) \\
&= |cz+d|^2\frac{kh(\gamma z)}{2i\mathrm{Im}z} + (cz+d)^2\left(\frac{\partial}{\partial z}\right)(h(\gamma z)) \\
&= |cz+d|^2(cz+d)^k\frac{kh(z)}{2i\mathrm{Im}z} + (cz+d)^2\left(kc(cz+d)^{k-1}h(z) + (cz+d)^k\frac{\partial}{\partial z}(h(z))\right) \\
&= k(cz+d)^{k+1}h(z)\left(\frac{\overline{cz+d}}{2i\mathrm{Im}z} + c\right) + (cz+d)^{k+2}\frac{\partial}{\partial z}(h(z)) \\
&= \left(\frac{k(cz+d)^{k+2}}{2i\mathrm{Im}z} + (cz+d)^{k+2}\frac{\partial}{\partial z}\right)(h(z)) \\
&= (cz+d)^{k+2}\left(\frac{k}{2i\mathrm{Im}\cdot} + \frac{\partial}{\partial z}\right)(h)(z) \\
&= (cz+d)^{k+2}(2\pi i)(\delta_k h)(z).
\end{aligned}$$

□

Now the result on a sum of eigenforms with distinct weights follows.

Proposition 15 (Proposition 2.6, [2]). *Suppose that $\{f_i\}_i$ is a collection of modular forms with distinct weights k_i. Then $\sum_{i=1}^{t} a_i \delta_{k_i}^{\left(n-\frac{k_i}{2}\right)}(f_i)$ $(a_i \in \mathbb{C}^*)$ is an eigenform if and only if every $\delta_{k_i}^{\left(n-\frac{k_i}{2}\right)}(f_i)$ is an eigenform and each function has the same set of eigenvalues.*

Proof. By induction we only need to consider $t = 2$.

($\Leftarrow$) : If $T_n\left(\delta_k^{(r)}(f)\right) = \lambda \delta_k^{(r)}(f)$, and $T_n\left(\delta_l^{\left(\frac{k-l}{2}+r\right)}(g)\right) = \lambda \delta_l^{\left(\frac{k-l}{2}+r\right)}(g)$, then by linearity of T_n,

$$T_n\left(\delta_k^{(r)}(f) + \delta_l^{\left(\frac{k-l}{2}+r\right)}(g)\right) = \lambda\left(\delta_k^{(r)}(f) + \delta_l^{\left(\frac{k-l}{2}+r\right)}(g)\right).$$

($\Rightarrow$) : Suppose $\delta_k^{(r)}(f) + \delta_l^{\left(\frac{k-l}{2}+r\right)}(g)$ is an eigenform. Then by Proposition 13 and linearity of $\delta_k^{(r)}$, we have that $f + \delta_l^{\left(\frac{k-l}{2}\right)}(g)$ is also an eigenform. We can write

$$T_n\left(f + \delta_l^{\left(\frac{k-l}{2}\right)}(g)\right) = \lambda_n\left(f + \delta_l^{\left(\frac{k-l}{2}\right)}(g)\right).$$

Applying linearity of T_n and Proposition 11 we obtain

$$T_n(f) + n^{\frac{k-l}{2}} \delta_l^{\left(\frac{k-l}{2}\right)}\left(T_n(g)\right) = \lambda_n f + \lambda_n \delta_l^{\left(\frac{k-l}{2}\right)}(g).$$

Rearranging this we have

$$T_n(f) - \lambda_n f = \delta_l^{\left(\frac{k-l}{2}\right)}\left(\lambda_n g - n^{\frac{k-l}{2}} T_n(g)\right).$$

Since the δ operator sends all non-zero modular forms to so called nearly holomorphic modular forms, the right hand side is either non-holomorphic or zero. However, the left hand side is holomorphic and of positive weight. Hence both sides must be zero. So we have

$$\begin{aligned} T_n(f) &= \lambda_n f \text{ and } T_n(g) \\ &= \lambda_n n^{\frac{-(k-l)}{2}} g. \end{aligned}$$

Therefore f is an eigenvector for T_n with eigenvalue λ_n, and g is an eigenvector for T_n with eigenvalue $\lambda_n n^{\frac{-(k-l)}{2}}$. By Proposition 13, we have that $\delta_l^{\left(\frac{k-l}{2}\right)}(g)$ is an eigenvector for T_n with eigenvalue λ_n. Hence f and $\delta_l^{\left(\frac{k-l}{2}\right)}(g)$ are eigenvectors for T_n with eigenvalue λ_n. So $\delta_k^{(r)}(f)$ and $\delta_l^{\left(\frac{k-l}{2}+r\right)}(g)$ must have the same eigenvalue with respect to T_n as well. Thus for all $n \in \mathbb{N}$, $\delta_k^{(r)}(f)$ and $\delta_l^{\left(\frac{k-l}{2}+r\right)}(g)$ must be eigenforms with the same eigenvalues.

□

Using the above proposition we can show that when two holomorphic eigenforms of different weights are mapped to the same space of nearly holomorphic modular forms that different eigenvalues are obtained.

Lemma 16 (Lemma 2.7, [2]). *Let $l < k$ and $f \in M_k(\Gamma), g \in M_l(\Gamma)$ both be eigenforms. Then $\delta_l^{\left(\frac{k-l}{2}\right)}(g)$ and f do not have the same eigenvalues.*

Proof. For sake of contradiction, assume f and $\delta_l^{\left(\frac{k-l}{2}\right)}(g)$ have the same eigenvalues. That is, say g has eigenvalues $\lambda_n(g)$, then by Proposition 13 we are assuming that f has eigenvalues $n^{\frac{k-l}{2}}\lambda_n(g)$. We then have

$$\begin{aligned} f(z) &= \sum_{n=1}^{\infty} c n^{\frac{k-l}{2}} \lambda_n(g) q^n + c_0 \\ &= \frac{1}{(2\pi i)^{(k-l)/2}} \frac{\partial^{(k-l)/2}}{\partial z^{(k-l)/2}} \sum_{n=1}^{\infty} c\lambda_n(g) q^n + c_0 \\ &= \frac{1}{(2\pi i)^{(k-l)/2}} \frac{\partial^{(k-l)/2}}{\partial z^{(k-l)/2}} g(z) + c_0 \end{aligned}$$

which says that f is a derivative of g plus a constant. To see that this cannot be a modular form, consider $f - \delta_l^{\left(\frac{k-l}{2}\right)} g$:

$$\begin{aligned} f - \delta_l^{\left(\frac{k-l}{2}\right)} g &= \frac{1}{(2\pi i)^{(k-l)/2}} \frac{\partial^{(k-l)/2}}{\partial z^{(k-l)/2}} g(z) + c_0 - \frac{1}{(2\pi i)^{(k-l)/2}} \frac{\partial^{(k-l)/2}}{\partial z^{(k-l)/2}} g(z) - \frac{1}{(2\pi i)^{(k-l)/2}} \frac{l}{2i\mathrm{Im}z} g(z) \\ &= c_0 - \frac{1}{(2\pi i)^{(k-l)/2}} \frac{l}{2i\mathrm{Im}(z)} g(z) \in \widetilde{M}_k(\Gamma). \end{aligned}$$

In particular, using $\gamma = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ we find

$$z^k \left(c_0 - \frac{1}{(2\pi i)^{(k-l)/2}} \frac{l}{2i\mathrm{Im}z} g(z) \right) = c_0 - \frac{1}{(2\pi i)^{(k-l)/2}} \frac{l}{2i\mathrm{Im}-1/z} g(-1/z)$$
$$= c_0 - \frac{l}{(2\pi i)^{(k-l)/2}} \frac{|z|^2}{2i\mathrm{Im}z} z^l g(z).$$

Solving for g, we then have

$$g(z) = c_0(z^k - 1)\frac{2il^{-1}(2\pi i)^{(k-l)/2}\mathrm{Im}z}{z^k + |z|^2 z^l}$$

which is not invariant to translations by one since

$$c_0(z^k - 1)\frac{2il^{-1}(2\pi i)^{(k-l)/2}\mathrm{Im}z}{z^k + |z|^2 z^l} \neq c_0((z+1)^k - 1)\frac{2il^{-1}(2\pi i)^{(k-l)/2}\mathrm{Im}z}{(z+1)^k + |z+1|^2 (z+1)^l}.$$

Hence we have a contradiction. □

We shall need a special case of this lemma.

Corollary 17 (Corollary 2.8, [2]). *Let $k > l$ and $f \in M_k(\Gamma), g \in M_l(\Gamma)$. Then $\delta_l^{\left(\frac{k-l}{2}+r\right)}(g)$ and $\delta_k^{(r)}(f)$ do not have the same eigenvalues.*

From [51] we know for eigenforms f, g, that $[f,g]_j$ is a eigenform only finitely many times. Hypothetically, however, it could be zero. In particular, by the fact that $[f,g]_j = (-1)^j[g,f]_j$, and $f = g$ with j odd gives $[f,g]_j = 0$. Hence we need the following lemma, where E_k denotes the weight k Eisenstein series normalized to have constant term 1.

Lemma 18 (Lemma 2.9, [2]). *Let $\delta_k^{(r)}(f) \in \widetilde{M}_{k+2r}(\Gamma)$, $\delta_l^{(s)}(g) \in \widetilde{M}_{l+2s}(\Gamma)$. In the following cases $[f,g]_j \neq 0$:*

Case 1: f a cusp form, g not a cusp form.

Case 2: $f = g = E_k$, j *even.*

Case 3: $f = E_k, g = E_l$, $k \neq l$.

Proof. **Case 1:** Write $f = \sum_{j=1}^{\infty} A_j q^j, g = \sum_{j=0}^{\infty} B_j q^j$. Then a direct computation of the q-coefficient of $[f,g]_j$ yields

$$A_1 B_0 (-1)^j \binom{j+k-1}{j} \neq 0.$$

Case 2: Using the same notation, a direct computation of the q coefficient yields

$$A_0 B_1 \binom{j+l-1}{j} + A_1 B_0 \binom{j+k-1}{j} = 2A_0 A_1 \binom{j+k-1}{j} \neq 0.$$

Case 3: This is proven in [51] using L-series. We provide an elementary proof here. Without loss of generality, let $k > l$. A direct computation of the q coefficient yields $A_0 B_1 \binom{j+l-1}{j} + A_1 B_0 \binom{j+k-1}{j}$. Using the fact that $A_0 = B_0 = 1$, $A_1 = k/B_k$, $B_1 = l/B_l$, we obtain

$$\frac{-2l}{B_l} \binom{j+k-1}{j} + (-1)^j \frac{-2k}{B_k} \binom{j+l-1}{j}.$$

If j is even, then both of these terms are non-zero and of the same sign. If j is odd, then we note that for $l > 4$,

$$\left| \frac{B_k}{k} \binom{j+k-1}{j} \right| = \left| \frac{(j+k-1)\cdots(k+1)B_k}{j!} \right| > \left| \frac{(j+l-1)\cdots(l+1)B_l}{j!} \right| = \left| \frac{B_l}{l} \binom{j+l-1}{j} \right|$$

using the fact that $|B_k| > |B_l|$ for $l > 4$, l even. For $l = 4$, the inequality holds so long as $j > 1$. For $j = 1$ the above equation simplifies to $|B_k| > |B_l|$ which is true for $(k,l) \neq (8,4)$, with this remaining case handled individually. For $j = 0$, the Rankin-Cohen bracket operator reduces to multiplication. □

We will need the fact that a product is not an eigenform, given in the next lemma.

Lemma 19 (Lemma 2.10, [2]). *Let $\delta_k^{(r)}(f) \in \widetilde{M}_{k+2r}(\Gamma)$, $\delta_l^{(s)}(g) \in \widetilde{M}_{l+2s}(\Gamma)$ both be cuspidal eigenforms. Then $\delta_k^{(r)}(f)\delta_l^{(s)}(g)$ is not an eigenform.*

Proof. By Proposition 9 we may write $\delta_k^{(r)}(f)\delta_l^{(s)}(g)$ as a linear combination of $\delta_{k+l+2j}^{(r+s-j)}([f,g]_j)$. Then from [51], $[f,g]_j$ is never an eigenform. Hence by Proposition 13, $\delta_{k+l+2j}^{(r+s-j)}([f,g]_j)$ is never an eigenform. Finally Proposition 15 tells us that the sum, and thus $\delta_k^{(r)}(f)\delta_l^{(s)}(g)$ is not an eigenform. □

Finally, this last lemma is the driving force in the main result to come; one of the first two terms from Proposition 9 is non-zero.

Lemma 20 (Lemma 2.11, [2]). *Let $\delta_k^{(r)}(f) \in \widetilde{M}_{k+2r}(\Gamma)$, $\delta_l^{(s)}(g) \in \widetilde{M}_{l+2s}(\Gamma)$ both be eigenforms, but not both cusp forms. Then in the expansion given in Proposition 9, either the term including $[f,g]_{r+s}$ is non-zero, or the term including $[f,g]_{r+s-1}$ is non-zero.*

Proof. There are three cases.

Case 1: $f = g = E_k$.

If $r+s$ is even, then via Lemma 18, $[f,g]_{r+s} \neq 0$ and it is clear from Proposition 9 that the coefficient of $[f,g]_{r+s}$ is non-zero so we are done. If $r+s$ is odd, then $[f,g]_{r+s-1}$ is non-zero. Now because $wt(f) = wt(g)$, the coefficient of $[f,g]_{r+s-1}$ is non-zero. This is due to the fact that if it were zero, after simplification we would have $k = -(r+s)+1 \leq 0$, which cannot occur.

Case 2: If f is a cusp form and g is not then by Lemma 18, $[f,g]_{r+s}$, and thus the term including $[f,g]_{r+s}$ is non-zero.

Case 3: If $f = E_k$, $g = E_l$, $k \neq l$. Again by Lemma 18, $[f,g]_{r+s}$, and thus the term including $[f,g]_{r+s}$ is non-zero. □

3.2 Main Result

Recall that E_k is weight k Eisenstein series, and let Δ_k be the unique normalized cuspidal form of weight k for $k \in \{12, 16, 18, 20, 22, 26\}$. We have the following theorem.

Theorem 21 (Theorem 3.1, [2]). *Let $\delta_k^{(r)}(f) \in \widetilde{M}_{k+2r}(\Gamma)$, $\delta_l^{(s)}(g) \in \widetilde{M}_{l+2s}(\Gamma)$ both be eigenforms. Then $\delta_k^{(r)}(f)\delta_l^{(s)}(g)$ is not a eigenform aside from finitely many exceptions. In particular $\delta_k^{(r)}(f)\delta_l^{(s)}(g)$ is a eigenform only in the following cases:*

1. *The 16 holomorphic cases presented in [34] and [29]:*

$$E_4^2 = E_8, \quad E_4E_6 = E_{10}, \quad E_6E_8 = E_4E_{10} = E_{14},$$

$$E_4\Delta_{12} = \Delta_{16}, \quad E_6\Delta_{12} = \Delta_{18}, \quad E_4\Delta_{16} = E_8\Delta_{12} = \Delta_{20},$$

$$E_4\Delta_{18} = E_6\Delta_{16} = E_{10}\Delta_{12} = \Delta_{22},$$

$$E_4\Delta_{22} = E_6\Delta_{20} = E_8\Delta_{18} = E_{10}\Delta_{12} = E_{14}\Delta_{12} = \Delta_{26}.$$

2. $\delta_4(E_4) \cdot E_4 = \frac{1}{2}\delta_8(E_8)$.

Proof. By Proposition 9 we may write

$$\delta_k^{(r)}(f)\delta_l^{(s)}(g) = \sum_{j=0}^{r+s} \alpha_j \delta_{k+l+2j}^{(r+s-j)}\left([f,g]_j\right).$$

Now, by Proposition 15 this sum is an eigenform if and only if every summand is an eigenform with a single common eigenvalue or is zero. Note that by Corollary 17, $\alpha_j\delta_{k+l+2j}^{(r+s-j)}\left([f,g]_j\right)$ are always of different eigenvalues for different j. Hence for $\delta_k^{(r)}(f)\delta_l^{(s)}(g)$ to be an eigenform, all but one term in the summation must be zero and the remaining term must be an eigenform.

If both f, g are cusp forms, apply Lemma 19. Otherwise, from Lemma 20, either the term including $[f,g]_{r+s}$ or the term including $[f,g]_{r+s-1}$ is non-zero. By [51] this is an eigenform only finitely many times. Hence there are only finitely many f, g, r, s that yield the entire sum, $\delta_k^{(r)}(f)\delta_l^{(s)}(g)$, an eigenform. Each of these finitely many quadruples were enumerated and all eigenforms found. See the following comments for more detail. □

Remark 3. In general $2\delta_k\left(E_k\right)\cdot E_k = \delta_{2k}\left(E_k^2\right)$. However, for $k \neq 4$, this is not an eigenform.

Once we know that $\delta_k^{(r)}(f)\delta_l^{(s)}(g)$ is in general not an eigenform, we have to rule out the last finitely many cases. In particular consider each eigenform (and zero) as leading term $[f,g]_n$ in Proposition 9. From [51] we know that there are 29 cases with g a cusp form (12 with $n=0$), 81 cases with f, g both Eisenstein series (4 with $n=0$). By case we mean the instance of $[f,g]_n$ that is an eigenform. We also must consider the infinite class with $f = g = E_k$ and $r+s$ odd, where $[f,g]_{r+s} = 0$.

For the infinite class when $f = g$ and $r+s$ is odd, we have $[f,g]_{r+s} = 0$. By Lemma 20 the $[f,g]_{r+s-1}$ term is non-zero. If $r+s-1=0$, then this is covered in the $n=0$ case. Otherwise $r+s-1 \geq 2$. This is an eigenform only finitely many times. In each of these cases one computes that the $[f,g]_0$ term is non-zero. Thus because there are two non-zero terms, $\delta_k^{(r)}(f)\delta_l^{(s)}(g)$ is not an eigenform.

The 16 cases with $n=0$ are the 16 holomorphic cases. Now consider the rest. In the last finitely many cases we find computationally that there are two non-zero coefficients; the coefficient of $[f,g]_0$ and $[f,g]_{r+s}$. Now $[f,g]_0 \neq 0$ and $[f,g]_{r+s} \neq 0$, so in these cases $\delta_k^{(r)}(f)\delta_l^{(s)}(g)$ is not an eigenform.

The typical case, however, will involve many non-zero terms such as

$$\begin{aligned}\delta_4\left(E_4\right)\cdot\delta_4\left(E_4\right) &= \frac{-1}{45}[E_4,E_4]_2 + 0\cdot\delta_{10}\left([E_4,E_4]_1\right) + \frac{10}{45}\delta_8^{(2)}\left([E_4,E_4]_0\right)\\ &= \frac{-1}{45}\left(42\cdot E_4\frac{\partial^2}{\partial z^2}E_4 - 49\left(\frac{\partial}{\partial z}E_4\right)^2\right) + \frac{10}{45}\delta_8^{(2)}\left(E_8\right),\end{aligned}$$

$$\begin{aligned}\delta_6\left(E_6\right)\cdot E_8 &= \frac{-1}{14}[E_6,E_8]_1+\frac{3}{7}\delta_{14}\left([E_6,E_8]_0\right)\\ &= \frac{-1}{14}\left(6E_6\frac{\partial}{\partial z}E_8-8E_8\frac{\partial}{\partial z}E_6\right)+\frac{3}{7}\delta_{14}\left(E_6E_8\right)\end{aligned}$$

which cannot be eigenforms because of the fact that there are multiple terms of different holomorphic weight.

Chapter 4

Background on Elliptic Curves

4.1 Cubic Reciprocity

In order to estimate the rank of an elliptic curve, we will be using a combination of graph theory and linear algebra. In Chapter 5, the idea of cubic reciprocity will be needed. If the reader is unfamiliar with this material we will give some basic background in this section. Additional details on the following discussion can be found in [44, Chapter 9].

Since we will be discussing 3-descent, we will familiarize ourselves with the ring $\mathbb{Z}[\omega]$. Let ω be a primitive cube root of unity. Then for any $\alpha = a + b\omega \in \mathbb{Z}[\omega]$, we have $N(\alpha) = a^2 - ab + b^2$. It is not hard to show that $\alpha \in \mathbb{Z}[\omega]$ is a unit if and only if $N(\alpha) = 1$. So the units in $\mathbb{Z}[\omega]$ are $1, -1, \omega, -\omega, \omega^2, -\omega^2$.

One important observation is that primes in $\mathbb{Z}$ may no longer be primes in $\mathbb{Z}[\omega]$. For the remainder of this section, when we say rational prime, we mean a prime in $\mathbb{Z}$. The following proposition helps us classify if a rational prime is still prime in $\mathbb{Z}[\omega]$.

Proposition 22 (Proposition 9.1.4, [44]). *Suppose p and q are rational primes.*

1. *If $q \equiv 2 \pmod 3$, then q is prime in $\mathbb{Z}[\omega]$.*

2. *If* $p \equiv 1 \pmod 3$, *then* $p = \pi\overline{\pi}$ *with* π *prime in* $\mathbb{Z}[\omega]$.

3. *Finally* $3 = -\omega^2(1-\omega)^2$ *and* $1-\omega$ *is prime in* $\mathbb{Z}[\omega]$.

Now we will define the residue class ring modulo a prime π. To define a congruence class, we say that $\alpha \equiv \beta \pmod\gamma$ if γ divides $\alpha - \beta$ for $\alpha, \beta, \gamma \in \mathbb{Z}[\omega]$ with $\gamma \neq 0$ and a non-unit. Then we have the following proposition.

Proposition 23 (Proposition 9.2.1, [44]). *Let* $\pi \in \mathbb{Z}[\omega]$ *be a prime. Then* $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ *is a finite field with* $N(\pi)$ *elements.*

Now we are ready to define the cubic residue character. Let π be a prime. The multiplicative group of $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ has order $N(\pi) - 1$. So the analog of Fermat's Little Theorem tells us that if $\pi \nmid \alpha$ with $\alpha \in \mathbb{Z}[\omega]$, then

$$\alpha^{N(\pi)-1} \equiv 1 \pmod\pi .$$

We note that if the norm of π is not 3, then the residue classes of $1, \omega$ and ω^2 are distinct in $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$. And since $\{1, \omega, \omega^2\}$ is a cyclic group of order 3, it follows that $3 \mid (N(\pi) - 1)$.

Proposition 24 (Proposition 9.3.2, [44]). *Suppose* π *is a prime such that* $N(\pi) \neq 3$ *and* $\pi \nmid \alpha$ *where* $\alpha \in \mathbb{Z}[\omega]$;. *Then there exists a unique integer* $m = 0, 1, 2$ *such that* $\alpha^{(N(\pi)-1)/3} \equiv \omega^m \pmod\pi$.

Now we are ready to define the cubic residue character.

Definition 4. If $N(\pi) \neq 3$, the cubic residue character of α modulo π is given by

(a) $\left(\frac{\alpha}{\pi}\right)_3 = 0$ if $\pi \mid \alpha$

(b) $\alpha^{(N(\pi)-1)/3} \equiv \left(\frac{\alpha}{\pi}\right)_3 \pmod\pi$ with $\left(\frac{\alpha}{\pi}\right)_3 = 1, \omega, \omega^2$.

Just as the Legendre symbol is a key component in the theory of quadratic residues, the cubic residue character is key in the theory of cubic residues. If $\left(\frac{\alpha}{\pi}\right)_3 = 1$, we say that α is a cubic residue.

Next we will state some of the important properties of the cubic residue character. These will be extremely useful in the next chapter.

Proposition 25 (Proposition 9.3.3, [44]). *(a)* $\left(\frac{\alpha}{\pi}\right)_3 = 1$ *if and only if* $x^3 \equiv \alpha \pmod{\pi}$ *is solvable.*

(b) $\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3$

(c) If $\alpha \equiv \beta \pmod{\pi}$, *then* $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$

For the remainder of this chapter, we will define $\chi_\pi(\alpha) := \left(\frac{\alpha}{\pi}\right)_3$. The subsequent theorem contains important properties for the cubic residue character, which will be useful later.

Theorem 26 (Proposition 9.3.4, [44]). *Let* $\pi \in \mathbb{Z}[\omega]$ *and* $q \in \mathbb{Z}$ *be primes. Let* $\alpha \in \mathbb{Z}[\omega]$.

1. $\overline{\chi_\pi(\alpha)} = \chi_\pi(\alpha)^2 = \chi_\pi(\alpha^2)$.
2. $\overline{\chi_\pi(\alpha)} = \chi_{\overline{\pi}}(\overline{\alpha})$.
3. $\chi_q(\overline{\alpha}) = \chi_q(\alpha^2)$.
4. *If* $n \in \mathbb{Z}$ *with* $(n, q) = 1$, *then* $\chi_q(n) = 1$.
5. *If* q_1 *and* q_2 *are two distinct primes both equivalent to* 2 *mod* 3, *then* $\chi_{q_1}(q_2) = \chi_{q_2}(q_1)$.

A proof of this theorem can be found in [44], specifically Proposition 9.3.4 and its Corollary.

Since there are six units in $\mathbb{Z}[\omega]$, each element in $\mathbb{Z}[\omega]$ has six associates. Therefore we will introduce the idea of a primary prime.

Definition 5. If π is a prime in $\mathbb{Z}[\omega]$, we say that π is **primary** if $\pi \equiv 2 \pmod 3$.

So, if $\pi = q$ is rational, then π is primary. Otherwise, if $\pi = a + b\omega$ with $a, b \in \mathbb{Z}$, $b \neq 0$, then the definition of primary is equivalent to $a \equiv 2 \pmod 3$ and $b \equiv 0 \pmod 3$.

To conclude this section, we state the Law of Cubic Reciprocity.

Theorem 27 (Law of Cubic Reciprocity)**.** *Let π_1 and π_2 be primary with $N(\pi_1) \neq N(\pi_2)$ and $N(\pi_1), N(\pi_2) \neq 3$. Then*

$$\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1).$$

Ireland and Rosen present two proofs of the Law of Cubic Reciprocity in [44]. The reader should refer to Chapter 9, Sections 4 and 5.

4.2 Elliptic Curves

In this section we will give a quick review of the basic facts and definitions for elliptic curves. For additional details, we refer the reader to [12, 13, 14, 44, 62, 64].

4.2.1 Weierstrass Equations

Let K be any field. A *Weierstrass equation* over K is a cubic equation of the form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{4.1}$$

where $a_1, a_2, a_3, a_4, a_6 \in K$. Define the following values

$$b_2 := a_1^2 + 4a_2, \quad b_4 := a_1a_3 + 2a_4,$$

$$b_6 := a_3^2 + 4a_6, \quad b_8 := a_1^2a_6 - a_1a_3a_4 + a_2a_3^2 + 4a_2a_6 - a_4^2$$

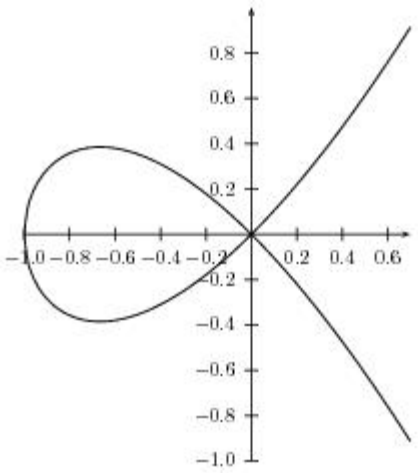


Figure 4.1: Singular Curve

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

We call the value $\Delta = \Delta(E)$ the *discriminant* of the equation E. If $\Delta \neq 0$, then we say that the equation is *non-singular*.

Figure 4.2.1 is a graph of the curve $y^2 = x^3 + x^2$ over $\mathbb{R}$, which is singular.

However, if we considered the curve $y^2 = x^3 - x$, it would be non-singular. A graph of this curve is given by Figure 4.2.1.

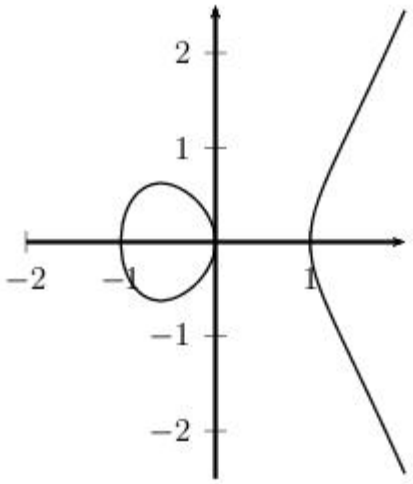


Figure 4.2: Non-Singular Curve

Definition 6. Let $\overline{K}$ be an algebraic closure of K. If E is a non-singular Weierstrass equation, then the set of $(x, y) \in \overline{K} \times \overline{K}$ satisfying (4.1) together with a *point at infinity*, denoted $\mathcal{O}$, is called an **elliptic curve**. The set of K-rational points on E is

$$E(K) := \{(x, y) \in K \times K : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\}.$$

The curve drawn in Figure 4.2.1 is an elliptic curve.

One can produce another Weierstrass equation while keeping the point at infinity fixed by making an *admissible change of variables* to an elliptic curve with Weierstrass equation (4.1). The most general admissible change of variables is of the form

$$x = u^2x' + r, \quad y = u^3y' + su^2x' + t, \quad u, r, s, t \in K, u \neq 0. \tag{4.2}$$

We say that two curves are *isomorphic* if their equations can be related by an admissible change.

Define the following values

$$c_4 := b_2^2 - 24b_4, \qquad c_6 := -b_2^3 + 36b_2b_4 - 216b_6. \tag{4.3}$$

If the characteristic of K is not 2 or 3, we can make a change of variables to Equation (4.1) by sending (x, y) to $((x - 3b_2)/36, y/108)$, from which, we obtain a Weierstrass equation of the form

$$E : y^2 = x^3 - 27c_4x - 54c_6. \tag{4.4}$$

In this case the discriminant is $\Delta = \dfrac{c_4^3 - c_6^2}{1728}$. Hence we can conclude that when the characteristic of K is not 2 or 3, we can write the elliptic curve in the form

$$E_{A,B} : y^2 = x^3 + Ax + B, \qquad A, B \in K. \tag{4.5}$$

Remark 4. There is only one admissible change of variables which will preserve the form of the elliptic curve given by (4.5). To make this change, let

$$x = u^2x', \quad y = u^3y', \quad u \in K^*$$

which yields

$$u^4A' = A, \quad u^6B' = B, \quad u^{12}\Delta' = \Delta.$$

4.2.2 Group Law and Isogenies

Next we are ready to define a group operation on $E(K)$ by using the point at infinity as an identity element.

Before giving the formal definition, we will present a rough idea of how to add points on an elliptic curve. Pick two distinct points on the curve, P and Q. Draw line connecting

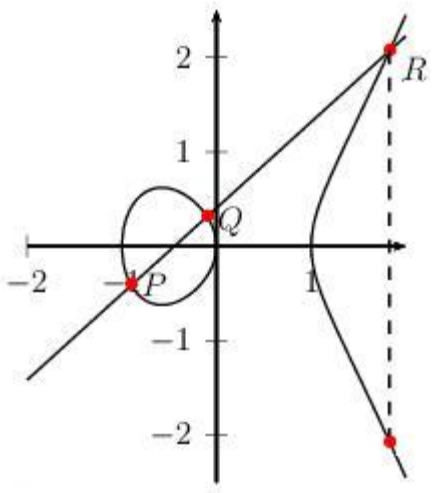


Figure 4.3: Group Law for Elliptic Curves

the two points, as illustrated in Figure 4.2.2. This will intersect the curve at a third point, call it R. Now reflecting over the x-axis, we obtain the point $P + Q$ and R is the inverse of $P + Q$.

Now that we have an idea of how the group law works, we give the formal definition.

Definition 7 (Group Law)**.** The point at infinity, $\mathcal{O}$, is the identity. Let $P = (x_P, y_P) \in E(K) \setminus \{\mathcal{O}\}$. Then the inverse of P is

$$-P := (x_P, -y_P - a_1 x_P - a_3)\,.$$

Now we can begin to define the $+$ operation. Let $Q = (x_Q, y_Q) \in E(K) \setminus \{\mathcal{O}\}$. If $x_P = x_Q$ and $y_Q = -y_P - a_1 x_P - a_3$ (i.e. $Q = -P$), then $P + Q = \mathcal{O}$. Otherwise, define

$$\lambda := \begin{cases} \dfrac{y_Q - y_P}{x_Q - x_P}, & x_P \neq x_Q \\ \\ \dfrac{3x_P^2 + 2a_2 x_P + a_4 - a_1 y_P}{a_1 x_P + a_3 + 2y_P}, & x_P = x_Q \end{cases}$$

and

$$\mu := \begin{cases} \dfrac{y_P x_Q - y_Q x_P}{x_Q - x_P}, & x_P \neq x_Q \\ \\ \dfrac{-x_P^3 + a_4 x_P + 2a_6 - a_3 y_P}{a_1 x_P + a_3 + 2y_P}, & x_P = x_Q. \end{cases}$$

Additionally, define the two following rational functions

$$r\left(x_P, y_P, x_Q, y_Q\right) := \lambda^2 + a_1\lambda - a_2 - x_P - x_Q,$$

$$s\left(x_P, y_P, x_Q, y_Q\right) := -\left(\lambda + a_1\right) r\left(x_P, y_P, x_Q, y_Q\right) - \mu - a_3.$$

Hence we define

$$P + Q := \left(r\left(x_P, y_P, x_Q, y_Q\right), s\left(x_P, y_P, x_Q, y_Q\right)\right).$$

Proposition 28 (Proposition 2.2, [62])**.** *The Group Law given in Definition 7 has the following properties;*

(a) If a line L intersects E at the (not necessarily distinct) points P, Q, R, then

$$(P + Q) + R = \mathcal{O}.$$

(b) $P + Q = Q + P$ for all $P, Q \in E(K)$.

(c) Let $P, Q, R \in E(K)$. Then

$$(P + Q) + R = P + (Q + R).$$

Thus $E(K)$ is an abelian group under $+$

By Bezout's Theorem [62, pp 55], if P and Q are two points on the curve, then the line

l connecting P and Q intersects the curve at a third point (counting the point at infinity). Call this third point R and so $P + Q = -R$. Note that if we work in the projective plane, the point at infinity, $\mathcal{O}$, is the only extra point.

Before discussing maps between elliptic curves, we will give some general background on maps betweens curves. Additional details can be found in [62, pp 15 - 31].

In order to define a morphism between two curves, it is natural to first introduce the generalization; a morphism between two projective varieties.

Definition 8. Let V_1 and V_2 be projective varieties. Let $\overline{K}(V_1))$ be the affine function field of V_1. A **rational map from** V_1 **to** V_2 is a map of the form

$$\phi : V_1 \to V_2$$

$$\phi = [f_1, \ldots, f_n],$$

where $f_0, \ldots, f_n \in \overline{K}(V_1)$ have the property that for every $P \in V_1$ at which $f_0, \ldots, f_n$ are all defined,

$$\phi(P) = [f_0(p), \ldots, f_n(P)].$$

Now we can define a morphism between two projective varieties.

Definition 9. A rational map

$$\phi = [f_0, \ldots, f_n] : V_1 \to V_2$$

is **regular** (or **defined**) **at** $P \in V_1$ if there is a function $g \in \overline{K}(V_1)$ such that

(i) each gf_i is regular at P and

(ii) for some i, $(gf_i)(P) \neq 0$.

If such a g exists, set

$$\phi(P) = [(gf_0)(P), \ldots, (gf_n)(P)].$$

(Note that it may be necessary to take different g's for each point.) A rational map which is regular at every point is called a **morphism**.

Next, we will narrow our focus to studying morphisms between curves. Recall a curve is a projective variety of dimension 1.

Proposition 29 (Proposition 2.1, [62]). *Let C be a curve, $V \subset \mathbb{P}^N$ a variety, $P \in C$ a smooth point and $\phi : C \to V$ a rational map. Then ϕ is regular at P. In particular, if C is smooth, then ϕ is a morphism.*

We have the following interesting property associated with morphisms between two curves.

Theorem 30 (Chapter 2, Theorem 2.3, [62]). *Let $\phi : C_1 \to C_2$ be a morphism of curves. Then ϕ is either constant or surjective.*

Let $\phi : C_1 \to C_2$ be a non-constant rational map defined over K where C_1/K and C_2/K are curves. Then if we compose ϕ with itself, it induces an injection of function fields fixing K,

$$\phi^* : K(C_2) \to K(C_1)$$

$$\phi^* f = f \circ \phi.$$

Definition 10. Let $\phi : C_1 \to C_2$ be map of curves defined over K. If ϕ is constant, we define the **degree of** ϕ to be 0; otherwise we say that ϕ is **finite** and define its **degree** by

$$\deg \phi = [K(C_1) : \phi^* K(C_2)] .$$

We say that ϕ is **separable** (**inseparable**, **purely inseparable**) if the extension $K(C_1)/\phi^* K(C_2)$ has the corresponding property.

One final observation we will make before returning to elliptic curves is the following.

Theorem 31 (Corollary 2.4.1, [62]). *Let C_1 and C_2 be smooth curves and let $\phi : C_1 \to C_2$ be a map of degree 1. Then ϕ is an isomorphism.*

Now that we have some background on maps and on elliptic curves, we will briefly discuss the maps between two elliptic curves. A detailed discussion of the following can be found in [62, pp. 70 - 79].

Definition 11. Let E_1 and E_2 be elliptic curves. An **isogeny** between E_1 and E_2 is a morphism

$$\phi : E_1 \to E_2$$

satisfying $\phi(\mathcal{O}) = \mathcal{O}$. We say E_1 and E_2 are **isogenous** if there is an isogeny ϕ between them with $\phi(E_1) \neq \{\mathcal{O}\}$.

Recall, that a morphism between two curves is either constant or surjective, Theorem 30. Therefore, we can deduce that for any isogeny ϕ, we either have $\phi(E_1) = \{\mathcal{O}\}$ or $\phi(E_1) = E_2$.

Definition 12. Let P be a point on the elliptic curve E and $m \in \mathbb{Z}$. Define **multiplication by m** to be the result of adding P to itself m times if $m > 0$, the result of adding $-P$ to itself $-m$ times if $m < 0$ and $\mathcal{O}$ if $m = 0$. We denote this operation by $[m]P$.

Definition 13. The set of **m-torsion points** or **m-division points** of an elliptic curve E is defined to be the set

$$E[m] := \ker[m] = \left\{ P \in E\left(\overline{K}\right) : [m]P = \mathcal{O} \right\}.$$

The **torsion subgroup** of E, denoted E_{tors}, is the set of points or finite order,

$$E_{\text{tors}} = \bigcup_{m=1}^{\infty} E[m].$$

It is not hard to show that $E[m]$ is a subgroup of $E(\overline{K})$.

Let $E[m](K)$ denote the m-torsion points which are K-rational.

The existence of the following morphism plays a key role in calculating the rank of an elliptic curve.

Proposition 32 (Theorem 6.1, [62]). *Let $\phi : E_1 \to E_2$ be a non-constant isogeny of degree m. Then there exists a unique isogeny*

$$\widehat{\phi} : E_2 \to E_1$$

satisfying

$$\widehat{\phi} \circ \phi = [m].$$

Definition 14. Let $\phi : E_1 \to E_2$ be an isogeny of degree m between two elliptic curves with m-torsion subgroups. The **dual isogeny** to ϕ is the isogeny given in Theorem 32.

Definition 15. Given an elliptic curve E defined over K and $m \in \mathbb{Z}$, the **m-division field** of E over K, denoted by $K(E[m])$, is the field obtained by adjoining K to the x and y coordinates of each point in $E[m] \setminus \{\mathcal{O}\}$.

Remark 5. Let E be an elliptic curve and m a positive integer. One can easily find a recursive formula which produces a polynomial $P_m(x) \in K[x]$ whose roots are precisely the x-coordinates of the points in $E[m] \setminus \{\mathcal{O}\}$, see [62, Exercise 3.7, p 105] for an example. We call a polynomial of this form a *division polynomial*. One can easily obtain the y-coordinates once the x-coordinates are known by using the equation for E.

4.2.3 Rank

The following theorem is a special case of the Mordell-Weil theorem.

Theorem 33 (Mordell)**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then the group $E(\mathbb{Q})$ is finitely generated.*

For a proof, we refer the reader to [43, Chapter 6] or [48, Chapter 5].

This leads us to the following important definition.

Definition 16. By Mordell's Theorem, we can conclude that

$$E(\mathbb{Q}) \cong E_{\text{tors}}(\mathbb{Q}) \times \mathbb{Z}^r \tag{4.6}$$

where r is a non-negative integer called the **rank** of E and is often written as $\text{rank}(E)$.

The torsion part, $E(\mathbb{Q})_{\text{tors}}$, is well understood. We have the following deep theorem of Mazur [62, Chapter 8, Theorem 7.5] which completely characterizes the possibilities for the torsion subgroup.

Theorem 34 (Mazur)**.** *If E is an elliptic curve, then $E_{tors}(\mathbb{Q})$ is one of the following* 15 *groups:*

(1) $\mathbb{Z}/n\mathbb{Z}$ *with* $1 \leq n \leq 10$, $n = 12$*;*

(2) $\mathbb{Z}/2m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ *with* $1 \leq m \leq 4$.

Further, given a specific elliptic curve E, $E(\mathbb{Q})_{\text{tors}}$ is easily computable by the Nagell-Lutz Theorem [62, Chapter 8, Corollary 7.2].

On the other hand, there is not much known about the rank of an elliptic curve. For example, the famous Birch and Swinnerton-Dyer Conjecture (see [4] or [57]) predicts that the rank of $E/\mathbb{Q}$ equals the order of vanishing of its L-series, $L(E, s)$, at $s = 1$. In general,

the rank of an elliptic curve is very difficult to compute. There is no known algorithm to calculate the rank(E) nor is it known what integers can occur as the rank of an elliptic curve. The only way, in practice, to give an upper bound for the rank of $E/\mathbb{Q}$ has been to prove upper bounds for the size of the m-Selmer group, $\mathrm{Sel}_m(E)$ (see [57] for more details). More precisely, for every natural number m we have an exact sequence [62, Theorem 10.4.2]

$$0 \to E(\mathbb{Q})/mE(\mathbb{Q}) \to \mathrm{Sel}_m(E) \to Ш_E[m] \to 0,$$

where $Ш_E$ is the Tate-Shafarevich group and $A[\phi]$ denotes the kernel of ϕ in the group A. Combining this with Mordell's theorem we have that

$$E(\mathbb{Q})/mE(\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^r \oplus E(\mathbb{Q})[m].$$

In particular, we show in Chapter 5 that $[E_{ab}(\mathbb{Q}) : 3E_{ab}(\mathbb{Q})] = 3^{r+1}$.

4.3 Selmer Groups: An Arithmetic Approach

In this section, we will discuss 3-descent maps and their relation to 3-isogenies. This material will be useful when we define Selmer groups in Chapter 5. For all proofs and additional details, we refer the reader to [14, pp 2-6] and [12, pp 557-564].

Recall that if $E(\mathbb{Q})$ has a rational 3-torsion subgroup, this means that there exists a subgroup of $E(\mathbb{Q})$ of order 3 that is stable under the action of Galois conjugation.

Definition 17. Let E be an elliptic curve defined over a perfect field K and let $\mathcal{T}$ be a finite subgroup of $E(\overline{K})$. We say that $\mathcal{T}$ is a **K-rational subgroup** of E if it is globally stable by any $\sigma \in \mathrm{Gal}(\overline{K}/K)$, i.e. if $T \in \mathcal{T}$, then $\sigma(T) \in \mathcal{T}$.

Proposition 35 (Proposition 8.4.2, [12])**.** *Let E be an elliptic curve defined over a perfect*

field K of characteristic different from 2 and having a K-rational subgroup of order 3 of the form $\mathcal{T} = \{\mathcal{O}, T, -T\}$.

1. *The abscissa, $x(T)$, of T is in K.*

2. *Up to a change of variables (i.e. x into $x - x_0$ for some $x_0 \in K$), the curve E has an equation of the form $y^2 = x^3 + D(ax + b)^2$ for some $b, D \in K^*$ and $a \in K$. From this we can conclude that $T = (0, b\sqrt{D})$.*

3. *If, in addition, E has a K-rational point T of order 3, up to the same change of variables, the equation of E is $y^2 = x^3 + (ax + b)^2$ for some $a \in K$, $b \in K^*$ and thus $T = (0, b)$.*

For a proof, see [12, pp 557]

It is important to note that when we work with a general equation of the form

$$y^2 = x^3 + D(ax + b)^2,$$

the discriminant of the curve E is given by

$$\Delta = 16D^2b^3\left(27b - 4a^3D\right)$$

with b, D and $27b - 4a^3D$ all non-zero.

The proof of the following lemma can be found in [14].

Lemma 36 (Lemma 1.2, [14])**.** *Assume E is an elliptic curve with K-rational subgroup of order 3. Then there exists a unique equation of E of the form $y^2 = x^3 + D\left(ax + b\right)^2$, where a, b and D are in $\mathbb{Z}$, D a fundamental discriminant (including 1), $b > 0$ and if we write $b = b_1b_3^3$ with b_1 cube-free, then $(a, b_3) = 1$.*

For the remainder of this section we will consider the elliptic curve E defined over $\mathbb{Q}$ with a rational subgroup of order 3. By the above proposition and lemma, we may assume that E is given by an equation of the form $y^2 = x^3 + D(ax+b)^2$. Fix the 3-torsion point $T = \left(0, b\sqrt{D}\right)$, which may not be in $E(\mathbb{Q})$, however $\mathcal{T} = \{\mathcal{O}, T, -T\}$ is a rational subgroup of order 3. Let $K = \mathbb{Q}\left(\sqrt{D}\right)$ be of discriminant 1. So $K = \mathbb{Q}$ if $D = 1$ and is a quadratic field otherwise. Let G_3 denote the subgroup of $K^*/\left(K^*\right)^3$ of classes whose norms are cubes. Note $G_3 = \mathbb{Q}^*/\left(\mathbb{Q}^*\right)^3$ when $D = 1$.

Now we will define the fundamental 3-isogeny and introduce the auxiliary curve, E', defined by the equation $y^2 = x^3 + D'\left(ax + b'\right)^2$ where

$$D' = -3D \text{ and } b' = \frac{27b - 4a^3D}{9}.$$

It is easy to show that E' is non-singular and therefore an elliptic curve.

Since E' has the same form as E, it has a K-rational subgroup of order 3 generated by

$$T' = \left(0, \frac{27b - 4a^3D}{9}\sqrt{-3D}\right).$$

This leads us to the following proposition.

Proposition 37 (Proposition 8.4.3, [12]). *For any $P = (x, y) \in E \setminus \mathcal{T}$, set*

$$\phi(P) = (x', y') = \left(\frac{x^3 + 4D\left((a^2/3)x^2 + abx + b^2\right)}{x^2}, \frac{y\left(x^3 - 4Db(ax + 2b)\right)}{x^3}\right). \tag{4.7}$$

Set $\phi(T) = \phi(-T) = \phi(\mathcal{O}) = \mathcal{O}'$. Then ϕ is a group homomorphism from E to E', whose kernel is equal to $\mathcal{T}$. Dually, there exists a homomorphism $\widehat{\phi}$ from E' to E defined for

$P' = (x', y')$ different from $\pm T'$ and $\mathcal{O}'$ by

$$\widehat{\phi}(P') = (x, y) = \left(\frac{x'^3 + 4D' \left((a^2/3)x'^2 + ab'x' + b'^2 \right)}{9x'^2}, \frac{y' \left(x'^3 - 4D'b'(ax' + 2b') \right)}{27x'^3} \right) \quad (4.8)$$

and by $\widehat{\phi}(T') = \widehat{\phi}(-T') = \widehat{\phi}(\mathcal{O}') = \mathcal{O}$. Furthermore, for all $P \in E$ we have $\widehat{\phi} \circ \phi(P) = 3P$ and for all $P' \in E'$, we have $\phi \circ \widehat{\phi}(P') = 3P'$.

We refer the reader to [12, Section 8.4] for the proof.

As we will see in Section 4.3.1, we are interested in calculating the images of ϕ and $\widehat{\phi}$. However, these are difficult to calculate, therefore we introduce the idea of the fundamental 3-descent map. As we will see, instead of calculating the images of ϕ and $\widehat{\phi}$, calculating the cardinality of the images 3-descent maps will suffice.

Definition 18. Let E be an elliptic curve defined over $\mathbb{Q}$, with $T = (0, b)$. Let E' be the auxiliary curve.

(1) The 3-descent map α is a map from $E(\mathbb{Q})$ to $\mathbb{Q}^* / (\mathbb{Q}^*)^3$ defined by $\alpha(\mathcal{O}) = 1$, $\alpha((0, b)) = 1/2b$ and $\alpha((x, y)) = y - (ax + b)$.

(2) The corresponding 3-descent map α' from $E'(\mathbb{Q})$ to $\mathbb{Q}\left(\sqrt{-3}\right)^* / \left(\mathbb{Q}\left(\sqrt{-3}\right)^*\right)^3$ defined analogously.

The following proposition states some important properties concerning the 3-descent maps.

Proposition 38 (Proposition 8.4.7, [12])**.** *1. The 3-descent maps α and α' are group homomorphisms.*

2. The kernel of α is equal to the subgroup $\widehat{\phi}(E'(\mathbb{Q}))$ of $\mathbb{Q}^* / (\mathbb{Q}^*)^3$. The kernel of α' is equal to $\phi(E(\mathbb{Q}))$.

For a proof of this proposition see [12, Section 8.4].

4.3.1 3-Descent with Rational 3-Isogeny

In this section we will explain how to use the 3-descent maps α and α' to give a precise estimate on the rank of the elliptic curve E. The reader should refer to [14] for all proofs and extended details.

We begin with the following lemma.

Lemma 39 (Lemma 2.1, [14]). *Let $y^2 = x^3 + D(ax+b)^2$ be the equation of an elliptic curve E with rational 3-torsion subgroup and assume as usual that this equation is written so that D is a fundamental discriminant. The rational 3-torsion points of E are the following:*

1. *If $D = 1$, the points $\mathcal{O}$ and $(0, \pm b)$.*
2. *If $D = -3$ and $2(9b + 4a^3) = t^3$ is the cube of a rational number $t \neq 0$, the point $\mathcal{O}$ and the points P such that $x(P) = \dfrac{t^2}{3} + \dfrac{3}{t^2}\left(4ab + \dfrac{16}{9}a^4\right) + \dfrac{4a^2}{3}$.*
3. *Otherwise, only the point $\mathcal{O}$.*

Note that if an elliptic curve does not have a rational 3-torsion subgroup (i.e. if it does not have an equation of the form $y^2 = x^3 + D(ax+b)^2$), the only rational 3-torsion point is $\mathcal{O}$.

Recall the following exact sequence, [62, Remark X.4.7 pp. 300-301]

$$0 \to \frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} \to \frac{E(\mathbb{Q})}{3E(\mathbb{Q})} \to \frac{E(\mathbb{Q})}{\widehat{\phi}\,(E'(\mathbb{Q}))} \to 0.$$

Combining the above exact sequence with Theorem 33, tells us that if we set $\text{rank}(E) = r$, then

$$\begin{aligned} 3^{r+\delta} &= [E(\mathbb{Q}) : 3E(\mathbb{Q})] && (4.9) \\ &= \left[E(\mathbb{Q}) : \widehat{\phi}\,(E'(\mathbb{Q}))\right]\left[\widehat{\phi}\,(E'(\mathbb{Q})) : \widehat{\phi}\,(\phi\,(E(\mathbb{Q})))\right] && (4.10) \end{aligned}$$

where

$$\delta = \begin{cases} 1 & E \text{ has rational point of order 3} \\ 0 & \text{otherwise} \end{cases}.$$

Hence, in order to compute the rank of E, it is sufficient to understand the images of ϕ and $\widehat{\phi}$. This leads us to the next proposition. See [14] and [12, Proposition 8.2.8].

Proposition 40 (Proposition 8.2.8, [12]). *Let E be the elliptic curve $y^2 = x^3 + D(ax+b)^2$ and E' the 3-isogenous curve with equation $y^2 = x^3 - 3D\left(ax + \left(27b - 4a^3D\right)/9\right)^2$ as above. Let α and α' be the corresponding 3-descent maps. Then*

$$|Im(\alpha)|\,|Im\,(\alpha')| = 3^{r+\delta}$$

where $r = rank(E) = rank\,(E')$, $\delta = 1$ if $D = 1, -3$ and $\delta = 0$ otherwise.

From now on we will specialize to the cases where $D = 1$, that is to elliptic curves of the form $E_{ab} : y^2 = x^3 + (ax+b)^2$ and the isogenous curve is of the form $E'_{ab'} : y^2 = x^3 - 3(ax+b')^2$ with $b' = \frac{27b-4a^3}{9}$. The reason for this is that elliptic curves of this form, $E/\mathbb{Q}$, have rational 3-torsion subgroup. It is natural to study 3-Selmer groups associated to elliptic curves with 3-torsion. For $D = 1$, Cohen and Pazuki [14] prove the following theorem describing the group $\mathrm{Im}\,(\alpha)$.

Theorem 41. *[14, Theorem 3.1] Let $[u] \in \mathbb{Q}^*/(\mathbb{Q}^*)^3$. Let u be the unique positive cube-free integer representative of $[u]$. Then write $u = u_1u_2^2$ where u_1 and u_2 are square-free, coprime integers in $\mathbb{Z}$. Then $[u] \in Im\,(\alpha)$ if and only if $u_1u_2 \mid 2b$ and the homogeneous cubic equation $F_u(x,y,z) = 0$ has an integer solution, where*

$$F_u(x,y,z) = u_1x^3 + u_2y^3 + \frac{2b}{u_1u_2}z^3 - 2axyz. \tag{4.11}$$

Remark 6. 1. The divisibility of $2b$ by u_1u_2 gives an upper bound on $|\mathrm{Im}(\alpha)|$.

2. When we speak of a solution to a homogeneous equation, we mean a non-trivial solution and thus when we speak of the solution set of such a homogeneous equation being non-empty we mean that there are non-trivial solutions.

For an integral domain R and $F \in R[x,y,z]$, let

$$C_F(R) = \{(x,y,z) \in R^3 \setminus \{(0,0,0)\} \mid F(x,y,z) = 0\}.$$

In light of Theorem 41, we would like to determine $C_{F_u}(\mathbb{Z})$ for each $u = u_1 u_2^2$ with $u_1 u_2 | 2b$. In general, however, this is not possible due to obstructions in the 3-part of the Tate-Shafarevich group. The reader should refer [14], [12] and [62] for any details concerning the Tate-Shafarevich group. Thus we are motivated to define the Selmer group $\mathrm{Sel}^{(\phi)}(E_{ab})$ as

$$\mathrm{Sel}^{(\phi)}(E_{ab}) = \{[u] \in \mathbb{Q}^*/(\mathbb{Q}^*)^3 \mid C_{F_u}(\mathbb{Q}_\nu) \neq \emptyset; \text{ for all places } \nu\},$$

where $F_u(X,Y,Z)$ is defined for E_{ab} in equation (4.11).

The reader should refer to Appendix A for a discussion on how this definition is related to the usual Cohomology definition of the Selmer group.

Cohen and Pazuki [14] also also give criteria in the isogenous case. As usual, $\mathcal{O}_K$ denotes the ring of integers of $K = \mathbb{Q}(\sqrt{-3})$. The following theorem describes the group $\mathrm{Im}\,(\alpha')$. Cohen and Pazuki state the following theorem in a different form than the one given here. To see that these two statements are equivalent, we refer the reader to Appendix B.

Theorem 42 (Theorem 4.1, [14]). *Let G_3' be the subgroup of $\mathbb{Q}(\omega)^*/(\mathbb{Q}(\omega)^*)^3$ of classes whose norms are cubes where ω is a primitive cubic root of unity. Let $[u'] \in G_3'$. Then $[u'] \in Im(\alpha')$ if and only if there exists a representative $u' \in \mathbb{Q}(\omega)^*$ such that $u' = \gamma\overline{\gamma}^2$ with $\gamma = c + d\omega \in \mathbb{Z}[\omega]$, $N(\gamma) = \gamma\overline{\gamma}$ is only divisible by split primes, $N(\gamma) \mid (2b')$ and the*

homogeneous cubic equation $F_{u'}(x,y,z)=0$ *has an integer solution where*

$$F_{u'}(X,Y,Z) := 2aX^2Z-2aXYZ+2aY^2Z+\frac{2b'}{N(\gamma)}Z^3-dX^3-dY^3-3cXY^2+3cX^2Y+3dXY^2. \tag{4.12}$$

Proof. It is easy to see that given $(x,y) \in E'(\mathbb{Q})$, we can find an integer solution to $F_{u'}(X,Y,Z)$. For further details, we refer the reader to Appendix B Sections B.1 through B.2 where we show the construction of the cubic equation.

Now assume that we have a non-trivial integer solution (X,Y,Z) to the cubic. Let

$$r = N(\gamma)\left(X^2-XY+Y^2\right)$$

and

$$\begin{aligned} s &= N(\gamma)\left(c+d\omega^2\right)(X+Y\omega)^3+\sqrt{-3}\left(arZ+bZ^3\right) \\ &= N(\gamma)\left(\left(c+d\omega^2\right)(X+Y\omega)^3+\sqrt{-3}Z\left(a\left(X^2-XY+Y^2\right)+\frac{b}{N(\gamma)}Z^2\right)\right). \end{aligned}$$

Let $x=\frac{r}{Z^2}$ and $y=\frac{s}{Z^3}$. We need to show that $(x,y)\in E'(\mathbb{Q})$. To see this, observe that

$$\begin{aligned} \alpha((x,y)) &= y-\sqrt{-3}(ax+b) \\ &= \frac{N(\gamma)\left(\left(c+d\omega^2\right)(X+Y\omega)^3+\sqrt{-3}Z\left(a\left(X^2-XY+Y^2\right)+\frac{b}{N(\gamma)}Z^2\right)\right)}{Z^3} \\ &\quad +\sqrt{-3}\left(a\frac{N(\gamma)\left(X^2-XY+Y^2\right)}{Z^2}+b\right). \end{aligned}$$

Expanding and doing some algebra we find that

$$\begin{aligned}\alpha\left((x,y)\right) &= \frac{1}{Z^3}\left(\left(c+d\omega\right)\left(c+d\omega^2\right)\left(X+Y\omega\right)^3\right)\\ &= u\left(\frac{X+Y\omega}{Z}\right)^3.\end{aligned}$$

It remains to show that $x, y \in \mathbb{Q}$.

Clearly since $N\left(\gamma\right) \in \mathbb{Z}$ and $X^2 - XY + Y^2 \in \mathbb{Z}$, it follows that $x \in \mathbb{Q}$. There is more work involved to show that $y \in \mathbb{Q}$. Notice that

$$(c+d\omega^2)(X+Y\omega)^3$$

$$= cX^3 + 3cX^2Y\omega + 3cXY^2\omega^2 + cY^3 + dX^3\omega^2 + 3dX^2Y + 3dXY^2\omega + dY^3\omega^2.$$

Making the appropriate substitutions for ω and ω^2 into the above equation we have

$$(c+d\omega^2)(X+Y\omega)^3$$

$$\begin{aligned}= &\frac{1}{2}\left(cX^3 - 3cX^2Y - 3cXY^2 + cY^3 - dX^3 + 3dX^2Y - 3dXY^2 - dY^3\right)\\ &+\frac{\sqrt{-3}}{2}\left(3cX^2Y - 3cXY^2 - dX^3 + 3dXY^2 - dY^3\right).\end{aligned}$$

Also, since

$$aZ\left(X^2 - XY + Y^2\right) + \frac{b}{N\left(\gamma\right)}Z^3 = \frac{1}{2}\left(dX^3 + dY^3 + 3cXY^2 - 3cX^2Y - 3dXY^2\right),$$

we can rewrite s as the following:

$$\begin{aligned} s &= N(\gamma)\frac{1}{2}\left(cX^3 - 3cX^2Y - 3cXY^2 + cY^3 - dX^3 + 3dX^2Y - 3dXY^2 - dY^3\right) \\ &\quad + N(\gamma)\frac{\sqrt{-3}}{2}\left(3cX^2Y - 3cXY^2 - dX^3 + 3dXY^2 - dY^3\right) \\ &\quad + N(\gamma)\frac{\sqrt{-3}}{2}\left(dX^3 + dY^3 + 3cXY^2 - 3cX^2Y - 3dXY^2\right) \\ &= \frac{N(\gamma)}{2}\left(cX^3 - 3cX^2Y - 3cXY^2 + cY^3 - dX^3 + 3dX^2Y - 3dXY^2 - dY^3\right) \end{aligned}$$

Thus $s \in \mathbb{Q}$ and hence $y \in \mathbb{Q}$. □

From Theorem 42 we are motivated to define the Selmer group $\mathrm{Sel}^{(\widehat{\phi})}(E'_{ab'})$ as

$$\mathrm{Sel}^{(\widehat{\phi})}(E'_{ab'}) = \{[u'] \in \mathbb{Q}(\sqrt{-3})^*/(\mathbb{Q}(\sqrt{-3})^*)^3 \mid C_{F_{u'}}(\mathbb{R}) \neq \emptyset; C_{F_{u'}}(\mathbb{Q}_p) \neq \emptyset \text{ for all primes } p\},$$

where $F_{u'}(X, Y, Z)$ is defined for $E'_{ab'}$ in equation (4.12).

To see a more in depth definition of this definition, we refer the reader to Appendix B.

Chapter 5

Selmer Groups

The aim of this chapter is to give an explicit way to estimate the rank of an elliptic curve over $\mathbb{Q}$ using 3-descent. As in Chapter 4, we will assume the elliptic curve, E, has a rational 3-torsion subgroup and is of the form

$$E : y^2 = x^3 + (ax + b)^2,$$

with $a, b \in \mathbb{Z}$. In addition, we will also explore the auxiliary curve, E', given by

$$E' : y^2 = x^3 - 3\left(ax + b'\right)^2$$

with $b' = \dfrac{27b - 4a^3}{9}$.

The results stated in Sections 5.2, 5.3 and 5.4 originated from a problem posed during the Summer 2010 Research Experience for Undergraduates in Computational Number Theory and Combinatorics. It is joint work with Kevin James and Hui Xue along with the REU students Tony Feng, Carolyn Kim and Eric Ramos.

5.1 Local Solubility

The following propositions give the local solubility conditions for the homogeneous cubic polynomials associated to both $E_{ab} : y^2 = x^3 + (ax+b)^2$ and $E'_{ab'} : y^2 = x^3 - 3(ax+b')^2$ where $b' = \dfrac{27b - 4a^3}{9}$. These propositions were stated in Cohen and Pazuki's paper [14]. For completeness, proofs of these results can be found in Appendices C and D.

Let $v_p(n)$, $n \in \mathbb{N}$, be the highest exponent of p that divides n, i.e. $v_p(n) = -\log_p |n|_p$. We set $v_p(0) = \infty$. So by Lemma 36, we may assume that either $v_p(a) = 0$ or $v_p(b) \leq 2$ for E.

5.1.1 The Elliptic Curve E_{ab}

The following two propositions give the local solubility criteria for the polynomial

$$F_u(X, Y, Z) = u_1X^3 + u_2Y^3 + u_3Z^3 - 2aXYZ$$

associated with E_{ab}.

Proposition 43 (Lemmas $5.3 - 5.5$, [14]). *Assume $p \neq 3$. Let*

$$F_u(X, Y, Z) = u_1X^3 + u_2Y^3 + u_3Z^3 - 2aXYZ$$

with p-integral coefficients where u_1 and u_2 are square-free and coprime and $u_3 = \dfrac{2b}{u_1u_2}$.

1. *If $p \neq 2$, $v_p(b) = 0$ and $v_p(27b - 4a^3) = 0$, then $F_u(X, Y, Z) = 0$ has a solution in $\mathbb{Q}_p$.*
2. *If $p \neq 2$, $v_p(b) = 0$ and $v_p(27b - 4a^3) > 0$, then $F_u(X, Y, Z) = 0$ has a solution in $\mathbb{Q}_p$ if and only if u_i/u_j is a cube in $\mathbb{F}_p^*$ for some $i \neq j$.*
3. *If $p \neq 2$ and $v_p(b) > 0$, then $F_u(X, Y, Z) = 0$ has a solution in $\mathbb{Q}_p$ if and only if one of the following is fulfilled:*

(a) $v_p(a) = 0$,

(b) $v_p(a) > 0$ *and exactly one of* $\{u_1, u_2, u_3\}$ *is divisible by* p *and the ratio of the other two is a cube in* $\mathbb{F}_p^*$,

(c) $v_p(a) > 0$ *and exactly two of* $\{u_1, u_2, u_3\}$ *are divisible by* p *and their ratio is a cube in* $\mathbb{F}_p^*$.

4. *If* $p = 2$, *then* $F_u(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}_2$ *if and only if one of the following is fulfilled:*

(a) *exactly one of* $\{u_1, u_2, u_3\}$ *is divisible by* 2 *and the ratio of the other two is a cube in* $\mathbb{F}_2^*$,

(b) *exactly two of* $\{u_1, u_2, u_3\}$ *is divisible by* 2 *each exactly once and their ratio is a cube in* $\mathbb{F}_2^*$.

The following proposition gives the solubility conditions for the prime $p = 3$.

Proposition 44 (Lemmas 5.6, 5.9, 5.10, [14]). *Let*

$$F_u(X, Y, Z) = u_1X^3 + u_2Y^3 + u_3Z^3 - 2aXYZ$$

with 3*-integral coefficients where* u_1 *and* u_2 *are square-free and coprime and* $u_3 = \dfrac{2b}{u_1u_2}$.

1. *If* $v_3(a) = 0$, *then* $F_u(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}_3$.

2. *If* $v_3(a) \geq 2$ *and* $v_3(b) = 0$ *then* $F_u(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}_3$ *if and only if* u_i/u_j *is a cube modulo* 9 *for some* $i \neq j$.

3. *If* $v_3(a) \geq 2$ *and exactly one of* $\{u_1, u_2, u_3\}$ *is divisible by* 3, *say* u_i, *then* $F_u(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}_3$ *if and only if either the ratio of the other two is a cube modulo* 9 *or* $v_3(u_i) = 1$.

4. *If* $v_3(a) \geq 2$ *and exactly two of* $\{u_1, u_2, u_3\}$ *are divisible by* 3*, then* $F_u(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}_3$ *if and only if their ratio is a cube modulo* 9*.*

5. *If* $v_3(a) = 1$ *and exactly one of* $\{u_1, u_2, u_3\}$ *is divisible by* 3*, then* $F_u(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}_3$ *if and only if either the ratio of the other two is a cube modulo* 9 *or there exists* $s_1, s_2 \in \{\pm 1\}$ *such that* $2a \equiv s_1u_1 + s_2u_2 + s_1s_2u_3 \pmod 9$*.*

6. *If* $v_3(a) = 1$ *and two of* $\{u_1, u_2, u_3\}$ *are divisible by* 3*, then* $F_u(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}_3$*.*

7. *If* $v_3(a) = 1$*,* $v_3(b) = 0$ *and* u_i/u_j *is a cube modulo* 9 *for some* $i \neq j$*, then* $F_u(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}_3$*.*

8. *If* $v_3(a) = 1$*,* $v_3(b) = 0$ *and* u_i/u_j *is not a cube modulo* 9 *for all* $i \neq j$ *then* $F_u(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}_3$ *if and only if there exists* $s_1, s_2 \in \{\pm 1\}$ *such that* $2a \equiv s_1u_1 + s_2u_2 + s_1s_2u_3 \pmod{27}$*.*

5.1.2 The Auxiliary Curve $E'_{ab'}$

The following propositions give the local solubility criteria for the polynomial

$$\begin{aligned} F_{u'}(X, Y, Z) \;:=\; & 2aX^2Z - 2aXYZ + 2aY^2Z + \frac{2b'}{N(\gamma)}Z^3 \\ & -dX^3 - dY^3 - 3cXY^2 + 3cX^2Y + 3dXY^2 \end{aligned}$$

associated to the auxiliary elliptic curve $E'_{ab'}$. Note that since we are working over $\mathbb{Q}\left(\sqrt{-3}\right)$, $p = 3$ is the only ramified prime. If $p \equiv 2 \pmod 3$, then p is an inert prime, and if $p \equiv 1 \pmod 3$, then p is a split prime.

Proposition 45. *[14, Corollary 6.3] Let* p *be any split prime. Then there exists* $d_p \in \mathbb{Q}_p$ *such that* $d_p^2 = -3$*. The equation* $F_{u'}(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}_p$ *if and only if the*

cubic

$$u_1X^3 + u_2Y^3 + u_3Z^3 - \mathbf{C}XYZ = 0$$

does, where $u_1 = \left(c - \frac{d}{2}\right) - \frac{d}{2}d_p$, $u_2 = \left(c - \frac{d}{2}\right) + \frac{d}{2}d_p$, $u_3 = \frac{2b'}{\gamma\overline{\gamma}}d_p$ *and* $\mathbf{C} = 2ad_p$.

Making some minor adjustments to Proposition 43, we have all the conditions necessary to find a solution for $F_{u'}(X, Y, Z) = 0$ in $\mathbb{Q}_p$ where p is a split prime. Before stating the Corollary, we make the following observation.

Lemma 46. *Let* $\Delta' = 27b' + 12a^3$. *If* $p \equiv 1 \pmod 3$, $p \mid \Delta'$ *and* $p \nmid b'$, *then* $2b'\sqrt{-3}$ *is a cube modulo* p.

So we can conclude that if u_i/u_j is a cube for some $i \neq j$, then this is true for all $i \neq j$.

Corollary 47. *Let* p *be any split prime. We can write* $p = \pi\overline{\pi}$ *where* $\pi \equiv 2 \pmod 3$ *and is in the upper-half plane. Let*

$$F_{u'}(X, Y, Z) \;=\; u_1X^3 + u_2Y^3 + u_3Z^3 - \boldsymbol{c}XYZ = 0$$

where $u_1 = \left(c - \frac{d}{2}\right) - \frac{d}{2}\sqrt{-3}$, $u_2 = \left(c - \frac{d}{2}\right) + \frac{d}{2}\sqrt{-3}$, $u_3 = \frac{2b'}{\gamma\overline{\gamma}}\sqrt{-3}$ *and* $\boldsymbol{c} = 2a\sqrt{-3}$ *with* $(c, d) = 1$.

1. *If* $v_p(b') = 0$ *and* $v_p(27b' + 12a^3) = 0$, *then* $F_{u'}(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}_p$.

2. *If* $v_p(b') = 0$ *and* $v_p(27b' + 12a^3) > 0$, *then* $F_{u'}(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}_p$ *if and only if* u_1/u_2 *is a cube in* $\mathbb{F}_p^*$.

3. *If* $v_\pi(b') > 0$, *then* $F_{u'}(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}(\omega)_\pi$ *if and only if one of the following is true*

   (a) $v_\pi(a) = 0$,

(b) $v_\pi(a) > 0$, π *divides exactly one of* $\{u_1, u_2, u_3\}$ *and the ratio of the other two is a cube modulo* π,

(c) $v_\pi(a) > 0$, π *divides two of* $\{u_1, u_2, u_3\}$ *and their ratio is a cube modulo* π.

Proposition 48 (Lemmas 6.5, 6.6, 6.7, [14]). *Assume* $p \neq 2$, $p \equiv 2 \bmod 3$ *and let* $F_{u'}(X, Y, Z)$ *be as in equation* (4.12).

1. *If* $v_p(\gamma\overline{\gamma}) = 0$, $v_p(2b') = 0$ *and* $v_p(27b' + 12a^3) = 0$, *then* $F_{u'}(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}_p$.

2. *If* $v_p(2b') = 0$ *and* $v_p(27b' + 12a^3) > 0$, *then* $F_{u'}(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}_p$ *if and only if* $\dfrac{\gamma}{\overline{\gamma}}$ *is a cube in* $\mathbb{F}^*_{p^2}$.

3. *If* $v_p(2b') > 0$ *and* $v_p(\gamma\overline{\gamma}) = 0$, *then* $F_{u'}(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}_p$ *if and only if one of the following is satisfied:*

   (a) $v_p(2a) = 0$.

   (b) $v_p(2a) > 0$ *and the class of* $\dfrac{\gamma}{\overline{\gamma}}$ *modulo* p *is a cube in* $\mathbb{F}^*_{p^2}$.

   Again, recall that by Lemma 36, we have that either $v_2(b') \leq 2$ or $v_2(a) = 0$.

Proposition 49 (Lemmas 6.5, 6.6, 6.7, [14]). *Let* $p = 2$ *and* $F_{u'}(X, Y, Z)$ *be as in equation* (4.12).

1. *If* $v_2(2b') \leq 2$, *then* $F_{u'}(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}_2$ *if and only if the class of* $\dfrac{\gamma}{\overline{\gamma}}$ *modulo* 2 *is a cube in* $\mathbb{Z}^*[\omega]/2\mathbb{Z}^*[\omega] \cong \mathbb{F}_4^*$. *Note that the only cube in* $\mathbb{F}_4^*$ *is* 1.

2. *If* $v_2(2b') \geq 3$, *then*

   (a) *if* $d \equiv 0 \pmod 4$ *and* $c \equiv \pm 1 \pmod 4$, *then* $F_{u'}(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}_2$.

(b) *if* $d \equiv 2 \pmod 4$ *and* $c \equiv \pm 1 \pmod 4$ *then* $F_{u'}(X,Y,Z) = 0$ *has a solution in* $\mathbb{Q}_2$.

(c) *if* $d \equiv 1 \pmod 2$, *then* $F_{u'}(X,Y,Z) = 0$ *has a solution in* $\mathbb{Q}_2$ *if and only if either* $v_2(2b') \geq 4$ *or* $v_2(a) > 0$.

Proposition 50. *Let* $p = 3$ *and* $F_{u'}(X,Y,Z)$ *be as in equation* (4.12).

1. *If* $v_3(2a) = 0$, *then* $F_{u'}(X,Y,Z) = 0$ *has a solution in* $\mathbb{Q}_3$ *if and only if one of the following conditions is satisfied:*

   (a) $v_3(d) > 0$,

   (b) $v_3(d) = v_3\left(2a + \dfrac{2b'}{N(\gamma)}\right) = 0$.

2. *If* $v_3(2a) \geq 2$, *then* $F_{u'}(X,Y,Z) = 0$ *has a solution in* $\mathbb{Q}_3$ *if and only if one of the following conditions is satisfied:*

   (a) $v_3(d) \geq 2$,

   (b) $v_3(d) = v_3(b) = 1$,

   (c) $v_3(d) = 0$ *and* $\dfrac{2b'}{dN(\gamma)}$ *is a cube modulo* 9,

   (d) $\dfrac{2b'}{N(\gamma)} \equiv \pm(6c - 3d)$ *modulo* 27.

3. *If* $v_3(2a) = 1$, *then* $F_{u'}(X,Y,Z) = 0$ *has a solution in* $\mathbb{Q}_3$ *if and only if one of the following is satisfied:*

   (a) $v_3(d) \geq 2$,

   (b) $v_3(d) = v_3\left(2a + \dfrac{2b'}{N(\gamma)}\right) = 1$,

   (c) $v_3(d) = 0$ *and* $\left(\dfrac{2b'}{N(\gamma)} + 2a\right)/d$ *is a cube modulo* 9,

(d) $v_3\left(\dfrac{2b'}{N(\gamma)}\right) = 1$, $v_3(d) = 0$ *and there exists* $s \in \{\pm 1\}$ *such that* $(d - 2c) \equiv s\left(\dfrac{2b'}{3N(\gamma)} + 2a\right) \pmod{27}$ *and* $s(2c - d) \equiv 2a/3 \pmod{3}$,

As one can see, the local solubility results associated with the primes 2 and 3 are complex. Therefore we exclude them when looking for solutions and define a larger group than the Selmer group. We will discuss this in more detail in Section 5.2.2

5.2 Graph Theory

We can use the propositions from the previous section to give a characterization of the Selmer group in terms of graphs. The goal is to generalize the results of Feng and Xiong [32] for 3-Selmer groups. In particular, we consider the results of Faulkner and James [31] for congruent number curves and give an equivalent approach for elliptic curves with 3 torsion. For each elliptic curve, we construct a directed graph whose edges are labeled by cubic roots of unity. In the case of $E_{ab} : y^2 = x^3 + (ax + b)^2$, if we define a "three-balanced" partition in terms of the following labeling, then the size of $\mathrm{Sel}^{(\phi)}(E_{ab})$ corresponds to the number of "three-balanced" partitions of the graph. Conversely, for $E'_{ab'} : y^2 = x^3 - 3(ax + b')^2$, we define the notion of a "good" labeling. Then the size of $\mathrm{Sel}^{(\hat{\phi})}(E'_{ab'})$ is bounded by the number of "good" labellings. These notions of "three-balanced" partitions and "good" labellings provide a visual interpretation of the Selmer group. We will make these notions more precise below.

5.2.1 The Elliptic Curve E_{ab}

We will begin by studying elliptic curves with rational 3-torsion of the form

$$y^2 = x^3 + (ax + b)^2$$

whose discriminant is

$$\Delta \;=\; 16b^3\Delta'$$

where $\Delta' = 4a^3 - 27b$. Recall by Lemma 36, we know that either $v_p(b) \leq 2$ or $v_p(a) = 0$.

Let ω be a primitive cubic root of unity. If $p \equiv 1 \pmod 3$ is a rational prime (i.e. p splits in $\mathbb{Z}[\omega]$), then we will write $p = \pi\overline{\pi}$ where $\pi \equiv 2 \pmod 3$ and π is in the upper-half plane. Recall that if $p \equiv 2 \pmod 3$, then every number is a cube modulo p.

Using these conventions, let p and q be primes. Then we define the following:

$$\chi_p(q) = \begin{cases} \left(\frac{q}{\pi}\right)_3 & \text{if } p \equiv 1 \pmod 3 \\ 1 & \text{if } p \equiv 2 \pmod 3 . \end{cases}$$

Recall that we have the following properties of χ_p:

1. $\chi_p(q) = 1$ if and only if q is a cube in $\mathbb{F}_p^*$
2. $\chi_p(ab) = \chi_p(a)\chi_p(b)$ for all $a, b \in \mathbb{Z}$.

So the above is true for all primes p not equal to 3. For $p = 3$, notice that $(\mathbb{Z}/9\mathbb{Z})^*$ is cyclic and generated by 2. Define χ_3 on $(\mathbb{Z}/9\mathbb{Z})^*$ by

$$\chi_3(q) = \omega^t$$

where $q = 2^t \in (\mathbb{Z}/9\mathbb{Z})^*$. Note that even though we are working modulo 9, we will still use χ_3 to avoid confusion later.

One important concept to notice is that for those primes q which divide Δ', but do

not divide $2b$, we can conclude that

$$2b \equiv \left(2\left(3^{-1}\right)a\right)^3 \pmod{q}$$

or equivalently that $\chi_q(2b) = 1$. Using this observation we can conclude that

$$\begin{aligned}\chi_q(u_2/u_3) &= \chi_q(u_3/u_1) \\ &= \chi_q(u_1/u_2)\end{aligned}$$

and

$$\begin{aligned}\chi_q(u_1/u_3) &= \chi_q(u_3/u_2) \\ &= \chi_q(u_1/u_2)\end{aligned}$$

where u_1, u_2 and u_3 are defined as in Proposition 43. Also $\chi_q(u_i/u_j) = 1$ if and only if $\chi_q(u_j/u_i) = 1$ for $i \neq j$. Therefore in Proposition 43.2, it is enough to show u_1/u_2 is a cube modulo a given prime.

For clarity, we will consider different families of elliptic curves.

5.2.1.1 The Family of Curves $\mathcal{E}_1$

Consider the family $\mathcal{E}_1$ of elliptic curves given by

$$E_{ab}/\mathbb{Q} : y^2 = x^3 + (ax + b)^2$$

where $3 \nmid b$ and $\Delta = 16b^3\Delta'$, with $\Delta' = 27b - 4a^3$.

Let G be a graph with g vertices where

$$g = 1 + \sum_{p|b} v_p(b).$$

Let G' be the graph containing G with g' vertices where

$$g' = g + \sum_{\substack{p|\Delta' \\ p\nmid(2b)}} 1.$$

So

$$V(G) = \{p : p \mid b\} \cup \left\{p : p^2 \mid b\right\} \cup \{2\}$$

and

$$V(G') = V(G) \cup \{p : p \mid \Delta', p \nmid 2b\}.$$

Example 3. Consider the elliptic curve

$$E : y^2 = x^3 + (7x + (5)(7)(19))^2$$

where $\Delta' = 7(23)(103)$. Then the vertices of G' are $\{2, 5, 7, 19, 23, 103\}$. The subgraph G is made up of the vertices $\{2, 5, 7, 19\}$. The graph is represented by Figure 5.1.

Next, draw directed edges from all primes $p \in V(G') \setminus V(G)$ to all primes $q \in V(G)$. Additionally draw directed edges from all primes $p \in V(G)$ to $q \in V(G)$ where $p \mid \Delta'$ and $p \neq q$. Label each directed edge from p to q as

$$\ell(p, q) := \chi_p(q).$$

Example 4. Adding edges to Figure 5.1, we have the directed graph in Figure 5.2.

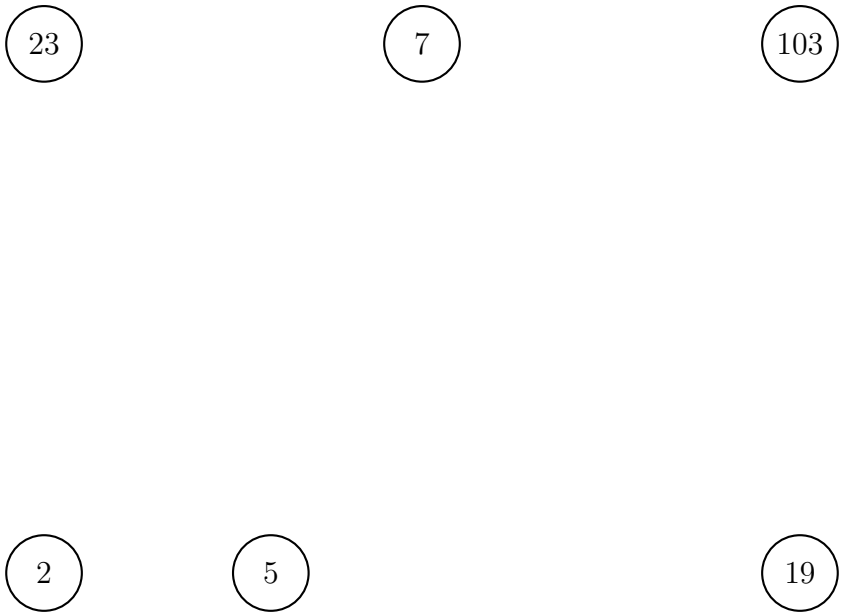


Figure 5.1: Vertices of G'

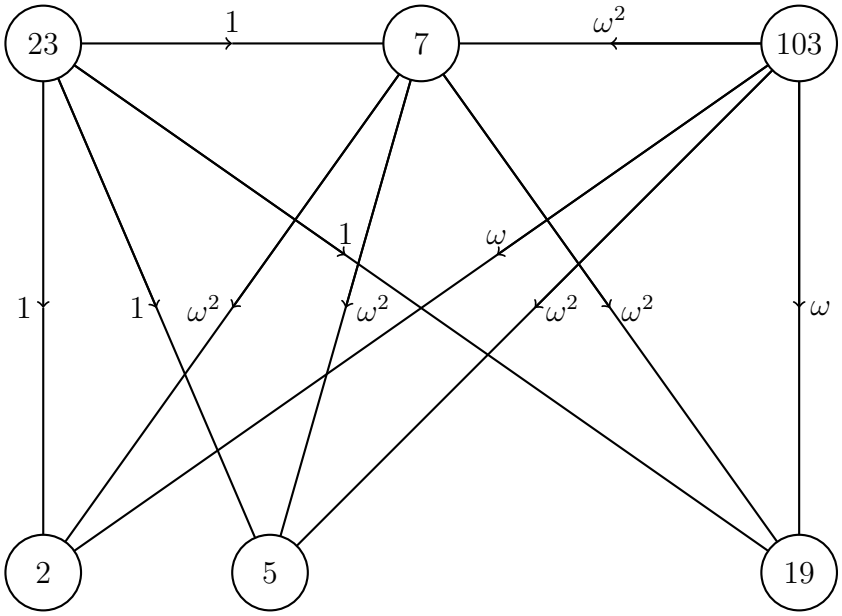


Figure 5.2: Directed Graph G'

In [31], Faulkner and James define even and quasi-even partitions of graphs associated to congruent number curves in order to calculate the size of 2-Selmer groups. In a similar way, we will define three-balanced and three-quasi-balanced partitions in order to calculated the size of 3-Selmer groups.

A *partition* of $V(G)$ into three parts is an ordered triple of subsets (S_1, S_2, S_3) such that $S_1 \cup S_2 \cup S_3 = V(G)$ and $S_1 \cap S_2 = S_1 \cap S_3 = S_2 \cap S_3 = \emptyset$. We will allow for the possibility that S_1, S_2 or S_3 is empty.

Definition 19. A partition, (S_1, S_2, S_3), of $V(G)$ is called **three-balanced** if and only if the following five conditions are satisfied:

1. if $p \in S_1 \cup S_2$ and $p^2 \,||\, 2b$, then the additional copy of p is in S_3 for all $p \in V(G)$

2. if $4 \mid b$, then all copies of 2 are in S_3

3. for every $p \in S_\nu$ such that the prime, p, is only in S_ν and $p \mid \Delta'$, we have

$$\left(\prod_{p_j \in S_{\nu+1}} \ell(p, p_j) \right) \left(\prod_{p_k \in S_{\nu+2}} \ell(p, p_k)^2 \right) \;=\; 1$$

   where we cycle the indices of the partitions (i.e. $S_1 = S_4$, etc.)

4. for every $p \in S_\eta$, $\eta = 1, 2$ such that p is also in S_3 and $p \mid \Delta'$, we have

$$\left(\prod_{\substack{p_j \in S_\eta \\ p_j \neq p}} \ell(p, p_j) \right) \left(\prod_{\substack{p_k \in S_3 \\ p_k \neq p}} \ell(p, p_k)^2 \right) \;=\; 1,$$

5. for every $p \in V(G') \setminus V(G)$

$$\left(\prod_{p_j \in S_1} \ell(p, p_j) \right) \left(\prod_{p_k \in S_2} \ell(p, p_k)^2 \right) \;=\; 1.$$

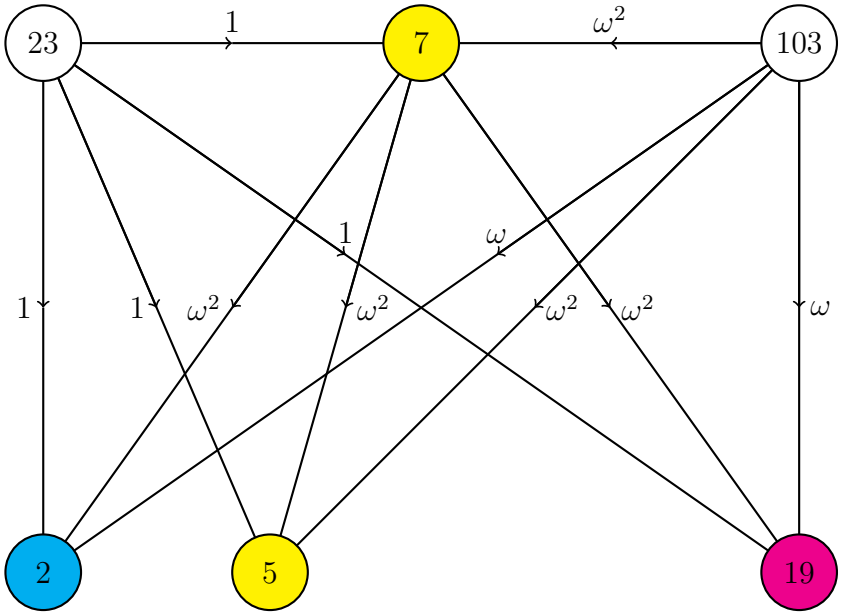


Figure 5.3: Three-Balanced Partition

Example 5. Continuing with the elliptic curve

$$E : y^2 = x^3 + (7x + (5)(7)(19))^2$$

where $\Delta' = 7(23)(103)$. Let $S_1 = \{5, 7\}$, $S_2 = \{2\}$ and $S_3 = \{19\}$.

To see this is a three-balanced partition, there are 3 primes we need to check 7, 23 and 103 since these are the primes which divide Δ'. Notice that $7 \in S_1$ and

$$\begin{aligned} \left(\prod_{p_j \in S_2} \ell(7, p_j) \right) \left(\prod_{p_k \in S_3} \ell(7, p_k)^2 \right) &= \omega^2 \left(\omega^2\right)^2 \\ &= 1. \end{aligned}$$

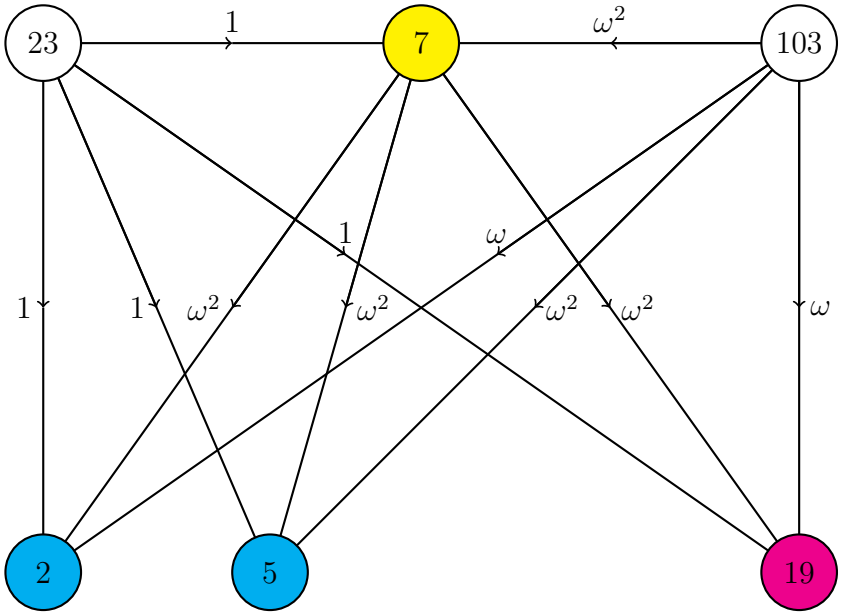


Figure 5.4: Not a Three-Balanced Partition

In addition, since $23 \equiv 2 \pmod 3$,

$$\left(\prod_{p_j \in S_1} \ell(23, p_j)\right)\left(\prod_{p_k \in S_2} \ell(23, p_k)^2\right) \;=\; 1.$$

Finally,

$$\left(\prod_{p_j \in S_1} \ell(103, p_j)\right)\left(\prod_{p_k \in S_2} \ell(103, p_k)^2\right) \;=\; 1.$$

Then (S_1, S_2, S_3) is three-balanced.

Now consider $S_1 = \{7\}$, $S_2 = \{2, 5\}$ and $S_3 = \{19\}$.

To see this is not a three-balanced partition, notice that

$$\begin{aligned}\left(\prod_{p_j\in S_2}\ell(7,p_j)\right)\left(\prod_{p_k\in S_3}\ell(7,p_k)^2\right) &= \omega^2\cdot\omega^2(\omega^2)^2\\ &\neq 1.\end{aligned}$$

We will also need another definition.

Definition 20. A partition, (S_1,S_2,S_3), of $V(G)$ is called **three-quasi-balanced** at 3 if and only if the following conditions are satisfied:

1. (S_1,S_2,S_3) satisfies condition (1) for a three-balanced partition for all primes and satisfies the remainder of the conditions for all primes except 3

2. Exclusively we have

$$\left(\prod_{p_j\in S_1}\ell(3,p_j)\right)\left(\prod_{p_k\in S_2}\ell(3,p_k)^2\right) = 1$$

or there exists $s_1,s_2\in\{\pm 1\}$ such that

$$2a\equiv s_1\left(\prod_{p_i\in S_1}p_i\right)+s_2\left(\prod_{p_j\in S_2}p_j\right)+s_1s_2\left(\prod_{p_k\in S_3}p_k\right)\pmod{27}.$$

Using these definitions, we have the following lemma.

Lemma 51. *Suppose (S_1,S_2,S_3) is a partition of $V(G)$. Let*

$$u_1=\prod_{p_i\in S_1}p_i \quad\text{and}\quad u_2=\prod_{p_j\in S_2}p_j.$$

Then the homogeneous equation

$$u_1X^3 + u_2Y^3 + \frac{2b}{u_1u_2}Z^3 - 2aXYZ = 0 \tag{5.1}$$

has a solution in every local field $\mathbb{Q}_p$ if and only if $v_3(a) = 1$ and (S_1, S_2, S_3) is three-quasi-balanced at 3 or $v_3(a) \neq 1$ and (S_1, S_2, S_3) is three-balanced.

Proof. Let $u_3 = 2b/(u_1u_2)$. We will begin by assuming (S_1, S_2, S_3) is a three-balanced partition. By Proposition 43, there are three things we need to show. First, for every prime $p \in S_\nu$, if p is only in S_ν and $p \mid \Delta'$, then $\chi_p(u_{\nu+1}/u_{\nu+2}) = 1$ where we cycle the indices. Second for every $p \in S_\eta$ with $\eta = 1$ or $\eta = 2$, such that p is also in S_3 and $p \mid \Delta'$, we have $\chi_p(u_\eta/u_3) = 1$. In addition, we must also show that for every $p \in V(G') \setminus V(G)$, $\chi_p(u_1/u_2) = 1$. Notice that for every $p \in S_\nu$, which is only in S_ν and $p \mid \Delta'$, we have

$$\begin{aligned}
\chi_p(u_{\nu+1}/u_{\nu+2}) &= \chi_p(u_{\nu+1})\,\chi_p(u_{\nu+2})^2 \\
&= \left(\prod_{p_j \in S_{\nu+1}} \chi_p(p_j)\right)\left(\prod_{p_k \in S_{\nu+2}} \chi_p(p_k)^2\right) \\
&= \left(\prod_{p_j \in S_{\nu+1}} \ell(p, p_j)\right)\left(\prod_{p_k \in S_{\nu+2}} \ell(p, p_k)^2\right) \\
&= 1
\end{aligned}$$

since (S_1, S_2, S_3) is three-balanced. In the case $p \in S_\eta$ for $\eta = 1$ or $\eta = 2$, $p \in S_3$ and $p \mid \Delta'$,

we have

$$\begin{aligned}
\chi_p\left(u_\eta/u_3\right) &= \chi_p\left(u'_\eta\right)\chi_p\left(u'_3\right)^2 \\
&= \left(\prod_{\substack{p_j\in S_\eta\\ p_j\neq p}}\chi_p(p_j)\right)\left(\prod_{\substack{p_k\in S_3\\ p_k\neq p}}\chi_p(p_k)^2\right) \\
&= \left(\prod_{\substack{p_j\in S_\eta\\ p_j\neq p}}\ell(p,p_j)\right)\left(\prod_{\substack{p_k\in S_3\\ p_k\neq p}}\ell(p,p_k)^2\right) \\
&= 1
\end{aligned}$$

where $u_\nu = pu'_\nu$ and $u_3 = pu'_3$.

We also know that for every $p \in V(G') \setminus (V(G) \cup \{3\})$,

$$\begin{aligned}
\chi_p\left(u_1/u_2\right) &= \chi_p\left(u_1\right)\chi_p\left(u_2\right)^2 \\
&= \left(\prod_{p_j\in S_1}\chi_p(p_j)\right)\left(\prod_{p_k\in S_2}\chi_p(p_k)^2\right) \\
&= \left(\prod_{p_j\in S_1}\ell(p,p_j)\right)\left(\prod_{p_k\in S_2}\ell(p,p_k)^2\right) \\
&= 1.
\end{aligned}$$

Note that the only time we will have to worry about three-quasi-balanced at 3 is when $3 \mid\mid a$ and $\chi_3(u_1/u_2) \neq 1$. However with the last condition of three-quasi-balanced, by Proposition 44, we are guaranteed a solution in $\mathbb{Q}_3$.

Conversely, suppose that (S_1, S_2, S_3) is not three-balanced or if $3 \mid\mid a$, it is not three-quasi-balanced at 3 as well. There are five cases we need to consider.

Case 1: There exists $p \in S_1 \cup S_2$ with $p^2 \mid\mid 2b$ such that the other copy of p is also in $S_1 \cup S_2$.

In this case, we either would have that $\gcd(u_1, u_2) \neq 1$ or u_i not square-free for $i = 1$ or $i = 2$. These are both requirements for the equation (5.1).

Case 2: If we have $v_2(b) = 2$ and $2 \in S_1 \cup S_2$, then in this case we are guaranteed there is no solution by Proposition 43.

Case 3: There exists p in some S_ν with p not in any other S_η and $p \mid \Delta'$, such that

$$\left(\prod_{p_j \in S_{\nu+1}} \ell(p, p_j) \right) \left(\prod_{p_k \in S_{\nu+2}} \ell(p, p_k)^2 \right) \neq 1.$$

Then

$$\begin{aligned} \chi_p\left(u_{\nu+1}/u_{\nu+2}\right) &= \chi_p\left(u_{\nu+1}\right) \chi_p\left(u_{\nu+2}\right)^2 \\ &= \left(\prod_{p_j \in S_{\nu+1}} \chi_p(p_j) \right) \left(\prod_{p_k \in S_{\nu+2}} \chi_p(p_k)^2 \right) \\ &= \left(\prod_{p_j \in S_{\nu+1}} \ell(p, p_j) \right) \left(\prod_{p_k \in S_{\nu+2}} \ell(p, p_k)^2 \right) \\ &\neq 1, \end{aligned}$$

where we cycle the indices. Hence by Proposition 43, equation (5.1) does not have a solution in $\mathbb{Q}_p$.

Case 4: There exists p in some S_η with $\eta = 1$ or $\eta = 2$, $p^2 \mid 2b$, the other copy of p in S_3 and $p \mid \Delta'$ such that

$$\left(\prod_{\substack{p_j \in S_\eta \\ p_j \neq p}} \ell(p, p_j) \right) \left(\prod_{\substack{p_k \in S_3 \\ p_k \neq p}} \ell(p, p_k)^2 \right) \neq 1.$$

Then

$$\begin{aligned}
\chi_p\left(u_\eta/u_3\right) &= \chi_p\left(u'_\eta\right)\chi_p\left(u'_3\right)^2 \\
&= \left(\prod_{\substack{p_j\in S_\eta \\ p_j\neq p}} \chi_p(p_j)\right)\left(\prod_{\substack{p_k\in S_3 \\ p_k\neq p}} \chi_p(p_k)^2\right) \\
&= \left(\prod_{\substack{p_j\in S_\eta \\ p_j\neq p}} \ell(p,p_j)\right)\left(\prod_{\substack{p_k\in S_3 \\ p_k\neq p}} \ell(p,p_k)^2\right) \\
&\neq 1,
\end{aligned}$$

where $u_\eta = pu'_\eta$ and $u_3 = pu'_3$.

Hence by Proposition 43, equation (5.1) does not have a solution in $\mathbb{Q}_p$.

Case 5**:** There exists a $p \in V(G') \setminus V(G)$, such that

$$\left(\prod_{p_j\in S_1} \ell(p,p_j)\right)\left(\prod_{p_k\in S_2} \ell(p,p_k)^2\right) \neq 1.$$

Since

$$\begin{aligned}
\chi_p\left(u_1/u_2\right) &= \chi_p\left(u_1\right)\chi_p\left(u_2\right)^2 \\
&= \left(\prod_{p_j\in S_1} \chi_p(p_j)\right)\left(\prod_{p_k\in S_2} \chi_p(p_k)^2\right) \\
&= \left(\prod_{p_j\in S_1} \ell(p,p_j)\right)\left(\prod_{p_k\in S_2} \ell(p,p_k)^2\right) \\
&\neq 1,
\end{aligned}$$

it follows that equation (5.1) would not have a solution in $\mathbb{Q}_p$ unless $p = 3$. The only way it would have a solution is if $3 \mid\mid a$, the above was true for $p = 3$ and we have $2a \equiv$

$s_1u_1 + s_2u_2 + s_1s_2u_3 \pmod{27}$ for some $s_1, s_2 \in \{\pm 1\}$. However, if $3 \,||\, a$ we assumed the partition was not three-quasi-balanced at 3. So we have covered most of the cases already with the partition not being three-balanced. We only need to consider that case that there must not exist $s_1, s_2 \in \{\pm 1\}$ such that $2a \equiv s_1u_1 + s_2u_2 + s_1s_2u_3 \pmod{27}$. But in this case, by Proposition 44, we do not have a solution in $\mathbb{Q}_3$. □

So we obtain the following theorem giving the size of the Selmer group, $\mathrm{Sel}^{(\phi)}(E_{ab})$, for the family $\mathcal{E}_1$.

Theorem 52. *Let $E_{ab} : y^2 = x^3 + (ax + b)^2$ with $3 \nmid b$. Let G and G' be defined as above. Then if $3 \,||\, a$, we have*

$$\left|\mathrm{Sel}^{(\phi)}(E_{ab})\right| \;=\; \#\left\{\mathrm{three-quasi-balanced\ at\ 3\ partitions\ of}\ V(G)\right\}.$$

Otherwise, we have

$$\left|\mathrm{Sel}^{(\phi)}(E_{ab})\right| \;=\; \#\left\{\mathrm{three-balanced\ partitions\ of}\ V(G)\right\}.$$

Proof. Assume $E_{ab} : y^2 = x^3 + (ax + b)^2$ where $v_3(b) = 0$ and $v_3(a) \neq 1$. Let $[u] \in \mathrm{Sel}^{(\phi)}(E_{ab})$ where we can find a representative for u such that there exists integers u_1 and u_2 with $\gcd(u_1, u_2) = 1$ and $u = u_1u_2^2$. Then $u_1u_2 \mid 2b$ and $F_u(X, Y, Z) = 0$ as in Equation (4.11) has a solution over $\mathbb{Q}_\nu$ for all places ν. By Lemma 51 there exists a three-balanced partition (S_1, S_2, S_3) where $S_1 = \{p : p \mid u_1\}$, $S_2 = \{p : p \mid u_2\}$ and $S_3 = \left\{p : p \mid \dfrac{2b}{u_1u_2}\right\}$.

Now assume (S_1, S_2, S_3) is a three-balanced partition. Let $u_1 = \prod_{p \in S_1} p$ and $u_2 = \prod_{p \in S_2} p$. Then by Lemma 51 $u_1X^3 + u_2Y^3 + \dfrac{2b}{u_1u_2}Z^3 - 2aXYZ = 0$ has a solution over $\mathbb{Q}_\nu$ for all places ν. And hence $u = u_1u_2^2$ is a representative for the element $[u]$ in $\mathrm{Sel}^{(\phi)}(E_{ab})$.

In the case that $v_3(a) = 1$, Proposition 44 gives extra solubility conditions on Equation (5.1). In this case, an additional condition must be placed on the definition of a three-

balanced partition. This is the condition stated in the definition of a three-quasi-balanced partition. The proof follows the same as before.

□

Example 6. Let us once again consider the curve

$$E : y^2 = x^3 + (7x + (5)(7)(19))^2$$

where $\Delta' = 7(23)(103)$. Earlier we gave an example of a three-balanced partition. There are actually 9 possible three-balanced partitions of the graph. Table 5.1 lists all 9 of the possible three-balanced partitions. Note these will actually correspond to different elements in the Selmer group. In addition, since this is such an easy example, the subsets can just be permuted to obtain new elements. The two main reasons for this is due to the fact that 3 does not divide b and each prime divides b exactly once. If a prime had divided b twice, then we could not longer just permute the subsets.

5.2.1.2 The Family of Curves $\mathcal{E}_2$

Next, consider the family $\mathcal{E}_2$ of elliptic curves given by

$$E_{ab}/\mathbb{Q} : y^2 = x^3 + (ax + b)^2$$

where $3 \mid b$ and $\Delta = 16b^3\Delta'$, with $\Delta' = 27b - 4a^3$. Again, recall that we may assume for every prime p, either $v_p(a) = 0$ or $v_p(b) \leq 2$.

Let G be a graph with g vertices where

$$g = 1 + \sum_{p|b} v_p(b).$$

S_1	S_2	S_3
$\{2, 5, 7, 19\}$	$\emptyset$	$\emptyset$
$\emptyset$	$\{2, 5, 7, 19\}$	$\emptyset$
$\emptyset$	$\emptyset$	$\{2, 5, 7, 19\}$
$\{7, 5\}$	$\{2\}$	$\{19\}$
$\{7, 5\}$	$\{19\}$	$\{2\}$
$\{19\}$	$\{7, 5\}$	$\{2\}$
$\{19\}$	$\{2\}$	$\{7, 5\}$
$\{2\}$	$\{19\}$	$\{7, 5\}$
$\{2\}$	$\{7, 5\}$	$\{19\}$

Table 5.1: Three-Balanced Partitions

Let G' be the graph, containing G, with g' vertices where

$$g' = g + \sum_{\substack{p|\Delta' \\ p\nmid(2b)}} 1.$$

So

$$V(G) = \{p : p \mid b\} \cup \left\{p : p^2 \mid b\right\} \cup \{2\}$$

and

$$V(G') = V(G) \cup \{p : p \mid \Delta', p \nmid (2b)\}.$$

Draw directed edges from all primes $p \in V(G') \setminus V(G)$ to all primes $q \in V(G)$. Additionally draw directed edges from all primes $p \in V(G)$ to $q \in V(G)$ where $p \mid \Delta'$ and $p \neq q$. Label each directed edge from p to q as

$$\ell(p, q) := \chi_p(q).$$

Again, a *partition* of $V(G)$ into three parts is an ordered triple of subsets (S_1, S_2, S_3) such that $S_1 \cup S_2 \cup S_3 = V(G)$ and $S_1 \cap S_2 = S_1 \cap S_3 = S_2 \cap S_3 = \emptyset$. We will allow for the possibility that S_1, S_2 or S_3 is empty.

Definition 21. A partition, (S_1, S_2, S_3), of $V(G)$ is called **three-balanced** if and only if the following conditions are satisfied:

1. if $p \in S_1 \cup S_2$ and $p^2 \mid\mid 2b$, then the additional copy of p is in S_3 for all $p \in V(G)$
2. if $4 \mid b$, then all copies of 2 are in S_3
3. for every $p \in S_\nu$, with $p \mid \Delta'$ and $p \neq 3$, such that the prime, p, is only in S_ν, we have

$$\left(\prod_{p_j \in S_{\nu+1}} \ell(p, p_j)\right)\left(\prod_{p_k \in S_{\nu+2}} \ell(p, p_k)^2\right) \;=\; 1$$

where we cycle the indices of the partitions (i.e. $S_1 = S_4$, etc.)

4. for every $p \in S_\eta$, with $p \mid \Delta'$, $\eta = 1$ or 2 and $p \neq 3$, such that $p \in S_3$, we have

$$\left(\prod_{\substack{p_j \in S_\eta \\ p_j \neq p}} \ell(p, p_j)\right)\left(\prod_{\substack{p_k \in S_3 \\ p_k \neq p}} \ell(p, p_k)^2\right) \;=\; 1$$

5. for every $p \in V(G') \setminus V(G)$,

$$\left(\prod_{p_j \in S_1} \ell(p, p_j)\right)\left(\prod_{p_k \in S_2} \ell(p, p_k)^2\right) \;=\; 1.$$

As in the previous case, the prime 3 is slightly problematic since Proposition 44 gives extensive conditions on when we obtain solutions. In order to account for these conditions, we will need two other definitions.

Definition 22. A partition, (S_1, S_2, S_3), of $V(G)$ is called **three-quasi-balanced** at 3 if and only if the following conditions are satisfied:

1. (S_1, S_2, S_3) is three-balanced
2. if $p = 3$ is in only one S_ν, then either

$$\left(\prod_{p_j \in S_{\nu+1}} \ell(3, p_j)\right)\left(\prod_{p_k \in S_{\nu+2}} \ell(3, p_k)^2\right) \;=\; 1$$

where we cycle the indices of the partitions (i.e. $S_1 = S_4$, etc.)

or there exists $s_1, s_2 \in \{\pm 1\}$ such that

$$2a \equiv s_1\left(\prod_{p_i \in S_1} p_i\right) + s_2\left(\prod_{p_j \in S_2} p_j\right) + s_1 s_2\left(\prod_{p_k \in S_3} p_k\right) \pmod 9.$$

Definition 23. A partition, (S_1, S_2, S_3), of $V(G)$ is called **three-quasi-balanced** at 9 if and only if the following conditions are satisfied:

1. (S_1, S_2, S_3) is three-balanced

2. if $9 \mid b$ and $3 \notin S_1 \cup S_2$ then

$$\left(\prod_{p_j \in S_1} \ell(3, p_j)\right)\left(\prod_{p_k \in S_2} \ell(3, p_k)^2\right) \;=\; 1.$$

Using the definitions for this family of elliptic curves $\mathcal{E}_2$, we have the following lemma.

Lemma 53. *Suppose (S_1, S_2, S_3) is a partition of $V(G)$. Let*

$$u_1 = \prod_{p_i \in S_1} p_i \quad \text{and} \quad u_2 = \prod_{p_j \in S_2} p_j.$$

Then the homogeneous equation

$$u_1 X^3 + u_2 Y^3 + \frac{2b}{u_1 u_2} Z^3 - 2aXYZ = 0 \tag{5.2}$$

has a solution in every local field $\mathbb{Q}_p$ if and only if $3 \nmid a$ and (S_1, S_2, S_3) is three-balanced or if $3 \,||\, a$ and (S_1, S_2, S_3) is three-quasi-balanced at 3 or if $9 \mid a$ and (S_1, S_2, S_3) is three-quasi-balanced at 9.

The proof follows in a similar manner to the one given for Lemma 51. A detailed proof can be found in Appendix E.

The following theorem gives us the size of the Selmer group $\mathrm{Sel}^{(\phi)}(E_{ab})$ in terms of graphs for the family of elliptic curves $\mathcal{E}_2$.

Theorem 54. *Let $E_{ab} : y^2 = x^3 + (ax + b)^2$ with $3 \mid b$. Let G and G' be defined as above.*

Then if $3 \nmid a$, *we have*

$$\left|\mathrm{Sel}^{(\phi)}(E_{ab})\right| \;=\; \#\left\{\mathrm{three-balanced\ partitions\ of}\ V(G)\right\}.$$

If $3 \,||\, a$, *then*

$$\left|\mathrm{Sel}^{(\phi)}(E_{ab})\right| \;=\; \#\left\{\mathrm{three-quasi-balanced\ partitions\ at\ 3\ of}\ V(G)\right\}.$$

Otherwise, if $9 \mid a$, *then*

$$\left|\mathrm{Sel}^{(\phi)}(E_{ab})\right| \;=\; \#\left\{\mathrm{three-quasi-balanced\ partitions\ at\ 9\ of}\ V(G)\right\}.$$

The proof is almost identical to the one given for Theorem 52. However in this case if $v_3(a) = 2$, an additional condition must be added to the definition of a three-balanced partition as well.

5.2.2 The Auxiliary Curve $E'_{ab'}$

In this section, we will be studying elliptic curves of the form

$$y^2 = x^3 - 3(ax + b')^2$$

whose discriminant is

$$\Delta = -144(b')^3\Delta'$$

where $\Delta' = 27b' + 12a^3$. Recall by Lemma 36, we know that for every prime, p, either $v_p(b') \leq 2$ or $v_p(a) = 0$.

Once again, let ω be a primitive cubic root of unity. If $p \equiv 1 \pmod 3$, then we know

that we can write $p = \pi\overline{\pi}$ with $\pi \equiv 2 \pmod 3$ and π in the upper-half plane. Define

$$\chi_p(q) = \chi_\pi(q) = \left(\frac{q}{\pi}\right)_3.$$

For $p \equiv 2 \pmod 3$, define

$$\chi_{p^2}(\delta) = \omega^i$$

where $\delta^{(p^2-1)/3} \equiv \omega^i \pmod p$.

Recall that we have the following properties of χ_p:

1. $\chi_p(q) = 1$ if and only if q is a cube in $\mathbb{F}_p^*$
2. $\chi_p(ab) = \chi_p(a)\chi_p(b)$.

For $p = 3$, notice that $(\mathbb{Z}/9\mathbb{Z})^*$ is cyclic and generated by 2. Define χ_3 on $(\mathbb{Z}/9\mathbb{Z})^*$ by

$$\chi_3(q) = \omega^t$$

where $q = 2^t \in (\mathbb{Z}/9\mathbb{Z})^*$. Note that even though we are working modulo 9, we will still use χ_3 to avoid confusion later.

Recall

$$\begin{aligned} F_{u'}(X,Y,Z) &= 2aX^2Z - 2aXYZ + 2aY^2Z + \frac{2b'}{\gamma\overline{\gamma}}Z^3 \\ &\quad -dX^3 - dY^3 - 3cXY^2 + 3cX^2Y + 3dXY^2 \end{aligned}$$

with $\gamma = c + d\omega$ where $\gamma\overline{\gamma}$ is only divisible by primes $p \equiv 1 \pmod 3$.

Consider the family $\mathcal{E}_3$ of elliptic curves given by

$$E'_{ab'} : y^2 = x^3 - 3(ax + b')^2.$$

Let G be a graph with vertex set $V(G) = \{p : p \equiv 1 \pmod 3,\ p \mid 2b'\}$. Additionally, let G' be a graph containing G with vertex set

$$V(G') = \{q : q \text{ satisfies one of } (1), (2) \text{ below}\} \cup V(G)$$

(1) $q \equiv 2 \pmod 3$, $q \mid \Delta'$

(2) $q \equiv 1 \pmod 3$, $q \mid \Delta'$ and $q \nmid 2b'$.

Finally, let G'' be a graph containing G' with

$$V(G'') = V(G') \cup \{q : q \text{ satisfies one of } (3), (4), (5), (6) \text{ below}\} \cup \{\sqrt{-3}\}$$

(3) $q \equiv 1 \pmod 3$, $q^2 \mid 2b'$

(4) $q \not\equiv 1 \pmod 3$, $q^2 \mid 2b'$

(5) all copies of 2 which divide $2b'$

(6) $q \mid b'$, $q = 3$.

Clearly, if $v_2(b') < 2$, then we do not need the additional copy of 2. And similarly with the prime $q = 3$, we only include it if $3 \mid b'$.

Example 7. Consider the elliptic curve

$$E : y^2 = x^3 - 3\left((3)(7)x + (3)(7)(23)(103)\right)^2$$

where $\Delta' = 3^7(5)(7)(19)$. There is actually a degree three isogeny between this curve and the one given in the previous example. The vertices of G are $\{7, 103\}$. The vertices of G' are $\{5, 19, 7, 103\}$ and the vertices of G'' are $\{2, 3, 23, \sqrt{-3}, 5, 19, 7, 103\}$. The graph is represented by Figure 5.5.

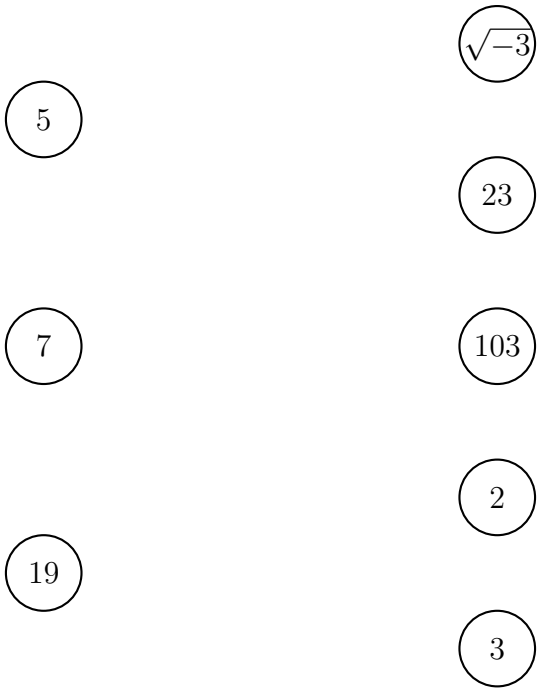


Figure 5.5: Vertices of G''

Next, draw directed edges from all primes $p \in V(G')$ to $q \in V(G'')$ where $p \mid 2b'$, $p \mid \Delta'$ and $q \mid 2b'\sqrt{-3}$.

Draw directed edges from all primes $p \in V(G')$ with $p \nmid 2b'\sqrt{-3}$ (the solubility condition primes) to primes $q \in V(G)$.

Label each directed edge from p to q as

$$\ell(p,q) = \begin{cases} \chi_\pi(\eta) \text{ and } \chi_\phi(\overline{\eta}) & p \equiv 1 \pmod 3,\ p \mid 2b' \\ \chi_p(q) & p \equiv 1 \pmod 3, p \nmid 2b' \\ \chi_{p^2}(q) & p \equiv 2 \pmod 3 \end{cases}$$

where if $q \equiv 1 \pmod 3$, there exists $\eta \equiv 2 \pmod 3$ and in the upper half plane such that $q = \eta\overline{\eta}$. When we just want the value $\chi_\pi(\eta)$, then denote the label as $\ell(p,\eta)$. Similarly, if we want the value $\chi_\pi(\overline{\eta})$, we will denote it as $\ell(p,\overline{\eta})$. Finally, observe that for $q \equiv 1 \pmod 3$,

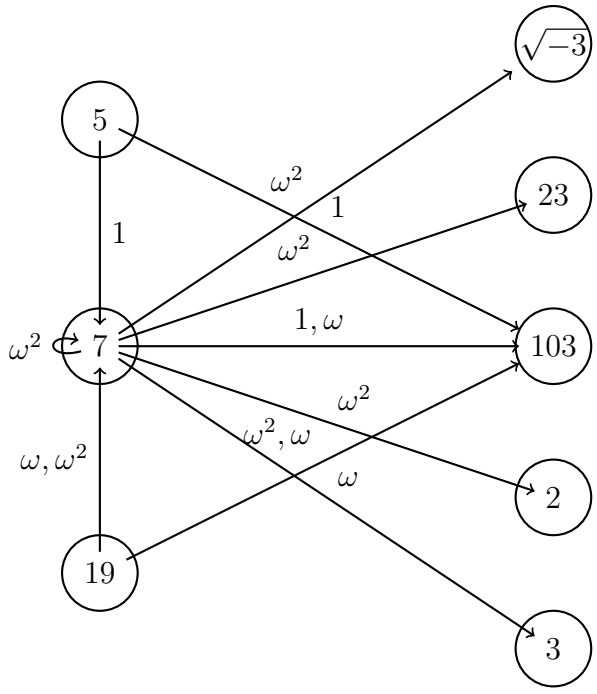


Figure 5.6: Directed Graph G''

$\ell(p, q) = \chi_p(q) = \chi_\pi(\eta)\chi_\pi(\overline{\eta})$.

Example 8. Adding edges to Figure 5.1 we obtain the directed graph in Figure 5.6.

For each point p in $V(G)$, randomly label it with $\mathcal{L}(p) \in \{0, 1, 2\}$.

Let $S_1 = \{p \in V(G) : \mathcal{L}(p) = 1\}$ and $S_2 = \{p \in V(G) : \mathcal{L}(p) = 2\}$.

Define

$$u_1 = \prod_{\substack{p \in S_1 \\ p = \pi\overline{\pi}}} \pi \prod_{\substack{p \in S_2 \\ p = \pi\overline{\pi}}} \overline{\pi}$$

and

$$u_2 = \prod_{\substack{p \in S_1 \\ p = \pi\overline{\pi}}} \overline{\pi} \prod_{\substack{p \in S_2 \\ p = \pi\overline{\pi}}} \pi.$$

As in Subsection 5.2.1, we are attempting to generalize the results of Feng and Xiong [32]. Recall that we are considering the results of Faulkner and James [31] for congruent number curves and demonstrate an equivalent approach for elliptic curves with 3 torsion.

In [31], Faulkner and James define even and quasi-even partitions of graphs associated to congruent number curves. In a similar manner, we defined three-balanced and three-quasi-balanced partitions of graphs associated to elliptic curves with 3 torsion. Unfortunately, this does not translate nicely when looking at graphs associated to the auxiliary curve $E'_{ab'}$. The reason is that instead of working over $\mathbb{Q}$, we are working over $\mathbb{Q}(\omega)$. So when looking for local solutions, some of the primes which divide $2b$ will split. In fact, the split primes are the only primes which will divide $N(\gamma)$ and these are the primes which will make up elements in $\text{Sel}^{(\widehat{\phi})}(E'_{ab'})$.

Suppose p is a split prime and we can write it as $p = \pi\overline{\pi}$ where $\pi \equiv 2 \pmod 3$ and π is in the upper half plane. Then we would like to partition π and $\overline{\pi}$ instead of p since $p \nmid \gamma$, but π could divide γ or $\overline{\gamma}$. Instead of putting π and $\overline{\pi}$ as vertices in the graph, we will place the prime p in the graph and label it with a 0, 1 or 2. If p is labeled with a 1, then π divides γ and if p is labeled with a 2, π divides $\overline{\gamma}$. Otherwise, if p is labeled with a 0, then $p \nmid N(\gamma)$.

Definition 24. We say a labeling, $\mathcal{L}$, on $V(G)$ is **good** if and only if it satisfies the following properties:

1. For all $p \in V(G)$ with $p \mid \Delta'$, if $\mathcal{L}(p) = 0$, then

$$\left(\prod_{\substack{q \in S_1 \\ q = \eta\overline{\eta}}} \ell(p,\eta)\ell(p,\overline{\eta})^2\right)\left(\prod_{\substack{q \in S_2 \\ q = \eta\overline{\eta}}} \ell(p,\overline{\eta})\ell(p,\eta)^2\right) = 1.$$

2. For all $p \in V(G)$ with $p \mid \Delta'$, if $\mathcal{L}(p) = 1$ and $p \notin V(G'') \setminus S_1$, then

$$\left(\prod_{\substack{q \in S_1 \\ q = \eta\overline{\eta}}} \ell(p,\overline{\eta})\right)\left(\prod_{\substack{q \in S_2 \\ q = \eta\overline{\eta}}} \ell(p,\eta)\right)\left(\prod_{\substack{q \in V(G'') \setminus (S_1 \cup S_2) \\ q \mid 2b'\sqrt{-3}}} \ell(p,q)^2\right) = 1.$$

3. For all $p \in V(G)$ with $p \mid \Delta'$, if $\mathcal{L}(p) = 2$ and $p \notin V(G'') \setminus S_2$, then

$$\left(\prod_{\substack{q \in S_1 \\ q = \eta\overline{\eta}}} \ell(p,\eta)\right)\left(\prod_{\substack{q \in S_2 \\ q = \eta\overline{\eta}}} \ell(p,\overline{\eta})\right)\left(\prod_{\substack{q \in V(G'') \setminus (S_1 \cup S_2) \\ q \mid 2b'\sqrt{-3}}} \ell(p,q)^2\right) = 1.$$

4. For all $p \in V(G)$ with $p \mid \Delta'$, if $\mathcal{L}(p) = 1$ and $p \in V(G'') \setminus S_1$, then

$$\left(\prod_{\substack{q \in S_1 \setminus \{p\} \\ q = \eta\overline{\eta}}} \ell(p,\eta)\right)\left(\prod_{\substack{q \in S_2 \\ q = \eta\overline{\eta}}} \ell(p,\overline{\eta})\right)\left(\prod_{\substack{q \in V(G'') \setminus (S_1 \cup S_2 \cup \{p\}) \\ q \mid 2b'\sqrt{-3}}} \ell(p,q)^2\right) = 1.$$

5. For all $p \in V(G)$ with $p \mid \Delta'$, if $\mathcal{L}(p) = 2$ and $p \in V(G'') \setminus S_2$, then

$$\left(\prod_{\substack{q \in S_1 \\ q = \eta\overline{\eta}}} \ell(p,\overline{\eta})\right)\left(\prod_{\substack{q \in S_2 \setminus \{p\} \\ q = \eta\overline{\eta}}} \ell(p,\eta)\right)\left(\prod_{\substack{q \in V(G'') \setminus (S_1 \cup S_2 \cup \{p\}) \\ q \mid 2b'\sqrt{-3}}} \ell(p,q)^2\right) = 1.$$

6. For all $q \in V(G') \setminus V(G)$, $q \neq 2$, then

$$\left(\prod_{\substack{p \in S_1 \\ p = \pi\overline{\pi}}} \ell(q,\pi)\ell(q,\overline{\pi})^2\right)\left(\prod_{\substack{p \in S_2 \\ p = \pi\overline{\pi}}} \ell(q,\overline{\pi})\ell(q,\pi)^2\right) = 1.$$

Using this definition, we have the following lemma.

Lemma 55. *Suppose $\mathcal{L}$ is a labeling of $V(G)$. Then the homogeneous cubic equation $F_{u'}(X,Y,Z) = 0$ has a solution in every local field $\mathbb{Q}_p$ with $p \neq 2,3$ if and only if $\mathcal{L}$ is a good labeling.*

Proof. Let

$$u_1 = \prod_{\substack{p \in S_1 \\ p=\pi\overline{\pi}}} \pi \prod_{\substack{p \in S_2 \\ p=\pi\overline{\pi}}} \overline{\pi}$$

and

$$u_2 = \prod_{\substack{p \in S_1 \\ p=\pi\overline{\pi}}} \overline{\pi} \prod_{\substack{p \in S_2 \\ p=\pi\overline{\pi}}} \pi.$$

Then, when necessary, let

$$u_3 = \frac{2b'\sqrt{-3}}{u_1 u_2}.$$

Assume that $\mathcal{L}$ is a good labeling. We need to check the following for every prime $p \in V(G)$ with $p \mid \Delta'$,

1. if $\mathcal{L}(p) = 0$, then $\chi_p(u_1/u_2) = 1$.
2. if $\mathcal{L}(p) = 1$, $p \notin V(G') \setminus S_1$, then $\chi_p(u_2/u_3) = 1$.
3. if $\mathcal{L}(p) = 2$, $p \notin V(G') \setminus S_2$, then $\chi_p(u_1/u_3) = 1$.
4. if $\mathcal{L}(p) = 1$ and $p \in V(G') \setminus S_1$, then $\chi_p(u_1/u_3) = 1$.
5. if $\mathcal{L}(p) = 2$ and $p \in V(G') \setminus S_2$, then $\chi_p(u_2/u_3) = 1$.

Additionally, we must check for every $q \in V(G') \setminus V(G)$, $q \neq 2$, then $\chi_q(u_1/u_2) = 1$.

First we will check the conditions for every prime $p \in V(G)$ with $p \mid \Delta'$. If $\mathcal{L}(p) = 0$,

then

$$\begin{aligned}
\chi_\pi(u_1/u_2) &= \chi_\pi(u_1)\chi_\pi(u_2)^2 \\
&= \left(\prod_{\substack{q\in S_1\\ q=\eta\overline{\eta}}} \chi_\pi(\eta)\chi_\pi(\overline{\eta})^2\right)\left(\prod_{\substack{q\in S_2\\ q=\eta\overline{\eta}}} \chi_\pi(\overline{\eta})\chi_\pi(\eta)^2\right) \\
&= \left(\prod_{\substack{q\in S_1\\ q=\eta\overline{\eta}}} \ell(p,\eta)\ell(p,\overline{\eta})^2\right)\left(\prod_{\substack{q\in S_2\\ q=\eta\overline{\eta}}} \ell(p,\overline{\eta})\ell(p,\eta)^2\right) \\
&= 1.
\end{aligned}$$

If $\mathcal{L}(p) = 1$ and $p \notin V(G') \setminus S_1$, then

$$\begin{aligned}
\chi_\pi(u_2/u_3) &= \chi_\pi(u_2)\chi_\pi(u_3)^2 \\
&= \left(\prod_{\substack{q\in S_1\\ q=\eta\overline{\eta}}} \chi_\pi(\overline{\eta})\right)\left(\prod_{\substack{q\in S_2\\ q=\eta\overline{\eta}}} \chi_\pi(\eta)\right)\left(\prod_{\substack{q\in V(G'')\setminus(S_1\cup S_2)\\ q|2b'\sqrt{-3}}} \chi_\pi(q)^2\right) \\
&= \left(\prod_{\substack{q\in S_1\\ q=\eta\overline{\eta}}} \ell(p,\overline{\eta})\right)\left(\prod_{\substack{q\in S_2\\ q=\eta\overline{\eta}}} \ell(p,\eta)\right)\left(\prod_{\substack{q\in V(G'')\setminus(S_1\cup S_2)\\ q|2b'\sqrt{-3}}} \ell(p,q)^2\right) \\
&= 1.
\end{aligned}$$

If $\mathcal{L}(p) = 2$ and $p \notin V(G') \setminus S_2$, then

$$\begin{aligned}
\chi_\pi(u_1/u_3) &= \chi_\pi(u_1)\chi_\pi(u_3)^2 \\
&= \left(\prod_{\substack{q\in S_1\\ q=\eta\overline{\eta}}} \chi_\pi(\eta)\right)\left(\prod_{\substack{q\in S_2\\ q=\eta\overline{\eta}}} \chi_\pi(\overline{\eta})\right)\left(\prod_{\substack{q\in V(G'')\setminus(S_1\cup S_2)\\ q|2b'\sqrt{-3}}} \chi_\pi(q)^2\right) \\
&= \left(\prod_{\substack{q\in S_1\\ q=\eta\overline{\eta}}} \ell(p,\eta)\right)\left(\prod_{\substack{q\in S_2\\ q=\eta\overline{\eta}}} \ell(p,\overline{\eta})\right)\left(\prod_{\substack{q\in V(G'')\setminus(S_1\cup S_2)\\ q|2b'\sqrt{-3}}} \ell(p,q)^2\right) \\
&= 1.
\end{aligned}$$

If $\mathcal{L}(p) = 1$ and $p \in V(G') \setminus S_1$, then

$$\begin{aligned}
\chi_\pi(u_1/u_3) &= \chi_\pi(u_1)\chi_\pi(u_3)^2 \\
&= \left(\prod_{\substack{q\in S_1\setminus\{p\}\\ q=\eta\overline{\eta}}} \chi_\pi(\eta)\right)\left(\prod_{\substack{q\in S_2\\ q=\eta\overline{\eta}}} \chi_\pi(\overline{\eta})\right)\left(\prod_{\substack{q\in V(G'')\setminus(S_1\cup S_2\cup\{p\})\\ q|2b'\sqrt{-3}}} \chi_\pi(q)^2\right) \\
&= \left(\prod_{\substack{q\in S_1\setminus\{p\}\\ q=\eta\overline{\eta}}} \ell(p,\eta)\right)\left(\prod_{\substack{q\in S_2\\ q=\eta\overline{\eta}}} \ell(p,\overline{\eta})\right)\left(\prod_{\substack{q\in V(G'')\setminus(S_1\cup S_2\cup\{p\})\\ q|2b'\sqrt{-3}}} \ell(p,q)^2\right) \\
&= 1.
\end{aligned}$$

If $\mathcal{L}(p) = 2$ and $p \in V(G') \setminus S_2$, then

$$\begin{aligned}
\chi_\pi(u_2/u_3) &= \chi_\pi(u_2)\chi_p(u_3)^2 \\
&= \left(\prod_{\substack{q\in S_1\\ q=\eta\overline{\eta}}} \chi_\pi(\overline{\eta})\right)\left(\prod_{\substack{q\in S_2\setminus\{p\}\\ q=\eta\overline{\eta}}} \chi_\pi(\eta)\right)\left(\prod_{\substack{q\in V(G'')\setminus(S_1\cup S_2\cup\{p\})\\ q|2b'\sqrt{-3}}} \chi_\pi(q)^2\right) \\
&= \left(\prod_{\substack{q\in S_1\\ q=\eta\overline{\eta}}} \ell(p,\overline{\eta})\right)\left(\prod_{\substack{q\in S_2\setminus\{p\}\\ q=\eta\overline{\eta}}} \ell(p,\eta)\right)\left(\prod_{\substack{q\in V(G'')\setminus(S_1\cup S_2\cup\{p\})\\ q|2b'\sqrt{-3}}} \ell(p,q)^2\right) \\
&= 1.
\end{aligned}$$

Finally, if $q \in V(G') \setminus V(G)$, $q \neq 2$, then

$$\begin{aligned}
\chi_q(u_1/u_2) &= \chi_q(u_1)\chi_p(u_2)^2 \\
&= \left(\prod_{\substack{p\in S_1\\ p=\pi\overline{\pi}}} \chi_q(\pi)\chi_q(\overline{\pi})^2\right)\left(\prod_{\substack{p\in S_2\\ p=\pi\overline{\pi}}} \chi_q(\overline{\pi})\chi_q(\pi)^2\right) \\
&= \left(\prod_{\substack{p\in S_1\\ p=\pi\overline{\pi}}} \ell(q,\pi)\ell(q,\overline{\pi})^2\right)\left(\prod_{\substack{p\in S_2\\ p=\pi\overline{\pi}}} \ell(q,\overline{\pi})\ell(q,\pi)^2\right) \\
&= 1.
\end{aligned}$$

Therefore, by Propositions 45, 48 and Corollary 47, we will always have a solution in $\mathbb{Q}_p$ for $p \neq 2, 3$.

Conversely assume $\mathcal{L}$ is not a good labeling of $V(G)$. There are a few cases we need to consider.

Case 1**:** There exists a $p \in V(G)$ such that $p \mid \Delta'$, $\mathcal{L}(p) = 0$ and

$$\left(\prod_{\substack{q \in S_1 \\ q = \eta\overline{\eta}}} \ell(p,\eta)\ell(p,\overline{\eta})^2 \right) \left(\prod_{\substack{q \in S_2 \\ q = \eta\overline{\eta}}} \ell(p,\overline{\eta})\ell(p,\eta)^2 \right) \neq 1.$$

But this implies that $\chi_\pi(u_1/u_2) \neq 1$, so u_1/u_2 is not a cube modulo π. This violates Corollary 47.3.b, so we will not have a solution in $\mathbb{Q}_p$.

Case 2**:** There exists a $p \in V(G)$ such that $p \mid \Delta'$, $\mathcal{L}(p) = 1$, $p \notin V(G') \setminus S_1$ and

$$\left(\prod_{\substack{q \in S_1 \\ q = \eta\overline{\eta}}} \ell(p,\overline{\eta}) \right) \left(\prod_{\substack{q \in S_2 \\ q = \eta\overline{\eta}}} \ell(p,\eta) \right) \left(\prod_{\substack{q \in V(G'') \setminus (S_1 \cup S_2) \\ q \mid 2b'\sqrt{-3}}} \ell(p,q)^2 \right) \neq 1.$$

But this implies that $\chi_\pi(u_2/u_3) \neq 1$, so u_2/u_3 is not a cube modulo π. This violates Corollary 47.3.b, so we will not have a solution in $\mathbb{Q}_p$.

Case 3**:** There exists $p \in V(G)$ such that $p \mid \Delta'$, $\mathcal{L}(p) = 2$, $p \notin V(G') \setminus S_2$ and

$$\left(\prod_{\substack{q \in S_1 \\ q = \eta\overline{\eta}}} \ell(p,\eta) \right) \left(\prod_{\substack{q \in S_2 \\ q = \eta\overline{\eta}}} \ell(p,\overline{\eta}) \right) \left(\prod_{\substack{q \in V(G'') \setminus (S_1 \cup S_2) \\ q \mid 2b'\sqrt{-3}}} \ell(p,q)^2 \right) \neq 1.$$

But this implies that $\chi_\pi(u_1/u_3) \neq 1$, so u_1/u_3 is not a cube modulo π. This violates Corollary 47.3.b, so we will not have a solution in $\mathbb{Q}_p$.

Case 4**:** There exists a $p \in V(G)$ such that $p \mid \Delta'$, $\mathcal{L}(p) = 1$, $p \in V(G') \setminus S_1$ and

$$\left(\prod_{\substack{q \in S_1 \setminus \{p\} \\ q = \eta\overline{\eta}}} \ell(p,\eta) \right) \left(\prod_{\substack{q \in S_2 \\ q = \eta\overline{\eta}}} \ell(p,\overline{\eta}) \right) \left(\prod_{\substack{q \in V(G'') \setminus (S_1 \cup S_2 \cup \{p\}) \\ q \mid 2b'\sqrt{-3}}} \ell(p,q)^2 \right) \neq 1.$$

But this implies that $\chi_\pi(u_1/u_3) \neq 1$, so u_1/u_3 is not a cube modulo π. This violates Corollary

47.3.c, so we will not have a solution in $\mathbb{Q}_p$.

Case 5**:** There exists a $p \in V(G)$ such that $p \mid \Delta'$, $\mathcal{L}(p) = 2$, $p \in V(G') \setminus S_2$ and

$$\left(\prod_{\substack{q \in S_1 \\ q = \eta\overline{\eta}}} \ell(p, \overline{\eta}) \right) \left(\prod_{\substack{q \in S_2 \setminus \{p\} \\ q = \eta\overline{\eta}}} \ell(p, \eta) \right) \left(\prod_{\substack{q \in V(G'') \setminus (S_1 \cup S_2 \cup \{p\}) \\ q \mid 2b'\sqrt{-3}}} \ell(p, q)^2 \right) \neq 1.$$

But this implies that $\chi_\pi(u_2/u_3) \neq 1$, so u_2/u_3 is not a cube modulo π. This violates Corollary 47.3.c, so we will not have a solution in $\mathbb{Q}_p$.

Case 6**:** There exists $q \in V(G') \setminus V(G)$ with $q \neq 2$ such that

$$\left(\prod_{\substack{p \in S_1 \\ p = \pi\overline{\pi}}} \ell(q, \pi)\ell(q, \overline{\pi})^2 \right) \left(\prod_{\substack{p \in S_2 \\ p = \pi\overline{\pi}}} \ell(q, \overline{\pi})\ell(q, \pi)^2 \right) \neq 1.$$

But this implies that $\chi_q(u_1/u_2) \neq 1$. If $q \equiv 1 \pmod 3$, then this means u_1/u_2 is not a cube modulo q and violates Corollary 47.2, so we will not have a solution in $\mathbb{Q}_q$. If $q \equiv 2 \pmod 3$, then this means u_1/u_2 is not a cube modulo q^2 and violates either Proposition 48.2 or 48.3.a. In either case, we will not have a solution in $\mathbb{Q}_p$.

□

Example 9. Continuing with the elliptic curve

$$E : y^2 = x^3 - 3\left((3)(7)x + (3)(7)(23)(103)\right)^2$$

where $\Delta' = 3^7(5)(7)(19)$. It turns out that there is only one good labeling of this graph; the trivial one which is obtained by labeling 7 and 103 with zeros. Let us look at why another example would fail to be a good labeling. Label 7 with a zero (denoted in blue) and 103 with a one (denoted in yellow).

Since 7 divides b and Δ', we must check solubility conditions for this prime. For the

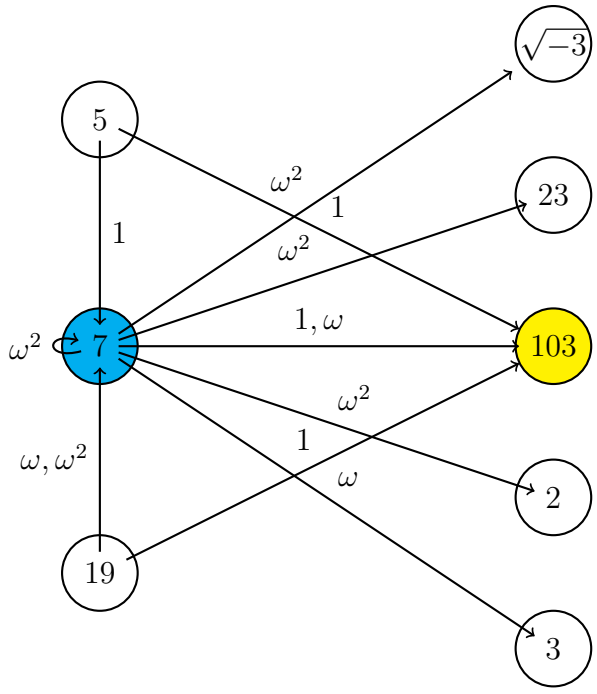


Figure 5.7: Not a Good Labeling

associated homogeneous cubic polynomial to have a solution modulo 7, u_1/u_2 must be a cube modulo 7 where $u_1 = 10 + \sqrt{-3}$ and $u_2 = 10 - \sqrt{-3}$. However, looking at the edge between 7 and 103, we see that $\chi_7(u_1/u_2) = 1(\omega)^2 \neq 1$. Therefore this is not a good labeling.

Let $G_3 = \mathbb{Q}\left(\sqrt{-3}^*\right) / \left(\mathbb{Q}\left(\sqrt{-3}\right)^*\right)^3$. Let $\mathcal{S}$ be a set of primes in $\mathbb{Q}$ containing 2 and 3. Define

$$\mathrm{Sel}_{\mathcal{S}}^{(\hat{\phi})}\left(E'_{ab'}\right) = \left\{[u'] \in G_3 : C_{F_{u'}}(\mathbb{Q}_\nu) \neq \emptyset \ \forall\ \nu \notin \mathcal{S}\right\}.$$

Proposition 56. $\mathrm{Sel}_{\mathcal{S}}^{(\hat{\phi})}\left(E'_{ab'}\right)$ *is a group.*

Proof. It is enough to show the existence for inverses and that given $[u], [w] \in \mathrm{Sel}_{\mathcal{S}}^{(\hat{\phi})}\left(E'_{ab'}\right)$, then $[uw] \in \mathrm{Sel}_{\mathcal{S}}^{(\hat{\phi})}\left(E'_{ab'}\right)$. We will cover the condition of inverses at the end of the proof.

We know that given $[u] \in \mathrm{Sel}_{\mathcal{S}}^{(\hat{\phi})}\left(E'_{ab'}\right)$, there exists $\gamma_1, \overline{\gamma_1}$ such that $u = \gamma_1\overline{\gamma_1}^2$ with γ_1 and $\overline{\gamma_1}$ coprime and square-free. Similarly, for $[w] \in \mathrm{Sel}_{\mathcal{S}}^{(\hat{\phi})}\left(E'_{ab'}\right)$, there exists $\gamma_2, \overline{\gamma_2}$ such that $w = \gamma_2\overline{\gamma_2}^2$ with γ_2 and $\overline{\gamma_2}$ coprime and square-free.

Define $\delta = \gcd(\gamma_1, \gamma_2)$ and $\epsilon = \gcd(\overline{\gamma_1}, \gamma_2)$. Then $\overline{\delta} = \gcd(\overline{\gamma_1}, \overline{\gamma_2})$ and $\overline{\epsilon} = \gcd(\gamma_1, \overline{\gamma_2})$.

Additionally, define

$$\gamma := \frac{\gamma_1 \gamma_2 \overline{\delta}}{\delta^2 \epsilon \overline{\epsilon}} \tag{5.3}$$

and so

$$\overline{\gamma} := \frac{\overline{\gamma_1 \gamma_2} \delta}{\overline{\delta}^2 \epsilon \overline{\epsilon}}. \tag{5.4}$$

Then $uw \equiv [uw]_{G_3} = [\gamma \overline{\gamma}]_{G_3}$.

To show $[uw] \in \mathrm{Sel}_{\mathcal{S}}^{(\hat{\phi})}(E'_{ab'})$, it is enough to show that for all $p \notin \mathcal{S}$, if $F_u = 0$ and $F_w = 0$ are soluble in $\mathbb{Q}_p$, then $F_{uw} = 0$ is soluble in $\mathbb{Q}_p$. There are numerous cases we need to consider.

Since $2b'$ and Δ' do not depend on u and w, if $p \nmid 2b'$ and $p \nmid \Delta'$ then $F_{uw} = 0$ is soluble in $\mathbb{Q}_p$.

If $p \nmid 2b'$ but $p \mid \Delta'$, then for $F_{uw} = 0$ to be soluble in $\mathbb{Q}_p$, we require $\gamma/\overline{\gamma}$ to be a cube modulo p. Notice that since $F_u = 0$ is soluble, there exists a c_1 such that $\gamma_1/\overline{\gamma_1} \equiv c_1^3 \pmod{p}$. And similarly, since $F_w = 0$ is soluble, there exists a c_2 such that $\gamma_2/\overline{\gamma_2} \equiv c_2^3 \pmod{p}$. Hence

$$\begin{aligned} \gamma/\overline{\gamma} &= \frac{\gamma_1 \gamma_2}{\overline{\gamma_1 \gamma_2}} \left(\frac{\overline{\delta}}{\delta} \right)^3 \\ &= \left(\frac{c_1 c_2 \overline{\delta}}{\delta} \right)^3 \pmod{p}. \end{aligned}$$

In the case that $p \equiv 2 \pmod 3$ and $p \mid 2b'$, we require $\gamma/\overline{\gamma}$ to be a cube modulo p if $p \mid a$. However, we are the same situation as above, so we are done.

If $p \equiv 1 \pmod 3$, we need to work a little harder. We may assume $p \mid a$, otherwise we know $F_{uw} = 0$ is soluble. Recall $p = \pi\overline{\pi}$ where $\pi \equiv 2 \pmod 3$ and π is in the upper-half plane.

Case 1: $\pi \,||\, 2b'$ with $\pi \mid \gamma_1$ and $\pi \mid \gamma_2$.

In this case, for $F_u = 0$ and $F_w = 0$ to be soluble, there must exist c_1 and c_2 such that

$$\overline{\gamma_1}/u_{3,1} \equiv c_1^3 \pmod{\pi}, \quad \overline{\gamma_2}/u_{3,2} \equiv c_2^3 \pmod{\pi}$$

where

$$u_{3,1} = \frac{2b'}{\gamma_1\overline{\gamma_1}}, \quad u_{3,2} = \frac{2b'}{\gamma_2\overline{\gamma_2}}.$$

Since $\pi \mid \gamma_1$ and $\pi \mid \gamma_2$, it follows that $\pi \mid \delta$. This implies that $\pi \mid \overline{\gamma}$. Therefore in order for $F_{uw} = 0$ to have a solution, we must have γ/u_3 equivalent to a cube modulo π where

$$u_3 = \frac{2b'}{\gamma\overline{\gamma}}.$$

Then

$$\begin{aligned}
\gamma/u_3 &= \frac{\gamma_1^2\gamma_2^2\overline{\gamma_1\gamma_2}}{2b'}\left(\frac{1}{\epsilon\bar{\epsilon}\delta}\right)^3 \\
&\equiv \gamma_1\gamma_2^2\overline{\gamma_1}^2\overline{\gamma_2}\left(\frac{c_1}{\epsilon\bar{\epsilon}\delta}\right)^3 \pmod{\pi} \quad \text{since} \quad \frac{1}{2b'} \equiv \frac{c_1^3}{\gamma_1\overline{\gamma_1}^2} \pmod{\pi} \\
&\equiv \left(\frac{c_1^3}{c_2\epsilon\bar{\epsilon}\delta}\right)^3 \pmod{\pi} \qquad \text{since} \quad \overline{\gamma_1}^2\gamma_1\gamma_2^2\overline{\gamma_2} \equiv \frac{c_1^3}{c_2^3} \pmod{\pi}.
\end{aligned}$$

Thus $F_{uw} = 0$ has a solution. The case that π divides $\overline{\gamma_1}$ and $\overline{\gamma_2}$ is identical.

Case 2: $\pi \,||\, 2b'$ with $\pi \mid \gamma_1$ and $\pi \mid \overline{\gamma_2}$.

In this case, for $F_u = 0$ and $F_w = 0$ to be soluble, there exists c_1 and c_2 such that

$$\overline{\gamma_1}/u_{3,1} \equiv c_1^3 \pmod{\pi}, , \quad \gamma_2/u_{3,2} \equiv c_2^3 \pmod{\pi}$$

where

$$u_{3,1} = \frac{2b'}{\gamma_1\overline{\gamma_1}}, \quad u_{3,2} = \frac{2b'}{\gamma_2\overline{\gamma_2}}.$$

Since $\pi \mid \gamma_1$ and $\pi \mid \overline{\gamma_2}$, it follows that $\pi \mid \bar{\epsilon}$. This implies that $\pi \mid u_3$. Therefore in order for

$F_{uw} = 0$ to have a solution, we must have $\gamma/\overline{\gamma}$ equivalent to a cube modulo π. Then

$$\begin{aligned}\gamma/\overline{\gamma} &= \frac{\gamma_1\gamma_2}{\overline{\gamma_1\gamma_2}}\left(\frac{\overline{\delta}}{\delta}\right)^3 \\ &\equiv \left(\frac{\overline{c_1\delta}}{c_2\delta}\right)^3 \pmod{\pi} \quad \text{since} \quad \frac{\gamma_1\gamma_2}{\overline{\gamma_1\gamma_2}} \equiv \left(\frac{c_1}{c_2}\right)^3 \pmod{\pi}.\end{aligned}$$

Thus $F_{uw} = 0$ has a solution. The case that π divides $\overline{\gamma_1}$ and γ_2 is identical.

Case 3: $\pi \,||\, 2b'$ with $\pi \mid \gamma_1$ and $\pi \nmid \gamma_2\overline{\gamma_2}$.

In this case, for $F_u = 0$ and $F_w = 0$ to be soluble, there exists c_1 and c_2 such that

$$\overline{\gamma_1}/u_{3,1} \equiv c_1^3 \pmod{\pi}, \qquad \gamma_2/\overline{\gamma_2} \equiv c_2^3 \pmod{\pi}$$

where

$$u_{3,1} = \frac{2b'}{\gamma_1\overline{\gamma_1}}.$$

Since $\pi \mid \gamma_1$ and $\pi \nmid \gamma_2\overline{\gamma_2}$, it follows that $\pi \mid \gamma$. Therefore, in order for $F_{uw} = 0$ to have a solution, we must have $\overline{\gamma}/u_3$ equivalent to a cube modulo π where

$$u_3 = \frac{2b'}{\gamma\overline{\gamma}}.$$

Then

$$\begin{aligned}\overline{\gamma}/u_3 &= \frac{\gamma_1\gamma_2\overline{\gamma_1}^2\overline{\gamma_2}^2}{2b'}\left(\frac{1}{\epsilon\overline{\epsilon}\overline{\delta}}\right)^3 \\ &\equiv \gamma_2\overline{\gamma_2}^2\left(\frac{c_1}{\epsilon\overline{\epsilon}\overline{\delta}}\right)^3 \pmod{\pi} \quad \text{since} \quad \frac{\gamma_1\overline{\gamma_1}^2}{2b'} \equiv c_1^3 \pmod{\pi} \\ &\equiv \left(\frac{c_1c_2}{\epsilon\overline{\epsilon}\overline{\delta}}\right)^3 \pmod{\pi} \qquad \text{since} \quad \gamma_2\overline{\gamma_2}^2 \equiv c_2^3 \pmod{\pi}.\end{aligned}$$

Thus $F_{uw} = 0$ has a solution. The cases that π divides $\overline{\gamma_1}$ and $u_{3,2}$, γ_2 and $u_{3,1}$, and $\overline{\gamma_2}$ and $u_{3,1}$ are identical.

Case 4: $\pi \nmid \gamma_1\overline{\gamma_1}$ and $\pi \nmid \gamma_2\overline{\gamma_2}$.

In this case, for $F_u = 0$ and $F_w = 0$ to be soluble, there must exist c_1 and c_2 such that

$$\gamma_1/\overline{\gamma} \equiv c_1^3 \pmod{\pi}, \qquad \gamma_2/\overline{\gamma_2} \equiv c_2^3 \pmod{\pi}.$$

Since $\pi \nmid \gamma_1\overline{\gamma_1}$ and $\pi \nmid \gamma_2\overline{\gamma_2}$, it follows that $\pi \nmid \gamma\overline{\gamma}$. Therefore in order for $F_{uw} = 0$ to have a solution, we must have $\gamma/\overline{\gamma}$ equivalent to a cube modulo π. Then

$$\begin{aligned} \gamma/\overline{\gamma} &= \frac{\gamma_1\gamma_2}{\overline{\gamma_1\gamma_2}}\left(\frac{\overline{\delta}}{\delta}\right)^3 \\ &\equiv \left(\frac{c_1c_2\overline{\delta}}{\delta}\right)^3 \pmod{\pi} \quad \text{since} \quad \frac{\gamma_1\gamma_2}{\overline{\gamma_1\gamma_2}} \equiv c_1^3c_2^3 \pmod{\pi}. \end{aligned}$$

Thus $F_{uw} = 0$ has a solution.

Case 5: $\pi^2 \,||\, 2b'$ with $\pi \mid \gamma_1$ and $\pi \mid \gamma_2$.

In this case, for $F_u = 0$ and $F_w = 0$ to be soluble, there must exist c_1 and c_2 such that

$$\gamma_1/u_{3,1} \equiv c_1^3 \pmod{\pi}, \qquad \gamma_2/u_{3,2} \equiv c_2^3 \pmod{\pi}$$

where

$$u_{3,1} = \frac{2b'}{\gamma_1\overline{\gamma_1}}, \qquad u_{3,2} = \frac{2b'}{\gamma_2\overline{\gamma_2}}.$$

Since $\pi \mid \gamma_1$ and $\pi \mid \gamma_2$, it follows that $\pi \mid \delta$. This implies that $\pi \mid \overline{\gamma}$. Therefore in order for $F_{uw} = 0$ to have a solution, we must have $\overline{\gamma}/u_3$ equivalent to a cube modulo π where

$$u_3 = \frac{2b'}{\gamma\overline{\gamma}}.$$

Then

$$\begin{aligned}
\overline{\gamma}/u_3 &= \frac{\gamma_1\gamma_2\overline{\gamma_1}^2\overline{\gamma_2}^2}{2b'}\left(\frac{1}{\epsilon\overline{\epsilon}\overline{\delta}}\right)^3 \\
&\equiv \gamma_1^2\gamma_2\overline{\gamma_1\gamma_2}^2\left(\frac{c_1}{\epsilon\overline{\epsilon}\overline{\delta}}\right)^3 \pmod{\pi} \quad \text{since} \quad \frac{1}{2b'} \equiv \frac{c_1^3}{\gamma_1^2\overline{\gamma_1}} \pmod{\pi} \\
&\equiv \left(\frac{c_1^3}{c_2\epsilon\overline{\epsilon}\overline{\delta}}\right)^3 \pmod{\pi} \qquad\qquad \text{since} \quad \gamma_1^2\overline{\gamma_1}\gamma_2\overline{\gamma_2}^2 \equiv \frac{c_1^3}{c_2^3} \pmod{\pi}.
\end{aligned}$$

Thus $F_{uw} = 0$ has a solution. The case that π divides $\overline{\gamma_1}$ and $\overline{\gamma_2}$ is identical.

Case 6: $\pi^2 \,||\, 2b'$ with $\pi \mid \gamma_1$ and $\pi \mid \overline{\gamma_2}$.

In this case, for F_u and F_w to be soluble, there must exist c_1 and c_2 such that

$$\gamma_1/u_{3,1} \equiv c_1^3 \pmod{\pi}, \qquad \overline{\gamma_2}/u_{3,2} \equiv c_2^3 \pmod{\pi}$$

where

$$u_{3,1} = \frac{2b'}{\gamma_1\overline{\gamma_1}}, \qquad u_{3,2} = \frac{2b'}{\gamma_2\overline{\gamma_2}}.$$

Since $\pi \mid \gamma_1$ and $\pi \mid \overline{\gamma_2}$, it follows that $\pi \mid \overline{\epsilon}$. This implies that $\pi \nmid \gamma\overline{\gamma}$. Therefore in order for $F_{uw} = 0$ to have a solution, we must have $\gamma/\overline{\gamma}$ equivalent to a cube modulo π. Then

$$\begin{aligned}
\gamma/\overline{\gamma} &= \frac{\gamma_1\gamma_2}{\overline{\gamma_1\gamma_2}}\left(\frac{\overline{\delta}}{\delta}\right)^3 \\
&\equiv \frac{\gamma_2\overline{\gamma_2}^2}{2b'}\left(\frac{\overline{\delta}}{c_1\delta}\right)^3 \pmod{\pi} \quad \text{since} \quad \frac{\gamma_1}{\overline{\gamma_1}} \equiv \frac{1}{2b'c_1^3} \pmod{\pi} \\
&\equiv \left(\frac{c_2\overline{\delta}}{c_1\delta}\right)^3 \pmod{\pi} \qquad\qquad \text{since} \quad \frac{\gamma_2\overline{\gamma_2}^2}{2b'} \equiv c_2^3 \pmod{\pi}.
\end{aligned}$$

Thus $F_{uw} = 0$ has a solution. The case that π divides $\overline{\gamma_1}$ and γ_2 is identical.

Case 7: $\pi^2 \,||\, 2b'$ with $\pi \mid \gamma_1$ and $\pi \nmid \gamma_2\overline{\gamma_2}$.

In this case, for F_u and F_w to be soluble, there must exist c_1 and c_2 such that

$$\gamma_1/u_{3,1} \equiv c_1^3 \pmod{\pi}, \qquad \gamma_2/\overline{\gamma_2} \equiv c_2^3 \pmod{\pi}$$

where

$$u_{3,1} = \frac{2b'}{\gamma_1\overline{\gamma_1}}.$$

Since $\pi \mid \gamma_1$ and $\pi \nmid \gamma_2\overline{\gamma_2}$, it follows that $\pi \mid \gamma$. Therefore in order for $F_{uw} = 0$ to have a solution, we must have γ/u_3 equivalent to a cube modulo π where

$$u_3 = \frac{2b'}{\gamma\overline{\gamma}}.$$

Then

$$\begin{aligned}\gamma/u_3 &= \frac{\gamma_1^2\gamma_2^2\overline{\gamma_1\gamma_2}}{2b'}\left(\frac{1}{\epsilon\overline{\epsilon}\delta}\right)^3 \\ &\equiv \left(\frac{c_1}{c_2\epsilon\overline{\epsilon}\delta}\right)^3 \pmod{\pi} \quad \text{since} \quad \frac{\gamma_1^2\gamma_2^2\overline{\gamma_1\gamma_2}}{2b'} \equiv \frac{c_1^3}{c_2^3} \pmod{\pi}.\end{aligned}$$

Thus $F_{uw} = 0$ has a solution. The cases that π divides $\overline{\gamma_1}$ and $u_{3,2}$, γ_2 and $u_{3,1}$, and $\overline{\gamma_2}$ and $u_{3,1}$ are identical.

Hence we have covered all cases, so $[uw] \in \mathrm{Sel}_S^{(\hat{\phi})}(E'_{ab'})$.

Let $[u] \in \mathrm{Sel}_S^{(\hat{\phi})}(E'_{ab'})$. Then there exists integers u_1, u_2 such that $\gcd(u_1, u_2) = 1$ and $u = u_1u_2^2$. Let $w = u_2u_1^2$. Notice that if (a, b, c) is a solution for $F_u(X, Y, Z) = 0$, then (b, a, c) is a solution for $F_w(X, Y, Z) = 0$, since the only difference between the two functions is that the coefficients of X^3 and Y^3 are switched. Hence $[w] \in \mathrm{Sel}_S^{(\hat{\phi})}(E'_{ab'})$. And $uw = u_1u_2^2u_2u_1^2 = u_1^3u_2^3$ which is a cube and hence equivalent to 1 in G_3. Thus $[w]$ is the inverse of $[u]$.

Therefore $\mathrm{Sel}_S^{(\hat{\phi})}(E'_{ab'})$ is a group.

□

The following theorem bounds the size of the Selmer group $\mathrm{Sel}^{(\widehat{\phi})}(E'_{ab'})$.

Theorem 57. *Let $E'_{ab'} : y^2 = x^3 - 3(ax + b')^2$. Let G, G' and G'' be the graphs with vertices*

defined above. Let $\mathcal{S} = \{2, 3\}$. *Then*

$$\left|\mathrm{Sel}^{(\hat{\phi})}(E'_{ab'})\right| \leq \left|\mathrm{Sel}^{(\hat{\phi})}_{\mathcal{S}}(E'_{ab'})\right| = \#\{\textit{good labeling of } V(G)\}.$$

5.3 Linear Algebra

In this section, we will transform the graphical interpretation of the Selmer group by way of graph theory into a linear algebra problem. Others have used such an approach to calculate the size of 3-Selmer groups, which yield results similar to the ones presented above. The interested reader should see [23] and [68]. We include this approach for completeness and hope to make use of it in future work.

Given a graph G with vertex set $V(G)$, as defined in the previous section, we can construct a characteristic matrix.

5.3.1 The Elliptic Curve E_{ab}

Consider an elliptic curve $E_{ab} : y^2 = x^3 + (ax + b)^2$ with $\Delta' = 27b - 4a^3$. Assume we have a graph G' with vertex set $V(G')$ and subgraph G with vertex set $V(G)$, as defined in the Sections 5.2.1.1 and 5.2.1.2. We want to construct a characteristic matrix to relate the graph theory problem with three-balanced and three-quasi-balanced partitions to a linear algebra problem.

We will index the rows and columns of the characteristic matrix by primes and we begin by ordering primes. Let $p_1, \ldots, p_l$ be the distinct primes which divide $2b$ exactly once and divide Δ'. Let $p_{l+1}, \ldots, p_r$ be the distinct primes which divide $2b$ exactly twice and divide Δ'. Next, let $p_{r+1}, \ldots, p_n$ be the distinct primes which divide $2b$ but do not divide Δ'. Also, let $p_{n+1}, \ldots, p_t$ be the second copy of the primes which divide $2b$ exactly twice. If $v_2(b) = 2$, then 2 is not one of the primes, p_i, for $1 \leq i \leq n$, so let $p_{t+1} = p_{t+2} = p_{t+3} = 2$.

Let $q_1, \ldots, q_m$ be the distinct primes dividing Δ', but not $2b$.

Define

$$t' = \begin{cases} t & \text{if } v_2(b) < 2 \\ t+3 & \text{if } v_2(b) = 2, \end{cases}$$

$$r' = \begin{cases} r & \text{if } v_2(b) < 2 \\ r+1 & \text{if } v_2(b) = 2, \end{cases}$$

and

$$p_{r'} = \begin{cases} p_r & \text{if } v_2(b) < 2 \\ 2 & \text{if } v_2(b) = 2. \end{cases}$$

Define the $(r'+m) \times t'$ matrix $A(G')$ by

$$a_{ij} = \begin{cases} \log_\omega \left(\ell\left(p_i, p_j\right)\right) & 1 \le i \le r', 1 \le j \le t', p_i \ne p_j \\ \log_\omega \left(\ell\left(q_{i-r'}, p_j\right)\right) & r'+1 \le i \le r'+m, 1 \le j \le t' \\ 0 & \text{otherwise.} \end{cases}$$

Let $D(G')$ be the $(r'+m) \times t'$ matrix with entries

$$d_{ij} = \begin{cases} \sum_{k=1}^{t'} a_{ik} & 1 \le i \le l, i = j \\ -\sum_{k=1}^{t'} a_{ik} & l+1 \le i \le r, i = j \\ 0 & \text{otherwise} \end{cases}$$

all reduced modulo 3.

Let

$$L'\left(G'\right) = A(G') - D(G')$$

again reduced modulo 3 and define $L(G)$ be the $(r'+m)\times n$ submatrix of $L'(G')$ with the $n+1$ to t' columns removed.

Remark 7. Notice that $\ker L(G) = \left\{\vec{w} : (\vec{w}, 0, \ldots, 0)^T \in \ker L'(G')\right\}$.

Let $\vec{w} = (w_1, w_2, \ldots, w_n)^T \in \mathbb{F}_3^n$. For each $\vec{w}$, associate subsets as follows:

$$S_1 = \{p_i : w_i = 1\},$$

$$S_2 = \{p_i : w_i = 2\},$$

and

$$S_3 = \{p_i : w_i = 0\} \cup \{p_{n+1}, \ldots, p_{t'}\}.$$

Now we will reduce to the case given in Section 5.2.1.1.

5.3.1.1 The Family of Curves $\mathcal{E}_1$

Assume E_{ab} has the property that $3 \nmid b$. If $v_3(a) = 1$, then we need to make the following adjustments. In this case we know that 3 must be one of the q_i's, so assume $q_m = 3$. Define $L_3(G')$ to be the $(r'+m-1)\times n$ submatrix of $L'(G')$ with the m-th row removed as well as the $n+1$ to t' columns removed.

Remark 8. Again, notice that $\ker L_3(G') = \left\{\vec{w} : (\vec{w}, 0, \ldots, 0)^T \in \ker L'(G')\right\}$.

The following lemma gives the relationship between partitions of the graph G and the submatrices $L(G)$ and $L_3(G')$ of the Laplacian matrix $L'(G')$.

Lemma 58. *1. If $v_3(a) \neq 1$, then the partition (S_1, S_2, S_3) corresponding to the vector $\vec{w}$ is three-balanced if and only if $\vec{w} \in \ker L(G)$.*

2. If $v_3(a) = 1$, then the partition (S_1, S_2, S_3) corresponding to the vector $\vec{w}$ is three-quasi-balanced if and only if either $\vec{w} \in \ker(L(G))$ or $\vec{w} \in \ker(L_3(G'))$ and there exists

$s_1, s_2 \in \{\pm 1\}$ *such that*

$$2a \equiv s_1 \left(\prod_{\substack{p_i \in S_1 \\ p_i | 2b}} p_i \right) + s_2 \left(\prod_{\substack{p_j \in S_2 \\ p_j | 2b}} p_j \right) + s_1 s_2 \left(\prod_{\substack{p_k \in S_3 \\ p_k | 2b}} p_k \right) \pmod{27}.$$

Proof. First assume that $v_2(b) < 2$. Then 2 is one of the primes $p_1, \ldots, p_r$ and $p'_r = p_r$. Next assume that $p_i \in S_1$ for $1 \leq i \leq l$, so there is only one copy of p_i. It is enough to show that $L'(G')\vec{w}' = \vec{0}$ with $\vec{w}' = (w_1, \ldots, w_{t'})^T = (\vec{w}, 0, \ldots, 0)^T$. Then

$$\begin{aligned}
\left(L'(G')\vec{w}'\right)_i &= \sum_{\substack{j=1 \\ p_j \neq p_i}}^{t'} \log_\omega \left(\ell\left(p_i, p_j\right)\right) w_j - \sum_{\substack{j=1 \\ p_j \neq p_i}}^{t'} \log_\omega \left(\ell\left(p_i, p_j\right)\right) w_i \\
&= \sum_{\substack{j=1 \\ p_j \neq p_i}}^{t'} \log_\omega \left(\ell\left(p_i, p_j\right)\right) \left(w_j - w_i\right) \\
&= \sum_{w_j = 2} \log_\omega \left(\ell\left(p_i, p_j\right)\right) + \sum_{w_j = 0} 2 \log_\omega \left(\ell\left(p_i, p_j\right)\right).
\end{aligned}$$

This is equivalent to zero modulo 3 if and only if

$$\omega^{\sum_{w_j=2} \log_\omega(\ell(p_i,p_j)) + \sum_{w_j=0} 2\log_\omega(\ell(p_i,p_j))} = 1.$$

And one can see that

$$\begin{aligned}
\omega^{\sum_{w_j=2} \log_\omega(\ell(p_i,p_j)) + \sum_{w_j=0} 2\log_\omega(\ell(p_i,p_j))} &= \omega^{\sum_{w_j=2} \log_\omega(\ell(p_i,p_j))} \omega^{\sum_{w_j=0} 2\log_\omega(\ell(p_i,p_j))} \\
&= \left(\prod_{p_j \in S_2} \ell\left(p_i, p_j\right) \right) \left(\prod_{p_k \in S_3} \ell\left(p_i, p_k\right)^2 \right).
\end{aligned}$$

Hence

$$\sum_{w_j = 2} \log_\omega \left(\ell\left(p_i, p_j\right)\right) + \sum_{w_j = 0} 2 \log_\omega \left(\ell\left(p_i, p_j\right)\right) \equiv 0 \pmod{3}$$

if and only if

$$\left(\prod_{p_j \in S_2} \ell\left(p_i, p_j\right)\right)\left(\prod_{p_k \in S_3} \ell\left(p_i, p_k\right)^2\right) = 1.$$

The cases that $p_i \in S_2$ and $p_i \in S_3$ with $1 \leq i \leq l$ are identical.

Now assume $p_i \in S_1$ with $l+1 \leq i \leq r$. So we know that p_i appears in more than one S_j. Then

$$\begin{aligned}
\left(L'(G')\vec{w}'\right)_i &= \sum_{\substack{j=1 \\ p_j \neq p_i}}^{t'} \log_\omega\left(\ell\left(p_i, p_j\right)\right) w_j + \sum_{\substack{j=1 \\ p_j \neq p_i}}^{t'} \log_\omega\left(\ell\left(p_i, p_j\right)\right) w_i \\
&= \sum_{\substack{j=1 \\ p_j \neq p_i}}^{t'} \log_\omega\left(\ell\left(p_i, p_j\right)\right)\left(w_j + w_i\right) \\
&= \sum_{w_j=0} \log_\omega\left(\ell\left(p_i, p_j\right)\right) + \sum_{w_j=1} 2\log_\omega\left(\ell\left(p_i, p_j\right)\right).
\end{aligned}$$

Once again, as before this is equivalent to zero modulo 3 if and only if

$$\left(\prod_{\substack{p_j \in S_3 \\ p_j \neq p_i}} \ell\left(p_i, p_j\right)\right)\left(\prod_{\substack{p_k \in S_1 \\ p_k \neq p_i}} \ell\left(p_i, p_k\right)^2\right) = 1.$$

Once again, the cases that $p_i \in S_2$ and $p_i \in S_3$ follow in a similar manner.

Now assume that $v_2(b) = 2$. Then we know that 2 is not one of the primes $p_1, \ldots, p_n$ and $p_{r'} = 2$. So we have that

$$\begin{aligned}
\left(L'(G')\vec{w}'\right)_{r'} &= \sum_{\substack{j=1 \\ p_j \neq 2}}^{t'} \log_\omega\left(\ell\left(2, p_j\right)\right) w_j \\
&= \sum_{w_j=1} \log_\omega\left(\ell\left(2, p_j\right)\right) + \sum_{w_j=2} 2\log_\omega\left(\ell\left(2, p_j\right)\right).
\end{aligned}$$

This is equivalent to zero modulo 3 if and only if

$$\left(\prod_{p_j \in S_1} \ell\left(2, p_j\right)\right)\left(\prod_{p_k \in S_2} \ell\left(2, p_k\right)^2\right) = 1.$$

Finally, consider rows i with i between $r'+1$ and $r'+m$. Then we have that

$$\begin{aligned}\left(L'(G')\vec{w}'\right)_i &= \sum_{j=1}^{t'} \log_\omega\left(\ell\left(q_{i-r'}, p_j\right)\right) w_j \\ &= \sum_{w_j=1} \log_\omega\left(\ell\left(q_{i-r'}, p_j\right)\right) + \sum_{w_j=2} 2\log_\omega\left(\ell\left(q_{i-r'}, p_j\right)\right).\end{aligned}$$

This is equivalent to zero modulo 3 if and only if

$$\left(\prod_{p_j \in S_1} \ell\left(q_{i-r'}, p_j\right)\right)\left(\prod_{p_k \in S_2} \ell\left(q_{i-r'}, p_k\right)^2\right) = 1.$$

If $v_3(a) \neq 1$, then we are done.

Otherwise, in the case that $v_3(a) = 1$, we need to re-examine the last row of $L(G)$. If

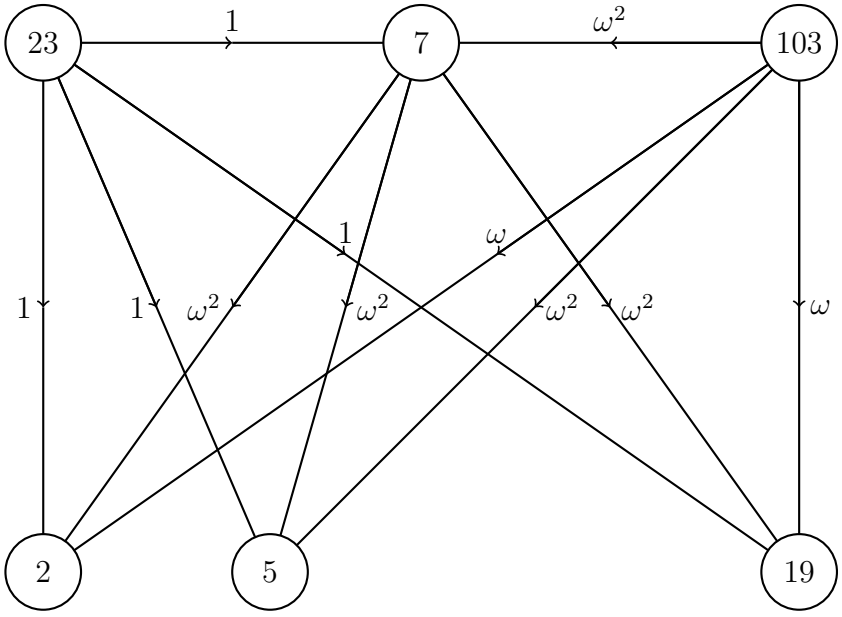
$$\begin{aligned}\left(L(G)\vec{w}\right)_i &= \sum_{j=1}^{t'} \log_\omega\left(\ell\left(q_m, p_j\right)\right) v_j \\ &= \sum_{w_j=1} \log_\omega\left(\ell\left(q_m, p_j\right)\right) + \sum_{w_j=2} 2\log_\omega\left(\ell\left(q_m, p_j\right)\right) \\ &\not\equiv 0 \pmod 3\end{aligned}$$

then look at $L_3(G')$. The argument is exactly the same as the one used for $L(G)$ except for the fact that the last row has been removed. And if there exists $s_1, s_2 \in \{\pm 1\}$ such that $2a \equiv s_1\left(\prod_{\substack{p_i \in S_1 \\ p_i \mid 2b}} p_i\right) + s_2\left(\prod_{\substack{p_j \in S_2 \\ p_j \mid 2b}} p_j\right) + s_1 s_2\left(\prod_{\substack{p_k \in S_3 \\ p_k \mid 2b}} p_k\right) \pmod{27}$ then we know by Proposition 43, there exists a solution to the equation. □

Example 10. Let us return to the example used in the previous section. Recall we considered the elliptic curve

$$E : y^2 = x^3 + (7x + 5 \cdot 7 \cdot 19)^2$$

where $\Delta' = 7 \cdot 23 \cdot 103$. The vertices of the graphs where $V(G') = \{2, 5, 7, 11, 19, 23, 103\}$ and $V(G) = \{2, 5, 7, 19\}$. Here is the corresponding graph.



When constructing the matrix A, we order the primes corresponding to the columns in the following order $7, 2, 5, 19$. The primes corresponding to the rows are ordered as $7, 23, 103$. It turns out that in this simple example, the matrix D is just the zero matrix. In addition, since no prime appears twice in the graph, it is not necessary to remove any columns. Therefore the matrices A, $L(G)$ and $L'(G')$ are the same and is given by

$$L(G) = \begin{bmatrix} 0 & 2 & 2 & 2 \\ 0 & 0 & 0 & 0 \\ 2 & 0 & 1 & 1 \end{bmatrix}.$$

To see this is the correct matrix, notice that the first row corresponds to the exponent power

of ω on the edge from 7 to the primes 2, 5 and 19. The first entry is a zero since the first column corresponds to the prime 7 and there is no loop from 7 to itself. The second row is entirely of zeros since 23 is equivalent to 2 modulo 3 and therefore all edges leaving 23 are labeled with a $1 = \omega^0$. Finally the third row corresponds to the exponent power of ω on the edge from 103 to the primes 2, 5, 7 and 19.

Corollary 59. *1. If $v_3(a) \neq 1$, the number of three-balanced partitions of G is 3^{n-s} where s is the rank of the $(r'+m) \times n$ matrix $L(G)$.*

2. If $v_3(a) = 1$, then the number of three-quasi-balanced partitions of G is between 3^{n-s_1} and 3^{n-s} where s is the rank of the $(r'+m) \times n$ matrix $L(G)$ and s_1 is the rank of the $(r'+m-1) \times n$ matrix $L_3(G')$.

As a result of Lemma 58 and Corollary 59, we can construct an element of $\mathrm{Sel}^{(\phi)}(E_{ab})$ for the family of elliptic curves $\mathcal{E}_1$.

Example 11. To see this, let us continue looking at Example 10. Recall, in Section 5.2, we gave an example of a three-balanced partition and an example of a partition that was not three-balanced.

Recall, the three-balanced partition was given by $S_1 = \{5, 7\}$, $S_2 = \{2\}$ and $S_3 = \{19\}$. Converting this to a vector, we have

$$\vec{w} = \begin{bmatrix} 1 \\ 2 \\ 1 \\ 0 \end{bmatrix}.$$

Since the first entry corresponds to 7 and it is contained in S_1, we place a 1 in the first entry. The third entry corresponds to 5, which is also in S_1, so we place a 1 in the third entry. The

second entry corresponds to the prime 2, which is in S_2, so it is labeled with a 2. Finally the last entry corresponds to the prime 19 which is in S_3 and therefore we have a 0 in the last vector entry. Since $\vec{w}$ corresponds to a three-balanced partition by Lemma 58 $\vec{w}$ should be in the kernel of $L(G)$ modulo 3. Verifying this we have

$$\begin{bmatrix} 0 & 2 & 2 & 2 \\ 0 & 0 & 0 & 0 \\ 2 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 4+2 \\ 0 \\ 2+1 \end{bmatrix}$$
$$\equiv \vec{0} \pmod 3 .$$

From $\vec{w}$, we can construct the corresponding element in $\mathrm{Sel}^{(\phi)}(E_{ab})$. The primes which correspond to entries with a 1 are the primes which divide u_1 and the primes that correspond to entries with a 2 are the primes which divide u_2. So the first and third entries of $\vec{w}$ contain a 1 and correspond to 7 and 5, hence, $u_1 = 5 \cdot 7$. The second entry of $\vec{w}$ contains a 2 and corresponds to 2, hence $u_2 = 2$. Therefore $u = u_1 u_2^2 = 5 \cdot 7(2^2)$ is a representative for the element $[u]$ in $\mathrm{Sel}^{(\phi)}(E_{ab})$.

Now, recall the partition which was not three-balanced was given by $S_1 = \{7\}$, $S_2 = \{2, 5\}$ and $S_3 = \{19\}$. Converting this to a vector, we have

$$\vec{v} = \begin{bmatrix} 1 \\ 2 \\ 2 \\ 0 \end{bmatrix} .$$

Since $\vec{v}$ does not corresponds to a three-balanced partition by Lemma 58 $\vec{v}$ should not be in

the kernel of $L(G)$ modulo 3. Verifying this we have

$$\begin{bmatrix} 0 & 2 & 2 & 2 \\ 0 & 0 & 0 & 0 \\ 2 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 2 \\ 0 \end{bmatrix} = \begin{bmatrix} 4+4 \\ 0 \\ 2+2 \end{bmatrix}$$
$$\not\equiv \vec{0} \pmod 3 .$$

Finally, we can easily calculate the rank of $L(G)$ which is 2 and since $L(G)$ is a 3×4 matrix, Corollary 59 implies that

$$\left|\mathrm{Sel}^{(\phi)}(E)\right| = 3^{4-2} = 3^2.$$

This is equal to the number of three-balanced partitions given in the corresponding graph theory example.

Corollary 60. *1. If $v_3(a) = 1$, then $\left|\mathrm{Sel}^{(\phi)}(E_{ab})\right| = 3^{n-s}$ where s is the rank of the $(r'+m) \times n$ matrix $L(G)$.*

2. If $v_3(a) \neq 1$, then $3^{n-s_1} \leq \left|\mathrm{Sel}^{(\phi)}(E_{ab})\right| \leq 3^{n-s}$ where s is the rank of the $(r'+m) \times n$ matrix $L(G)$ and s_1 is the rank of the $(r'+m-1) \times n$ matrix $L_3(G')$, with possible equality on the right.

5.3.1.2 The Family of Curves $\mathcal{E}_2$

Now we will assume that E_{ab} has the property that $3 \mid b$. Construct the matrix $L'(G')$ as before.

In this case, we know that 3 is one of the primes p_i with $1 \leq i \leq t$. Let $\overline{L(G')}$ be the $(r'+m-1) \times t'$ submatrix of $L'(G')$ with the $\log_\omega(\ell(3,-))$ row removed. Define $L_3(G)$ to

be the $(r'+m-1)\times n$ submatrix of $\overline{L(G')}$ with the $n+1$ to t' columns removed.

Remark 9. Notice that $\ker L_3(G) = \left\{\vec{w} : (w,0,\ldots,0)^T \in \ker \overline{L(G')}\right\}$.

Recall given $\vec{w} = (w_1, w_2, \ldots, w_n)^T \in \mathbb{F}_3^n$, for each $\vec{w}$, we associate subsets as follows:

$$S_1 = \{p_i : w_i = 1\},$$

$$S_2 = \{p_i : w_i = 2\},$$

and

$$S_3 = \{p_i : w_i = 0\} \cup \{p_{n+1}, \ldots, p_{t'}\}.$$

Lemma 61. *1. If $v_3(a) = 0$, then the partition (S_1, S_2, S_3) corresponding to the vector $\vec{w}$ is three-balanced if and only if $\vec{w} \in \ker L(G)$.*

2. If $v_3(a) = 1$, then the partition (S_1, S_2, S_3) corresponding to the vector $\vec{w}$ is three-quasi-balanced at 3 if and only if one of the following holds:

(a) $p_i = 3$ is in only one S_j and $\vec{w} \in \ker L(G)$

(b) $p_i = 3$ is in only one S_j, $\vec{w} \in \ker L_3(G)$ and there exists $s_1, s_2 \in \{\pm 1\}$ such that

$$2a \equiv s_1 \left(\prod_{\substack{p_i \in S_1 \\ p_i | 2b}} p_i \right) + s_2 \left(\prod_{\substack{p_j \in S_2 \\ p_j | 2b}} p_j \right) + s_1 s_2 \left(\prod_{\substack{p_k \in S_3 \\ p_k | 2b}} p_k \right) \pmod 9.$$

(c) $p_i = 3$ is in two S_j's and $\vec{w} \in \ker L(G_E)$.

3. If $v_3(a) = 2$, then the partition (S_1, S_2, S_3) corresponding to the vector $\vec{w}$ is three-quasi-balanced at 9 if and only if one of the following holds:

(a) if $v_3(b) = 2$, $p_i = 3$ is in S_3 only then $\vec{w} \in \ker L(G)$

(b) if $v_3(b) \neq 2$ or $p_i = 3$ is in more than one S_j then $\vec{w} \in \ker L_3(G)$.

Proof. First assume that $v_2(b) < 2$, then 2 is one of the primes $p_1, \ldots, p_r$ and $p'_r = p_r$. Next assume that $p_i \in S_1$ for $1 \leq i \leq l$. So there is only one copy of p_i. It is enough to show that $L'(G')\vec{w}' = \vec{0}$ with $\vec{w}' = (w_1, \ldots, w_{t'})^T = (\vec{w}, 0, \ldots, 0)^T$. Then

$$\begin{aligned}
\left(L'(G')\vec{w}'\right)_i &= \sum_{\substack{j=1 \\ p_j \neq p_i}}^{t'} \log_\omega\left(\ell\left(p_i, p_j\right)\right) w_j - \sum_{\substack{j=1 \\ p_j \neq p_i}}^{t'} \log_\omega\left(\ell\left(p_i, p_j\right)\right) w_i \\
&= \sum_{\substack{j=1 \\ p_j \neq p_i}}^{t'} \log_\omega\left(\ell\left(p_i, p_j\right)\right)\left(w_j - w_i\right) \\
&= \sum_{w_j=2} \log_\omega\left(\ell\left(p_i, p_j\right)\right) + \sum_{w_j=0} 2\log_\omega\left(\ell\left(p_i, p_j\right)\right).
\end{aligned}$$

This is equivalent to zero modulo 3 if and only if

$$\left(\prod_{p_j \in S_2} \ell\left(p_i, p_j\right)\right)\left(\prod_{p_k \in S_3} \ell\left(p_i, p_k\right)^2\right) = 1.$$

The cases that $p_i \in S_2$ and $p_i \in S_3$ with $1 \leq i \leq l$ are identical.

Now assume $p_i \in S_1$ with $l+1 \leq i \leq r$. So we know that p_i appears in more than one S_j. Then

$$\begin{aligned}
\left(L'(G')\vec{w}'\right)_i &= \sum_{\substack{j=1 \\ p_j \neq p_i}}^{t'} \log_\omega\left(\ell\left(p_i, p_j\right)\right) w_j + \sum_{\substack{j=1 \\ p_j \neq p_i}}^{t'} \log_\omega\left(\ell\left(p_i, p_j\right)\right) w_i \\
&= \sum_{\substack{j=1 \\ p_j \neq p_i}}^{t'} \log_\omega\left(\ell\left(p_i, p_j\right)\right)\left(w_j + w_i\right) \\
&= \sum_{w_j=0} \log_\omega\left(\ell\left(p_i, p_j\right)\right) + \sum_{w_j=1} 2\log_\omega\left(\ell\left(p_i, p_j\right)\right).
\end{aligned}$$

This is equivalent to zero modulo 3 if and only if

$$\left(\prod_{\substack{p_j \in S_3 \\ p_j \neq p_i}} \ell\left(p_i, p_j\right)\right)\left(\prod_{\substack{p_k \in S_1 \\ p_k \neq p_i}} \ell\left(p_i, p_k\right)^2\right) = 1.$$

Once again, the cases that $p_i \in S_2$ and $p_i \in S_3$ follow in a similar manner.

Now assume that $v_2(b) = 2$. Then we know that 2 is not one of the primes $p_1, \ldots, p_n$ and $p_{r'} = 2$. So we have that

$$\begin{aligned}\left(L'(G')\vec{w}'\right)_{r'} &= \sum_{\substack{j=1 \\ p_j \neq 2}}^{t'} \log_\omega\left(\ell\left(2, p_j\right)\right) w_j \\ &= \sum_{w_j=1} \log_\omega\left(\ell\left(2, p_j\right)\right) + \sum_{w_j=2} 2\log_\omega\left(\ell\left(2, p_j\right)\right).\end{aligned}$$

This is equivalent to zero modulo 3 if and only if

$$\left(\prod_{p_j \in S_1} \ell\left(2, p_j\right)\right)\left(\prod_{p_k \in S_2} \ell\left(2, p_k\right)^2\right) = 1.$$

Finally, consider rows i with i between $r' + 1$ and $r' + m$. Then we have that

$$\begin{aligned}\left(L'(G')\vec{w}'\right)_i &= \sum_{j=1}^{t'} \log_\omega\left(\ell\left(q_{i-r'}, p_j\right)\right) w_j \\ &= \sum_{w_j=1} \log_\omega\left(\ell\left(q_{i-r'}, p_j\right)\right) + \sum_{w_j=2} 2\log_\omega\left(\ell\left(q_{i-r'}, p_j\right)\right).\end{aligned}$$

This is equivalent to zero modulo 3 if and only if

$$\left(\prod_{p_j \in S_1} \ell\left(q_{i-r'}, p_j\right)\right)\left(\prod_{p_k \in S_2} \ell\left(q_{i-r'}, p_k\right)^2\right) = 1.$$

If $v_3(a) = 0$, then we are done.

In the case that $v_3(a) = 1$, we need to reexamine the $\log_\omega(\ell(3,-))$ row of $L(G)$. If 3 is in only one S_j and

$$\begin{aligned}(L(G)\vec{w})_i &= \sum_{j=1}^{t'} \log_\omega(\ell(q_m, p_j))\, v_j \\ &= \sum_{w_j=1} \log_\omega(\ell(q_m, p_j)) + \sum_{w_j=2} 2\log_\omega(\ell(q_m, p_j)) \\ &\not\equiv 0 \pmod 3,\end{aligned}$$

then look at $L_3(G)$. And if there exists $s_1, s_2 \in \{\pm 1\}$ such that $2a \equiv s_1 \left(\prod_{\substack{p_i \in S_1 \\ p_i | 2b}} p_i\right) + s_2 \left(\prod_{\substack{p_j \in S_2 \\ p_j | 2b}} p_j\right) + s_1 s_2 \left(\prod_{\substack{p_k \in S_3 \\ p_k | 2b}} p_k\right) \pmod{27}$ then we know by Proposition 43, there exists a solution to the equation. Otherwise we do not have a solution.

Finally, in the case that $v_3(a) = 2$, we also need to reexamine the $\log_\omega(\ell(3,-))$ row of $L(G)$. If either $v_3(b) \neq 2$ or 3 is in more than one S_j, then look at $L_3(G)$. The argument is exactly the same as the one used for $L(G)$ except for the last row since it has been removed.

□

Corollary 62. *1. If $v_3(a) = 0$, the number of three-balanced partitions of G is 3^{n-s} where s is the rank of the $(r'+m) \times n$ matrix $L(G)$.*

2. If $v_3(a) > 0$, then the number of three-quasi-balanced partitions at 3 of G is between 3^{n-s_1} and 3^{n-s} where s is the rank of the $(r'+m) \times n$ matrix $L(G)$ and s_1 is the rank of the $(r'+m-1) \times n$ matrix $L_3(G)$.

Using the results of Lemma 61 and Corollary 62, we can calculate the cardinality of $\mathrm{Sel}^{(\phi)}(E_{ab})$ for the family of elliptic curves $\mathcal{E}_2$.

Corollary 63. *1. If $v_3(a) = 0$, then $\left|\text{Sel}^{(\phi)}(E_{ab})\right| = 3^{n-s}$ where s is the rank of the $(r'+m) \times n$ matrix $L(G)$.*

2. If $v_3(a) > 0$, then $3^{n-s_1} \leq \left|\text{Sel}^{(\phi)}(E_{ab})\right| \leq 3^{n-s}$ where s is the rank of the $(r'+m) \times n$ matrix $L(G)$ and s_1 is the rank of the $(r'+m-1) \times n$ matrix $L_3(G)$, with possible equality on the right.

5.3.2 The Auxiliary Curve $E'_{ab'}$

Consider a graph G'' with vertex set $V(G'')$ and subgraphs G' and G with vertex sets $V(G')$ and $V(G)$ respectively, as defined in the previous section. Once again, we want to construct a characteristic matrix to relate the graph theory problem to a linear algebra problem.

We will index the rows and columns of the characteristic matrix by primes and we begin by ordering the primes which will correspond to the columns of the characteristic matrix. Let $\pi_1, \overline{\pi_1}, \ldots, \pi_{n/2}, \overline{\pi_{n/2}}$ be the $n/2$ distinct primes equivalent to 1 modulo 3 which divide $2b'$. Let $\pi_{n/2+1}, \overline{\pi_{n/2+1}}, \ldots, \pi_{(l-n-1)/2}, \overline{\pi_{(l-n-1)/2}}$ be the second copy of $(l-n-1)/2$ primes equivalent to 1 modulo 3 which divide $2b'$. Next, let $p_{l+1}, \ldots, p_t$ be all copies of primes not equivalent to 1 modulo 3 which divide $2b'$. Finally, we will also need $p_{t+1} = \sqrt{-3}$. Note that for each prime equivalent to 1 modulo 3, it splits as $\pi\overline{\pi}$ with $\pi \equiv 2 \pmod 3$ and π in the upper half plane.

Next, we will order the primes which will correspond to the rows of the characteristic matrix. Let $q_1, \ldots, q_\nu$ be the distinct primes equivalent to 1 modulo 3 which divide $2b'$ exactly once and divide $\Delta' = 27b' + 12a^3$. Let $q_{\nu+1}, \ldots, q_m$ be the distinct primes equivalent to 1 modulo 3 which divide $2b'$ exactly twice and divide Δ'. Next, let $q_{m+1}, \ldots, q_l$ be the distinct primes equivalent to 1 modulo 3 which divide Δ', but do not divide $2b'$. Finally, let $q_{l+1}, \ldots, q_r$ be the distinct primes equivalent to 2 modulo 3, not including 2, which divide

Δ'.

Now we are ready to define the $r \times (t+1)$ matrix, $A(G'')$. Define the entries of $A(G'')$ by

$$a_{ij} = \begin{cases} \log_\omega(\ell(q_i, p_j)) & 1 \leq i \leq m, 1 \leq j \leq t+1, q_i \neq p_j \\ \log_\omega(\ell(q_i, p_j)) & m+1 \leq i \leq r, 1 \leq j \leq l, q_i \neq p_j \\ 0 & \text{otherwise.} \end{cases}$$

Again, note that for $1 \leq j \leq l$, when we say $\ell(q_i, p_j)$, we mean $\ell(q_i, \pi_j)$ and $\ell(q_i, \overline{\pi_j})$ Let $D(G'')$ be the $r \times (t+1)$ diagonal matrix with entries

$$d_{ij} = \begin{cases} \sum_{k=0}^{t+1} a_{ik} & 1 \leq i \leq \nu, i = j \\ -\sum_{k=0}^{t+1} a_{ik} & \nu+1 \leq i \leq m, i = j \\ 0 & \text{otherwise} \end{cases}$$

reduced modulo 3. Let

$$L'(G'') = A(G'') - D(G'')$$

again reduced modulo 3 and define $L(G'')$ to be the $r \times n$ submatrix of $L'(G'')$ with the $n+1$ through $t+1$ columns removed.

Remark 10. Notice that $\ker L(G'') = \left\{ \vec{w} : (\vec{w}, 0, \ldots, 0)^T \in \ker L'(G'') \right\}$.

Let $\vec{w} = (w_1, \ldots, w_n)^T \in \mathbb{F}_3^n$. Recall there are $n/2$ distinct prime equivalent to 1 modulo 3 which divide $2b'$, denoted by $p_1, p_3, \ldots, p_n$. For $1 \leq i \leq n$, let

$$S_1 = \{p_i : w_i = 1\}$$

$$S_2 = \{p_i : w_i = 2\}$$

and

$$S_3 = \{p_i : w_i = 0\} \cup \{p_{n+1}, \ldots, p_{t+1}\}.$$

Define the labeling $\mathcal{L}$ on $V(G)$ by $\mathcal{L}(p_i) = w_i$. Then we have the following lemma.

Lemma 64. *The labeling $\mathcal{L}$ of $V(G)$ corresponding to $\vec{w}$ is good if and only if $\vec{w} \in \ker L(G'')$ and $\vec{w}$ satisfies the fact that for each i odd, $1 \leq i \leq n$, $w_i + w_{i+1} \equiv 0 \pmod 3$.*

Proof. We begin by observing the additional condition guarantees that if $\pi \mid u_i$ $i = 1, 2$, then $\overline{\pi} \nmid u_i$.

Without loss of generality, assume $w_i = 1$ for $1 \leq i \leq \nu$. So there is only one copy of p_i which divides $2b'$. It is enough to show that $L'(G'')\vec{w}' = \vec{0}$ with $\vec{w}' = (w_1, \ldots, w_{t'})^T = (\vec{w}, 0, \ldots, 0)^T$. Then

$$\begin{aligned} L'(G'')\vec{w} &= \sum_{\substack{j=1 \\ p_j \neq q_i}}^{t+1} \log_\omega \left(\ell\left(q_i, p_j\right)\right) w_j - \sum_{\substack{j=1 \\ p_j \neq q_i}}^{t+1} \log_\omega \left(\ell\left(q_i, p_j\right)\right) w_i \\ &= \sum_{\substack{j=1 \\ p_j \neq q_i}}^{t+1} \log_\omega \left(\ell\left(q_i, p_j\right)\right) \left(w_j - w_i\right) \\ &= \sum_{w_j = 2} \log_\omega \left(\ell\left(q_i, p_j\right)\right) + \sum_{w_j = 0} 2 \log_\omega \left(\ell\left(q_i, p_j\right)\right). \end{aligned}$$

This is equivalent to zero modulo 3 if and only if

$$\left(\prod_{\substack{p \in S_1 \\ p = \eta\overline{\eta}}} \ell(q_i, \overline{\eta})\right) \left(\prod_{\substack{p \in S_2 \\ p = \eta\overline{\eta}}} \ell(q_i, \eta)\right) \left(\prod_{\substack{p \in V(G'') \setminus (S_1 \cup S_2) \\ p \mid 2b'\sqrt{-3}}} \ell(p, q)^2\right) = 1.$$

The cases that $w_i = 2$ and $w_i = 0$ are identical.

Now assume $w_i = 1$ for $\nu + 1 \leq i \leq m$. So there are two copies of p_i which divide $2b'$. Once again, it is enough to show that $L'(G'')\vec{w}' = \vec{0}$ with $\vec{w}' = (w_1, \ldots, w_{t'})^T = (\vec{w}, 0, \ldots, 0)^T$.

Then

$$\begin{aligned}
\left(L'(G'')\vec{w}'\right)_i &= \sum_{\substack{j=1\\ p_j\neq q_i}}^{t+1} \log_\omega\left(\ell\left(q_i,p_j\right)\right) w_j + \sum_{\substack{j=1\\ p_j\neq q_i}}^{t+1} \log_\omega\left(\ell\left(q_i,p_j\right)\right) w_i \\
&= \sum_{\substack{j=1\\ p_j\neq q_i}}^{t+1} \log_\omega\left(\ell\left(q_i,p_j\right)\right)\left(w_j+w_i\right) \\
&= \sum_{w_j=0} \log_\omega\left(\ell\left(q_i,p_j\right)\right) + \sum_{w_j=1} 2\log_\omega\left(\ell\left(q_i,p_j\right)\right).
\end{aligned}$$

This is equivalent to zero modulo 3 if and only if

$$\left(\prod_{\substack{p\in S_1\setminus\{q_i\}\\ p=\eta\overline{\eta}}} \ell(q,\eta)\right)\left(\prod_{\substack{p\in S_2\\ p=\eta\overline{\eta}}} \ell(q_i,\overline{\eta})\right)\left(\prod_{\substack{p\in V(G'')\setminus(S_1\cup S_2\cup\{q_i\})\\ p|2b'\sqrt{-3}}} \ell(q_i,p)^2\right)=1.$$

The cases that $w_i = 2$ and $w_i = 0$ are identical.

Finally, consider rows i with $m+1 \leq i \leq r$. Then we have that

$$\begin{aligned}
\left(L'(G'')\vec{w}'\right)_i &= \sum_{j=1}^{t+1} \log_\omega\left(\ell\left(q_i,p_j\right)\right) w_j \\
&= \sum_{w_j=1} \log_\omega\left(\ell\left(q_i,p_j\right)\right) + \sum_{w_j=2} 2\log_\omega\left(\ell\left(q_i,p_j\right)\right).
\end{aligned}$$

This is equivalent to zero modulo 3 if and only if

$$\left(\prod_{\substack{p\in S_1\\ p=\pi\overline{\pi}}} \ell(q_i,\pi)\ell(q_i,\overline{\pi})^2\right)\left(\prod_{\substack{p\in S_2\\ p=\pi\overline{\pi}}} \ell(q_i,\overline{\pi})\ell(q_i,\pi)^2\right)=1.$$

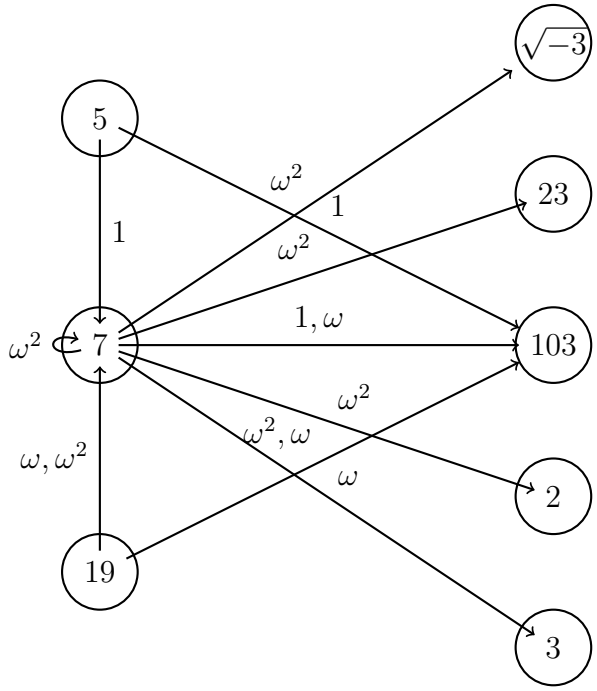
□

Example 12. Let us return to the example used in the previous section. Recall we considered

the elliptic curve

$$E : y^2 = x^3 - 3(3 \cdot 7 + 3 \cdot 7 \cdot 23 \cdot 103$$

where $\Delta' = 7 \cdot 5 \cdot 19$. The vertices of G' are $\{5, 19, 7, 103\}$ and the vertices of G'' are $\{2, 3, 23, \sqrt{-3}, 5, 19, 7, 103\}$. Recall the corresponding graph given below.



When constructing the matrix A, we order the primes corresponding to the columns in the following order $2 + \sqrt{-3}, 2 - \sqrt{-3}, 10 + \sqrt{-3}, 10 - \sqrt{-3}, 2, 3, 23, \sqrt{-3}$. The primes corresponding to the rows are ordered as 7, 5, 19. It turns out that in this simple example, the matrix $D(G'')$ is just the zero matrix. So the matrix A and $L'(G'')$ are the same and given by

$$A = L'(G'') = \begin{bmatrix} 0 & 2 & 0 & 1 & 2 & 1 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 2 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

The matrix $L(G'')$ is formed by removing the columns which correspond to the primes

$2, 3, 23, \sqrt{-3}$ and is given by

$$L(G'') = \begin{bmatrix} 0 & 2 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 2 & 2 & 1 \end{bmatrix}.$$

Corollary 65. *The number of good labellings of $V(G)$ is at most $3^{n/2-s}$ where s is the rank of the $r \times n$ matrix $L(G)$.*

By calculating the cardinality of the modified Selmer group $\mathrm{Sel}_{\mathcal{S}}^{(\hat{\phi})}(E'_{ab'})$ through the results stated in Lemma 64 and Corollary 65, we can give an upper bound on the size of the Selmer group $\mathrm{Sel}^{(\hat{\phi})}(E'_{ab'})$.

Corollary 66. $\left|\mathrm{Sel}^{(\hat{\phi})}(E'_{ab'})\right| \leq \left|\mathrm{Sel}_{\mathcal{S}}^{(\hat{\phi})}(E'_{ab'})\right| \leq 3^{n/2-s}$, *where s is the rank of the $r \times n$ matrix $L(G)$ and $\mathcal{S} = \{2, 3\}$.*

Example 13. Returning to the previous example, we can see that the rank of $L(G'')$ is 2 and since $L(G'')$ is a 3×4 matrix, Corollaries 65 and 66 imply that

$$\left|\mathrm{Sel}^{(\hat{\phi})}(E'_{ab'})\right| \leq \left|\mathrm{Sel}_{\mathcal{S}}^{(\hat{\phi})}(E'_{ab'})\right| = 3^{2-2} = 1.$$

This is equal to the number of good partitions given in the corresponding graph theory example.

5.4 Conclusion

Let $L_1(G)$ and $L_{3_1}(G')$ be the matrices defined in Section 5.3.1.1. Similarly, let $L_2(G)$ and $L_{3_2}(G)$ be the matrices defined in Section 5.3.1.2. Finally, let $L(G)$ be the matrix defined in Section 5.3.2. Then combining Corollaries 60, 63 and 66 we obtain the following results:

Theorem 67. *1. If $3 \nmid b$ and $v_3(a) = 0$, then*

$$r \leq n_1 + n_2/2 - s_1 - s - 1$$

where s_1 is the rank of the $(r_1' + m_1) \times n_1$ matrix $L_1(G)$, s is the rank of the $r_2 \times n_2$ matrix $L(G)$ and r is the rank of E_{ab}.

2. If $3 \nmid b$ and $v_3(a) > 0$, then

$$r \leq R_1 + R_2 - 1$$

where

$$n_1 + n_2/2 - s_2 - s \leq R_1 + R_2 \leq n_1 + n_2/2 - s_1 - s$$

and s_1 is the rank of the $(r_1' + m_1) \times n_1$ matrix $L_1(G)$, s_2 is the rank of the $(r_1' + m_1 - 1) \times n_2$ matrix $L_{3_1}(G')$, s is the rank of the $r_2 \times n_2$ matrix $L(G)$ and r is the rank of E_{ab}.

3. If $3 \mid b$ and $v_3(a) = 1$, then

$$r \leq n_1 + n_2/2 - s_1 - s - 1$$

where s_1 is the rank of the $(r_1' + m_1) \times n_1$ matrix $L_2(G)$, s is the rank of the $r_2 \times n_2$ matrix $L(G)$ and r is the rank of E_{ab}.

4. If $3 \mid b$ and $v_3(a) \neq 1$, then

$$r \leq R_1 + R_2 - 1$$

where

$$n_1 + n_2/2 - s_2 - s \leq R_1 + R_2 \leq n_1 + n_2/2 - s_1 - s$$

where s_1 is the rank of the $(r_1' + m_1) \times n_1$ matrix $L_2(G)$, s_2 is the rank of the $(r_1' + m_1 - 1) \times n$ matrix $L_{3_2}(G)$, s is the rank of the $r_2 \times n_2$ matrix $L(G)$ and r is the rank of E_{ab}.

Remark 11. Once one has computed $\mathrm{Sel}_S^{(\hat{\phi})}(E'_{ab'})$ using linear algebra, applying Propositions 49 and 50 to the elements of $\mathrm{Sel}_S^{(\hat{\phi})}(E'_{ab'})$, one can compute $\mathrm{Sel}^{(\widehat{\phi})}(E'_{ab'})$.

Chapter 6

Introduction to Drinfeld Modules

In 1973, Vladimir Drinfeld invented elliptic modules commonly referred to as Drinfeld modules. The following year he produced a proof of Langland's conjectures for GL_2 over a global function field of positive characteristic. Langland's conjecture for function fields roughly states that there exists a bijection between cuspidal automorphic representations of GL_n and certain representations of a Galois group. Drinfeld used these modules in his proofs of these conjectures. Continued research enabled Drinfeld to generalize Drinfeld modules to shtukas, which allowed him to fully prove Langland's conjecture for GL_2. In 1990, Drinfeld was awarded the Fields Medal for his work.

6.1 Brief Overview of Drinfeld Modules

In order to understand Drinfeld modules, we need to set-up some notation. Here, we will give a general set-up, which we will specialize later. Let X be a smooth, projective geometrically connected curve over the finite field $\mathbb{F}_q$. Let $P_\infty \in X$ be a fixed closed rational point over $\mathbb{F}_q$. Set k to be the function field of X and $\mathbb{A} \subset k$ to be the ring of functions which are regular outside P_∞. Let v_∞ be the valuation associated to the point P_∞ and let

$K = k_\infty$ be the completion of k with respect to v_∞. Let $\overline{K}$ be a fixed algebraic closure of K and $\mathbb{C}_\infty$ be the completion of $\overline{K}$. This comes from the canonical extension of v_∞ to $\overline{K}$. Define τ to be the q^{th} power mapping, i.e. $\tau^i(x) := x^{q^i}$. Let M be a complete extension of K contained in $\mathbb{C}_\infty$. Then $M\{\tau\}$ is the composition ring of Frobenius polynomials in τ.

6.1.1 Properties of $M\{\tau\}$

The following is a concise overview of properties of $M\{\tau\}$. For a more thorough explanation, the reader should refer to [37].

It can be shown that $\tau^i(x)$ is an additive polynomial for all i and hence all polynomials spanned by τ^i are additive. Using properties of additive polynomials, we have that $M\{\tau\}$ forms a ring under composition. Since $M \neq \mathbb{F}_q$, q a power of p, it follows that $M\{\tau\}$ is not commutative, however

$$\tau\alpha = \alpha^q\tau \quad \forall\ \alpha \in M.$$

In addition, due to the fact that M is a field of characteristic p, it can be shown that the set of absolutely additive polynomials over M is $M\{\tau\}$.

Remark 12.

1. If $P(x)$ is additive, then $P(\tau)$ will denote its representation in $M\{\tau\}$. Similarly, if $P(x)$ is $\mathbb{F}_q$-linear, then $P(\tau)$ is its representation in $M\{\tau\}$. It is important to note that $P(\tau)$ is not obtained from $P(x)$ by substituting τ in for x.

2. The multiplication, $P(\tau) \cdot Q(\tau)$, will refer to multiplication in $M\{\tau\}$.

3. $P(\tau)$ is monic if and only if $P(x)$ is monic.

4. Let $P(\tau) = \sum_{i=0}^{t} \alpha_i \tau^i$ with $\alpha_t \neq 0$. Set $t = \deg(P(\tau))$. Then

$$q^t = \deg(P(x)).$$

The following theorem demonstrates the relationship between $M[x]$ and $M\{\tau\}$. A proof can be found in [37, Theorem 1.4.1] or [54].

Theorem 68. *Let $f(x) \in M[x]$. Then there exists $g(\tau) \in M\{\tau\}$ such that $f(x)$ divides $g(x)$.*

With some work, it can be shown that the set of all $g(\tau)$ satisfying the condition of the theorem forms a left ideal in $M\{\tau\}$.

Next, we will briefly discuss the left and right division algorithms for $M\{\tau\}$. Let $\{f(\tau), g(\tau)\} \subset M\{\tau\}$. Notice that $f(\tau) \cdot g(\tau) = 0$ in $M\{\tau\}$ implies that $f(\tau)$ or $g(\tau)$ must be 0. Therefore multiplication in $M\{\tau\}$ has both left and right cancellation properties.

Definition 25. 1. $f(\tau)$ is **right divisible** by $g(\tau)$ if there exists $h(\tau) \in M\{\tau\}$ such that

$$f(\tau) = h(\tau) \cdot g(\tau).$$

2. $f(\tau)$ is **left divisible** by $g(\tau)$ if there exists $m(\tau) \in M\{\tau\}$ such that

$$f(\tau) = g(\tau) \cdot m(\tau).$$

We can see that if $f(\tau)$ is right divisible by $g(\tau)$ then $g(x)$ divides $f(x)$.

The following proposition is the right division algorithm in $M\{\tau\}$.

Proposition 69. *Let $\{f(\tau), g(\tau)\} \subset M\{\tau\}$ with $g(\tau) \neq 0$. Then there exists $\{h(\tau), r(\tau)\} \subset M\{\tau\}$ with $\deg(r(\tau)) < \deg(g(\tau))$ such that*

$$f(\tau) = h(\tau) \cdot g(\tau) + r(\tau).$$

Moreover, $h(\tau)$ and $r(\tau)$ are uniquely determined.

The proof follows in the same fashion as the classical division algorithm.

Now that we have a right division algorithm, the following corollary gives us an important property about left ideals in $M\{\tau\}$.

Corollary 70. *Every left ideal of $M\{\tau\}$ is principal.*

A proof can be found in [37, Corollary 1.6.3].

To state the left division algorithm, we need the following definition.

Definition 26. M is **perfect** if and only if $\tau M = M$.

Since τ has trivial kernel, a counting argument can be used to show that all finite fields are perfect. Furthermore, every algebraically closed field is perfect. It can be shown that every finite extension of a perfect field is separable. Now we can define the left division algorithm on $M\{\tau\}$ with an additional assumption on M.

Proposition 71. *Let M be perfect and let $\{f(\tau), g(\tau)\} \subset M\{\tau\}$ with $g(\tau) \neq 0$. Then there exists $\{h(\tau), r(\tau)\} \subset M\{\tau\}$ with $\deg(r(\tau)) < \deg(g(\tau))$ such that*

$$f(\tau) = g(\tau) \cdot h(\tau) + r(\tau).$$

Furthermore, $h(\tau)$ and $r(\tau)$ are uniquely determined.

The left division algorithm leads to the following corollary concerning right ideals.

Corollary 72. *If M is perfect, then every right ideal of $M\{\tau\}$ is principal.*

Using the Euclidean Algorithm we can compute the right greatest common divisor of $f(\tau)$ and $g(\tau)$. It is defined as the monic generator of the left ideal generated by $f(\tau)$ and $g(\tau)$. We will denote it as $(f(\tau), g(\tau))$. This leads us to the final lemma we will discuss about $M\{\tau\}$.

Lemma 73. *Let $h(\tau) = (f(\tau), g(\tau))$. Then $h(x)$ is the greatest common divisor of $f(x)$ and $g(x)$.*

A discussion concerning Proposition 71, Corollary 72 and Lemma 73 can be found in [37, pp 12-14].

6.1.2 Background Definitions and Theorems

To state the general definition of a Drinfeld module, we will present the following definitions and theorem. For further details, the reader should refer to [37, 66].

Recall $\mathbb{A} \subset K$ is the ring of functions which are regular outside P_∞.

Definition 27. An $\mathbb{A}$-submodule $L \subset \mathbb{C}_\infty$ (with the usual multiplication of $\mathbb{A}$) is called an M**-lattice** (or lattice) if and only if

1. L is finitely generated as an $\mathbb{A}$-module,
2. L is discrete in the topology of $\mathbb{C}_\infty$,
3. Let $M^{\text{sep}} \subseteq \mathbb{C}_\infty$ be the separable closure of M. Then L is contained in M^{sep} and is stable under $\text{Gal}(M^{\text{sep}}/M)$.

The rank of L is its rank as a finitely generated torsion-free submodule of $\mathbb{C}_\infty$. Define $d := \text{rank}_{\mathbb{A}}(L)$.

Definition 28. Let L be an M-lattice. Then set

$$e_L(x) = x \prod_{\substack{\alpha \in L \\ \alpha \neq 0}} (1 - x/\alpha).$$

Drinfeld proved the following result, which is fundamental to the theory behind Drinfeld modules.

Theorem 74. *Let* $0 \neq a \in \mathbb{A}$. *Then*

$$e_L(ax) = a e_L(x) \prod_{0 \neq \alpha \in a^{-1}L/L} \left(1 - e_L(x)/e_L(\alpha)\right).$$

We shall not go through the proof here (see [37, Theorem 4.3.1]), however, it leads us to the following definition.

Definition 29. Let $0 \neq a \in \mathbb{A}$. Then define

$$\phi_a := ax \prod_{0 \neq \alpha \in a^{-1}L/L} (1 - x/e_L(\alpha)) .$$

From the proof of Theorem 74, we can conclude that $\phi_a \in M\{\tau\}$. With some work, it can be shown that $\deg(\phi_a(\tau)) = d \cdot \deg(a)$ where $d = \text{rank}(L)$. For $a \in \mathbb{A}$, the mapping $a \mapsto \phi_a$ is $\mathbb{F}_q$-linear. Also, if $a \in \mathbb{F}_q \subset \mathbb{A}$, then $\phi_a = a\tau^0$. Finally,

$$\phi_{ab}(\tau) = \phi_a(\tau)\phi_b(\tau) = \phi_b(\tau)\phi_a(\tau) = \phi_{ba}(\tau).$$

This last property is not obvious since multiplication in $M\{\tau\}$ is not commutative.

6.1.3 Definition of a Drinfeld Module

Now we are ready to define a Drinfeld module.

Definition 30. The injection which maps $\mathbb{A}$ into $M\{\tau\}$ by $a \mapsto \phi_a$, associated to L is called the **Drinfeld module** associated to L. Its rank is $d = \text{rank}_{\mathbb{A}}(L)$.

We can actually give a more general definition of a Drinfeld module. For this, we will use the following definitions.

Definition 31. An **$\mathbb{A}$-field**, $\mathcal{F}$, is a field equipped with a fixed morphism $\iota : \mathbb{A} \to \mathcal{F}$. Define the characteristic of $\mathcal{F}$, $\wp$, to be the kernel of ι which is a prime ideal. We say $\mathcal{F}$ has **generic characteristic** if and only if $\wp = (0)$; otherwise we say that $\wp$ is finite and $\mathcal{F}$ has **finite characteristic**.

Over $\mathcal{F}$ we have the ring $\mathcal{F}\{\tau\}$. Let

$$f(\tau) = \sum_{i=0}^{v} a_i \tau^i \in \mathcal{F}\{\tau\}.$$

Set

$$Df := a_0 = f'(\tau).$$

Then the mapping from $\mathcal{F}\{\tau\}$ to $\mathcal{F}$ defined by $f \mapsto Df$ is a morphism of $\mathbb{F}_q$-algebras.

So an equivalent definition of a Drinfeld module is given by the following.

Definition 32. Let $\phi : \mathbb{A} \to \mathcal{F}\{\tau\}$ be a homomorphism of $\mathbb{F}_q$-algebras. Then ϕ is a **Drinfeld module** over $\mathcal{F}$ if and only if

1. $D \circ \phi = \iota$
2. For some $a \in \mathbb{A}$, $\phi_a \neq \iota(a)\tau^0$.

6.2 The Carlitz Module

Prior to Drinfeld's discovery, Leonard Carlitz discovered the Carlitz module in 1938. He used the Carlitz module to give an explicit construction of the class field theory of $\mathbb{F}_q(t)$. The Carlitz module is a dimension one rank one Drinfeld module. Here, we let $\mathbb{A} = \mathbb{F}_q[t]$ and $L = \mathbb{A}$, which implies that $k = \mathbb{F}_q(t)$. For $d \geq 0$, define

$$\mathbb{A}(d) = \{\alpha \in \mathbb{A} : \deg(\alpha) < d\}.$$

So $\mathbb{A}(d)$ is a d-dimensional $\mathbb{F}_q$-vector space of polynomials of degree less than d. And

$$\mathbb{A} = \bigcup \mathbb{A}(d).$$

In order to define the Carlitz modules, we need to introduce the Carlitz exponential. For additional details, the reader should refer to [37] and [69].

Definition 33. Set $e_0(x) = x$ and for $d > 0$,

$$\begin{aligned} e_d(x) &= \prod_{\alpha \in \mathbb{A}(d)} (x - \alpha) \\ &= \prod_{\alpha \in \mathbb{A}(d)} (x + \alpha). \end{aligned}$$

It is not difficult to show $e_d(x)$ is an $\mathbb{F}_q$-linear polynomial. Thus $e_d(\tau) \in \mathbb{A}\{\tau\}$.

Definition 34. 1. For $i > 0$, define

$$[i] := t^{q^i} - t.$$

2. Let $D_0 = 1$ and for $i > 0$, define

$$D_i = [i][i-1]^q \dots [1]^{q^{i-1}}.$$

3. Let $L_0 = 1$ and for $i > 0$, define

$$L_i = [i][i-1] \dots [1].$$

The numbers D_i and L_i have "factorial-like" properties associated to them as demonstrated by the following proposition.

Proposition 75. *1.* $[i] = \prod_{\substack{f \text{ monic polynomial} \\ \deg(f) | i}} f$

2. $D_i = [i] D_{i-1}^q = \prod_{\substack{g \text{ monic} \\ \deg(g) = i}} g$

3. $L_i = \text{lcm of all polynomials of degree } i$

The interested reader can find a proof in [37, Proposition 3.1.6].

The following theorem of Carlitz relates the numbers D_i and L_i to $e_d(x)$.

Theorem 76 (Carlitz)**.**

$$\begin{aligned} e_d(x) &= \prod_{\alpha \in \mathbb{A}(d)} (x - \alpha) \\ &= \sum_{i=0}^{d} (-1)^{d-i} x^{q^i} \frac{D_d}{D_i L_{d-i}^{q^i}}. \end{aligned}$$

Additional details pertaining to the proof can be found in [6, 37, 35]. Expanding $e_d(x)$, we find that $\dfrac{D_d}{D_i L_{d-i}^{q^i}} \in \mathbb{A}$, so the coefficients are integral.

To form the Carlitz exponential, divide $e_d(x)$ by

$$\prod_{0 \neq \alpha \in \mathbb{A}(d)} \alpha = (-1)^d \frac{D_d}{L_d}.$$

So we obtain,

$$x \prod_{0 \neq \alpha \in \mathbb{A}(d)} (1 + x/\alpha) = \sum_{j=0}^{d} (-1)^j \frac{x^{q^i}}{D_j} \frac{L_d}{L_{d-j}^{q^j}}.$$

Then taking the limit as d approaches infinity, we can define the **Carlitz exponential** as

$$e_C(x) = \sum_{j=0}^{\infty} \frac{x^{q^j}}{D_j}.$$

The following proposition and corollary demonstrate properties associated to the Carlitz exponential. For proofs, please see [37, Section 3.3].

Proposition 77. *Let $x \in \mathbb{C}_\infty$. Then*

$$e_C(tx) = t e_C(x) + e_C(x)^q$$

Corollary 78. *For $x \in \mathbb{C}_\infty$ and $a \in \mathbb{A}$ with $a = \sum_{j=0}^{v} a_j t^j$ where $a_j \in \mathbb{F}_q$ and $a_v \neq 0$ we have that*

$$e_C(ax) = ae_C(x) + \sum_{j=1}^{v} C_a^{(j)} e_C(x)^{q^j}$$

where $\{C_a^{(j)}\} \subset \mathbb{A}$ and $C_a^{(v)} = a_v$.

This leads us to the following definition.

Definition 35. Let $\{C_a^{(j)}\}$ be as in Corollary 78. Then, set

$$C_a(\tau) = a\tau^0 + \sum_{j=1}^{v} C_a^{(j)} \tau^j.$$

So,

$$e_C(ax) = C_a(e_C(x)).$$

Recall the q^{th} power mapping, $\tau : \mathbb{C}_\infty \to \mathbb{C}_\infty$ is defined by $\tau(x) = x^q$. And for any subfield M of $\mathbb{C}_\infty$, $M\{\tau\}$ is the composition ring of $\mathbb{F}_q$-linear polynomials.

Now, we will use $e_C(x)$ to describe the module action of $\mathbb{A} = \mathbb{F}_q[t]$ on $\mathbb{C}_\infty$.

Definition 36. The mapping $C : \mathbb{A} \to k\{\tau\}$ defined by $a \mapsto C_a$ which is an injection of $\mathbb{F}_q$-algebras is called the **Carlitz Module**.

As mentioned earlier, this is the simplest example of a Drinfeld module. The zeta function in characteristic p associated to the Carlitz module is the analogue to the classical zeta function. It is much easier to study the Carlitz module rather than a general Drinfeld module. However, due to its simplicity, properties associated to the Carlitz module often times do not translate to the general case. We will discuss a specific example of this concerning zeros of the zeta function in the next Chapter.

Chapter 7

Zeta Functions of Drinfeld Modules

In this chapter, we build a zeta function for Drinfeld modules by comparing it to L-series for elliptic curves. The first obstacle we incur involves exponentiating elements. When working over extensions of finite fields, raising elements to the p^{th} powers, it is the same as raising elements to the first power. In order to correct this issue, Goss defines a way to exponentiate over function fields in a specific way so we obtain a characteristic p output [37, 38]. The goal of this chapter is to introduce zeta functions over function fields and explore special values of these functions, known as special polynomials. Additionally, we will introduce a group which appears to act on the zeros of the special polynomials. Throughout the chapter, we will give concrete examples in order to demonstrate this action.

7.1 Background

We will begin with some standard notation to be used throughout this chapter. Let X be a smooth, geometrically connected curve over $\mathbb{F}_q$. Recall a smooth curve is a projective variety of dimension 1 with no singular points [39].

Let $\infty \in X$ be a fixed closed point (not necessarily rational) of degree d_∞ over $\mathbb{F}_q$.

When $d_\infty = 1$, everything behaves 'nicely'; otherwise we need to make adjustments. Let $\mathbb{A}$ be the ring of functions regular away from ∞. It is not hard to show that $\mathbb{A}$ is a Dedekind domain with finite class group where d_∞ divides the order of the class group. Therefore we can conclude that $\mathbb{A}^* \simeq \mathbb{F}_q^*$. In addition, let k be the quotient field of $\mathbb{A}$ and $K = k_\infty$ be completion of k at ∞. We represent the constants in k_∞ by $\mathbb{F}_\infty$ which is isomorphic to $\mathbb{F}_{q^{d_\infty}}$. Finally, let $\overline{K}$ be a fixed algebraic closure of K and $\mathbb{C}_\infty$ be the completion of $\overline{K}$.

The reader should keep the following basic analogies in mind:

$$\begin{aligned} \mathbb{A} &\sim \mathbb{Z} \\ k &\sim \mathbb{Q} \\ K &\sim \mathbb{R} \\ \mathbb{C}_\infty &\sim \mathbb{C}. \end{aligned}$$

Note that $\overline{K}$ is not locally compact or complete, so it is more convenient to use $\mathbb{C}_\infty$.

Example 14. In Chapter 6 Section 6.2, we defined the Carlitz Module which is a dimension one rank one Drinfeld module. Therefore X is the projective line, $\mathbb{P}^1$. We can set $\infty = \left(\frac{1}{t}\right)$, so $d_\infty = 1$. The ring of functions in the Carlitz module is $\mathbb{A} = \mathbb{F}_q[t]$ where $q = p^r$ and hence $k = \mathbb{F}_q(t)$ with constant field $\mathbb{F}_\infty = \mathbb{F}_q$. Therefore $K = \mathbb{F}_q\left(\left(\frac{1}{t}\right)\right)$ is a Laurent series in terms of $\frac{1}{t}$ with coefficients in $\mathbb{F}_q$.

The next example will be used throughout this chapter, so it is important for the reader to make note of the following specifications.

Example 15. In this example we consider a rank one dimension two Drinfeld module. In this case set $X = \mathbb{F}_3[t, \mathbf{y}]/(\mathbf{y}^2 - t + t^2)$ with $\infty = \frac{1}{t}$ and hence $d_\infty = 2$. The global ring is $\mathbb{A} = \mathbb{F}_3[t]\left[\sqrt{t - t^2}\right]$, with field of constants $\mathbb{F}_\infty = \mathbb{F}_9 = \mathbb{F}_3[\mathbf{y}]/(\mathbf{y}^2 + 1)$. Therefore

$k = \mathbb{F}_3(t)\left(\sqrt{t-t^2}\right)$ and

$$K = \mathbb{F}_3\left(\left(\frac{1}{t}\right)\right)\left(\left(\sqrt{\frac{1}{t}-\frac{1}{t^2}}\right)\right).$$

Since this example will be used throughout the chapter, we will provide more details than in the Carlitz Module. Additional details and proofs can be found in [69].

We define a valuation $v_\infty : \mathbb{F}_3(t) \to \mathbb{R} \cup \{\infty\}$ by $v_\infty(1/t) = 1$. We can extend this to k by defining $v_\infty\left(\frac{1}{\sqrt{t-t^2}}\right) = 1$. For all $\alpha \in \mathbb{A} \setminus \mathbb{F}_3$ with

$$\alpha = \sum_{i=0}^{k_1} a_i t^i + \sqrt{t-t^2}\sum_{j=0}^{k_2} b_j t^j$$

where $a_i, b_j \in \mathbb{F}_3$, we have

$$v_\infty(\alpha) = -\max\left\{k_1, k_2+1\right\}.$$

So for all non-constant elements in the ring, we know how to calculate its valuation. Also, we have that for all $a \in \mathbb{A}$,

$$\deg_k(a) = -d_\infty v_\infty(a) = -2v_\infty(a)$$

where $\deg_k(a)$ is the residue degree.

Now we return to the general theory. Choose $\pi \in k$ to be a uniformizer, i.e. $v_\infty(\pi) = 1$.

Definition 37. If $u \in K^*$ such that

$$v_\infty(u-1) > 0$$

or equivalently if

$$u \equiv 1 \mod \pi,$$

then we say that u is a 1-**unit**. Let U_1 be the set of 1-units in K.

Let $x \in K^*$, then we can write x as

$$x = \zeta_x \pi^{v_\infty(x)} u_x$$

where $\zeta_x \in \mathbb{F}_\infty^*$, $u_x \in U_1$.

Definition 38. We define the 1-unit part of x by

$$\langle x \rangle := \langle x \rangle_\pi := u_x.$$

Definition 39. An element x is **positive** or **monic** with respect to π if and only if $\zeta_x = 1$.

Remark 13. It is not hard to show that a positive element times another positive element produces a positive element. However, the sum of a finite number of positive elements is not necessarily positive.

Example 16. Let $\mathbb{A} = \mathbb{F}_q[t]$ and $\pi = \dfrac{1}{t}$. Then the positive elements in $\mathbb{A}$ are the monic polynomials.

In the above example of the Carlitz setting, everything is very simple. Therefore we will look at 1-units in the rank one dimension two Drinfeld module example.

Example 17. Let $\mathbb{A} = \mathbb{F}_3[t]\left[\sqrt{t - t^2}\right]$. Assume that $\pi = \dfrac{1}{t}$.

Recall that for any $\alpha \in \mathbb{A} \setminus \mathbb{F}_3$,

$$\alpha = \sum_{i=0}^{k_1} a_i t^i + \sqrt{t - t^2} \sum_{j=0}^{k_2} b_j t^j$$

and $\mathbf{y} = \sqrt{-1} \in \mathbb{F}_9$. There are three cases we need to consider.

Case 1: $k_1 > k_2 + 1$

In this case,

$$\langle\alpha\rangle_\pi = 1 + \sum_{i=0}^{k_1-1} a_{k_1}^{-1} a_i \left(\frac{1}{t}\right)^{k_1-i} + \sqrt{t-t^2} \sum_{j=0}^{k_2} a_{k_1}^{-1} b_j \left(\frac{1}{t}\right)^{k_1-j}.$$

Case 2: $k_1 < k_2 + 1$

Here,

$$\langle\alpha\rangle_\pi = \frac{2\mathbf{y}\sqrt{t-t^2}}{t} + \sum_{i=0}^{k_1} 2\mathbf{y} b_{k_2}^{-1} a_i \left(\frac{1}{t}\right)^{k_2+1-i} + \sqrt{t-t^2} \sum_{j=0}^{k_2-1} 2\mathbf{y} b_{k_2}^{-1} b_j \left(\frac{1}{t}\right)^{k_2+1-j}.$$

Case 3: $k_1 = k_2 + 1$

Finally,

$$\begin{aligned}\langle\alpha\rangle_\pi &= 2 + 2\sqrt{1+\frac{1}{t}} + a_{k_1} b_{k_2} \left(1 - \mathbf{y}\sqrt{1-\frac{1}{t}}\right) \\ &\quad + \sum_{i=0}^{k_1-1} a_i \left(a_{k_1} + b_{k_2}\mathbf{y}\right)^{-1} \left(\frac{1}{t}\right)^{k_1-i} + \sqrt{t-t^2} \sum_{j=0}^{k_2-1} b_j \left(a_{k_1} + b_{k_2}\mathbf{y}\right)^{-1} \left(\frac{1}{t}\right)^{k_1-j}.\end{aligned}$$

Let's look at two specific elements in $\mathbb{A}$ with $\pi = \frac{1}{t}$,

$$\begin{aligned}\alpha_1 &= t^2 + \sqrt{t-t^2} - 1 \\ \alpha_2 &= 2t^2 + 2\sqrt{t-t^2} + 1.\end{aligned}$$

So $v_\infty(\alpha_1) = v_\infty(\alpha_2) = -2$.

Then dividing out by the highest power of $1/t$, we obtain a Laurent series. Next we divide out by the constant term and are left with an element that is equivalent to 1 mod π. So we have

$$\langle\alpha_1\rangle = \zeta_{\alpha_1}^{-1} \pi^2 \alpha_1 = \zeta_{\alpha_1}^{-1} \left(1 + \frac{\sqrt{t-t^2}}{t^2} - \frac{1}{t^2}\right).$$

Since $1 + \dfrac{\sqrt{t-t^2}}{t^2} - \dfrac{1}{t^2}$ is a 1-unit, it follows that $\zeta_{\alpha_1} = 1$ and hence α_1 is positive. Now,

$$\langle \alpha_2 \rangle = \zeta_{\alpha_2}^{-1} \pi^2 \alpha_2 = \zeta_{\alpha_2}^{-1} \left(2 + \frac{2\sqrt{t-t^2}}{t^2} + \frac{1}{t^2} \right).$$

Notice that $2 + \dfrac{2\sqrt{t-t^2}}{t^2} + \dfrac{1}{t^2}$ is not a 1-unit. This implies that $\zeta_{\alpha_2} = 2$. Hence α_2 is not positive.

Actually, $\alpha_2 = 2\alpha_1$. And so

$$\langle \alpha_1 \rangle = \langle \alpha_2 \rangle = 1 + \frac{\sqrt{t-t^2}}{t^2} - \frac{1}{t^2}.$$

7.2 Exponentiation

Now we have arrived at the main question in this chapter; "How do we exponentiate elements?" To begin, we need to know what the exponent group looks like. We know that we need a copy of $\mathbb{C}_\infty$ due to its roots and the fact that it is complete. However, we will also need some notion of integer exponents. Since we are working over a finite field, we know $x^q = x$. So there is a natural embedding of the integers into the p-adic integers. After a moments thought, it is easy to see that a copy of the p-adic integers should show up in the exponent group since it is the completion of the integers with respect to the p-adic norm. Goss suggests to define the exponent group in the following manner [38].

Definition 40. The exponent group of $\mathbb{A}$ is $\mathbb{S}_\infty := \mathbb{C}_\infty^* \times \mathbb{Z}_p$.

Notice first term is defined multiplicatively, and the second is defined additively. Additionally, the exponentiation depends on the choice of the uniformizer.

7.2.1 Exponentiation of Elements

Now we are ready to exponentiate elements. Let $a \in \mathbb{A}$ and $s = (x, y) \in \mathbb{S}_\infty$ so $x \in \mathbb{C}_\infty^*$ and $y \in \mathbb{Z}_p$.

Definition 41. Set

$$a^{(x,y)} = a_\pi^{(x,y)} := x^{\deg_k(a)} \langle a \rangle_\pi^y$$

Remark 14.

1. Given $s_0, s \in \mathbb{S}_\infty$, we have $a^{s_0+s} = a^{s_0} a^s$.
2. If a_0, a_1 are positive, then $(a_0 a_1)^s = a_0^s a_1^s$. So we have the usual properties which appear in exponentiation.

Let's look at how exponentiation works with the rank one dimension two example.

Example 18. Let $\mathbb{A} = \mathbb{F}_3[t]\left[\sqrt{t-t^2}\right]$. Assume that $\pi = \dfrac{1}{t}$. Consider the element $\alpha = t^2 + \sqrt{t-t^2} - 1$. Recall that the valuation of this element is -2 and we have already calculated its 1-unit part.

Then for $s = (x, y) \in \mathbb{S}_\infty = \mathbb{C}_\infty^* \times \mathbb{Z}_3$, we have

$$\begin{aligned} \alpha^{(x,y)} &= x^{-2v_\infty(\alpha)} \langle \alpha \rangle_\pi^y \\ &= x^4 \left(1 + \frac{\sqrt{t-t^2}}{t^2} - \frac{1}{t^2}\right)^y. \end{aligned}$$

The idea here is to extend the normal definition of exponentiation to $y \in \mathbb{Z}_p$. To do this, suppose $v = \langle \alpha \rangle$ with $|v| < 1$. Then

$$\begin{aligned} \langle \alpha \rangle^y &= (1+v)^y \\ &= \sum_{k=0}^{y} \binom{y}{k} v^{y-k} \end{aligned}$$

which is computed via the binomial theorem.

7.2.2 Exponentiation of Ideals

Recall that $\mathbb{A}$ is a Dedekind domain. Let $\mathfrak{I}$ be the group of $\mathbb{A}$ fractional ideals. Let $\mathbf{P} \subseteq \mathfrak{I}$ be the group of principal ideals and let $\mathbf{P}^+ \subseteq \mathbf{P}$ be the group of positively generated principal ideals. Since we are working over finite fields, we remind the reader that for $\wp \in \mathbf{P}$, we have $\wp^{|\mathbb{F}_\infty|-1} = (1)$.

Definition 42. We define

$$\begin{aligned} \langle\ \rangle_\pi : \quad \mathbf{P}^+ &\to U_1 \\ (a) &\mapsto \langle a \rangle_\pi \end{aligned}$$

with a positive, so $\zeta_a = 1$.

We set $\overline{U_1} \subset \overline{K}$ to be the group of 1-units of $\overline{K}$.

Proposition 79. *The map*

$$\langle\ \rangle_\pi : \boldsymbol{P}^+ \to \overline{U_1}$$

extends uniquely to $\mathfrak{I}$.

A proof of the above proposition can be found in [37, Corollary 8.2.4].

It is important to note that this is not a canonical extension. Also, given any $I \in \mathfrak{I}$, since the class group is finite, eventually we will have $I^n \in \mathbf{P}^+$. So we can define the map on I^n and extend it multiplicatively since $\mathfrak{I}/\mathbf{P}^+$ is finite.

Now we are ready to exponentiate ideals.

Definition 43. Let $I \subseteq \mathbb{A}$ be a non-zero ideal, possibly $\mathbb{A}$. Let $(x, y) \in \mathbb{S}_\infty$. We set

$$I^{(x,y)} := x^{\deg_k I} \langle I \rangle_\pi^y .$$

Example 19. Continuing with the rank one dimension two example, recall we set $\mathbb{A} = \mathbb{F}_3[t]\left[\sqrt{t - t^2}\right]$. One can show that every ideal in $\mathbb{A}$ is either principal or of the form $(\gamma)\, I$

with $\gamma \in \mathbb{A}$, where

$$I = \left(t, \sqrt{t - t^2}\right).$$

Additionally, since the class number of $\mathbb{A}$ is 2, we know that every ideal squared gives us a positively generated principal ideal. So for $\pi = \frac{1}{t}$,

$$I^{(x,y)} = x.$$

Thus far, we have been using the same uniformizer in all of the examples. One may wonder if there is a way to change uniformizers without calculating 1-units again. The following lemma give an explicit formula to change from one uniformizer to another. See [38] for a proof.

Lemma 80. *Let π_1, π_2 be two positive uniformizing parameters. Let I be a non-zero ideal of $\mathbb{A}$. Then*

$$\langle I \rangle_{\pi_1} = \left(\frac{\pi_1}{\pi_2}\right)^{\deg_k(I)/d_\infty} \langle I \rangle_{\pi_2}.$$

Example 20. Let $\mathbb{A} = \mathbb{F}_3[t]\left[\sqrt{t - t^2}\right]$ and $\mathbb{F}_\infty = \mathbb{F}_3[\mathbf{y}]/(\mathbf{y}^2 + 1)$. Let $\pi_1 = \frac{1}{t}$ and $\pi_2 = \frac{\mathbf{y}}{\sqrt{t - t^2}}$. Let

$$\alpha = t^2 + \sqrt{t - t^2} - 1.$$

Then

$$\langle \alpha \rangle_{\pi_1} = 1 + \frac{\sqrt{t - t^2}}{t^2} - \frac{1}{t^2}.$$

So using the lemma, we know that

$$\begin{aligned} \langle \alpha \rangle_{\pi_2} &= \left(\frac{\mathbf{y}/\sqrt{t - t^2}}{1/t}\right)^{4/2} \langle \alpha \rangle_{\pi_1} \\ &= \frac{-t^2}{t - t^2} - \frac{1}{\sqrt{t - t^2}} + \frac{1}{t - t^2}. \end{aligned}$$

7.3 Zeta Functions

Now we are ready to define zeta functions in the present setting.

Definition 44. We set

$$\begin{aligned}\zeta_{\mathbb{A}}(x,y) &:= \zeta_{\mathbb{A},\pi}(x,y)\\ &= \sum_{I\subseteq\mathbb{A}} I^{-s}\end{aligned}$$

which converges for all $s=(x,y)\in\mathbb{S}_\infty$ with $|x|_\infty>1$. Here the sum is over non-zero ideals in $\mathbb{A}$ and the inverse of $s\in\mathbb{S}_\infty$ is $-s=(1/x,-y)$.

Notice that the definition requires $|x|_\infty>1$ for $x\in\mathbb{C}_\infty$. We would like $\zeta_{\mathbb{A},\pi}(x,y)$ to be defined for all $x\in\mathbb{C}_\infty^*$. To analytically continue $\zeta_{\mathbb{A},\pi}(s)$ to all of $\mathbb{C}_\infty^*$, rewrite

$$\begin{aligned}\zeta_{\mathbb{A},\pi}(s) &= \sum_{e=0}^{\infty}\left(\sum_{\deg_k(I)=e} I^{-s}\right)\\ &= \sum_{e=0}^{\infty} x^{-e}\left(\sum_{\deg_k I=e}\langle I\rangle_\pi^{-y}\right).\end{aligned}$$

For a power series over local fields, we know that if its coefficients converge to zero, then the power series converges. Using Riemann-Roch theorem, one can show that $\sum_{\deg_k I=e}\langle I\rangle_\pi^{-y}$ converges to zero exponentially as e approaches infinity. So $\zeta_{\mathbb{A},\pi}(s)$ is an entire power series in x^{-1}. Since we are working over local fields and the coefficients converge, it follows that the series must converge. Thus $\zeta_{\mathbb{A},\pi}(s)$ is defined for all $s\in\mathbb{S}_\infty=\mathbb{C}_\infty^*\times\mathbb{Z}_p$.

Example 21. Let $\mathbb{A}=\mathbb{F}_3[t]\left[\sqrt{t-t^2}\right]$ and $\pi=\dfrac{1}{t}$. We know that every ideal in $\mathbb{A}$ is either principal or a principal ideal times $I=\left(t,\sqrt{t-t^2}\right)$. Therefore, we can split up the sum into two parts. Recall that $I^{-s}=x^{-1}$.

$$\begin{aligned}\zeta_{\mathbb{A},\pi}(s) &= \sum_{0\neq(\alpha)\subseteq\mathbb{A}} (\alpha)^{-s} + \sum_{0\neq(\beta)\subseteq\mathbb{A}} (\beta)^{-s} I^{-s} \\ &= \frac{1}{2}\left(\sum_{\alpha\in\mathbb{A}\setminus\{0\}} x^{2v_\infty(\alpha)} \langle\alpha\rangle_\pi^{-y}\right) + \frac{1}{2}\left(\sum_{\beta\in\mathbb{A}\setminus\{0\}} x^{2v_\infty(\beta)-1} \langle\beta\rangle_\pi^{-y}\right) \\ &= \sum_{k=0}^{\infty}\frac{1}{2}\left(\sum_{v_\infty(\alpha)=-k} \langle\alpha\rangle_\pi^{-y}\right) x^{-2k} + \sum_{k=0}^{\infty}\frac{1}{2}\left(\sum_{v_\infty(\beta)=-k} \langle\beta\rangle_\pi^{-y}\right) x^{-2k-1}.\end{aligned}$$

Note that we need to multiply by $1/2$ since there are two generators for every ideal, α and 2α, so we are double counting.

Just as we have a way to go from one uniformizer to another in terms of 1-units, from the definition of the zeta function, it is not hard to see that we can go from one uniformizer to another in terms of the zeros of the zeta function.

Lemma 81. *Let π_1 and π_2 be two positive parameters, $\alpha \in \mathbb{C}_\infty^*$ and $y_0 \in \mathbb{Z}_p$. Then*

$$\zeta_{\mathbb{A},\pi_2}(\alpha, y_0) = \zeta_{\mathbb{A},\pi_1}\left(\left(\pi_1/\pi_2\right)^{-y_0/d_\infty}\alpha, y_0\right).$$

Proof. From Lemma 80, we know that

$$\langle I\rangle_{\pi_1} = \left(\frac{\pi_1}{\pi_2}\right)^{\deg_k(I)/d_\infty} \langle I\rangle_{\pi_2}.$$

Then,

$$\begin{aligned}
\zeta_{\mathbb{A},\pi_2}(\alpha, y_0) &= \sum_{e=0}^{\infty} \alpha^{-e} \left(\sum_{\deg_k(I)=e} \langle I \rangle_{\pi_2}^{-y_0} \right) \\
&= \sum_{e=0}^{\infty} \alpha^{-e} \left(\sum_{\deg_k(I)=e} \left(\left(\frac{\pi_2}{\pi_1} \right)^{\deg_k(I)/d_\infty} \langle I \rangle_{\pi_1} \right)^{-y_0} \right) \\
&= \sum_{e=0}^{\infty} \alpha^{-e} \sum_{\deg_k(I)=e} \left(\frac{\pi_2}{\pi_1} \right)^{-ey_0/d_\infty} \langle I \rangle_{\pi_1}^{-y_0} \\
&= \sum_{e=0}^{\infty} \left(\alpha \left(\frac{\pi_1}{\pi_2} \right)^{y_0/d_\infty} \right)^{-e} \sum_{\deg_k(I)=e} \langle I \rangle_{\pi_1}^{-y_0} \\
&= \zeta_{\mathbb{A},\pi_1} \left(\left(\frac{\pi_1}{\pi_2} \right)^{-y_0/d_\infty} \alpha, y_0 \right).
\end{aligned}$$

□

Example 22. Now consider $\pi = \dfrac{\mathbf{y}}{\sqrt{t - t^2}}$. We have chosen a different uniformizer, however we will use the same notion of positive. Then

$$I^{(x,y)} = x \left(t\pi \right)^{y/2}.$$

So $I^{-s} = x^{-1} \left(t\pi \right)^{-y/2}$. We will need to redefine the extension map in terms of the new uniformizer.

$$\begin{aligned}
\zeta_{\mathbb{A},\pi}(s) &= \sum_{0 \neq (\alpha) \subseteq \mathbb{A}} (\alpha)^{-s} + \sum_{0 \neq (\beta) \subseteq \mathbb{A}} (\beta)^{-s} I^{-s} \\
&= \frac{1}{2} \left(\sum_{\alpha \in \mathbb{A} \setminus \{0\}} x^{2v_\infty(\alpha)} \langle \alpha \rangle_\pi^{-y} \right) + \frac{1}{2} \left(\sum_{\beta \in \mathbb{A} \setminus \{0\}} x^{2v_\infty(\beta)-1} \left(t\pi \right)^{-y/2} \langle \beta \rangle_\pi^{-y} \right) \\
&= \sum_{k=0}^{\infty} \frac{1}{2} \left(\sum_{v_\infty(\alpha)=-k} \langle \alpha \rangle_\pi^{-y} \right) x^{-2k} + \sum_{k=0}^{\infty} \frac{1}{2} \left(\sum_{v_\infty(\beta)=-k} \langle \beta \rangle_\pi^{-y} \right) \left(t\pi \right)^{-y/2} x^{-2k-1}.
\end{aligned}$$

Once again, we must multiply by $1/2$ since we are double counting.

Let's look at a specific example of how the zeros of the zeta function change when we choose a different uniformizer.

Example 23. Once again working over $\mathbb{A} = \mathbb{F}_3[t]\left[\sqrt{t-t^2}\right]$ and $\mathbb{F}_\infty = \mathbb{F}_3[\mathbf{y}]/(\mathbf{y}^2+1)$, consider $y=-8$. If we set $\pi_1 = \dfrac{1}{t}$, then

$$\zeta_{\mathbb{A},\pi_1}(x,-8) = \frac{1}{x^3}(x+1)\left(x+\pi_1^4\right)\left(x-\pi_1^4\right).$$

And for $\pi_2 = \dfrac{\mathbf{y}}{\sqrt{t-t^2}}$,

$$\zeta_{\mathbb{A},\pi_2}(x,-8) = 1 + (t\pi_2)^4 x^{-1} + 2\pi_2^8 x^{-2} + 2t^4\pi_2^{12}x^{-3}.$$

Computationally we find that the zeros of $\zeta_{\mathbb{A},\pi_1}(x,-8)$ are

$$(2,-8), \quad \left(2\pi_1^4,-8\right), \quad \left(\pi_1^4,-8\right).$$

Then using the lemma, we can see that the zeros of $\zeta_{\mathbb{A},\pi_2}(x,-8)$ are

$$\left(2(t\pi_2)^4,-8\right), \quad \left(2\pi_2^4,-8\right), \quad \left(\pi_2^4,-8\right).$$

7.3.1 Special Polynomials

Now we are ready to define certain zeta functions which are of interest to us.

Definition 45. For j a positive integer, we set

$$z(x,-j) = z_{\mathbb{A}}(x,-j) := \zeta_{\mathbb{A},\pi}(x,-j) = \sum_{e=0}^{\infty} x^{-e}\left(\sum_{\deg_k(\mathfrak{I})=e}\mathfrak{I}^{(j)}\right).$$

We know that the sum in parenthesis vanishes for sufficiently large e. Therefore $z(x,-j)$ is a polynomial in x^{-1}. These polynomials occur as special zeta values and, as such, are called **special polynomials**.

We are interested in how these polynomials are affected by the symmetric group $S_{(q)}$, which we will define momentarily. Since these are just special values of the zeta function, we will use $\zeta_{\mathbb{A},\pi}(x,-j)$ to avoid confusion.

Continuing with the rank one dimension two setting, let's look at some examples.

Example 24. Let $\pi = \dfrac{1}{t}$ and recall $\mathbb{F}_\infty = \mathbb{F}_3[\mathbf{y}]/(\mathbf{y}^2+1)$. Then we have the following special polynomials.

$$\zeta_{\mathbb{A},\pi}(x,-j) = 1 + x^{-1}$$

for $j = 1, 2, 4, 5, 6, 7, 10, 12, 13, 15, 18, 21$.

$$\zeta_{\mathbb{A},\pi}(x,-8) = 1 + x^{-1} + 2\pi^8 x^{-2} + 2\pi^8 x^{-3}$$

$$\zeta_{\mathbb{A},\pi}(x,-11) = 1 + x^{-1} + 2\pi^{11} C_{11} x^{-2} + 2\pi^{11} C_{11} x^{-3}$$

where $C_{11} = \mathbf{y}\sqrt{t-t^2} - \mathbf{y}(t-t^2)^{9/2} - t^9 + t$.

$$\zeta_{\mathbb{A},\pi}(x,-16) = 1 + x^{-1} + 2\pi^{16} x^{-2} + 2\pi^{16} x^{-3}$$

$$\zeta_{\mathbb{A},\pi}(x,-19) = 1 + x^{-1} + \pi^{19} C_{19} x^{-2} + \pi^{19} C_{19} x^{-3}$$

where $C_{19} = \mathbf{y}\sqrt{t-t^2} - \mathbf{y}(t-t^2)^{9/2} - t^9 + t$.

$$\zeta_{\mathbb{A},\pi}(x,-20) = 1 + x^{-1} + \pi^{20} C_{20} x^{-2} + \pi^{20} C_{20} x^{-3}$$

where $C_{20} = t + t^5 + t^6 + t^7 + 2t^8$.

$$\zeta_{\mathbb{A},\pi}(x, -24) = 1 + x^{-1} + 2\pi^{24}x^{-2} + 2\pi^{24}x^{-3}.$$

The reader will notice that we have omitted the zeta functions for $j = 14, 17, 22, 23$. The reason for this is due to their complicated coefficients in the x^{-2} and x^{-3} terms.

Example 25. Now let $\pi = \dfrac{\mathbf{y}}{\sqrt{t - t^2}}$. Then we have the following special polynomials.

$$\zeta_{\mathbb{A},\pi}(x, -j) = 1 + (t\pi)^{j/2}x^{-1}$$

for $j = 1, 2, 4, 5, 6, 7, 10, 12, 13, 15, 18, 21$.

$$\zeta_{\mathbb{A},\pi_2}(x, -8) = 1 + (t\pi_2)^4x^{-1} + 2\pi_2^8x^{-2} + 2t^4\pi_2^{12}x^{-3}.$$

$$\zeta_{\mathbb{A},\pi}(x, -11) = 1 + (t\pi)^{11/2}x^{-1} + 2(\pi)^{11}C_{11}x^{-2} + 2(t\pi)^{11/2}\pi^{11}C_{11}x^{-3}$$

where $C_{11} = \mathbf{y}\sqrt{t - t^2} - \mathbf{y}(t - t^2)^{9/2} - t^9 + t$.

$$\zeta_{\mathbb{A},\pi}(x, -16) = 1 + (t\pi)^8x^{-1} + 2\pi^{16}x^{-2} + 2(t\pi)^8\pi^{16}x^{-3}$$

$$\zeta_{\mathbb{A},\pi}(x, -19) = 1 + (t\pi)^{19/2}x^{-1} + \pi^{19}C_{19}x^{-2} + (t\pi)^{19/2}\pi^{19}C_{19}x^{-3}$$

where $C_{19} = \mathbf{y}\sqrt{t - t^2} - \mathbf{y}(t - t^2)^{9/2} - t^9 + t$.

$$\zeta_{\mathbb{A},\pi}(x, -20) = 1 + (t\pi)^{10}x^{-1} + 2\pi^{20}C_{20}x^{-2} + 2(t\pi)^{10}\pi^{20}C_{20}x^{-3}$$

where $C_{20} = t + t^5 + t^6 + t^7 + 2t^8$.

$$\zeta_{\mathbb{A},\pi}(x, -24) = 1 + (t\pi)^{12}x^{-1} + 2\pi^{24}x^{-2} + 2(t\pi)^{12}\pi^{24}x^{-3}.$$

7.4 Symmetric Group

In this section we will introduce the automorphism groups of interest to us. These are subgroups of the group of homeomorphisms of $\mathbb{Z}_p$ and they stabilize, and so permute, both the non-positive and non-negative integers sitting in $\mathbb{Z}_p$.

Recall q is a power of p. Let $y \in \mathbb{Z}_p$. We can write y q-adically as

$$y = \sum_{i=0}^{\infty} c_i q^i$$

where $0 \leq c_i < q$ for all i. If y is a non-negative integer, then this sum is finite.

Let ρ be a permutation of $\{0, 1, 2, \ldots\}$.

Definition 46. For $y \in \mathbb{Z}_p$, define

$$\rho_*(y) = \sum_{i=0}^{\infty} c_i q^{\rho(i)}.$$

So we are just permuting the coefficients of y. Clearly the map which sends y to $\rho_*(y)$ gives a representation of ρ as a set permutation of $\mathbb{Z}_p$.

Definition 47. Let $S_{(q)}$ be the **group of permutations** of $\mathbb{Z}_p$ obtained as ρ varies over all permutations of $\{0, 1, 2, \ldots\}$.

Example 26. Let $q = p = 3$. Let ρ be the permutation $(0, 1)$. We will calculate $\rho_*(5)$.

We know that $5 = 2 \cdot 3^0 + 1 \cdot 3^1$. So

$$\begin{aligned} \rho_*(5) &= 2 \cdot 3^{\rho(0)} + 1 \cdot 3^{\rho(1)} \\ &= 2 \cdot 3^1 + 1 \cdot 3^0 \\ &= 7. \end{aligned}$$

Next, let's calculate $\rho_*(36)$.

We know that $36 = 0 \cdot 3^0 + 0 \cdot 3^1 + 1 \cdot 3^2 + 1 \cdot 3^3$. So

$$\rho_*(36) = 36.$$

As demonstrated in the above example, sometimes elements are permuted and other times they are fixed.

7.4.1 Action on Zeta Functions

We are interested in how $S_{(q)}$ acts on the zeros of the zeta function, specifically the zeros of the special polynomials. Recall that zeros of the zeta function lie in $\mathbb{S}_\infty = \mathbb{C}_\infty^* \times \mathbb{Z}_p$. So we must extend the definition of ρ_*. Additionally, since we want to look at $j \in \mathbb{Z}_p$ and apply ρ_* to $-j$, we want to avoid rewriting $-j$ in terms of its q-adic expansion. This leads us to the following definition.

Definition 48. Let ρ be a permutation of $\{0, 1, 2, \ldots\}$ and let $y \in \mathbb{Z}_p$. We define

$$\widehat{\rho_*}(y) = -\rho_*(-y).$$

Remark 15. Note that $\widehat{\rho_*}$ stabilizes both the non-negative and non-positive integers.

Now, fix π_* to be a d_∞-th roots of π. Note there is some ambiguity here because we need to make a choice when $d_\infty \neq 1$.

Definition 49. Define

$$K_1 := \mathbb{F}_\infty \left((\pi_*) \right) \simeq K \left(\pi_* \right).$$

Let's look at an example of K_1.

Example 27. For $\mathbb{A} = \mathbb{F}_3[t]\left[\sqrt{t-t^2}\right]$ and $\pi = \frac{1}{t}$, we can choose $\pi_* = \frac{1}{\sqrt{t}}$. Then

$$K_1 = \mathbb{F}_9\left(\left(\frac{1}{\sqrt{t}}\right)\right).$$

Next, one may ask what elements in K_1 look like. Let $x \in K_1^*$. Then we can write

$$x = \sum_{i \gg -\infty} c_i \pi_*^i$$

with $c_i \in \mathbb{F}_\infty$. So writing x in terms of its π_* expansion we can define ρ_* on K_1. Once again we are just permuting coefficients.

Definition 50. Let ρ be a permutation of $\{0, 1, 2, \ldots\}$ and let $x \in K_1^*$. Then set

$$\rho_*(x) := \sum_{i \gg -\infty} c_i \pi_*^{\rho_*(i)} \in K_1^*.$$

Currently, we do not know how to extend the definition of ρ_* to all of $\mathbb{C}_\infty$, hence to all of $\mathbb{S}_\infty$. Therefore we define the following subset of $\mathbb{S}_\infty$.

Definition 51. Let

$$\mathbb{S}_{\infty,\pi} := K_1^* \times \mathbb{Z}_p \subset \mathbb{S}_\infty.$$

For $(x, y) \in \mathbb{S}_{\infty,\pi}$, we set

$$\rho_*(x, y) := (\rho_*(x), \widehat{\rho}_*(y)) \in \mathbb{S}_{\infty,\pi}.$$

In [38], Goss presents evidence that for $\mathbb{A} = \mathbb{F}_q[t]$, $S_{(q)}$ acts as symmetries of $\zeta(s)$ arising from the negative integers. He proves the following theorem.

Theorem 82 (Goss, [38])**.** *Let j be a non-negative integer with associated special polynomial $z(x, -j)$. Let $\rho_* \in S_{(q)}$. Then $z(x, -j)$ and $z\left(x, \widehat{\rho}_*(-j)\right)$ have the same degree in x^{-1}.*

One may wonder if this is true for Drinfeld modules other than the Carlitz module. It does not take much effort to answer the question.

Example 28. Consider $\mathbb{A} = \mathbb{F}_3[t]\left[\sqrt{t-t^2}\right]$, and j a non-negative integer with associated special polynomial $\zeta_{\mathbb{A},\pi}(x,-j)$. Let $\rho_* \in S_{(3)}$. Then $\zeta_{\mathbb{A},\pi}(x,-j)$ and $\zeta_{\mathbb{A},\pi}\left(x,\widehat{\rho_*}(-j)\right)$ have the same degree in x^{-1}. Let $\pi = \dfrac{1}{t}$ and consider $\rho = (1,2)$ and $\rho_* \in S_{(3)}$. So $\rho_*(7) = 19$. But as we saw earlier,

$$\zeta_{\mathbb{A},\pi}(x,-7) = 1 + x^{-1}$$

and

$$\zeta_{\mathbb{A},\pi}(x,-19) = 1 + x^{-1} + \pi^{19}C_{19}x^{-2} + \pi^{19}C_{19}x^{-3}.$$

Therefore Theorem 82 does not hold for all Drinfeld modules. So perhaps this is not the correct question we wish to answer. This leads us to the following definition.

Definition 52. Let $y \in \mathbb{Z}_p$. Write y q_∞-adically, $q_\infty = q^{d_\infty}$

$$y = \sum_{i=0}^{\infty} c_i q_\infty^i$$

where $0 \leq c_i < q_\infty$ for all i. Let $S_{(q_\infty)}$ be the **group of permutations** of $\mathbb{Z}_p$ obtained as ρ varies over all permutations of $\{0,1,2,\ldots\}$ when $y \in \mathbb{Z}_p$ is written q_∞-adically.

A better conjecture may be the following.

Conjecture 1. For $\mathbb{A} = \mathbb{F}_3[t]\left[\sqrt{t-t^2}\right]$, and j a non-negative integer with associated special polynomial $\zeta_{\mathbb{A},\pi}(x,-j)$. Let $\rho_* \in S_{(9)}$. Then $\zeta_{\mathbb{A}\,\pi}(x,-j)$ and $\zeta_{\mathbb{A},\pi}\left(x,\widehat{\rho_*}(-j)\right)$ have the same degree in x^{-1}.

Once again, let's look at an example.

Example 29. Let $\pi = \dfrac{1}{t}$. Consider $\rho = (0,1)$ and $\rho_* \in S_{(9)}$. So $\rho_*(24) = 56$. We can

calculate that

$$\zeta_{\mathbb{A},\pi}(x,-24) = 1 + x^{-1} + 2\pi^{24}x^{-2} + 2\pi^{24}x^{-3}$$

and

$$\zeta_{\mathbb{A},\pi}(x,-56) = 1 + x^{-1} + 2\pi^{56}x^{-2} + 2\pi^{56}x^{-3}.$$

The zeros for $\zeta_{\mathbb{A},\pi}(x,-24)$ are

$$(2,-24) \quad (2\pi^{12},-24) \quad (\pi^{12},-24)\,.$$

Then

$$\begin{aligned}
\rho_*(2,-24) &= (\rho_*(2), \widehat{\rho}_*(-24)) \\
&= (2,-56) \\
\rho_*(2\pi^{12},-24) &= (\rho_*(2\pi^{12}), \widehat{\rho}_*(-24)) \\
&= (2\pi^{28},-56) \\
\rho_*(\pi^{12},-24) &= (\rho_*(\pi^{12}), \widehat{\rho}_*(-24)) \\
&= (\pi^{28},-56)
\end{aligned}$$

which are the zeros of $\zeta_{\mathbb{A},\pi}(x,-56)$.

As demonstrated by the above example, there appears to be some relationship between zeros of the zeta function and $S_{(q_\infty)}$. A concrete explanation of this relationship is currently unknown. Due to the complicated nature of these zeta functions, an effective way to study this relationship is to construct examples. The reader can find a summary of ideas for future work in this area as well as other topics related to Drinfeld modules in Chapter 8.

Chapter 8

Future Work

This final chapter briefly discusses directions for future research. We will concentrate on the material presented in Chapters 5 and 7.

8.1 Selmer Groups

In Chapter 5, we discussed a graph theoretic approach to 3-Selmer groups for a family of elliptic curves. A natural question to ask is "How often do elliptic curves in this family have 3-Selmer groups of size N?" Robert Rhoades discusses such a question for 2-Selmer groups of congruent number curves [55]. In a pair of papers, Heath-Brown explores Selmer groups for congruent number curves and their sizes on average [41, 42]. He does so by counting the number of square-free integers up to X that have 2-Selmer group of a given size. He gives a precise, yet complicated asymptotic formula. In [55], Rhoades uses different techniques which are more elementary, however not as precise as Heath-Brown's results. Using the work of Feng and Xiong [32] and Faulkner and James [31], he builds on a similar graph theoretical approach (See [5]). In addition, he discusses the relationship between counting 2-Selmer groups and the Birch Swinnerton-Dyer Conjecture. It would be interesting to explore

this relationship using 3-Selmer groups. One could adapt Rhoades' methods to the graphs discussed in Chapter 5 and hopefully obtain similar results.

Perhaps a simpler question would be to explore the size of the modified Selmer groups. As mentioned in Chapter 5, the primes 2 and 3 are more challenging to study. By defining a modified Selmer group which requires local solutions everywhere except in $\mathbb{Q}_2$ and $\mathbb{Q}_3$, it may be easier to extend Rhoades' results for this group. In addition, one could explore how the modified and actual 3-Selmer groups differ. On average, how many more elements does the modified Selmer group contain verses the 3-Selmer group? Is this number significant, if so, how much of an over-estimate on the rank do we expect? If this number is, on average, negligible, then we could just study the modified Selmer group and ignore the problems encountered with 2 and 3.

Another possible direction would be to investigate the average rank of Selmer groups. Recently, Manjul Bhargava has calculated the average Selmer rank over all elliptic curves. In 2010, Bhargava and Shankar proved the following theorem in their paper [3].

Theorem 83. *When averaged over their height, elliptic curves E defined over $\mathbb{Q}$ have an average rank of less than* 1.5.

They proved that when elliptic curves are ordered by height, the mean size of the 2-Selmer group is 3. Therefore, one can conclude that when all elliptic curves over $\mathbb{Q}$ are ordered by height, their average 2-Selmer rank is at most 1.5, implying the above result. The curves studied in Chapter 5 are a density zero subset of all elliptic curves. It would be intriguing to investigate their average rank and compare it to Bhargava's results.

8.2 Zeta Functions

In Chapter 7, we discuss the work of Goss, Thakur and Diaz-Vargas for characteristic p zeta functions and the relation between zeros of special polynomials and the symmetric

group $S_{(q)}$. As mentioned in Section 7.4.1, there are currently only results in the Carlitz module setting. It would be interesting if one could prove an analogous result to Theorem 82. This would give further evidence that $S_{(q_\infty)}$ acts as symmetries of $\zeta(s)$ arising from the negative integers. Before proving such a theorem, it would be informative to calculate more examples and explore how the coefficients of these zeta functions are affected by ρ^*. These calculations might shed some light on the proper statement of the conjecture.

Anderson and Thakur establish a fundamental relationship between logarithms associated to the Carlitz modules and special zeta values [1]. Yu used this relationship to establish important transcendence results, which are not yet known in classical number theory [72]. Thakur expands on these results and presents evidence that such relationships will exist for a general A in addition to the Carlitz setting [65]. Using the setting described in Example 15, one could compute the associated logarithms and attempt to establish relationships between them and the special zeta values.

Finally, one can explore the traces of the Frobenius endomorphism for Drinfeld modules using an analytical approach. In [22], Chantal David investigates the distribution of traces of Frobenius endomorphisms on the reductions of a rank 2 Drinfeld module over $\mathbb{F}_q(T)$. She proves the following theorem.

Theorem 84. *Let φ be a Drinfeld module over $\mathbb{F}_q(T)$ of rank 2 without complex multiplication. Let k be a positive integer. Define*

$$\pi_t(k) := \{\textit{primes } \ p \in \mathbb{F}_q[T] \textit{ of degree } k \textit{ such that } a_p(\varphi) = t\}$$

Then

$$\pi_t(k) \ll \frac{rq^{k\theta(r)}}{k} \tag{8.1}$$

where $\theta(r) = 1 - 1/(2r^2 + 4r)$ and the constant only depends on φ.

David also has established results concerning the supersingular reduction of Drinfeld modules. In [20], she proves the following theorem.

Theorem 85. *Let φ be a Drinfeld $\mathbb{F}_q[T]$-module over $\mathbb{F}_q(T)$ of rank 2. Consider any positive real number x. Let $\pi_\varphi(x)$ be the set of all monic irreducible polynomials p where φ has good reduction and $q^{deg(p)} \leq x$. Then*

$$\pi_\varphi(x) \gg \log\log(x). \tag{8.2}$$

There are many directions one could look to for future work. Are there similar results for Drinfeld modules of rank 1 dimension 2? What type of bound would we expect for a Drinfeld module of dimension 2 in the analogous case to Equation (8.1)? What about to Equation (8.2)? How good of a bound do we expect for each of these?

Appendices

Appendix A Cohomology Definition of the Selmer Group

The Selmer Group is typically defined as the kernel of maps between Cohomology groups. This section will give the reader an idea of how the definition given in Section 4.3.1 is related to the usual definition. This section is not necessary to understand the results stated in Chapter 5. All results and definitions of this section can be found in [62], specifically Chapters 8, 10 and Appendix B.

A.1 Group Cohomology of Finite Groups

Let G be a finite group and M an abelian group. We denote the action of $\sigma \in G$ on M by $m \mapsto m^\sigma$. If this action satisfies the following properties, then we say M is a G-module

$$\begin{aligned} m^1 &= m, \\ (m_1 + m_2)^\sigma &= m_1^\sigma + m_2^\sigma, \\ (m^\sigma)^\tau &= m^{\sigma\tau}. \end{aligned}$$

For a given G-module, it is natural to calculate the largest submodule on which G acts trivially. The elements of this group are said to be *G-invariant*.

Definition 53. The **0^{th}-cohomology group of the G-module** M, denoted M^G or $H^0(G, M)$ is defined by

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

Let

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

be an exact sequence of G-modules. Taking G-invariants, we obtain the following exact sequence

$$0 \to P^G \to M^G \to N^G.$$

Note that the last map may no longer be surjective. One can measure the lack of surjectivity of this map, by making the following definitions.

Definition 54. Let M be a G-module. The **group of 1-cochains** from G to M is given by

$$C^1(G, M) = \{\text{maps } \xi : G \to M\}.$$

The **group of 1-cocyles** from G to M is defined by

$$Z^1(G, M) = \left\{\xi \in C^1(G, M) : \xi_{\sigma\tau} = \xi_\sigma^\tau + \xi_\tau \ \forall\ \sigma, \tau \in G\right\}.$$

The **group of 1-coboundaries** from G to M is given by

$$B^1(G, M) = \left\{\xi \in C^1(G, M) : \exists\ m \in M \text{ s. t. } \xi_\sigma = m^\sigma - m \ \forall\ \sigma \in G\right\}.$$

Notice that $B^1(G, M) \subseteq Z^1(G, M)$. The $1^{\mathbf{st}}$**-cohomology group of the** G**-module** M is the quotient group

$$H^1(G, M) = Z^1(G, M)/B^1(G, M).$$

Remark 16.

1. $H^1(G, M)$ is the group of 1-cocycles $\xi : G \to M$, modulo the equivalence relation that any two cycles are identified if their difference is of the form $\sigma \to m^\sigma - m$ for some $m \in M$.

2. If the action of G on M is trivial, then

$$H^0(G, M) = M$$

and

$$H^1(G, M) = \text{Hom}(G, M).$$

Let $\phi : M \to N$ be a G-module homomorphism. Let $\xi \in Z^1(G, M)$, then composition with ϕ maps $Z^1(G, M)$ to $Z^1(G, N)$. In a similar manner, it takes $B^1(G, M)$ to $B^1(G, N)$. Hence ϕ induces a map on cohomologies, $\phi : H^1(G, M) \to H^1(G, N)$.

Proposition 86 (Proposition 1.2, [62]). *Let*

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

be an exact sequence of G-modules. Then there exists a long exact sequence

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

where δ is defined as follows.

Let $n \in H^0(G, N) = N^G$. Choose an $m \in M$ such that $\psi(m) = n$ (such an m exists since ψ is surjective). Define a cochain $\xi : C^1(G, M)$ by

$$\xi_\sigma = m^\sigma - m.$$

Then $\xi \in Z^1(G, P)$ and $\delta(n)$ is the cohomology class in $H^1(G, P)$ of the 1-cocycle ξ.

A.2 Galois Cohomology

Let K be a perfect field and $G_{\overline{K}/K}$ be the Galois group of $\overline{K}$ over K. One can show that $G_{\overline{K}/K}$ is a profinite group since it is the inverse limit of finite groups. Therefore one can define a topology on $G_{\overline{K}/K}$ which consists of a basis of open sets around the identity which are the collection of normal subgroups which have finite index in $G\overline{K}/K$.

Definition 55. A (discrete) $G_{\overline{K}/K}$**-module** is an abelian group M on which $G_{\overline{K}/K}$ acts such that the action is continuous for the profinite topology on $G_{\overline{K}/K}$ and the discrete topology

on M.

Equivalently, the action of $G_{\overline{K}/K}$ on M has the property that for all $m \in M$, the stabilizer of m, $\{\sigma \in G : m^\sigma = m\}$ is a subgroup of finite index in $G_{\overline{K}/K}$.

The 0^{th}-cohomology group is defined in the manner as for finite groups.

Definition 56. The **0^{th}-cohomology of the $G_{\overline{K}/K}$-module** M is the group of $G_{\overline{K}/K}$-invariant elements of M,

$$H^0(G_{\overline{K}/K}, M) = \left\{ m \in M : m^\sigma = m \ \forall \ \sigma \in G_{\overline{K}/K} \right\}.$$

When defining H^1, we use the fact that $G_{\overline{K}/K}$ is profinite and the module is discrete in order to put some restrictions on the allowable cycles.

Definition 57. Let M be a $G_{\overline{K}/K}$-module. A map $\xi : G_{\overline{K}/K} \to M$ is **continuous** if it is continuous for the profinite topology on $G_{\overline{K}/K}$ and the discrete topology on M. We define the **group of continuous 1-cocycles from $G_{\overline{K}/K}$ to** M, $Z^1_{\text{cont}}(G_{\overline{K}/K}, M)$, to be the group of continuous maps $\xi : G_{\overline{K}/K} \to M$ satisfying the cocycle condition

$$\xi_{\sigma\tau} = \xi_\sigma^\tau + \xi_\tau.$$

(Note that this a subgroup of the full group of 1-cocycles $Z^1(G_{\overline{K}/K}, M)$.) Since M is discrete, any coboundary $\sigma \to m^\sigma - m$ will automatically be continuous. The **1^{st}-cohomology group of the $G_{\overline{K}/K}$-module** M is given by

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

Remark 17. If $G_{\overline{K}/K}$ acts trivially on M, then we have a similar result to the one given in

the finite group case

$$H^0(G_{\overline{K}/K}, M) = M,$$

and

$$H^1(G_{\overline{K}/K}, M) = \mathrm{Hom}_{\mathrm{cont}}(G_{\overline{K}/K}, M)$$

where $\mathrm{Hom}_{\mathrm{cont}}(G_{\overline{K}/K}, M)$ means the group of continuous homomorphisms.

The fundamental exact sequences given by Proposition 86 for finite groups is exactly the same for $G_{\overline{K}/K}$.

A.3 Selmer Group

In order to present the cohomology definition of the Selmer group, we need a few definitions.

Definition 58. Let E/K be an elliptic curve. A **(principal) homogeneous space for** E/K is a smooth curve C/K together with a simply transitive algebraic group action of E on C defined over K.

Remark 18. We often think of a homogeneous space for E/K as a pair (C, μ), where C/K is a smooth curve and $\mu : C \times E \to C$ is a morphism defined over K with the following properties:

1. $\mu(p, \mathcal{O}) = p$ for all $p \in C$
2. $\mu(\mu(p, P), Q) = \mu(p, P + Q)$ for all $p \in C$ and $P, Q \in E$
3. For all $p, q \in C$, there exists a unique $P \in E$ satisfying $\mu(p, P) = q$.

Often times we denote $\mu(p, P)$ as $p + P$.

Definition 59. Two homogeneous spaces C/K and C'/K for E/K are **equivalent** if there is an isomorphism $\theta : C \to C'$ defined over K which is compatible with the action of E on C and C'. This means that for all $p \in C$ and $P \in E$, the map θ satisfies $\theta(p + P) = \theta(p) + P$.

The equivalence class containing E, acting on itself by translation, is called the **trivial class**. The collection of equivalence classes of homogeneous spaces for E/K is called the **Weil-Châtelet group for** E/K which we denote by $WC(K/K)$.

One can characterize the trivial homogeneous spaces using the following proposition.

Proposition 87 (Proposition 3.3, [62])**.** *Let C/K be a homogeneous space for E/K. Then C/K is in the trivial class if and only if $C(K)$ is not empty.*

The following theorem relates the Weil-Châtele group to the first cohomology group. Moreover since $H^1(G_{\overline{K}/K}, E)$ is a group, this theorem defines a group structure on $WC(E/K)$.

Theorem 88 (Theorem 3.6, [62])**.** *Let E/K be an elliptic curve. There is a natural bijection*

$$WC(E/K) \to H^1(G_{\overline{K}/K}, E)$$

defined as follows: Let C/K be a homogeneous space and choose any point $p_0 \in C$. Then

$$\{C/K\} \to \{\sigma \to p_0^\sigma - p_0\},$$

where the brackets denote an equivalence class.

Recall in Chapter 4, we were considering an elliptic curve E and an auxiliary curve E' with an isogeny $\phi : E \to E'$. Then there is an exact sequence of $G_{\overline{K}/K}$-modules,

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

where $E[\phi]$ denotes the kernel of ϕ. Taking Galois cohomology yields the long exact sequence

$$\begin{array}{rcccl} 0 & \to & E(K)[\phi] & \to E(K) & \stackrel{\phi}{\to} E'(K) \\ & \stackrel{\delta}{\to} & H^1(G_{\overline{K}/K}, E[\phi]) & \to H^1(G_{\overline{K}/K}, E) & \to H^1(G_{\overline{K}/K}, E') \to; \end{array}$$

and from this we obtain the fundamental short exact sequence

$$0 \to E'(K)/\phi(E(K)) \stackrel{\delta}{\to} H^1(G_{\overline{K}/K}, E[\phi]) \to H^1(G_{\overline{K}/K}, E)[\phi] \to 0. \tag{3}$$

We observe that Theorem 88, tells us that we can identify the last term of (3) with the ϕ-torsion in the Weil-Châtelet group $WC(E/K)$.

The next step in calculating the Mordell-Weil group of E/K, requires one to replace the second and third terms of (3) with specific finite groups. In order to do this, we must localize. Let M_K denote the be the set of standard absolute values on K. Then for each $v \in M_K$, one can fix an extension of v to $\overline{K}$ which in turn fixes an embedding $\overline{K} \subset K_v$ and a decomposition group $G_v \subset G_{\overline{K}/K}$. Then since G_v acts on $E(K_v)$ and $E'(K_v)$, we obtain the following exact sequence

$$0 \to E'(K_v)/\phi(E(K_v)) \stackrel{\delta}{\to} H^1(G_v, E[\phi]) \to H^1(G_v, E)[\phi] \to 0. \tag{4}$$

We notice that $G_v \subset G_{\overline{K}/K}$ and $E(\overline{K}) \subset E(K_v)$, we obtain restriction maps on cohomology and hence obtain the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E'(K)/\phi(E(K)) & \xrightarrow{\delta} & H^1(G_{\overline{K}/K}, E[\phi]) & \longrightarrow & WC(E/K)[\phi] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E'(K_v)/\phi(E(K_v)) & \xrightarrow{\delta} & \prod_{v \in M_K} H^1(G_v, E[\phi]) & \longrightarrow & \prod_{v \in M_K} WC(E/K_v)[\phi] & \longrightarrow & 0. \end{array} \tag{5}$$

Now we are ready to define the Selmer group and the Tate-Shafarevich group.

Definition 60. Let $\phi : E/K \to E'/K$ be an isogeny. The **ϕ-Selmer group of** E/K is the subgroup of $H^1(G_{\overline{K}/K}, E[\phi])$ defined by

$$S^{(\phi)}(E/K) = \ker \left\{ H^1(G_{\overline{K}/K}, E[\phi]) \to \prod_{v \in M_K} WC(E/K_v) \right\}. \tag{6}$$

The **Tate-Shafarevich group of** E/K is the subgroup of $WC(E/K)$ defined by

$$Ш(E/K) = \ker \left\{ WC(E/K) \to \prod_{v \in M_K} WC(E/K_v) \right\}.$$

Remark 19. One can think of $Ш(E/K)$ as the group of homogeneous spaces which are everywhere locally trivial, modulo equivalence.

The following theorem relates the elliptic curves to the Selmer and Tate-Shafarevich groups.

Theorem 89 (Theorem 4.2, [62])**.** *Let $\phi : E/K \to E'/K$ be an isogeny of elliptic curves defined over K.*

(a) There is an exact sequence

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

(b) The Selmer group $S^{(\phi)}(E/K)$ is finite.

From this one can conclude that

$$\left|S^{(\phi)}(E/K)\right| = |E'(K)/\phi(E(K))| \, |Ш(E/K)[\phi]| \, .$$

Therefore, in order to give a bound on the rank, it is sufficient to calculate the size of the Selmer group.

We will conclude this section by attempting to give the reader an idea of how the definition in (6) is equivalent to the one given in Section 4.3.1. We begin by recalling the following definition.

Definition 61. A **twist** of C/K is a smooth curve C'/K which is isomorphic to C over $\overline{K}$.

One can show that every cohomology class in $H^1(G_{\overline{K}/K}, \mathrm{Isom}(C))$ comes from some twist of C/K. Since $S^{(\phi)}(E/K)$ is a subset of $H^1(G_{\overline{K}/K}, E[\phi])$, if we can find a geometric object X such that $\mathrm{Aut}_{\overline{K}}(X) \cong E[\phi]$, we can interpret the elements of the Selmer group as twists of the object X.

The plane cubic given by Equation (4.11) in Theorem 41 is the equation of a twist C of the elliptic curve E. So every homogeneous cubic equation which has local solutions everywhere should correspond to an element in the kernel of the map from $H^1(G_{\overline{K}/K}, E[\phi]) \to \prod_{v \in M_K} WC(E/K_v)$. Thus the definition given in Section 4.3.1 is equivalent to the one presented above. For additional details and other interpretations of the elements of the Selmer group, see [17, 18].

Appendix B Derivation for Auxiliary Curve

B.1 Defining the Selmer Group

The interested reader may notice that equation (4.12) differs from the one stated in [14]. The following section provides details on the derivation of equation (4.12). This section is not necessary to understand the results stated in Chapter 5.

Recall, we are considering an elliptic curve of the form

$$E'_{ab'} : y^2 = x^3 - 3(ax + b')^2$$

with $b' = \frac{27b-4a^3}{9}$. Suppose that (x, y) is a rational point on $E'_{ab'}$. Let $y = s/t^3$, $x = r/t^2$ with $(rs, t) = 1$. Substituting and simplifying we obtain

$$\begin{aligned} r^3 &= \left[s - \left(art + b't^3\right)\sqrt{-3}\right]\left[s - \left(art + b't^3\right)\sqrt{-3}\right] \\ &= \left[(s + art + bt^3) + 2t(ar + bt^2)\omega\right]\left[(s - t(ar + bt^2)) - 2t(ar + bt^2)\omega\right], \end{aligned} \tag{7}$$

where $\omega = \frac{-1+\sqrt{-3}}{2}$ is a cube root of unity and $\sqrt{-3} = 2\omega + 1$. Letting

$$u' = \alpha(x, y) \quad = \alpha(r, s, t) = \quad s - \left(ar + b't^2\right)t\sqrt{-3} = s - t(ar + b't^2) - 2t(ar + b't^2)\omega,$$

implies

$$\bar{u'} = s + \left(ar + b't^2\right)t\sqrt{-3} = s + t(ar + b't^2) + 2t(ar + b't^2)\omega.$$

Note that this differs from Cohen and Patzuki's definition by a multiple of $\dfrac{1}{t^3}$ which is a cube. We may use either definition since they are equivalent in G'_3. Recall G'_3 is the subgroup of $\mathbb{Q}(\omega)^*/(\mathbb{Q}(\omega)^*)^3$ of classes whose norms are cubes.

From this we can conclude that

$$\begin{aligned} s &= u' + t\sqrt{-3}\left(ar + b't^2\right) \\ &= \bar{u}' - t\sqrt{-3}\left(ar + b't^2\right). \end{aligned}$$

Equivalently,

$$2s = u' + \bar{u}'.$$

Let $\mathbf{d} = \gcd(u', \bar{u}')$. Then

$$\mathbf{d} \mid \gcd(u' + \bar{u}', u' - \bar{u}')$$

and $\gcd(u' + \bar{u}', u' - \bar{u}') = 2\gcd(s, \sqrt{-3}(ar + b't^2))$. Since $s, (ar + b't^2) \in \mathbb{Z}$, it follows that $\gcd(s, \sqrt{-3}(ar + b't^2)) \in \mathbb{Z}$ or $\sqrt{-3}\mathbb{Z}$. So, we can write

$$\gcd(u' + \bar{u}', u' - \bar{u}') = 2(\sqrt{-3})^{\epsilon}k'$$

where $k' \in \mathbb{Z}$ and $\epsilon \in \{0, 1\}$. Note also that

$$\gcd(u', \bar{u}') \mid \gcd(u' + \bar{u}', u' - \bar{u}') \mid 2\gcd(u', \bar{u}'),$$

that is $\mathbf{d}|2(\sqrt{-3})^{\epsilon}k'|2d$. Since $\mathbb{Z}[\omega]$ is a unique factorization domain, $\mathbf{d} = (\sqrt{-3})^{\epsilon}k$ where $k = k'$ or $2k'$ and $\epsilon \in \{0, 1\}$.

Thus we have

$$\begin{aligned} u' &= (\sqrt{-3})^{\epsilon}k\beta, \\ \bar{u}' &= (-\sqrt{-3})^{\epsilon}k\bar{\beta}, \end{aligned}$$

hence

$$r^3 = u'\bar{u}' = 3^{\epsilon}k^2\beta\bar{\beta}$$

where $1 = (\frac{u'}{d}, \frac{\bar{u}'}{d}) = (\beta, \bar{\beta})$. Since $(\beta, \bar{\beta}) = 1$, β is not divisible by integral primes of $\mathbb{Z}[\omega]$ and is not divisible by $\sqrt{-3}$.

Write $k = 3^{\epsilon}k_0(k_1)^2(k_2)^3$ where $(k_0, k_1) = 1$ and k_0, k_1 are square free integers. Then we have

$$r^3 = k_0^2k_1(3^{\epsilon}k_1k_2^2)^3\beta\bar{\beta}$$

So, $k_0(k_1)^2 \mid \beta\bar{\beta}$ and the quotient is a cube. Writing $k_0 = p_1 \cdot \ldots \cdot p_t$ and $k_1 = q_1 \cdot \ldots \cdot q_s$ we have

$$\begin{aligned}
u' &= (\sqrt{-3})^{\epsilon}3^{\epsilon}k_0k_1^2k_2^3\pi_1 \cdot \ldots \cdot \pi_t\eta_1^2 \cdot \ldots \cdot \eta_s^2\gamma^3 \\
&= k_0\pi_1 \cdot \ldots \cdot \pi_t(k_1\eta_1 \cdot \ldots \cdot \eta_s)^2(k_2\gamma\left(\sqrt{-3}\right)^{\epsilon})^3 \\
&= (\pi_1 \cdot \ldots \cdot \pi_t)^2\overline{(\pi_1 \cdot \ldots \cdot \pi_t)}(\eta_1 \cdot \ldots \cdot \eta_s)^4(\overline{\eta_1 \cdot \ldots \cdot \eta_s})^2(k_2\gamma\left(\sqrt{-3}\right)^{\epsilon})^3 \\
&= (\overline{\pi_1 \cdot \ldots \cdot \pi_t} \cdot \eta_1 \cdot \ldots \cdot \eta_s)(\pi_1 \cdot \ldots \cdot \pi_t \cdot \overline{\eta_1 \cdot \ldots \cdot \eta_s})^2\left(k_2\gamma\left(\sqrt{-3}\right)^{\epsilon} \cdot \eta_1 \cdot \ldots \cdot \eta_s\right)^3 \\
&= (\overline{\pi_1 \cdot \ldots \cdot \pi_t} \cdot \eta_1 \cdot \ldots \cdot \eta_s)\overline{(\overline{\pi_1 \cdot \ldots \cdot \pi_t} \cdot \eta_1 \cdot \ldots \cdot \eta_s)}^2\left(k_2\gamma\left(\sqrt{-3}\right)^{\epsilon} \cdot \eta_1 \cdot \ldots \cdot \eta_s\right)^3
\end{aligned}$$

where $p_i = \pi_i\bar{\pi}_i$ and $q_i = \eta_i\bar{\eta}_i$ and $\gamma \in \mathbb{Z}[\omega]$.

Recall that the map α is from $E'_{ab'}(\mathbb{Q})$ to the subgroup G'_3 of $\mathbb{Q}(\omega)^*/\left(\mathbb{Q}(\omega)^*\right)^3$ of classes $[u']$ of elements u' whose norm is a cube. From the previous work, we can show that $r^3 = u'\bar{u}'$ and for $[u'] \in G'_3$, we can write $[u'] = \gamma\bar{\gamma}^2\delta^3$. Without loss of generality, we may assume the following:

1. $(\gamma, \bar{\gamma}) = 1$,

2. γ and $\bar{\gamma}$ are square-free,

3. γ and $\bar{\gamma}$ are only divisible by primes π with $N(\pi) \equiv 1 \pmod 3$ and $\pi \notin \mathbb{Z}$ (i.e. not

integer primes and not $\sqrt{-3}$).

So

$$\begin{aligned} r^3 &= \gamma\bar{\gamma}\left(\gamma\right)^2\left(\bar{\gamma}\right)^2\delta^3\bar{\delta}^3 \\ &= \left(\gamma\bar{\gamma}\right)^3\left(\delta\bar{\delta}\right)^3. \end{aligned}$$

Hence $r = \gamma\bar{\gamma}\delta\bar{\delta}$.

Also,

$$u' = s - \sqrt{-3}\left(art + b't^3\right)$$

and

$$\bar{u'} = s + \sqrt{-3}\left(art + b't^3\right).$$

Let $\delta = z_1 + z_2\omega$, $\gamma = c + d\omega$ and $\bar{\gamma} = c + d\omega^2$ where $c, d \in \mathbb{Z}$ and we may assume that δ is an algebraic integer.

Then

$$N\left(\gamma\right) = c^2 - dc + d^2,$$

$$\delta^3 = (z_1^3 + z_2^3) + 3z_1^2z_2\omega + 3z_1z_2^2\omega^2,$$

$$\bar{\delta}^3 = (z_1^3 + z_2^3) + 3z_1z_2^2\omega + 3z_1^2z_2\omega^2,$$

$$N\left(\delta\right) = z_1^2 - z_1z_2 + z_2^2,$$

and

$$\begin{aligned} r &= \gamma\bar{\gamma}\delta\bar{\delta} \\ &= N\left(\gamma\right)N\left(\delta\right). \end{aligned}$$

Notice that

$$\bar{u'} - u' = 2t\sqrt{-3}\left(ar + b't^2\right).$$

Rewriting the left hand side of the equation:

$$\begin{aligned}\bar{u'} - u' &= \bar{\gamma}\left(\gamma\right)^2\bar{\delta}^3 - \gamma\left(\bar{\gamma}\right)^2\delta^3 \\ &= \gamma\bar{\gamma}\left(\gamma\bar{\delta}^3 - \bar{\gamma}\delta^3\right) \\ &= N\left(\gamma\right)\left(\gamma\bar{\delta}^3 - \bar{\gamma}\delta^3\right).\end{aligned}$$

Substituting in for γ, $\bar{\gamma}$, δ and $\bar{\delta}$, we can see that

$$\gamma\bar{\delta}^3 - \bar{\gamma}\delta^3 =$$

$$(c + d\omega)\left((z_1^3 + z_2^3) + 3z_1z_2^2\omega + 3z_1^2z_2\omega^2\right) - \left(c + d\omega^2\right)\left((z_1^3 + z_2^3) + 3z_1^2z_2\omega + 3z_1z_2^2\omega^2\right).$$

Expanding and canceling we find that

$$\gamma\bar{\delta}^3 - \bar{\gamma}\delta^3 =$$

$$\left(dz_1^3 + dz_2^3 + 3cz_1z_2^2 - 3cz_1^2z_2 - 3dz_1z_2^2\right)\omega - \left(dz_1^3 + dz_2^3 + 3cz_1z_2^2 - 3cz_1^2z_2 - 3dz_1z_2^2\right)\omega^2.$$

Substituting in for ω and ω^2, we have

$$\gamma\bar{\delta}^3 - \bar{\gamma}\delta^3 = \sqrt{-3}\left(dz_1^3 + dz_2^3 + 3cz_1z_2^2 - 3cz_1^2z_2 - 3dz_1z_2^2\right).$$

Now consider the right hand side of the equation. Substituting in and reducing we

have:

$$2t\sqrt{-3}\left(ar+bt^2\right) \;=\; 2tN\left(\gamma\right)\sqrt{-3}\left(az_1^2-az_1z_2+az_2^2+\frac{b}{N\left(\gamma\right)}t^2\right).$$

Therefore setting the left hand side equal to the right hand side and doing a little algebra, we can define the following equation:

$$2az_1^2t-2az_1z_2t+2az_2^2t+\frac{2b'}{N\left(\gamma\right)}t^3-dz_1^3-dz_2^3-3cz_1z_2^2+3cz_1^2z_2+3dz_1z_2^2 \;=\; 0.$$

From this we obtain the following formula:

$$F_{u'}(X,Y,Z) :=$$

$$2aX^2Z-2aXYZ+2aY^2Z+\frac{2b'}{N\left(\gamma\right)}Z^3-dX^3-dY^3-3cXY^2+3cX^2Y+3dXY^2.$$

Since we want $F_{u'}(X,Y,Z)=0$ to have solutions in the integers, we need to check that $N(\gamma) \mid (2b')$.

Since $(\gamma,\bar{\gamma})=1$, and γ and $\bar{\gamma}$ are both square-free, we know that $N(\gamma)=\gamma\bar{\gamma}$ is square-free. Suppose p is a prime such that $p \mid N(\gamma)$. Since $\sqrt{-3} \nmid \gamma$ and $\sqrt{-3} \nmid \bar{\gamma}$, we know that $p \neq \sqrt{-3}$.

Recall that

$$\begin{aligned} N(\gamma)\left(\bar{\gamma}\delta^3-\gamma\bar{\delta}^3\right) &= \bar{u'}-u' \\ &= 2t\sqrt{-3}\left(ar+b't^2\right). \end{aligned}$$

Therefore $p \mid 2t\sqrt{-3}\,(ar+b't^2)$.

We know that $p \neq \sqrt{-3}$, so $p \mid 2t\,(ar+b't^2)$. Furthermore, since $(r,t)=1$ and $p \mid N(\gamma) \mid r$,

$p \nmid t$. Thus,

$$p \mid \left(2ar + 2b't^2\right).$$

Since we know that $p \mid 2ar$, it follows that $p \mid 2b'$. Hence $N(\gamma) \mid 2b'$.

Thus the definition of $\mathrm{Sel}^{(\widehat{\phi})}(E'_{ab'})$ given in Section 4.3.1 is correct.

B.2 Comparing Equations

The equation we have constructed is

$$F_{u'}(X, Y, Z) :=$$

$$2aX^2Z - 2aXYZ + 2aY^2Z + \frac{2b'}{N(\gamma)}Z^3 - dX^3 - dY^3 - 3cXY^2 + 3cX^2Y + 3dXY^2.$$

Cohen states that for the auxiliary curve, we have the following equation:

$$2v_2\mathbf{X}^3 + 2Dv_1\mathbf{Y}^3 + \frac{2b'}{v_1^2 - Dv_2^2}\mathbf{Z}^3 + 6v_1\mathbf{X}^2\mathbf{Y} + 6v_2D\mathbf{X}\mathbf{Y}^2 + 2a\left(\mathbf{X}^2\mathbf{Z} - D\mathbf{Y}^2\mathbf{Z}\right) = 0$$

where $[u] \in G_3$, $u = v^2\tau(v)$, $v = v_1 + v_2\sqrt{D}$ and $\tau(v) = v_1 - v_2\sqrt{D}$.

Let $\mathbf{X} = \frac{-1}{2}(X + Y)$, $\mathbf{Y} = \frac{1}{2}(X - Y)$, $\mathbf{Z} = Z$, $v_1 = c - \frac{d}{2}$, $v_2 = \frac{-d}{2}$ and $D = -3$. Making this substitution into Cohen's equation, we obtain the equation written above.

Here, we also note that Cohen's equation can be written as

$$\left(v\left(X + Y\sqrt{-3}\right)^3 - \tau(v)\left(X - Y\sqrt{-3}\right)^3\right)/\sqrt{-3}$$
$$+2aZ\left(X + Y\sqrt{-3}\right)\left(X - Y\sqrt{-3}\right) + \left(2b'/\left(v\tau(v)\right)\right)Z^3.$$

when $D = -3$. Since all of these equations are equivalent, we will use them interchangeably.

Appendix C Local Solubility for Curve

Here are proofs of the local solubility results as stated in Chapter 5 for the curve

$$E_{ab} : y^2 = x^3 + (ax + b)^2.$$

For additional details, we refer the reader to [14].

We begin by recalling Hensel's Lemma. See [62, pp 112 - 115] for a proof.

Lemma 90 (Hensel's Lemma)**.** *Let $f(x)$ be a polynomial with integer (p-adic) coefficients and let k, m be positive integers such that $m \leq k$. If r is an integer such that $f(r) \equiv 0 (mod\ p^k)$ and $f'(r) \not\equiv 0 (mod\ p^{k+1})$ then there exists an integer s such that $f(s) \equiv 0 (mod\ p^{k+m})$ and $r \equiv s (mod\ p^k)$.*

Let $v_p(n)$, $n \in \mathbb{N}$, be the largest exponent of p that divides n, i.e. $v_p(n) = -\log_p |n|_p$. We set $v_p(0) = \infty$. So by Lemma 36, we may assume that either $v_p(a) = 0$ or $v_p(b) \leq 2$ for E.

The following two propositions give the local solubility criteria for the polynomial

$$F_u(X, Y, Z) = u_1 X^3 + u_2 Y^3 + u_3 Z^3 - 2aXYZ$$

associated with E_{ab}.

Proposition 91 (Lemmas $5.3 - 5.5$, [14])**.** *Assume $p \neq 3$. Let*

$$F_u(X, Y, Z) = u_1 X^3 + u_2 Y^3 + u_3 Z^3 - 2aXYZ$$

with p-integral coefficients where u_1 and u_2 are square-free and coprime and $u_3 = \dfrac{2b}{u_1 u_2}$.

1. *If $p \neq 2$, $v_p(b) = 0$ and $v_p(27b - 4a^3) = 0$, then $F_u(X, Y, Z) = 0$ has a solution in $\mathbb{Q}_p$.*

2. *If* $p \neq 2$, $v_p(b) = 0$ *and* $v_p(27b - 4a^3) > 0$, *then* $F_u(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}_p$ *if and only if* u_i/u_j *is a cube in* $\mathbb{F}_p^*$ *for some* $i \neq j$.

3. *If* $p \neq 2$ *and* $v_p(b) > 0$, *then* $F_u(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}_p$ *if and only if one of the following is fulfilled:*

   (a) $v_p(a) = 0$,

   (b) $v_p(a) > 0$ *and exactly one of* $\{u_1, u_2, u_3\}$ *is divisible by* p *and the ratio of the other two is a cube in* $\mathbb{F}_p^*$,

   (c) $v_p(a) > 0$ *and exactly two of* $\{u_1, u_2, u_3\}$ *are divisible by* p *and their ratio is a cube in* $\mathbb{F}_p^*$.

4. *If* $p = 2$, *then* $F_u(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}_2$ *if and only if one of the following is fulfilled:*

   (a) *exactly one of* $\{u_1, u_2, u_3\}$ *is divisible by* 2 *and the ratio of the other two is a cube in* $\mathbb{F}_2^*$,

   (b) *exactly two of* $\{u_1, u_2, u_3\}$ *is divisible by* 2 *each exactly once and their ratio is a cube in* $\mathbb{F}_2^*$.

Proof. 1. Assume $p \neq 2, 3$, $v_p(b) = 0$ and $v_p(27b - 4a^3) = 0$. We would like to show that there are no singular points in this case, and therefore we can use Hensel's lemma. We begin by assuming $Z = 0$ and see if there are any singular points in this case. If $Z = 0$, we are left with the equation

$$u_1X^3 + u_2Y^3 = 0,$$

and to have a singular point we must have

$$\frac{\partial F}{\partial X} = 3u_1X^2 \equiv 0 \pmod{p}$$

and

$$\frac{\partial F}{\partial Y} = 3u_2Y^2 \equiv 0 \pmod{p}.$$

But since $p \neq 3$ and $u_1u_2 \mid 2b$, it follows that $X = Y = 0$, which is not possible.

Therefore we can conclude that if there is a singular point on the curve, it must have $Z \neq 0$. So without loss of generality, we can assume $Z = 1$.

Then we have a singular point if and only if

$$\frac{\partial F}{\partial X} = 3u_1X^2 - 2aYZ = 0,$$

$$\frac{\partial F}{\partial Y} = 3u_2Y^2 - 2aXZ = 0,$$

and

$$\frac{\partial F}{\partial Z} = 3u_3Z^2 - 2aXY = 0.$$

If $v_p(2a) > 0$, then $3u_3Z^2 - 2aXY = 0$ implies that $v_p(u_3) > 0$, a contradiction. Hence $v_p(2a) = 0$. Therefore we have

$$Y = \frac{3u_1X^2}{2a}$$

and

$$X = \frac{3u_2Y^2}{2a}.$$

Combining these two equations, we have

$$X = \frac{27u_1^2u_2X^4}{8a^3}.$$

If $X = 0$, then $Y = 0$. And using $3u_3Z^2 - 2aXY = 0$ and the fact that $Z = 1$, we would again have that $v_p(u_3) > 0$, which is not possible. Therefore $X \neq 0$.

So

$$X^3 = \frac{8a^3}{27u_1^2u_2}.$$

Again using $3u_3Z^2 - 2aXY = 0$ and the fact that $Z = 1$, we obtain that

$$3u_3 = 2aXY$$

and substituting in for Y, and the equation for X^3,

$$\begin{aligned} 3u_3 &= 2aX\left(\frac{3u_1X^2}{2a}\right) \\ &= 3u_1\left(\frac{8a^3}{27u_1^2u_2}\right) \\ &= \frac{8a^3}{9u_1u_2}. \end{aligned}$$

Therefore

$$27u_1u_2u_3 - 8a^3 = 2\left(27b - 4a^3\right) = 0.$$

But since $p \neq 2$, this implies that $v_p\left(27b - 4a^3\right) > 0$, a contradiction. Hence there are no singular points on this curve, so it is non-singular over $\mathbb{F}_p$.

Since it is a curve of genus 1, we know via the Weil bounds that

$$p + 1 - 2\sqrt{p} \leq \#E(\mathbb{F}_p) \leq p + 1 + 2\sqrt{p}.$$

Since the smallest prime which could satisfy the conditions listed above is 5 and

$$6 - 2\sqrt{5} > 0$$

we know that for every prime p, the curve has a non-trivial point in $\mathbb{F}_p$. Therefore for every p satisfying the above conditions, we can perform a Hensel lift to $\mathbb{Z}_p$ as soon as we know there is a solution modulo p. Thus $F_u(X,Y,Z) = 0$ has a solution in $\mathbb{Q}_p$ for all p satisfying the given conditions.

2. Assume $p \neq 2$, $v_p(b) = 0$ and $v_p\left(27b - 4a^3\right) > 0$.

   Without loss of generality, we may assume that u_2/u_1 is a cube modulo p. Then there exists a c such that $1 \leq c \leq p-1$ and $u_2/u_1 \equiv c^3 \pmod{p}$.

   Assume $Z = 0$, then we have

$$u_1 X^3 + u_2 Y^3 \equiv 0 \pmod{p}.$$

   This implies that

$$\frac{u_2}{u_1} \equiv \left(\frac{-X}{Y}\right)^3 \pmod{p}$$

   or equivalently that

$$\frac{-X}{Y} \equiv c \pmod{p}.$$

   So let $Y = 1$ and thus $X = -c$. Then we have a solution at $(-c, 1, 0)$. To verify this, notice that

$$\begin{aligned} F_u(-c,1,0) &= u_1(-c)^3 + u_2(1)^3 + 0 - 0 \\ &\equiv u_1\left(\frac{-u_2}{u_1}\right) + u_2 \pmod{p} \\ &\equiv 0 \pmod{p}. \end{aligned}$$

   In order to lift this solution using Hensel's Lemma, we must show that this point is

non-singular. To see this, we observe that

$$\begin{aligned}\frac{\partial F}{\partial X} &= 3u_1X^2 - 2aYZ,\\ \frac{\partial F}{\partial Y} &= 3u_2Y^2 - 2aXZ,\\ \frac{\partial F}{\partial Z} &= 3u_3Z^2 - 2aXY.\end{aligned}$$

And at the solution $(-c, 1, 0)$ we have that

$$\begin{aligned}\frac{\partial F}{\partial X} &= 3u_1c^2,\\ \frac{\partial F}{\partial Y} &= 3u_2,\\ \frac{\partial F}{\partial Z} &= 0.\end{aligned}$$

And since $p \neq 2, 3$, $v_p(u_1u_2) = 0$ and $1 \leq c \leq p-1$, it follows that $\dfrac{\partial F}{\partial X} \neq 0$ and $\dfrac{\partial F}{\partial Y} \neq 0$. Thus the solution is non-singular. So for every prime satisfying the given conditions, we can perform a Hensel lift to $\mathbb{Z}_p$.

Assume (x_0, y_0, z_0) is a solution modulo p to $F_u(X, Y, Z) = 0$. We may assume that $\min\{v_p(x_0), v_p(y_0), v_p(z_0)\} = 0$. We also have that

$$4v_p(x_0) + 4v_p(y_0) + 4v_p(z_0) > 0.$$

So at least one one of $\{x_0, y_0, z_0\}$ must be divisible by p. Observe that if two of $\{x_0, y_0, z_0\}$ were divisible by p, say x_0 and z_0, then the equation becomes

$$u_2y_0^3 \equiv 0 \pmod{p}.$$

Since $v_p(u_2) = 0$, this implies that $v_p(y_0) > 0$, a contradiction. Thus, at most one of

$\{x_0, y_0, z_0\}$ is divisible by p. Without loss of generality, assume $v_p(z_0) > 0$. Then we have

$$u_1 x_0^3 + u_2 y_0^3 \equiv 0 \pmod{p},$$

or equivalently

$$\frac{u_2}{u_1} \equiv \left(\frac{-X}{Y}\right)^3 \pmod{p}.$$

Hence u_i/u_j is a cube modulo p for some $i \neq j$.

Thus proving this part of the proposition.

3. Assume $p \neq 2, 3$ and $v_p(b) > 0$. Recall that we know $v_p(b) \leq 2$.

   (a) Assume $v_p(a) = 0$. Since $0 < v_p(b) \leq 2$, there are two cases we need to consider.

   Case 1: p divides only one of $\{u_1, u_2, u_3\}$.

   Without loss of generality, we may assume that $v_p(u_1) = v_p(u_2) = 0$ and $v_p(u_3) > 0$. Then the equation becomes

$$F_u(X, Y, Z) = u_1 X^3 + u_2 Y^3 - 2aXYZ.$$

   We claim that in this case,

$$\left(\frac{1}{u_1}, \frac{1}{u_2}, \frac{u_1^2 + u_2^2}{2au_1u_2}\right)$$

is a solution to $F_u(X,Y,Z) \equiv 0$ modulo p. To verify this, we see

$$\begin{aligned} F_u\left(\frac{1}{u_1}, \frac{1}{u_2}, \frac{u_1^2+u_2^2}{2au_1u_2}\right) &= u_1\left(\frac{1}{u_1}\right)^3 + u_2\left(\frac{1}{u_2}\right)^3 - 2a\left(\frac{1}{u_1}\right)\left(\frac{1}{u_2}\right)\left(\frac{u_1^2+u_2^2}{2au_1u_2}\right) \\ &= \frac{1}{u_1^2} + \frac{1}{u_2^2} - \frac{u_1^2+u_2^2}{u_1^2u_2^2} \\ &\equiv 0 \pmod{p}. \end{aligned}$$

Now it remains to verify that this point is non-singular. It is enough to show that one partial derivative is non-zero. Consider

$$\frac{\partial F}{\partial Z} = -2aXY,$$

and evaluating at the solution we see that

$$\frac{\partial F}{\partial Z} = \frac{-2a}{u_1u_2}.$$

And since $v_p(a) = v_p(u_1u_2) = 0$, it follows that $\dfrac{\partial F}{\partial Z} \not\equiv 0 \pmod{p}$.

Case 2: p divides exactly two of $\{u_1, u_2, u_3\}$

Since $v_p(b) \leq 2$, we can conclude that if p divides u_i, then it divides u_i exactly once. Without loss of generality, assume that $v_p(u_2) = v_p(u_3) = 1$, hence $v_p(u_1) = 0$. Then the equation becomes

$$F_u(X,Y,Z) = u_1X^3 - 2aXYZ$$

It is easy to see that $(0,1,1)$ is a solution modulo p. It remains to show that this point is non-singular. Again, it is enough to show that one of the partial

derivatives is non-zero. Consider

$$\frac{\partial F}{\partial X} = 3u_1X^2 - 2aYZ$$

and at the point $(0, 1, 1)$, we have that

$$\begin{aligned}\frac{\partial F}{\partial X} &= -2a \\ &\not\equiv 0 \pmod{p}\end{aligned}$$

since $v_p(2a) = 0$.

Hence if $v_p(a) = 0$, then we can find a solution modulo p which is non-singular. Thus we can perform a Hensel lift to $\mathbb{Z}_p$.

(b) Assume $v_p(a) > 0$, p divides exactly one of $\{u_1, u_2, u_3\}$ and the ratio of the other two is a cube modulo p. Without loss of generality, assume $v_p(u_3) > 0$ and u_1/u_2 is a cube modulo p. Then there exists a c such that $1 \leq c \leq p-1$ and $u_1/u_2 \equiv c^3 \pmod{p}$. We claim that $(1, -c, 0)$ is a solution modulo p. Let's verify this:

$$\begin{aligned}F_u(1, -c, 0) &= u_1(1)^3 + u_2(-c)^3 \\ &\equiv u_1 + u_2\left(\frac{-u_1}{u_2}\right) \pmod{p} \\ &\equiv 0 \pmod{p}.\end{aligned}$$

It is easy to see that the point is not singular since

$$\frac{\partial F}{\partial X} = 3u_1X^2,$$

which is clearly not equivalent to zero modulo p at the solution. So we can perform

a Hensel lift to $\mathbb{Z}_p$.

(c) Assume $v_p(a) > 0$, p divides exactly two of $\{u_1, u_2, u_3\}$ and the ratio of these two coefficients is a cube modulo p. Without loss of generality, assume $v_p(u_2) = 0$. Then since $v_p(b) \leq 2$, it follows that $v_p(u_1) = v_p(u_3) = 1$. So there exists a c such that $1 \leq c \leq p-1$ and $u_1/u_3 \equiv c^3 \pmod{p}$. Note that since p divides u_1 and u_3 exactly once, $v_p(u_1/u_3) = 0$. In addition, we can write $u_1 = p\overline{u_1}$ and $u_3 = p\overline{u_3}$. Let's make the following substitution, $Y = py$. Then the equation becomes

$$F_u(X, py, Z) \;=\; p\overline{u_1}X^3 + pu_2p^2y^3 + p\overline{u_3}Z^3 - 2aXpyZ.$$

Let $U_2 = u_2p^2$, then we have that

$$\frac{1}{p}F_u(X, py, Z) \;=\; \overline{u_1}X^3 + U_2y^3 + \overline{u_3}Z^3 - 2aXyZ.$$

Thus we are in the situation of (b) from above. Hence we can find a non-singular solution and it lifts.

Assume that (x_0, y_0, z_0) is a non-singular solution of $F_u(X, Y, Z) \equiv 0 \pmod{p}$. We may assume that $\min\{v_p(x_0), v_p(y_0), v_p(z_0)\} = 0$. In addition, since $v_p(b) > 0$, without loss of generality we may assume $v_p(u_3) > 0$. There are two cases we need to consider.

Case 1: $v_p(u_1u_2) = 0$

In this case the equation becomes

$$u_1x_0^3 + u_2y_0^3 - 2ax_0y_0z_0 \;\equiv\; 0 \pmod{p}.$$

If $v_p(a) > 0$, then we have

$$u_1x_0^3 + u_2y_0^3 \;\equiv\; 0 \pmod{p}.$$

The partial derivatives at the solution are

$$\begin{aligned}\frac{\partial F}{\partial X} &= 3u_1x_0^2,\\ \frac{\partial F}{\partial Y} &= 3u_2y_0^2,\\ \frac{\partial F}{\partial Z} &= 0.\end{aligned}$$

Since the point is non-singular, this implies that both x_0 and y_0 are non-zero modulo p. Hence

$$\frac{u_1}{u_2} \equiv \left(\frac{-y_0}{x_0}\right)^3 \pmod{p}.$$

Otherwise, $v_p(a) = 0$ and we obtain no additional information.

Case 2: $v_p(u_1u_2) > 0$

Without loss of generality, assume $v_p(u_2) > 0$. Since $v_p(b) \leq 2$, this implies that $v_p(u_2) = v_p(u_3) = 1$. So the equation becomes

$$u_1x_0^3 - 2ax_0y_0z_0 \equiv 0 \pmod{p}.$$

If $v_p(a) = 0$, we obtain no additional information.

If $v_p(a) > 0$, then $x_0 \equiv 0 \pmod{p}$. So we can divide out a p from the equation and reduce modulo p to obtain

$$\frac{u_2}{p}y_0^3 + \frac{u_3}{p}z_0^3 \equiv 0 \pmod{p}.$$

In this case, the partials derivatives are

$$\begin{aligned}\frac{\partial F}{\partial X} &= 0,\\ \frac{\partial F}{\partial Y} &= \frac{3u_2}{p}y_0^2,\\ \frac{\partial F}{\partial Z} &= \frac{3u_3}{p}z_0^2.\end{aligned}$$

Since the solution is non-singular, we know that both y_0 and z_0 are non-zero modulo p. Therefore,

$$\frac{u_3}{u_2} \equiv \left(\frac{-y_0}{z_0}\right)^3 \pmod{p}.$$

Hence if we have a solution to $F_u(X,Y,Z) = 0$ in $\mathbb{Q}_p$ for all p satisfying the given conditions then either $v_p(a) = 0$, $v_p(a) > 0$ with p dividing exactly one of $\{u_1, u_2, u_3\}$ and the ratio of the other two is a cube in $\mathbb{F}_p^*$, or $v_p(a) > 0$, exactly two of $\{u_1, u_2, u_3\}$ are divisible by p and their ratio is a cube in $\mathbb{F}_p^*$.

4. These proofs are almost identical to the ones given in $3b$ and $3c$. The only things we have to show is that if $4 \mid b$, and $2 \mid u_1u_2$, then we do not have a solution in $\mathbb{Q}_2$.
   It suffices to show that there is no non-singular solution modulo 8. For sake of contradiction, assume there exists a non-singular solution, (x, y, z) modulo 8. Then $2 \mid u_1u_2$ and $4 \mid u_3$. Without loss of generality, assume $2 \mid u_1$. So modulo 8, the equation is of the form:

$$2\overline{u_1}x^3 + u_2y^3 + 4\overline{u_3}z^3 - 2axyz \equiv 0 \pmod{8}$$

where $u_1 = 2\overline{u_1}$ and $u_3 = 4\overline{u_3}$. Also, notice that

$$\begin{aligned}
\left.\frac{\partial F}{\partial X}\right|_{(x,y,z)} &= 2\left(3\overline{u_1}x^2 - ayz\right) \\
\left.\frac{\partial F}{\partial Y}\right|_{(x,y,z)} &= 3u_2y^2 - 2axz \\
\left.\frac{\partial F}{\partial Z}\right|_{(x,y,z)} &= 2\left(6\overline{u_3}z^2 - axy\right).
\end{aligned}$$

Rearranging the equation, we have

$$2\left(\overline{u_1}x^3 + 2\overline{u_3}z^3 - axyz\right) \equiv -u_2y^3 \pmod{8},$$

which is true if and only if $2 \mid y^3$. So we have that $2 \mid y$. Since we also assumed the solution was non-singular, we know at least one of the partial derivatives must be non-zero. Begin by assuming $\left.\frac{\partial F}{\partial X}\right|_{(x,y,z)} \neq 0$. This implies $3\overline{u_1}x^2 - ayz \not\equiv 0 \pmod 4$ or equivalently $3\overline{u_1}x^2 \not\equiv ayz \pmod 4$. So we can conclude that $2 \nmid x$. Using this, we can look at the original equation modulo 8 and notice that

$$\begin{aligned}
2\left(\overline{u_1}x^3 + 2\overline{u_3}z^3 - axyz\right) &\equiv -u_2y^3 \pmod 8 \\
\overline{u_1}x^3 + 2\overline{u_3}z^3 - axyz &\equiv 0 \pmod 4 \\
2\left(\overline{u_3}z^3 - ax\overline{y}z\right) &\equiv \overline{u_1}x^3 \pmod 4
\end{aligned}$$

where $y = 2\overline{y}$. However this is a contradiction since we assumed $2 \nmid x$. Thus $\left.\frac{\partial F}{\partial X}\right|_{(x,y,z)} = 0$ and so it must be the case that $2 \mid x$.

Now assume $\left.\frac{\partial F}{\partial Z}\right|_{(x,y,z)} \neq 0$. Then $6\overline{u_3}z^2 - axy \not\equiv 0 \pmod 4$. Since $2 \mid x$ and $2 \mid y$, it follows that for this to be true, we must have $2 \nmid z$. But looking at the original

equation since $2 \mid x$ and $2 \mid y$ we have

$$2\overline{u_3}z^3 \equiv 0 \pmod{4},$$

which is a contradiction since we assumed $2 \nmid z$. Therefore $\left.\frac{\partial F}{\partial Z}\right|_{(x,y,z)} = 0$. This implies $2 \mid z$, which tells us that $\left.\frac{\partial F}{\partial Y}\right|_{(x,y,z)} = 0$. Therefore we cannot find a non-singular solution.

□

The following proposition gives the solubility conditions for the prime $p = 3$.

Proposition 92 (Lemmas 5.6, 5.9, 5.10, [14]). *Let*

$$F_u(X, Y, Z) = u_1X^3 + u_2Y^3 + u_3Z^3 - 2aXYZ$$

with 3-integral coefficients where u_1 and u_2 are square-free and coprime and $u_3 = \frac{2b}{u_1u_2}$.

1. *If $v_3(a) = 0$, then $F_u(X, Y, Z) = 0$ has a solution in $\mathbb{Q}_3$.*

2. *If $v_3(a) \geq 2$ and $v_3(b) = 0$ then $F_u(X, Y, Z) = 0$ has a solution in $\mathbb{Q}_3$ if and only if u_i/u_j is a cube modulo 9 for some $i \neq j$.*

3. *If $v_3(a) \geq 2$ and exactly one of $\{u_1, u_2, u_3\}$ is divisible by 3, say u_i, then $F_u(X, Y, Z) = 0$ has a solution in $\mathbb{Q}_3$ if and only if either the ratio of the other two is a cube modulo 9 or $v_3(u_i) = 1$.*

4. *If $v_3(a) \geq 2$ and exactly two of $\{u_1, u_2, u_3\}$ are divisible by 3, then $F_u(X, Y, Z) = 0$ has a solution in $\mathbb{Q}_3$ if and only if their ratio is a cube modulo 9.*

5. *If $v_3(a) = 1$ and exactly one of $\{u_1, u_2, u_3\}$ is divisible by 3, then $F_u(X, Y, Z) = 0$ has a solution in $\mathbb{Q}_3$ if and only if either the ratio of the other two is a cube modulo 9 or*

there exists $s_1, s_2 \in \{\pm 1\}$ *such that* $2a \equiv s_1u_1 + s_2u_2 + s_1s_2u_3 \pmod 9$.

6. *If* $v_3(a) = 1$ *and two of* $\{u_1, u_2, u_3\}$ *are divisible by* 3, *then* $F_u(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}_3$.

7. *If* $v_3(a) = 1$, $v_3(b) = 0$ *and* u_i/u_j *is a cube modulo* 9 *for some* $i \neq j$, *then* $F_u(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}_3$.

8. *If* $v_3(a) = 1$, $v_3(b) = 0$ *and* u_i/u_j *is not a cube modulo* 9 *for all* $i \neq j$ *then* $F_u(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}_3$ *if and only if there exists* $s_1, s_2 \in \{\pm 1\}$ *such that* $2a \equiv s_1u_1 + s_2u_2 + s_1s_2u_3 \pmod{27}$.

In order to prove the above proposition, we need a slight strengthening of Hensel's lemma.

Lemma 93 (Lemma 5.7, [14]). *Assume* $v_3(a) > 0$. *Set* $P_0 = (X_0, Y_0, Z_0)$ *and let* $k \geq 1$. *Assume that* $v_3(F_u(P_0)) \geq 2k$ *and that*

$$\min\left\{v_3\left(\left.\frac{\partial F}{\partial X}\right|_{P_0}\right), v_3\left(\left.\frac{\partial F}{\partial Y}\right|_{P_0}\right), v_3\left(\left.\frac{\partial F}{\partial Z}\right|_{P_0}\right)\right\} = k.$$

Assume that all second and third partial derivatives of F_u *are divisible by* 3 *at the point* P_0, *the condition on the third derivatives being required only if* $k = 1$. *There exists a* 3*-adic point* P *such that* $F_u(P) = 0$ *with* $P \equiv P_0 \pmod{3^k}$.

Proof. We will give a general idea of the proof of this lemma. Assume $v_3(a) > 0$. Let $P_0 = (X_0, Y_0, Z_0)$ and let $k \geq 1$. Assume that $v_3(F_u(P_0)) \geq 2k$ and that

$$\min\left\{v_3\left(\left.\frac{\partial F}{\partial X}\right|_{P_0}\right), v_3\left(\left.\frac{\partial F}{\partial Y}\right|_{P_0}\right), v_3\left(\left.\frac{\partial F}{\partial Z}\right|_{P_0}\right)\right\} = k.$$

Then we can write $F_u(P_0) = 3^{2k}N$, $\left.\frac{\partial F}{\partial X}\right|_{P_0} = 3^k m_1$, $\left.\frac{\partial F}{\partial Y}\right|_{P_0} = 3^k m_2$ and $\left.\frac{\partial F}{\partial Z}\right|_{P_0} = 3^k m_3$,

where $N = \dfrac{F_u(P_0)}{3^{2k}} \in \mathbb{Z}$ and at least one of $m_1, m_2, m_3 \in \mathbb{Z}$ is not divisible by 3. Without loss of generality, assume $v_3(m_1) = 0$.

Consider $P_1 = \left(X_0 + 3^k l_1, Y_0 + 3^k l_2, Z_0 + 3^k l_3\right)$. Then

$$\begin{aligned} F_u(P_1) &= u_1\left(X_0 + 3^k l_1\right) + u_2\left(Y_0 + 3^k l_2\right) + u_3\left(Z_0 + 3^k l_3\right) \\ &\quad -2a\left(X_0 + 3^k l_1\right)\left(Y_0 + 3^k l_2\right)\left(Z_0 + 3^k l_3\right). \end{aligned}$$

Expanding we have

$$F_u(P_1) = 3^{2k}N + \left.\frac{\partial F}{\partial X}\right|_{P_0} 3^k l_1 + \left.\frac{\partial F}{\partial Y}\right|_{P_0} 3^k l_2 + \left.\frac{\partial F}{\partial Z}\right|_{P_0} 3^k l_3 + 3^{2k+1}(\star)$$

where $\star$ represents the terms having a factor of 3^{2k+1}. Then reducing modulo 3^{2k+1}, we have

$$F_u(P_1) \equiv 3^{2k}N + 3^{2k}m_1 l_1 + 3^{2k}m_2 l_2 + 3^{2k}m_3 l_3 \pmod{3^{2k+1}}.$$

Dividing by 3^{2k} and rearranging we have

$$l_1 \equiv -m_1^{-1}\left(m_2 l_2 + m_3 l_3 + N\right) \pmod 3.$$

Therefore we can solve for l_1. The rest of the lemma follows from here. □

One thing to notice is that in the case of Lemma 93

$$\begin{aligned} \frac{\partial F}{\partial X} &= 3u_1X^2 - 2aYZ, \\ \frac{\partial F}{\partial Y} &= 3u_2Y^2 - 2aXZ, \\ \frac{\partial F}{\partial Y} &= 3u_3Z^2 - 2aXY. \end{aligned}$$

Since $v_3(a) > 0$, it follows that all partial derivatives are divisible by 3 at any point. Therefore

it is enough to find a point P_0 such that $F_u(P_0) \equiv 0 \pmod{3^{2k}}$ and

$$\min\left\{ v_3\left(\left.\frac{\partial F}{\partial X}\right|_{P_0}\right), v_3\left(\left.\frac{\partial F}{\partial Y}\right|_{P_0}\right), v_3\left(\left.\frac{\partial F}{\partial Z}\right|_{P_0}\right)\right\} = k.$$

Now we are able to prove the proposition.

Proof. 1. Assume $v_3(a) = 0$. There are a few cases we need to consider.

Case 1: 3 divides exactly one of $\{u_1, u_2, u_3\}$

Without loss of generality, we may assume $v_3(u_1u_2) = 0$ and $v_3(u_3) > 0$. In this case, the equation reduces modulo 3 to

$$F_u(X,Y,Z) \;=\; u_1X^3 + u_2Y^3 - 2aXYZ.$$

We claim that in this case,

$$\left(\frac{1}{u_1}, \frac{1}{u_2}, \frac{u_1^2+u_2^2}{2au_1u_2}\right)$$

is a solution to $F_u(X,Y,Z) \equiv 0 \pmod 3$. Let us verify this:

$$\begin{aligned} F_u\left(\frac{1}{u_1}, \frac{1}{u_2}, \frac{u_1^2+u_2^2}{2au_1u_2}\right) &= u_1\left(\frac{1}{u_1}\right)^3 + u_2\left(\frac{1}{u_2}\right)^3 - 2a\left(\frac{1}{u_1}\right)\left(\frac{1}{u_2}\right)\left(\frac{u_1^2+u_2^2}{2au_1u_2}\right) \\ &= \frac{1}{u_1^2} + \frac{1}{u_2^2} - \frac{u_1^2+u_2^2}{u_1^2u_2^2} \\ &\equiv 0 \pmod 3. \end{aligned}$$

Now it remains to verify that this point is non-singular. It is enough to show that one partial derivative is non-zero. Consider

$$\frac{\partial F}{\partial Z} \;=\; -2aXY.$$

Evaluating at the solution we see that

$$\frac{\partial F}{\partial Z} = \frac{-2a}{u_1 u_2}.$$

Since $v_p(a) = v_p(u_1 u_2) = 0$, it follows that $\frac{\partial F}{\partial Z} \not\equiv 0 \pmod 3$. So we can perform a Hensel lift to $\mathbb{Z}_3$.

Case 2: 3 divides two of $\{u_1, u_2, u_3\}$

Without loss of generality, assume $v_3(u_2) > 0$ and $v_3(u_3) > 0$. Since $v_3(b) \leq 2$, it follows that $v_3(u_2) = v_3(u_3) = 1$. In this case, the equation over $\mathbb{F}_3$ becomes

$$F_u(X, Y, Z) = u_1 X^3 - 2aXYZ.$$

It is easy to see that $(0, 1, 1)$ is a solution. To show that this solution is non-singular, it is enough to show that one partial derivative is non-zero. Consider

$$\frac{\partial F}{\partial X} = -2aYZ.$$

This is clearly non-zero at the solution. Thus we can perform a Hensel lift to $\mathbb{Z}_3$.

Case 3: $v_3(b) = 0$

From this assumption and the fact that $v_3(a) = 0$, we can conclude that $v_3(27b - 4a^3) = 0$. Note that the partial derivatives in this case are

$$\begin{aligned} \frac{\partial F}{\partial X} &= -2aYZ, \\ \frac{\partial F}{\partial Y} &= -2aXY, \\ \frac{\partial F}{\partial Z} &= -2aXY. \end{aligned}$$

If $Z = 0$, then for us to have a singular point, either X or Y must be zero. Without loss of generality assume that $X = 0$. Then the equation over $\mathbb{F}_3$ becomes

$$F_u(0, Y, 0) \quad = \quad u_2 Y^3,$$

which implies Y must be zero for us to have a solution modulo 3. Therefore, if there is a singular point, it must have $Z \neq 0$. So without loss of generality, assume $Z = 1$. However, in this case for us to have a singular point, we must have both X and Y being zero. Then the equation becomes over $\mathbb{F}_3$

$$F_u(0, 0, Z) \quad = \quad u_3 Z^3,$$

which is a solution if $Z = 0$. Therefore there are no singular points on the curve. Since it is a curve of genus 1, the Weil bounds give

$$p + 1 - 2\sqrt{p} \leq \#E(\mathbb{F}_p) \leq p + 1 + 2\sqrt{p}.$$

Since

$$4 - 2\sqrt{3} > 0,$$

we know that the curve has a non-trivial point in $\mathbb{F}_3$. Therefore we can perform a Hensel lift to $\mathbb{Z}_3$ as soon as we know there is a solution modulo 3.

2. Assume $v_3(a) \geq 2$, $v_3(b) = 0$ and u_i/u_j is a cube modulo 9. Without loss of generality, we may assume $u_1/u_2 \equiv c^3 \pmod 9$ for some c. We claim that $P_0 = (1, -c, 0)$ is a

non-singular solution modulo 9. To verify this notice that

$$\begin{aligned} F_u(1,-c,0) &= u_1 - u_2 c^3 \\ &\equiv u_1 - u_2 \frac{u_1}{u_2} \pmod 9 \\ &\equiv 0 \pmod 9 \end{aligned}$$

and

$$\begin{aligned} \left.\frac{\partial F}{\partial X}\right|_{P_0} &= 3u_1 \\ &\not\equiv 0 \pmod 9 . \end{aligned}$$

Thus the solution is non-singular and therefore we perform a Hensel lift.

To see that there exists a solution modulo 3, notice that

$$\min\left\{ v_3\left(\left.\frac{\partial F}{\partial X}\right|_{P_0}\right), v_3\left(\left.\frac{\partial F}{\partial Y}\right|_{P_0}\right), v_3\left(\left.\frac{\partial F}{\partial Z}\right|_{P_0}\right)\right\} = 1.$$

Therefore by Lemma 93, we know there exists a P such that $P \equiv P_0 \pmod 3$ and $F_u(P) \equiv 0 \pmod 3$.

The reverse direction is nothing more than a simple calculation.

3. Assume $v_3(a) \geq 2$ and 3 divides exactly one of $\{u_1, u_2, u_3\}$, say u_i.

   There are two cases we need to consider in the forward direction.

   Case 1: u_j/u_k is a cube modulo 9 for $j,k \neq i$ and $j \neq k$.

   Without loss of generality, assume $v_3(u_3) > 0$ and $u_1/u_2 \equiv c^3 \pmod 9$. In this case, we claim that $P_0 = (1,-c,0)$ is a solution modulo 9 which is non-singular. Verifying

this we see

$$\begin{aligned} F_u(1,-c,0) &= u_1(1)^3 + u_2(-c)^3 \\ &\equiv u_1 - u_2\frac{u_1}{u_2} \pmod 9 \\ &\equiv 0 \pmod 9 \end{aligned}$$

and

$$\begin{aligned} \left.\frac{\partial F}{\partial X}\right|_{P_0} &= 3u_1 \pmod 9 \\ &\not\equiv 0 \pmod 9 . \end{aligned}$$

Therefore we can lift the solution. Now it only remains to show there is a solution modulo 3. However from the above partial derivative, we can easily see

$$\min\left\{ v_3\left(\left.\frac{\partial F}{\partial X}\right|_{P_0}\right), v_3\left(\left.\frac{\partial F}{\partial Y}\right|_{P_0}\right), v_3\left(\left.\frac{\partial F}{\partial Z}\right|_{P_0}\right)\right\} = 1.$$

Hence by Lemma 93, there exists P such that $P \equiv P_0 \pmod 3$ and $F_u(P) \equiv 0 \pmod 3$.

Case 2: $v_3(u_i) = 1$

Without loss of generality, assume $u_i = u_3$.

Since we know that setting $Z = 0$ we can find a solution when u_1/u_2 is a cube modulo 9, we may assume u_1/u_2 is not a cube modulo 9. Equivalently this means that $u_1 \not\equiv \pm u_2 \pmod 9$. Therefore for us to have a solution modulo 9, $Z \neq 0$. In addition, we

know that reducing modulo 9,

$$\begin{aligned} \frac{\partial F}{\partial X} &= 3u_1X^2, \\ \frac{\partial F}{\partial Y} &= 3u_2Y^2, \\ \frac{\partial F}{\partial Z} &= 0. \end{aligned}$$

So in order to have a non-singular point either $X \neq 0$ or $Y \neq 0$.

Notice that reducing the equation modulo 9, we have

$$F_u(X,Y,Z) = u_1X^3 + u_2Y^3 + 3u_3'Z^3$$

where $u_3 = 3u_3'$.

Since by symmetry we can switch X and Y, we may assume that $u_1 < u_2$.

Suppose that $Y \equiv 0 \pmod 3$. Then the equation reduces modulo 9 to

$$F_u(X,0,Z) = \pm u_1 \pm 3u_3'$$

since $X^3 \equiv \pm 1 \pmod 9$ and $Z^3 \equiv \pm 1 \pmod 9$. But then for us to have a solution, this implies that

$$\pm u_1 \equiv \pm 3u_3' \pmod 9$$

which is not possible since $v_3(u_1) = 0$.

Thus the equation reduces modulo 9 to

$$\pm u_1 \pm u_2 \pm 3 \equiv 0 \pmod 9$$

A simple calculation shows that we can always find a solution.

Assume $v_3(a) \geq 2$ and 3 divides exactly one of $\{u_1, u_2, u_3\}$. Without loss of generality, assume $v_3(u_3) > 0$. Let (x_0, y_0, z_0) be a solution modulo 9 to $F_u(X, Y, Z) = 0$. Then if $v_2(u_3) \geq 2$, we have

$$u_1 x_0^3 + u_2 y_0^3 \equiv 0 \pmod 9.$$

Hence u_1/u_2 is a cube modulo 9. Otherwise, $v_3(u_3) = 1$.

4. Assume $v_3(a) \geq 2$ and exactly two of $\{u_1, u_2, u_3\}$ are divisible by 3.

   Without loss of generality, assume $v_3(u_1) > 0$ and $v_3(u_3) > 0$. Since $v_3(b) \leq 2$, it follows that $v_3(u_1) = v_3(u_3) = 1$. In addition, assume $u_1/u_3 \equiv c^3 \pmod 9$. Note this makes sense since they are both divisible by 3 exactly once, so $v_3(u_1/u_3) = 0$. In addition, we can write $u_1 = 3\widetilde{u_1}$ and $u_3 = 3\widetilde{u_3}$.

   Let us make the following substitution, $Y = 3y$. Then the equation becomes

$$F_u(X, 3y, Z) = 3\widetilde{u_1}X^3 + 3u_2(9)y^3 + 3\widetilde{u_3}Z^3 - 2aX(3y)Z.$$

   Let $U_2 = u_2(9)$, then we have that

$$\begin{aligned} \widetilde{F_u}(X, 3y, Z) &:= \frac{1}{3}F_u(X, 3y, Z) \\ &= \widetilde{u_1}X^3 + U_2 y^3 + \widetilde{u_3}Z^3 - 2aXyZ. \end{aligned}$$

   We claim that $P_0 = (1, 3, -c)$ is a solution modulo 9 to the modified equation. To see

this note

$$\begin{aligned}\widetilde{F_u}(1,3,-c) &\equiv \widetilde{u_1} + \widetilde{u_3}(-c)^3 \pmod 9 \\ &\equiv \widetilde{u_1} - \widetilde{u_3}\frac{\widetilde{u_1}}{\widetilde{u_3}} \pmod 9 .\end{aligned}$$

Also, this point is non-singular since

$$\left.\frac{\partial \widetilde{F}}{\partial X}\right|_{P_0} = u_1 \pmod 9 .$$

Therefore we can lift the solution. Now it only remains to show there is a solution modulo 3. However from the above partial derivative, we can easily see

$$\min\left\{ v_3\left(\left.\frac{\partial \widetilde{F}}{\partial X}\right|_{P_0}\right), v_3\left(\left.\frac{\partial \widetilde{F}}{\partial Y}\right|_{P_0}\right), v_3\left(\left.\frac{\partial \widetilde{F}}{\partial Z}\right|_{P_0}\right)\right\} = 1.$$

Hence by Lemma 93, there exists P such that $P \equiv P_0 \pmod 3$ and $F_u(P) \equiv 0 \pmod 3$.

Assume that $v_3(u_2) = v_3(u_3) = 1$. Also, assume that $P_0 = (x_0, y_0, z_0)$ is a solution modulo 9.

If $x_0 \equiv 0 \pmod 3$, then

$$\begin{aligned}F_u(x_0, y_0, z_0) &= u_2 y_0^3 + u_3 z_0^3 \\ &\equiv 0 \pmod 9 .\end{aligned}$$

Hence u_2/u_3 is a cube modulo 9.

If $x_0 \not\equiv 0 \pmod 9$, then $x_0^3 \equiv \pm 1 \pmod 9$. So the equation reduces to

$$F_u(x_0, y_0, z_0) \equiv \pm u_1 + u_2 y_0^3 + u_3 z_0^3 \pmod 9 .$$

By symmetry, we can switch y_0 and z_0. So without loss of generality, suppose $y_0 \equiv 0 \pmod 3$. Then

$$F_u(x_0, y_0, z_0) \equiv \pm u_1 + u_3 z_0^3 \pmod 9$$

which implies

$$\pm u_1 \equiv -3z_0^3 \pmod 9 .$$

This is a contradiction since $v_3(u_1) = 0$. Therefore $y_0 \not\equiv 0 \pmod 3$ and hence $z_0 \not\equiv 0 \pmod 3$. But then since

$$u_2 \equiv \pm 3 \pmod 9$$

and

$$u_3 \equiv \pm 3 \pmod 9$$

it follows that

$$u_2 \equiv \pm u_3 \pmod 9$$

which implies that u_2/u_3 is a cube modulo 9.

5. Assume $v_3(a) = 1$ and exactly one of $\{u_1, u_2, u_3\}$ is divisible by 3, say u_i.

   In the forward direction, there are two cases we need to consider.

   Case 1: $u_j/u_k \equiv c^3 \pmod 9$ where $j \neq i$, $k \neq i$ and $j \neq k$

   Without loss of generality, assume $v_3(u_3) > 0$ and $u_1/u_2 \equiv c^3 \pmod 9$. In this case, we claim that $P_0 = (1, -c, 0)$ is a non-singular solution modulo 9. Verifying this we

see

$$\begin{aligned} F_u(1,-c,0) &= u_1(1)^3 + u_2(-c)^3 \\ &\equiv u_1 - u_2\frac{u_1}{u_2} \pmod 9 \\ &\equiv 0 \pmod 9 \end{aligned}$$

and

$$\begin{aligned} \left.\frac{\partial F}{\partial X}\right|_{P_0} &= 3u_1 \pmod 9 \\ &\not\equiv 0 \pmod 9 . \end{aligned}$$

Therefore we can lift the solution. Now it only remains to show there is a solution modulo 3. However from the above partial derivative, we can easily see

$$\min\left\{ v_3\left(\left.\frac{\partial F}{\partial X}\right|_{P_0}\right), v_3\left(\left.\frac{\partial F}{\partial Y}\right|_{P_0}\right), v_3\left(\left.\frac{\partial F}{\partial Z}\right|_{P_0}\right)\right\} = 1.$$

Hence by Lemma 93, there exists P such that $P \equiv P_0 \pmod 3$ and $F_u(P) \equiv 0 \pmod 3$.

Case 2: There exists $s_1, s_2 \in \{\pm 1\}$ such that $2a \equiv s_1u_1 + s_2u_2 + s_1s_2u_3 \pmod 9$. Without loss of generality we may assume $u_i = u_3$. We claim that $P_0 = (s_1, s_2, s_1s_2)$ is a non-singular solution modulo 9. To see this, notice that

$$\begin{aligned} F_u(P_0) &= u_1(s_1)^3 + u_2(s_2)^3 + u_3(s_1s_2)^3 - 2as_1^2s_2^2 \\ &\equiv u_1s_1 + u_2s_2 + u_3s_1s_2 - (u_1s_1 + u_2s_2 + u_3s_1s_2) \pmod 9 \\ &\equiv 0 \pmod 9 \end{aligned}$$

since $s_i^2 = 1$ and $s_i^3 = s_i$ and

$$\begin{aligned} \left.\frac{\partial F}{\partial Z}\right|_{P_0} &= -2as_1s_2 \\ &\not\equiv 0 \pmod 9 . \end{aligned}$$

This implies

$$\min\left\{ v_3\left(\left.\frac{\partial F}{\partial X}\right|_{P_0}\right), v_3\left(\left.\frac{\partial F}{\partial Y}\right|_{P_0}\right), v_3\left(\left.\frac{\partial F}{\partial Z}\right|_{P_0}\right)\right\} = 1.$$

Hence by Lemma 93, there exists P such that $P \equiv P_0 \pmod 3$ and $F_u(P) \equiv 0 \pmod 3$.

Assume $v_3(a) = 1$ and exactly one of $\{u_1, u_2, u_3\}$ is divisible by 3. Let $P_0 = (x_0, y_0, z_0)$ be a solution modulo 9. Without loss of generality, assume $v_3(u_3) > 0$.

If $z_0 \equiv 0 \pmod 3$, then we have

$$u_1x_0^3 + u_2y_0^3 \equiv 0 \pmod 9 ,$$

which implies that u_1/u_2 is a cube modulo 9.

Now assume $z_0 \not\equiv 0 \pmod 3$. Note that by symmetry, we can interchange x_0 and y_0. So without loss of generality, if $x_0 \equiv 0 \pmod 3$, then

$$u_2y_0^3 + u_3z_0^3 \equiv 0 \pmod 9 .$$

This implies

$$\pm u_2 \equiv \pm 3\widetilde{u_3} \pmod 9$$

where $u_3 = 3\widetilde{u_3}$. This is a contradiction since $v_3(u_2) = 0$. Hence $x_0 \not\equiv 0 \pmod 3$ and thus $y_0 \not\equiv 0 \pmod 3$. A simple calculation shows that in this case u_1/u_2 cannot be a

cube modulo 9. However, one can find $s_1, s_2 \in \{\pm 1\}$ such that

$$2a \equiv s_1u_1 + s_2u_2 + s_1s_2u_3 \pmod 9.$$

6. Assume $v_3(a) = 1$ and exactly two of $\{u_1, u_2, u_3\}$ are divisible by 3. Without loss of generality, assume that $v_3(u_2) = 0$. Then since $v_3(b) \leq 2$, it follows that $v_3(u_1) = v_3(u_3) = 1$. Notice that this means

$$u_1 \equiv \pm 3 \pmod 9$$

and

$$u_3 \equiv \pm 3 \pmod 9.$$

Hence we can conclude that

$$u_1/u_3 \equiv c^3 \pmod 9$$

for some c where $\gcd(c, 9) = 1$. Note this makes sense since they are both divisible by 3 exactly once, so $v_3(u_1/u_3) = 0$.

We claim that $P_0 = (1, 0, -c)$ is a solution modulo 9. To see this notice that

$$\begin{aligned} F_u(1, 0, -c) &= u_1 + u_3(-c)^3 \\ &\equiv u_1 - u_3\left(\frac{u_1}{u_3}\right) \pmod 9 \\ &\equiv 0 \pmod 9. \end{aligned}$$

Since

$$\begin{aligned} \left.\frac{\partial F}{\partial X}\right|_{P_0} &= 3u_1(0)^2 - 2a(1)(-c) \\ &\not\equiv 0 \pmod 9, \end{aligned}$$

we know that P_0 is non-singular. Therefore we can lift a solution. Now it only remains to show there is a solution modulo 3. However from the above partial derivative we can easily see

$$\min\left\{v_3\left(\left.\frac{\partial F}{\partial X}\right|_{P_0}\right), v_3\left(\left.\frac{\partial F}{\partial Y}\right|_{P_0}\right), v_3\left(\left.\frac{\partial F}{\partial Z}\right|_{P_0}\right)\right\} = 1.$$

Hence by Lemma 93, there exists P such that $P \equiv P_0 \pmod 3$ and $F_u(P) \equiv 0 \pmod 3$.

7. Assume $v_3(a) = 1$, $v_3(b) = 0$ and u_i/u_j is a cube modulo 9 for $i \neq j$. Without loss of generality, assume $u_1/u_2 \equiv c^3 \pmod 9$. We claim that $P_0 = (1, -c, 0)$ is a non-singular solution modulo 9. To see this, we observe that

$$\begin{aligned} F_u(P_0) &= u_1(1)^3 + u_2(-c)^3 \\ &\equiv u_1 - u_2\frac{u_1}{u_2} \pmod 9 \\ &\equiv 0 \pmod 9 \end{aligned}$$

and

$$\begin{aligned} \left.\frac{\partial F}{\partial X}\right|_{P_0} &= 3u_1 \\ &\not\equiv 0 \pmod 9. \end{aligned}$$

Therefore we can lift the solution. Now it only remains to show there is a solution modulo 3. However from the above partial derivative, we can easily see

$$\min\left\{v_3\left(\left.\frac{\partial F}{\partial X}\right|_{P_0}\right), v_3\left(\left.\frac{\partial F}{\partial Y}\right|_{P_0}\right), v_3\left(\left.\frac{\partial F}{\partial Z}\right|_{P_0}\right)\right\} = 1.$$

Hence by Lemma 93, there exists P such that $P \equiv P_0 \pmod 3$ and $F_u(P) \equiv 0 \pmod 3$.

8. Assume $v_3(a) = 1$, $v_3(b) = 0$ and u_i/u_j is not a cube modulo 9 for all $i \neq j$. Notice that the last assumption implies that $u_1u_2u_3 \equiv \pm 1 \pmod 9$.

   Begin by assuming there exists $s_1, s_2 \in \{\pm 1\}$ such that

$$2a \equiv s_1u_1 + s_2u_2 + s_1s_2u_3 \pmod{27}.$$

   We claim that $P_0 = (s_1, s_2, s_1s_2)$ is a non-singular solution modulo 27. To see this, notice that

$$\begin{aligned} F_u(P_0) &= u_1(s_1)^3 + u_2(s_2)^3 + u_3(s_1s_2)^3 - 2as_1^2s_2^2 \\ &\equiv u_1s_1 + u_2s_2 + u_3s_1s_2 - (u_1s_1 + u_2s_2 + u_3s_1s_2) \pmod{27} \\ &\equiv 0 \pmod{27} \end{aligned}$$

   since $s_i^2 = 1$ and $s_i^3 = s_i$.

   There is a little more work involved to show that this solution is non-singular modulo 27. By symmetry, we may assume that $u_1 < u_2 < u_3$ and since u_i/u_j is not a cube modulo 9 for all $i \neq j$, modulo 9 there are only 6 possible combinations for u_1, u_2 and u_3:

$$\begin{aligned} u_1 = 1 \quad u_2 = 2 \quad u_3 = 4, \\ u_1 = 1 \quad u_2 = 2 \quad u_3 = 5, \\ u_1 = 1 \quad u_2 = 4 \quad u_3 = 7, \\ u_1 = 1 \quad u_2 = 5 \quad u_3 = 7, \\ u_1 = 2 \quad u_2 = 4 \quad u_3 = 8, \\ u_1 = 2 \quad u_2 = 5 \quad u_3 = 8. \end{aligned}$$

Notice that

$$\begin{aligned}\left.\frac{\partial F}{\partial X}\right|_{P_0} &= 3u_1 - 2(3\widetilde{a})s_1 \pmod{27} \\ &\equiv u_1 - 2\widetilde{a}s_1 \pmod{9}\end{aligned}$$

where $a = 3\widetilde{a}$. A few simple calculations shows that there are only 4 cases when

$$\left.\frac{\partial F}{\partial X}\right|_{P_0} \equiv 0 \pmod{9}.$$

However, in all four cases, one can show that we always have

$$\left.\frac{\partial F}{\partial Y}\right|_{P_0} \not\equiv 0 \pmod{9}.$$

Thus the solution P_0 is non-singular modulo 27. So we may lift it.

It is not hard to find a solution modulo 3, since the equation reduces modulo 3 to

$$F_u(X, Y, Z) = u_1X^3 + u_2Y^3 + u_3Z^3.$$

Therefore we claim that (u_1, u_2, u_3) is a solution modulo 3 since

$$\begin{aligned}F_u(u_1, u_2, u_3) &= u_1^4 + u_2^4 + u_3^4 \\ &\equiv 1 + 1 + 1 \pmod{3} \\ &\equiv 0 \pmod{3}.\end{aligned}$$

To find a solution modulo 9, we can again use symmetry and assume $u_1 < u_2 < u_3$. So there are 12 equations we have to consider. Doing some calculations, we find that half of these equations do not have solutions. However further examination shows that in

these situations, for all $s_1, s_2 \in \{\pm 1\}$,

$$2a \not\equiv u_1 s_1 + u_2 s_2 + u_3 s_1 s_2 \pmod{27}.$$

Finally, assume that $P_0 = (x_0, y_0, z_0)$ is a solution modulo 27. By symmetry, we can interchange x_0, y_0 and z_0. So, without loss of generality, assume that $x_0 \equiv 0 \pmod 3$. Then the equation becomes

$$u_2 y_0^3 + u_3 z_0^3 \equiv 0 \pmod{27}.$$

This implies that u_2/u_3 is a cube modulo 27. But all cubes modulo 27 reduce to cubes modulo 9. A contradiction. Thus we can conclude that $x_0 \not\equiv 0 \pmod 3$ and hence $y_0 \not\equiv 0 \pmod 3$ and $z_0 \not\equiv 0 \pmod 3$.
Rewrite $F_u(X, Y, Z) \equiv 0 \pmod{27}$ as

$$2a \equiv u_1 \frac{x_0^2}{y_0 z_0} + u_2 \frac{y_0^2}{x_0 z_0} + u_3 \frac{z_0^2}{x_0 y_0} \pmod{27}.$$

Let $\widetilde{s_1} \equiv \dfrac{x_0^2}{y_0 z_0} \pmod 3$, and $\widetilde{s_2} \equiv \dfrac{y_0^2}{x_0 z_0} \pmod 3$. Then $s_1 s_2 \equiv \dfrac{z_0^2}{x_0 y_0} \pmod 3$. So modulo 3, we know the equivalence holds. A tedious lifting calculation shows that we can find $s_1, s_2 \in \{\pm 1\}$ such that

$$2a \equiv u_1 s_1 + u_2 s_2 + u_3 s_1 s_1 \pmod{27}.$$

□

Appendix D Local Solubility for Auxiliary Curve

Here are detailed proofs of the local solubility results as stated in Chapter 5 for the curve

$$E'_{ab'} : y^2 = x^3 + (ax + b')^2$$

where $b' = \dfrac{27b - 4a^3}{9}$. For additional details, we refer the reader to [14].

The following propositions give the local solubility criteria for the polynomial

$$\begin{aligned} F_{u'}(X,Y,Z) \;:=\; & 2aX^2Z - 2aXYZ + 2aY^2Z + \frac{2b'}{N(\gamma)}Z^3 \\ & -dX^3 - dY^3 - 3cXY^2 + 3cX^2Y + 3dXY^2 \end{aligned}$$

associated to the auxiliary elliptic curve $E'_{ab'}$. Note that since we are working over $\mathbb{Q}\left(\sqrt{-3}\right)$, $p = 3$ is the only ramified prime. If $p \equiv 2 \pmod 3$, then p is an inert prime, and if $p \equiv 1 \pmod 3$, then p is a split prime.

Proposition 94 (Corollary 6.3, [14]). *Let p be any split prime. Then there exists $d_p \in \mathbb{Q}_p$ such that $d_p^2 = -3$. The equation $F_{u'}(X,Y,Z) = 0$ has a solution in $\mathbb{Q}_p$ if and only if the cubic*

$$u_1X^3 + u_2Y^3 + u_3Z^3 - \star XYZ = 0$$

does, where $u_1 = \left(c - \dfrac{d}{2}\right) - \dfrac{d}{2}d_p$, $u_2 = \left(c - \dfrac{d}{2}\right) + \dfrac{d}{2}d_p$, $u_3 = \dfrac{2b'}{\gamma\overline{\gamma}}d_p$ and $\star = 2ad_p$.

Proof. Let $d_p \in \mathbb{Q}_p$ such that $d_p^2 = -3$. Let

$$G_{u'}(X,Y,Z) = u_1X^3 + u_2Y^3 + u_3Z^3 - \star XYZ,$$

where $u_1 = \left(c - \dfrac{d}{2}\right) - \dfrac{d}{2}d_p$, $u_2 = \left(c - \dfrac{d}{2}\right) + \dfrac{d}{2}d_p$, $u_3 = \dfrac{2b'}{\gamma\overline{\gamma}}d_p$ and $\star = 2ad_p$.

Since there are numerous ways to write $F_{u'}(X,Y,Z)$, for this proof, we assume

$$\begin{aligned} F_{u'}(X,Y,Z) &= \left(\overline{\gamma}\left(X+Y\sqrt{-3}\right)^3 - \gamma\left(X-Y\sqrt{-3}\right)^3\right)/\sqrt{-3} \\ &\quad +2aZ\left(X+Y\sqrt{-3}\right)\left(X-Y\sqrt{-3}\right) + \left(2b'/N(\gamma)\right)Z^3. \end{aligned}$$

First we will show that given a non-trivial solution to $F_{u'}(X,Y,Z)=0$, we can find a non-trivial solution to $G_{u'}(X,Y,Z)=0$.

We must choose a value for d_p. However, we obtain the same equation $F_{u'}(X,Y,Z)=0$ when choosing $\sqrt{-3}$ verses $-\sqrt{-3}$. Therefore it does not matter which root we choose.

Assume $d_p=\sqrt{-3}$ and suppose (A,B,C) is a non-trivial solution to $F_{u'}(X,Y,Z)=0$. Let $X'=A+Bd_p$ and $Y'=-A+Bd_p$. Then

$$\begin{aligned} 0 &= F_{u'}(A,B,C) \\ &= \frac{1}{d_p}\left(u_1\left(X'\right)^3 + u_2\left(Y'\right)^3\right) + \frac{2b'}{\gamma\overline{\gamma}}C^3 - 2aX'Y'C. \end{aligned}$$

Multiplying both sides by d_p, we have

$$\begin{aligned} 0 &= u_1\left(X'\right)^3 + u_2\left(Y'\right)^3 + \frac{2b'}{\gamma\overline{\gamma}}d_pC^3 - 2ad_pX'Y'C \\ &= G_{u'}\left(X',Y',C\right). \end{aligned}$$

Hence (X',Y',C) is a solution to $G_{u'}(X,Y,Z)=0$.

Now assume that (x,y,z) is a non-trivial solution to $G_{u'}(X,Y,Z)=0$. Let

$$A=\frac{x-y}{2}, \quad B=\frac{x+y}{2d_p}, \quad \text{and} \quad C=z.$$

Then

$$\begin{aligned} 0 &= G_{u'}(x,y,z) \\ &= u_1x^3 + u_2y^3 + \frac{2b'}{\gamma\overline{\gamma}}d_pz^3 - 2ad_pxyz \\ &= u_1\left(A+Bd_p\right)^3 - u_2\left(A-Bd_p\right)^3 + \frac{2b'}{\gamma\overline{\gamma}}d_pC^3 - 2ad_pC\left(A+Bd_p\right)\left(A-Bd_p\right). \end{aligned}$$

Dividing both sides by d_p, we find that (A,B,C) is a solution for $F_{u'}(X,Y,Z)=0$.

Therefore we have a non-trivial solution to $F_{u'}(X,Y,Z)=0$ if and only if we have a non-trivial solution to $G_{u'}(X,Y,Z)=0$.

□

Making some minor adjustments to Proposition 43, we have all the conditions necessary to find a solution for $F_{u'}(X,Y,Z)=0$ in $\mathbb{Q}_p$ where p is a split prime. Before stating the Corollary, we make the following observation.

Lemma 95. *Let $\Delta' = 27b' + 12a^3$. If $p \equiv 1 \pmod 3$, $p \mid \Delta'$ and $p \nmid b'$, then $2b'\sqrt{-3}$ is a cube modulo p.*

Proof. Suppose $p \mid \Delta'$. Then $27b' + 12a^3 \equiv 0 \pmod p$. Hence

$$27b' \equiv -3(2)^2a^3 \pmod p$$

or equivalently

$$2b' \equiv -3\left(3^{-1}\right)^3(2a)^3 \pmod p.$$

Notice that $\sqrt{-3}^3 = -3\sqrt{-3}$. Thus

$$\begin{aligned} 2b'\sqrt{-3} &\equiv \left(-3\sqrt{-3}\right)\left(3^{-1}\right)^3(2a)^3 \pmod p \\ &\equiv \left(2a\sqrt{-3}\right)^3\left(3^{-1}\right)^3 \pmod p. \end{aligned}$$

Thus $2b'\sqrt{-3}$ is a cube modulo p. $\square$

We can conclude that if u_i/u_j is a cube for some $i \neq j$, then this is true for all $i \neq j$.

Corollary 96. *Let p be any split prime. We can write $p = \pi\overline{\pi}$ where $\pi \equiv 2 \pmod 3$ and is in the upper-half plane. Let*

$$F_{u'}(X,Y,Z) \;=\; u_1X^3 + u_2Y^3 + u_3Z^3 - \boldsymbol{c}XYZ = 0$$

where $u_1 = \left(c - \frac{d}{2}\right) - \frac{d}{2}\sqrt{-3}$, $u_2 = \left(c - \frac{d}{2}\right) + \frac{d}{2}\sqrt{-3}$, $u_3 = \frac{2b'}{\gamma\overline{\gamma}}\sqrt{-3}$ and $\boldsymbol{c} = 2a\sqrt{-3}$ with $(c,d) = 1$.

1. *If $v_p(b') = 0$ and $v_p(27b' + 12a^3) = 0$, then $F_{u'}(X,Y,Z) = 0$ has a solution in $\mathbb{Q}_p$.*
2. *If $v_p(b') = 0$ and $v_p(27b' + 12a^3) > 0$, then $F_{u'}(X,Y,Z) = 0$ has a solution in $\mathbb{Q}_p$ if and only if u_1/u_2 is a cube in $\mathbb{F}_p^*$.*
3. *If $v_\pi(b') > 0$, then $F_{u'}(X,Y,Z) = 0$ has a solution in $\mathbb{Q}(\omega)_\pi$ if and only if one of the following is true*
   (a) *$v_\pi(a) = 0$,*
   (b) *$v_\pi(a) > 0$, π divides exactly one of $\{u_1,u_2,u_3\}$ and the ratio of the other two is a cube modulo π,*
   (c) *$v_\pi(a) > 0$, π divides two of $\{u_1,u_2,u_3\}$ and their ratio is a cube modulo π.*

Proof. 1. Assume $v_p(27b' + 12a^3) = 0$ with $p \equiv 1 \pmod 3$. We would like to show that there are no singular points in this case, and therefore we can use Hensel's lemma. Let us begin by assuming $Z = 0$ and see if there are any singular points in this case. If $Z = 0$, we are left with the equation

$$u_1X^3 + u_2Y^3 = 0,$$

and for us to have a singular point we must have

$$\frac{\partial F}{\partial X} = 3u_1X^2 = 0$$

and

$$\frac{\partial F}{\partial Y} = 3u_2Y^2 = 0.$$

But since $p \neq 3$ and $u_1u_2 \mid (2b')$, it follows that $X = Y = 0$, which is not possible. Therefore we can conclude that if there is a singular point on the curve, it must have $Z \neq 0$. So without loss of generality, we can assume $Z = 1$.

Then we have a singular point if and only if

$$\frac{\partial F}{\partial X} = 3u_1X^2 - 2a\sqrt{-3}YZ = 0,$$

$$\frac{\partial F}{\partial Y} = 3u_2Y^2 - 2a\sqrt{-3}XZ = 0,$$

and

$$\frac{\partial F}{\partial Z} = 3u_3Z^2 - 2a\sqrt{-3}XY = 0.$$

If $v_p(2a) > 0$, then $3u_3Z^2 - 2a\sqrt{-3}XY = 0$ implies that $v_p(u_3) > 0$, a contradiction. Hence $v_p(2a) = 0$. Therefore we have

$$Y = \frac{3u_1X^2}{2a\sqrt{-3}}$$

and

$$X = \frac{3u_2Y^2}{2a\sqrt{-3}}.$$

Combining these two equations, we have

$$X = \frac{27u_1^2u_2X^4}{8a^3\left(\sqrt{-3}\right)^3}.$$

If $X = 0$, then $Y = 0$. And using $3u_3Z^2 - 2a\sqrt{-3}XY = 0$ and the fact that $Z = 1$, we would again have that $v_p(u_3) > 0$, which is not possible. Therefore $X \neq 0$.

So

$$X^3 = \frac{8a^3\left(\sqrt{-3}\right)^3}{27u_1^2u_2}.$$

Again using $3u_3Z^2 - 2a\sqrt{-3}XY = 0$ and the fact that $Z = 1$, we obtain that

$$3u_3 = 2a\sqrt{-3}XY$$

and substituting in for Y with $\dfrac{3u_1X^2}{2a\sqrt{-3}}$, and the equation for X^3, we have

$$\begin{aligned} 3u_3 &= 2a\sqrt{-3}X\left(\frac{3u_1X^2}{2a\sqrt{-3}}\right) \\ &= 3u_1\left(\frac{8a^3\left(\sqrt{-3}\right)^2}{27u_1^2u_2}\right) \\ &= \frac{8a^3\left(\sqrt{-3}\right)^2}{9u_1u_2}. \end{aligned}$$

Therefore

$$27u_1u_2u_3 - 8a^3\left(\sqrt{-3}\right)^2 = 2\left(27b' + 12a^3\right) = 0.$$

But since $p \neq 2$, this implies that $v_p\left(27b' + 12a^3\right) > 0$, a contradiction. Hence there are no singular points on this curve, so it is non-singular over $\mathbb{F}_p$.

Since it is a curve of genus 1, we know via the Weil bounds that

$$p + 1 - 2\sqrt{p} \leq \#E(\mathbb{F}_p) \leq p + 1 + 2\sqrt{p}.$$

Since the smallest prime which could satisfy the conditions listed above is 5 and

$$6 - 2\sqrt{5} > 0$$

we know that for every prime p, the curve has a non-trivial point in $\mathbb{F}_p$. Therefore for every p satisfying the above conditions, we can preform a Hensel lift to $\mathbb{Z}_p$ as soon as we know there is a solution modulo p. Thus proving this part of the proposition.

2. Assume $p \equiv 1 \pmod 3$, $v_p(b') = 0$ and $v_p\left(27b' + 12a^3\right) > 0$.

   Assume that u_1/u_2 is a cube modulo p. Then there exists a c such that $1 \leq c \leq p-1$ and $u_1/u_2 \equiv c^3 \pmod p$.

   Assume $Z = 0$, then we have

$$u_1X^3 + u_2Y^3 \equiv 0 \pmod p.$$

   We can conclude that both X and Y are not equivalent to zero modulo p, otherwise it would be a trivial solution. This implies that

$$\frac{u_1}{u_2} \equiv \left(\frac{-Y}{X}\right)^3 \pmod p$$

   or equivalently that

$$\frac{-Y}{X} \equiv c \pmod p.$$

   Let $Y = -c$ and thus $X = 1$.

We have a solution at $(1, -c, 0)$. Let us verify this

$$\begin{aligned} F_{u'}(1,-c,0) &= u_1(1)^3 + u_2(-c)^3 + 0 - 0 \\ &\equiv u_1 + u_2\left(\frac{-u_2}{u_1}\right) \pmod{p} \\ &\equiv 0 \pmod{p}. \end{aligned}$$

In order to lift this solution using Hensel's Lemma, we must show that this point is non-singular. To see this, we observe that

$$\begin{aligned} \frac{\partial F}{\partial X} &= 3u_1X^2 - 2a\sqrt{-3}YZ, \\ \frac{\partial F}{\partial Y} &= 3u_2Y^2 - 2a\sqrt{-3}XZ, \\ \frac{\partial F}{\partial X} &= 3u_3Z^2 - 2a\sqrt{-3}XY. \end{aligned}$$

At the solution $(1, -c, 0)$ we have that

$$\begin{aligned} \frac{\partial F}{\partial X} &= 3u_1, \\ \frac{\partial F}{\partial Y} &= 3u_2c^2, \\ \frac{\partial F}{\partial X} &= 0. \end{aligned}$$

Since $p \neq 2, 3$, $v_p(u_1u_2) = 0$ and $1 \leq c \leq p-1$, it follows that $\dfrac{\partial F}{\partial X} \neq 0$ and $\dfrac{\partial F}{\partial Y} \neq 0$. Thus the solution is not a singular point. So for every prime satisfying the given conditions, we can preform a Hensel lift to $\mathbb{Z}_p$.

Assume (x_0, y_0, z_0) is a solution modulo p to $F_{u'}(X, Y, Z) = 0$. We may assume that $\min\{v_p(x_0), v_p(y_0), v_p(z_0)\} = 0$. We also have that

$$4v_p(x_0) + 4v_p(y_0) + 4v_p(z_0) > 0.$$

So at least one one of $\{x_0, y_0, z_0\}$ must be divisible by p. Observe that if two of $\{x_0, y_0, z_0\}$ were divisible by p, say x_0 and z_0, then the equation becomes

$$u_2 y_0^3 \equiv 0 \pmod{p}.$$

Since $v_p(u_2) = 0$, this implies that $v_p(y_0) > 0$, a contradiction. Thus, at most one of $\{x_0, y_0, z_0\}$ is divisible by p. Without loss of generality, assume $v_p(z_0) > 0$. Then we have

$$u_1 x_0^3 + u_2 y_0^3 \equiv 0 \pmod{p},$$

or equivalently

$$\frac{u_2}{u_1} \equiv \left(\frac{-x_0}{u_0}\right)^3 \pmod{p}.$$

Hence u_i/u_j is a cube modulo p for some $i \neq j$. Therefore by Lemma 95, u_1/u_2 is a cube. Thus proving this part of the proposition.

3. Assume $p \equiv 1 \pmod{3}$ and $v_\pi(b') > 0$. Recall that we know $v_\pi(b') \leq 2$.

   (a) Assume $v_\pi(a) = 0$. Since $0 < v_\pi(b') \leq 2$, there are two cases we need to consider.

   Case 1: π divides only one of $\{u_1, u_2, u_3\}$.

   Without loss of generality, we may assume that $v_\pi(u_1) = v_\pi(u_2) = 0$ and $v_\pi(u_3) > 0$. Then reducing modulo π the equation becomes

$$F_{u'}(X, Y, Z) = u_1 X^3 + u_2 Y^3 - 2a\sqrt{-3}XYZ.$$

   We claim that in this case,

$$\left(\frac{1}{u_1}, \frac{1}{u_2}, \frac{u_1^2 + u_2^2}{2a\sqrt{-3}u_1 u_2}\right)$$

is a solution to $F_{u'}(X,Y,Z) \equiv 0$ modulo π. Let us verify this:

$$\begin{aligned} F_{u'}\left(\frac{1}{u_1}, \frac{1}{u_2}, \frac{u_1^2+u_2^2}{2a\sqrt{-3}u_1u_2}\right) &\equiv u_1\left(\frac{1}{u_1}\right)^3 + u_2\left(\frac{1}{u_2}\right)^3 - 2a\sqrt{-3}\left(\frac{1}{u_1}\right)\left(\frac{1}{u_2}\right)\left(\frac{u_1^2+u_2^2}{2a\sqrt{-3}u_1u_2}\right) \\ &\equiv \frac{1}{u_1^2} + \frac{1}{u_2^2} - \frac{u_1^2+u_2^2}{u_1^2u_2^2} \\ &\equiv 0 \pmod{\pi}. \end{aligned}$$

Now it remains to verify that this point is non-singular. It is enough to show that one partial derivative is non-zero. Consider

$$\frac{\partial F}{\partial Z} = -2a\sqrt{-3}XY.$$

Evaluating at the solution we see that

$$\frac{\partial F}{\partial Z} = \frac{-2a\sqrt{-3}}{u_1u_2},$$

and since $v_\pi(a) = v_\pi(u_1u_2) = 0$, it follows that $\dfrac{\partial F}{\partial Z} \not\equiv 0 \pmod{\pi}$.

Case 2: π divides exactly two of $\{u_1, u_2, u_3\}$

Since $v_\pi(b') \leq 2$, we can conclude that if π divides u_i, then it divides u_i exactly once. Without loss of generality, assume that $v_\pi(u_2) = v_\pi(u_3) = 1$, hence $v_\pi(u_1) = 0$. The equation becomes

$$F_{u'}(X,Y,Z) = u_1X^3 - 2a\sqrt{-3}XYZ \pmod{\pi}.$$

It is easy to see that $(0,1,1)$ is a solution modulo π. It remains to show that this point is non-singular. Again, it is enough to show that one of the partial

derivatives is non-zero. Consider

$$\frac{\partial F}{\partial X} = 3u_1X^2 - 2a\sqrt{-3}YZ.$$

At the point $(0,1,1)$ we have

$$\begin{aligned}\frac{\partial F}{\partial X} &= -2a\sqrt{-3} \\ &\not\equiv 0 \pmod{\pi}\end{aligned}$$

since $v_\pi(2a) = 0$. Hence if $v_\pi(a) = 0$, then we can find a solution modulo π which is non-singular. Thus we can preform a Hensel lift.

(b) Assume $v_\pi(a) > 0$, π divides exactly one of $\{u_1, u_2, u_3\}$ and the ratio of the other two is a cube modulo π. Without loss of generality, assume $v_\pi(u_3) > 0$ and u_1/u_2 is a cube modulo π. Then there exists a c such that $u_1/u_2 \equiv c^3 \pmod{\pi}$. We claim that $(1,-c,0)$ is a solution modulo π. Let us verify this:

$$\begin{aligned}F_{u'}(1,-c,0) &= u_1(1)^3 + u_2(-c)^3 \\ &\equiv u_1 + u_2\left(\frac{-u_1}{u_2}\right) \pmod{\pi} \\ &\equiv 0 \pmod{\pi}.\end{aligned}$$

It is easy to see that the point is not singular since

$$\frac{\partial F}{\partial X} = 3u_1X^2,$$

which is clearly not equivalent to zero modulo π at the solution. So we can preform a Hensel lift.

(c) Assume $v_\pi(a) > 0$, π divides exactly two of $\{u_1, u_2, u_3\}$ and their ratio is a cube

modulo π. Without loss of generality, assume $v_\pi(u_2) = 0$. Then since $v_\pi(b') \leq 2$, it follows that $v_\pi(u_1) = v_\pi(u_3) = 1$. So there exists a c such that $u_1/u_3 \equiv c^3 \pmod{\pi}$. Note that since π divides u_1 and u_3 exactly once, $v_\pi(u_1/u_3) = 0$. In addition, we can write $u_1 = \pi\widetilde{u_1}$ and $u_3 = \pi\widetilde{u_3}$ for some $\widetilde{u_1}$ and $\widetilde{u_3}$.

Let us make the following substitution, $Y = \pi y$. Then the equation becomes

$$F_{u'}(X, \pi y, Z) \;=\; \pi\widetilde{u_1}X^3 + \pi u_2\pi^2 y^3 + \pi\widetilde{u_3}Z^3 - 2a\sqrt{-3}X\pi yZ.$$

Let $U_2 = u_2\pi^2$, then we have that

$$\frac{1}{\pi}F_{u'}(X, \pi y, Z) \;=\; \widetilde{u_1}X^3 + U_2 y^3 + \widetilde{u_3}Z^3 - 2a\sqrt{-3}XyZ.$$

Thus we are in situation (b) from above. Hence we can find a non-singular solution and it lifts.

Assume that (x_0, y_0, z_0) is a non-singular solution to $F_{u'}(X, Y, Z) \equiv 0 \pmod{\pi}$. We may assume that $\min\{v_\pi(x_0), v_\pi(y_0), v_\pi(z_0)\} = 0$. In addition, since $v_\pi(b') > 0$, without loss of generality we may assume $v_\pi(u_3) > 0$. There are two cases we need to consider.

Case 1: $v_\pi(u_1u_2) = 0$

In this case the equation becomes

$$u_1x_0^3 + u_2y_0^3 - 2a\sqrt{-3}x_0y_0z_0 \;\equiv\; 0 \pmod{\pi}.$$

If $v_\pi(a) > 0$, then we have

$$u_1x_0^3 + u_2y_0^3 \;\equiv\; 0 \pmod{\pi}.$$

The partial derivatives at the solution are

$$\begin{aligned}\frac{\partial F}{\partial X} &= 3u_1x_0^2,\\ \frac{\partial F}{\partial Y} &= 3u_2y_0^2,\\ \frac{\partial F}{\partial Y} &= 0.\end{aligned}$$

Since the point is non-singular, this implies that both x_0 and y_0 are non-zero modulo π. Hence

$$\frac{u_1}{u_2} \equiv \left(\frac{-y_0}{x_0}\right)^3 \pmod{\pi}.$$

Otherwise, $v_\pi(a) = 0$ and we obtain no additional information.

Case 2: $v_\pi(u_1u_2) > 0$

Without loss of generality, assume $v_\pi(u_2) > 0$. Since $v_\pi(b) \leq 2$, this implies that $v_\pi(u_2) = v_\pi(u_3) = 1$. So the equation becomes

$$u_1x_0^3 - 2a\sqrt{-3}x_0y_0z_0 \equiv 0 \pmod{\pi}.$$

If $v_\pi(a) = 0$, we obtain no additional information.

If $v_\pi(a) > 0$, then $x_0 \equiv 0 \pmod{\pi}$. So we can divide out a π from the equation and reduce modulo π to obtain

$$\widetilde{u_2}y_0^3 + \widetilde{u_3}z_0^3 \equiv 0 \pmod{\pi}$$

where $u_2 = \pi\widetilde{u_2}$ and $u_3 = \pi\widetilde{u_3}$. In this case, the partial derivatives are

$$\begin{aligned}\frac{\partial F}{\partial X} &= 0,\\ \frac{\partial F}{\partial Y} &= \widetilde{u_2}y_0^2,\\ \frac{\partial F}{\partial Y} &= \widetilde{u_3}z_0^2.\end{aligned}$$

Since the solution is non-singular, we know that both y_0 and z_0 are non-zero modulo π. Therefore,

$$\frac{u_3}{u_2} \equiv \left(\frac{-y_0}{z_0}\right)^3 \pmod{\pi}.$$

Thus we have proven the corollary. □

Recall from Theorem 42 G_3 is the subgroup of $\mathbb{Q}^*(\omega)/(\mathbb{Q}^*(\omega))^3$ of classes whose norms are cubes where ω is a primitive cubic root of unity and $[u'] \in G_3$. Write $u' = \gamma\overline{\gamma}^2$ with $\gamma = c + d\omega \in \mathbb{Z}[\omega]$ and $N(\gamma) = \gamma\overline{\gamma}$ is only divisible by split primes. The following lemma will be useful in proving the solubility propositions.

Lemma 97 (Lemma 6.4, [14]). *Let $p \neq 3$ be an inert prime. The following conditions are equivalent:*

1. *There exists X and Y such that*

$$\gamma/\overline{\gamma} \equiv \left(\frac{X + Y\sqrt{-3}}{X - Y\sqrt{-3}}\right)^3 \pmod{p}.$$

2. *The class of $\gamma/\overline{\gamma}$ is a cube in $\mathbb{F}_{p^2}^*$.*

3. *$p \equiv 2 \pmod 3$ and $\overline{\gamma}^{(p^2-1)/3} \equiv 1 \pmod p$.*

Now we are ready to state and prove the solubility propositions.

Proposition 98 (Lemmas 6.5, 6.6, 6.7, [14]). *Assume $p \neq 2$, $p \equiv 2 \bmod 3$ and let $F_{u'}(X,Y,Z)$ be as in equation (4.12).*

1. *If $v_p(\gamma\overline{\gamma}) = 0$, $v_p(2b') = 0$ and $v_p(27b' + 12a^3) = 0$, then $F_{u'}(X,Y,Z) = 0$ has a solution in $\mathbb{Q}_p$.*

2. *If $v_p(2b') = 0$ and $v_p(27b' + 12a^3) > 0$, then $F_{u'}(X,Y,Z) = 0$ has a solution in $\mathbb{Q}_p$ if and only if $\dfrac{\gamma}{\overline{\gamma}}$ is a cube in $\mathbb{F}_{p^2}^*$.*

3. *If $v_p(2b') > 0$ and $v_p(\gamma\overline{\gamma}) = 0$, then $F_{u'}(X,Y,Z) = 0$ has a solution in $\mathbb{Q}_p$ if and only if one of the following is satisfied:*

   (a) $v_p(2a) = 0$.

   (b) $v_p(2a) > 0$ and the class of $\dfrac{\gamma}{\overline{\gamma}}$ modulo p is a cube in $\mathbb{F}_{p^2}^*$.

Proof. Assume $p \neq 2$ and $p \equiv 2 \pmod 3$.

1. In addition, assume that $v_p(\gamma\overline{\gamma}) = 0$, $v_p(2b') = 0$ and $v_p(27b' + 12a^3) = 0$. One can show that in order for us to have a singular point if $Z = 0$, then both X and Y must be zero. So we may assume that $Z = 1$. Then we can rearrange $F_{u'}(X,Y,1)$ so it is in Weierstrass form and calculating its determinant we find

$$\Delta = 9b'\left(27b' + 12a^3\right)^3.$$

   Therefore since $p \neq 3$, $v_p(b') = 0$ and $v_p(27b' + 12a^3) = 0$, it follows that the curve is non-singular. Since the curve is of genus 1, we know via the Weil bounds give

$$p + 1 - 2\sqrt{p} \leq \#E(\mathbb{F}_p) \leq p + 1 + 2\sqrt{p}.$$

The smallest prime which could satisfy the conditions listed above is 5 and

$$6 - 2\sqrt{5} > 0.$$

Thus we know that for every prime p the curve has a non-trivial point over $\mathbb{F}_p$. Therefore for every p satisfying the above conditions, we can preform a Hensel lift to $\mathbb{Z}_p$ as soon as we know there is a solution modulo p. Thus proving this part of the proposition.

2. Assume that $v_p(2b') = 0$ and $v_p(27b' + 12a^3) > 0$.

   Assume $\gamma/\overline{\gamma}$ is a cube modulo p in $\mathbb{F}_{p^2}^*$. Then by Lemma 97 there exists x_0 and y_0 such that

$$\gamma/\overline{\gamma} \equiv \left(\left(x_0 + y_0\sqrt{-3}\right) / \left(x_0 - y_0\sqrt{-3}\right)\right)^3 \pmod{p}.$$

   Hence

$$\gamma \equiv \overline{\gamma}\left(\frac{x_0 + y_0\sqrt{-3}}{x_0 - y_0\sqrt{-3}}\right)^3 \pmod{p}.$$

   Let $P_0 = (x_0, y_0, 0)$. Then

$$\begin{aligned} F_{u'}(P_0) &= \frac{1}{\sqrt{-3}}\left(\overline{\gamma}\left(x_0 + y_0\sqrt{-3}\right)^3 - \gamma\left(x_0 - y_0\sqrt{-3}\right)^3\right) \\ &\equiv \frac{1}{\sqrt{-3}}\left(\overline{\gamma}\left(x_0 + y_0\sqrt{-3}\right)^3 - \overline{\gamma}\left(\frac{x_0 + y_0\sqrt{-3}}{x_0 - y_0\sqrt{-3}}\right)^3\left(x_0 - y_0\sqrt{-3}\right)^3\right) \pmod{p} \\ &\equiv 0 \pmod{p}. \end{aligned}$$

   So P_0 is a solution to $F_{u'}(X, Y, Z) = 0$. Also, notice that since $v_p(2a) = 0$ and

$$v_p\left(\left(x_0 + y_0\sqrt{-3}\right)\left(x_0 - y_0\sqrt{-3}\right)\right) = 0,$$

it follows that

$$\begin{aligned} \left.\frac{\partial F}{\partial Z}\right|_{P_0} &= 2a\left(x_0+y_0\sqrt{-3}\right)\left(x_0-y_0\sqrt{-3}\right) \\ &\not\equiv 0 \pmod{p}. \end{aligned}$$

Thus P_0 is non-singular, so we can lift to find solutions.

Now assume (x,y,z) is a solution to $F_{u'}(X,Y,Z) \equiv 0 \pmod{p}$. We may assume that

$$\min\left\{v_p(x), v_p(y), v_p(z)\right\} = 0.$$

We know that since $F_{u'}(x,y,z) \equiv 0 \pmod{p}$,

$$4v_p\left(x+y\sqrt{-3}\right) + 4v_p\left(x-y\sqrt{-3}\right) + 4v_p(z) > 0.$$

Since p is inert, $v_p\left(x \pm y\sqrt{-3}\right) = 0$. Hence $v_p(z) > 0$. Therefore the equation becomes

$$\frac{1}{\sqrt{-3}}\left(\overline{\gamma}\left(x+y\sqrt{-3}\right)^3 - \gamma\left(x-y\sqrt{-3}\right)^3\right) \equiv 0 \pmod{p}$$

or equivalently,

$$\gamma/\overline{\gamma} \equiv \left(\left(x+y\sqrt{-3}\right)/\left(x-y\sqrt{-3}\right)\right)^3 \pmod{p}.$$

Hence by Lemma 97, $\gamma/\overline{\gamma}$ is a cube modulo p in $\mathbb{F}_{p^2}^*$.

3. Assume $v_p(2b) > 0$ and $v_p(\gamma\overline{\gamma}) = 0$.

(a) In addition assume that $v_p(2a) = 0$. Then we claim that

$$P_0 = \left(\frac{c - d/2}{N(\gamma)}, \frac{d/2}{N(\gamma)}, \frac{\overline{\gamma}^2 - \gamma^2}{2a\sqrt{-3}N(\gamma)} \right)$$

is a non-singular solution to $F_{u'}(X, Y, Z) \equiv 0 \pmod{p}$. To see this we begin by noticing that

$$\begin{aligned} \frac{c - d/2}{N(\gamma)} + \frac{d/2}{N(\gamma)}\sqrt{-3} &= \frac{\gamma}{N(\gamma)} \\ &= \frac{1}{\overline{\gamma}} \end{aligned}$$

and

$$\begin{aligned} \frac{c - d/2}{N(\gamma)} - \frac{d/2}{N(\gamma)}\sqrt{-3} &= \frac{\overline{\gamma}}{N(\gamma)} \\ &= \frac{1}{\gamma}. \end{aligned}$$

Then

$$\begin{aligned} F_{u'}(P_0) &= \frac{1}{\sqrt{-3}} \left(\overline{\gamma} \left(\frac{1}{\overline{\gamma}} \right)^3 - \gamma \left(\frac{1}{\gamma} \right)^3 \right) + 2a \left(\frac{\overline{\gamma}^2 - \gamma^2}{2a\sqrt{-3}N(\gamma)} \right) \left(\frac{1}{\overline{\gamma}\gamma} \right) \\ &= \frac{1}{\sqrt{-3}} \left(\frac{\gamma^2 - \overline{\gamma}^2}{N(\gamma)^2} \right) + \frac{\overline{\gamma}^2 - \gamma^2}{\sqrt{-3}N(\gamma)^2} \\ &\equiv 0 \pmod{p}. \end{aligned}$$

Since

$$\begin{aligned} \left. \frac{\partial F}{\partial Z} \right|_{P_0} &= 2aN(\gamma) \\ &\not\equiv 0 \pmod{p}, \end{aligned}$$

it follows that P_0 is non-singular and therefore we can lift to find solutions.

(b) Now assume that $v_p(2a) > 0$ and $\gamma/\overline{\gamma}$ modulo p is a cube in $\mathbb{F}_{p^2}^*$. Then by Lemma 97 there exists x_0 and y_0 such that

$$\gamma/\overline{\gamma} \equiv \left(\left(x_0 + y_0\sqrt{-3}\right) / \left(x_0 - y_0\sqrt{-3}\right)\right)^3 \pmod{p}.$$

Hence

$$\gamma \equiv \overline{\gamma}\left(\frac{x_0 + y_0\sqrt{-3}}{x_0 - y_0\sqrt{-3}}\right)^3 \pmod{p}.$$

Let $P_0 = (x_0, y_0, 0)$. Then

$$\begin{aligned} F_{u'}(P_0) &= \frac{1}{\sqrt{-3}}\left(\overline{\gamma}\left(x_0 + y_0\sqrt{-3}\right)^3 - \gamma\left(x_0 - y_0\sqrt{-3}\right)^3\right) \\ &\equiv \frac{1}{\sqrt{-3}}\left(\overline{\gamma}\left(x_0 + y_0\sqrt{-3}\right)^3 - \overline{\gamma}\left(\frac{x_0 + y_0\sqrt{-3}}{x_0 - y_0\sqrt{-3}}\right)^3\left(x_0 - y_0\sqrt{-3}\right)^3\right) \pmod{p} \\ &\equiv 0 \pmod{p}. \end{aligned}$$

So P_0 is a solution to $F_{u'}(X, Y, Z) = 0$.

It remains to show that P_0 is non-singular. To see this, we notice that

$$\left.\frac{\partial F}{\partial X}\right|_{P_0} = \frac{3}{\sqrt{-3}}\left(\overline{\gamma}(x_0 + y_0\sqrt{-3})^2 - \gamma(x_0 - y_0\sqrt{-3})^2\right) \pmod{p}.$$

If $\left.\dfrac{\partial F}{\partial X}\right|_{P_0} = 0 \pmod{p}$, then we have that

$$\gamma/\overline{\gamma} \equiv \left(\left(x_0 + y_0\sqrt{-3}\right) / \left(x_0 - y_0\sqrt{-3}\right)\right)^2 \pmod{p}.$$

However, this implies that

$$x_0 + y_0\sqrt{-3} \equiv x_0 - y_0\sqrt{-3} \pmod{p}$$

which means $y_0 \equiv 0 \pmod{p}$, a contradiction. Thus P_0 is non-singular and we can lift to find solutions.

Finally, assume that $v_p(2b') > 0$, $v_p(\gamma\overline{\gamma}) = 0$ and (x_0, y_0, z_0) is a solution modulo p to $F_{u'}(X, Y, Z) \equiv 0 \pmod{p}$. If $v_p(2a) > 0$, then

$$\frac{1}{\sqrt{-3}}\left(\overline{\gamma}\left(x_0 + y_0\sqrt{-3}\right)^3 - \gamma\left(x_0 - y_0\sqrt{-3}\right)^3\right) \equiv 0 \pmod{p},$$

which implies that

$$\gamma/\overline{\gamma} \equiv \left(\frac{x_0 + y_0\sqrt{-3}}{x_0 - y_0\sqrt{-3}}\right)^3 \pmod{p}.$$

So by Lemma 97, this implies that $\gamma/\overline{\gamma}$ is a cube modulo p in $\mathbb{F}_{p^2}^*$.

Otherwise, $v_p(2a) = 0$.

□

Again, recall that by Lemma 36 we have that either $v_2(b') \leq 2$ or $v_2(a) = 0$.

Proposition 99 (Lemmas 6.5, 6.6, 6.7, [14]). *Let $p = 2$ and $F_{u'}(X, Y, Z)$ be as in equation (4.12).*

1. *If $v_2(2b') \leq 2$, then $F_{u'}(X, Y, Z) = 0$ has a solution in $\mathbb{Q}_2$ if and only if the class of $\dfrac{\gamma}{\overline{\gamma}}$ modulo 2 is a cube in $\mathbb{Z}^*[\omega]/2\mathbb{Z}^*[\omega] \cong \mathbb{F}_4^*$. Note that the only cube in $\mathbb{F}_4^*$ is 1.*

2. *If $v_2(2b') \geq 3$, then*

   (a) *if $d \equiv 0 \pmod{4}$ and $c \equiv \pm 1 \pmod{4}$, then $F_{u'}(X, Y, Z) = 0$ has a solution in $\mathbb{Q}_2$.*

(b) if $d \equiv 2 \pmod 4$ *and* $c \equiv \pm 1 \pmod 4$ *then* $F_{u'}(X,Y,Z) = 0$ *has a solution in* $\mathbb{Q}_2$.

(c) if $d \equiv 1 \pmod 2$, *then* $F_{u'}(X,Y,Z) = 0$ *has a solution in* $\mathbb{Q}_2$ *if and only if either* $v_2(2b') \geq 4$ *or* $v_2(a) > 0$.

Proof. 1. Assume $v_2(2b') \leq 2$. Since 2 is inert, $v_2(\gamma\overline{\gamma}) = 0$.

Assume $\gamma/\overline{\gamma}$ is a cube modulo 2 in $\mathbb{F}_4^*$. Write $\omega = x_0 + y_0\sqrt{-3}$, then $\omega^2 = x_0 - y_0\sqrt{-3}$. So

$$\gamma/\overline{\gamma} \equiv \left(\left(x_0 + y_0\sqrt{-3}\right) / \left(x_0 - y_0\sqrt{-3}\right)\right)^3 \pmod 2 .$$

Hence

$$\gamma \equiv \overline{\gamma}\left(\frac{x_0 + y_0\sqrt{-3}}{x_0 - y_0\sqrt{-3}}\right)^3 \pmod 2 .$$

We claim that $P_0 = (x_0, y_0, 0)$ is a non-singular solution to $F_{u'}(X,Y,Z) \equiv 0 \pmod 2$. To see this, notice that

$$\begin{aligned} F_{u'}(x_0,y_0) &= \frac{1}{\sqrt{-3}}\left(\overline{\gamma}\left(x_0 + y_0\sqrt{-3}\right)^3 - \gamma\left(x_0 - y_0\sqrt{-3}\right)^3\right) \\ &\equiv \frac{1}{\sqrt{-3}}\left(\overline{\gamma}\left(x_0 + y_0\sqrt{-3}\right)^3 - \overline{\gamma}\left(\frac{x_0 + y_0\sqrt{-3}}{x_0 - y_0\sqrt{-3}}\right)^3\left(x_0 - y_0\sqrt{-3}\right)^3\right) \pmod 2 \\ &\equiv 0 \pmod 2 . \end{aligned}$$

In addition,

$$\begin{aligned}\left.\frac{\partial F}{\partial X}\right|_{P_0} &= \frac{3}{\sqrt{-3}}\left(\overline{\gamma}\left(x_0+y_0\sqrt{-3}\right)^2-\gamma\left(x_0-y_0\sqrt{-3}\right)^2\right)\\ &= \frac{3}{\sqrt{-3}}\left(\overline{\gamma}\omega^2-\gamma\left(\omega^2\right)^2\right)\\ &= \frac{3}{\sqrt{-3}}\left(\overline{\gamma}\omega^2-\gamma\omega\right)\\ &\not\equiv 0 \pmod 2.\end{aligned}$$

Therefore P_0 is non-singular. Hence we can lift.

Now assume (x_0, y_0, z_0) is a solution modulo 2 . Then we have

$$\frac{1}{\sqrt{-3}}\left(\overline{\gamma}\left(x_0+y_0\sqrt{-3}\right)^3-\gamma\left(x_0-y_0\sqrt{-3}\right)^3\right) \equiv 0 \pmod 2.$$

Hence it follows that $\overline{\gamma}/\gamma$ is a cube modulo 2.

2. Assume $v_2(2b') \geq 3$. Then by Lemma 36, we know that either $v_2(a) > 0$ and $v_2(2b') = 3$ or $v_2(a) = 0$.

   (a) In addition, assume $d \equiv 0 \pmod 4$ and $c \equiv \pm 1 \pmod 4$. Then $(1, 1, 1)$ is clearly a solution modulo 2. However all solutions are singular. So we will look modulo 4. Notice that modulo 4, the equation reduces to

$$F_{u'}(X, Y, Z) = 2aX^2Z - 2aXYZ + 2aY^2Z - 3cXY^2 + 3cX^2Y.$$

   It is not hard to see that $P_0 = (1, 1, 0)$ is a solution modulo 4 and since

$$\begin{aligned}\left.\frac{\partial F}{\partial X}\right|_{P_0} &= -3c(1)^2 + 6c(1)(1)\\ &\equiv 3c \pmod 4\end{aligned}$$

is non-zero, P_0 is non-singular. Therefore we can lift to find solutions.

(b) Now assume $d \equiv 2 \pmod 4$ and $c \equiv \pm 1 \pmod 4$. Again, $(1,1,1)$ is a solution modulo 2, however all solutions are singular. Therefore, we will look for solutions modulo 4 to lift. We claim that $P_0 = (1,-1,0)$ is a non-singular solution modulo 4. To see this, notice that

$$\begin{aligned} F_{u'}(1,-1,0) &= -2(1)^3 - 2(-1)^3 - 3c(1)(-1)^2 + 3c(1)^2(-1) + 2(1)(-1)^2 \\ &\equiv -6c + 2 \pmod 4, \end{aligned}$$

which is equivalent to -4 if $c \equiv 1 \pmod 4$ and to 8 if $c \equiv -1 \pmod 4$. Also,

$$\begin{aligned} \left.\frac{\partial F}{\partial X}\right|_{P_0} &= -3d(1)^2 - 3c(-1)^2 + 6c(1)(-1) + 3d(-1)^2 \\ &\equiv 3c \pmod 4 \end{aligned}$$

which is clearly non-zero. Therefore we can lift to find solutions.

(c) Finally, assume that $d \equiv 1 \pmod 2$. Note that from this we can deduce that $2v_1 \equiv 2v_2 \equiv 1 \pmod 2$. For this we will use the following form of the equation:

$$F_{u'}(X,Y,Z) = 2v_2X^3 - 6v_1Y^3 + \frac{2b}{N(\gamma)}Z^3 + 6v_1X^2Y - 18v_2XY^2 + 2a\left(X^2Z + 3Y^2Z\right).$$

Notice that reducing modulo 2, we have

$$X^3 + Y^3 + X^2Y + XY^2 \equiv 0 \pmod 2.$$

So $(1,1,0)$ is solution. However all solutions modulo 2 are singular. Looking modulo 4 and modulo 8, we find that $P_0 = (1,-1,1)$ is a solution. However, it is a singular solution. We claim that $P_0 = (2,2,2)$ is a non-singular solution modulo

16. To see this, let us first assume that $v_2(2b') = 3$ and $v_2(a) > 0$. Then

$$F_{u'}(2,2,2) =$$

$$2v_2(8) - 3(2v_1)(8) + \frac{2b}{N(\gamma)}(8) + 3(2v_1)(8) - 9(2v_2)(8) + 2a(8 + 3(8)) \pmod{16}$$

$$\equiv 0 \pmod{16}$$

and

$$\begin{aligned} \left.\frac{\partial F}{\partial Y}\right|_{P_0} &= 14(2v_1) + 8(2v_2) \\ &= 2(7(2v_1) + 4(2v_2)) \pmod{16}. \end{aligned}$$

Note that $\left.\frac{\partial F}{\partial Y}\right|_{P_0}$ will never be zero modulo 16, since $2v_2$ and $2v_1$ are both odd. Thus P_0 is a non-singular solution, so we can lift.

To see the reverse, one observes that there are no solutions when $v_2(2b') = 3$ and $v_2(a) = 0$.

□

Proposition 100 (Lemmas 6.11, 6.12, [14]). *Let $p = 3$ and $F_{u'}(X,Y,Z)$ be as in equation (4.12).*

1. *If $v_3(2a) = 0$, then $F_{u'}(X,Y,Z) = 0$ has a solution in $\mathbb{Q}_3$ if and only if one of the following conditions is satisfied:*

   (a) $v_3(d) > 0$,

   (b) $v_3(d) = v_3\left(2a + \frac{2b'}{N(\gamma)}\right) = 0$.

2. *If $v_3(2a) \geq 2$, then $F_{u'}(X,Y,Z) = 0$ has a solution in $\mathbb{Q}_3$ if and only if one of the following conditions is satisfied:*

(a) $v_3(d) \geq 2$,

(b) $v_3(d) = v_3(b) = 1$,

(c) $v_3(d) = 0$ *and* $\dfrac{2b'}{dN(\gamma)}$ *is a cube modulo* 9,

(d) $\dfrac{2b'}{N(\gamma)} \equiv \pm(6c - 3d)$ *modulo* 27.

3. *If* $v_3(2a) = 1$, *then* $F_{u'}(X, Y, Z) = 0$ *has a solution in* $\mathbb{Q}_3$ *if and only if one of the following is satisfied:*

(a) $v_3(d) \geq 2$,

(b) $v_3(d) = v_3\left(2a + \dfrac{2b'}{N(\gamma)}\right) = 1$,

(c) $v_3(d) = 0$ *and* $\left(\dfrac{2b'}{N(\gamma)} + 2a\right)/d$ *is a cube modulo* 9,

(d) $v_3\left(\dfrac{2b'}{N(\gamma)}\right) = 1$, $v_3(d) = 0$ *and there exists* $s \in \{\pm 1\}$ *such that* $(d - 2c) \equiv s\left(\dfrac{2b'}{3N(\gamma)} + 2a\right) \pmod{27}$ *and* $s(2c - d) \equiv 2a/3 \pmod{3}$,

Proof. 1. Assume $v_3(2a) = 0$.

(a) In addition, assume that $v_3(d) > 0$. Then the equation reduces modulo 3

$$F_{u'}(X, Y, Z) \equiv 2aX^2Z - 2aXYZ + 2aY^2Z + \frac{2b'}{N(\gamma)}Z^3 \pmod{3}.$$

We claim that $P_0 = (1, 1, 0)$ is a non-singular solution to this equation. Clearly this is a solution and since

$$\begin{aligned} \left.\frac{\partial F}{\partial Z}\right|_{P_0} &\equiv 2a(1)^2 - 2a(1)(1) + 2a(1)^2 \pmod{3} \\ &\equiv 2a \pmod{3} \end{aligned}$$

which is non-zero modulo 3, it follows that P_0 is non-singular. Hence we can lift to find solutions.

(b) Now assume that $v_3(d) = v_3\left(2a + \dfrac{2b'}{N(\gamma)}\right) = 0$. If $2a + \dfrac{2b'}{N(\gamma)} \equiv 1 \pmod 3$, then we claim that $P_0 = \left(\dfrac{1}{d}, \dfrac{1}{d}, 2\right)$ is a non-singular solution modulo 3. Otherwise if $2a + \dfrac{2b'}{N(\gamma)} \equiv 2 \pmod 3$, then we claim that $P_0 = \left(\dfrac{1}{d}, \dfrac{1}{d}, 1\right)$ is a non-singular solution modulo 3.

In either case, substituting in for X and Y, combining like terms and reducing, we have

$$F_{u'}\left(\frac{1}{d}, \frac{1}{d}, Z\right) \equiv \frac{2N(\gamma)aZ + 2b'd^2Z^3 + N(\gamma)}{N(\gamma)d^2} \pmod 3.$$

Notice that since $v_3(d) = 0$, $d^2 \equiv 1 \pmod 3$. Hence in case one we have

$$\begin{aligned} F_{u'}\left(\frac{1}{d}, \frac{1}{d}, Z\right) &\equiv a + \frac{b'}{N(\gamma)} + 1 \pmod 3 \\ &\equiv 2 + 1 \pmod 3 \\ &\equiv 0 \pmod 3. \end{aligned}$$

In case two, we have

$$\begin{aligned} F_{u'}\left(\frac{1}{d}, \frac{1}{d}, Z\right) &\equiv 2a + \frac{2b'}{N(\gamma)} + 1 \pmod 3 \\ &\equiv 2 + 1 \pmod 3 \\ &\equiv 0 \pmod 3. \end{aligned}$$

To see that both solutions are non-singular, notice that

$$\begin{aligned} \left.\frac{\partial F}{\partial Z}\right|_{P_0} &\equiv 2a\left(\frac{1}{d}\right)^2 - 2a\left(\frac{1}{d}\right)^2 + 2a\left(\frac{1}{d}\right)^2 \pmod 3 \\ &\equiv \frac{2a}{d^2} \pmod 3, \end{aligned}$$

which is clearly non-zero modulo 3. Thus we can lift to find solutions.

Now assume that (x, y, z) is a non-trivial, non-singular solution modulo 3.

If $v_3(d) = 0$, then the equation reduces to

$$F_{u'}(X, Y, Z) \equiv 2aX^2Z - 2aXYZ + 2aY^2Z + \frac{2b'}{N(\gamma)}Z^3 - dX^3 - dY^3 \pmod 3.$$

Notice by symmetry, we can interchange X and Y.

Without loss of generality, if $x = 0$, then the equation becomes

$$F_{u'}(0, y, z) \equiv 2ay^2z + \frac{2b'}{N(\gamma)}z^3 - dy^3 \pmod 3.$$

Since the solution is non-singular, a quick calculation shows that $y \neq 0$ and $z \neq 0$. Hence $y \equiv \pm 1 \pmod 3$ and $z \equiv \pm 1 \pmod 3$. Exhausting all possibilities, we find that we must have

$$v_3\left(2a + \frac{2b'}{N(\gamma)}\right) = 0.$$

Otherwise, if $x \neq 0$, then a simple calculation shows we must have $z \neq 0$ and $x \equiv y \pmod 3$. Hence the equation becomes

$$2az + \frac{2b'}{N(\gamma)}z^3 + d \equiv 0 \pmod 3,$$

which implies that

$$v_3\left(2a + \frac{2b'}{N(\gamma)}\right) = 0.$$

Therefore if $v_3(d) = 0$, then $v_3\left(2a + \frac{2b'}{N(\gamma)}\right) = 0$. Otherwise we have $v_3(d) > 0$.

2. Assume $v_3(2a) \geq 2$.

   (a) In addition, assume that $v_3(d) \geq 2$. Then since $3 \mid d$, it follows that $3 \nmid c$. It is easy to find a solution modulo 3, however all solutions are singular. Therefore we must look for a solution modulo 9. Notice that modulo 9, the equation reduces to

$$F_{u'}(X, Y, Z) \equiv \frac{2b'}{N(\gamma)} Z^3 - 3cXY^2 + 3cX^2Y \pmod 9.$$

   It is easy to see that $P_0 = (1, 1, 0)$ is a solution modulo 9 and since

$$\begin{aligned} \left.\frac{\partial F}{\partial X}\right|_{P_0} &= -3c(1^2) + 6c(1)(1) \\ &\equiv 3c \pmod 9, \end{aligned}$$

   is non-zero, it follows that P_0 is non-singular and therefore we can lift to find solutions.

   (b) Now assume that $v_3(d) = v_3(b') = 1$. Once again, we have $v_3(c) = 0$. Notice that in this case, every term of $F_{u'}(X, Y, Z)$ is divisible by 3. So we can reduce to finding solutions modulo 3 of the modified equation $\frac{1}{3}F_{u'}(X, Y, Z) \equiv 0 \pmod 3$. Note that the modified equation is

$$\frac{2\overline{b}}{N(\gamma)} Z^3 - \overline{d}X^3 - \overline{d}Y^3 - cXY^2 + cX^2Y \equiv 0 \pmod 3,$$

where $b' = 3\overline{b}$ and $d = 3\overline{d}$. By the above assumptions this implies that $\dfrac{2\overline{b}}{N(\gamma)} \equiv \pm 1 \pmod 3$ and $\overline{d} \equiv \pm 1 \pmod 3$. If $\overline{d} \equiv \dfrac{2\overline{b}}{N(\gamma)} \pmod 3$, then we claim that $P_0 = (0,1,1)$ is a non-singular solution to the above equation. Otherwise, if $\overline{d} \equiv -\dfrac{2\overline{b}}{N(\gamma)} \pmod 3$, then we claim that $P_1 = (0,-1,1)$ is a non-singular solution to the above equation. In the first case, we have

$$\frac{2\overline{b}}{N(\gamma)} - \overline{d} \equiv \frac{2\overline{b}}{N(\gamma)} - \frac{2\overline{b}}{N(\gamma)} \pmod 3 .$$

And since

$$\left.\frac{\partial F}{\partial X}\right|_{P_0} = -c \pmod 3 ,$$

is non-zero modulo 3, it follows that P_0 is non-singular and we can lift to find solutions.

In the second case, we have

$$\frac{2\overline{b}}{N(\gamma)} + \overline{d} \equiv \frac{2\overline{b}}{N(\gamma)} - \frac{2\overline{b}}{N(\gamma)} \pmod 3 .$$

And since

$$\left.\frac{\partial F}{\partial X}\right|_{P_1} = c \pmod 3 ,$$

which is non-zero modulo 3, it follows that P_1 is non-singular and we can lift to find solutions.

(c) In this part, assume $v_3(d) = 0$ and $\dfrac{2b'}{dN(\gamma)} \equiv k^3 \pmod 9$ where $(9,k) = 1$. We

begin by noticing that modulo 3, the equation becomes

$$\frac{2b'}{N(\gamma)}Z^3 - dX^3 - dY^3 \equiv 0 \pmod 3$$

which has the singular solution $(1, -1, 0)$. Since all solutions are singular modulo 3, we will look for non-singular solutions modulo 9. It is not hard to see that $(k, 0, 1)$ is a non-singular solution modulo 9, since

$$\begin{aligned} F_{u'}(-k, 0, 1) &\equiv \frac{2b'}{N(\gamma)}(1)^3 - d(k)^3 \pmod 3 \\ &\equiv \frac{2b'}{N(\gamma)} - d\left(\frac{2b'}{dN(\gamma)}\right) \pmod 3 \\ &\equiv 0 \pmod 3, \end{aligned}$$

and

$$\begin{aligned} \left.\frac{\partial F}{\partial X}\right|_{P_0} &\equiv -3dk^2 \pmod 9 \\ &\not\equiv 0 \pmod 9, \end{aligned}$$

it follows that P_0 is a non-singular solution modulo 9 and therefore we can lift to find other solutions.

(d) Finally assume that $\dfrac{2b'}{N(\gamma)} \equiv \pm(6c - 3d) \pmod{27}$. Reducing the equation modulo 3, we have

$$\frac{2b'}{N(\gamma)}Z^3 - dX^3 - dY^3 \equiv 0 \pmod 3,$$

which has the singular solution $(1, -1, 0)$. A simple calculation reveals that all solutions modulo 9 are singular. Therefore we must look for non-singular solutions modulo 27.

There are two cases we need to consider.

Case 1: $\dfrac{2b'}{N(\gamma)} \equiv (6c - 3d) \pmod{27}$.

We claim that $P_0 = (1, -1, 1)$ is a non-singular solution modulo 27. To see this notice

$$\begin{aligned} F_{u'}(1,-1,1) &= 3(2a) + \frac{2b'}{N(\gamma)} - 6c + 3d \\ &\equiv 6c - 3d - 6c + 3d \pmod{27} \\ &\equiv 0 \pmod{27} \end{aligned}$$

and

$$\begin{aligned} \left.\frac{\partial F}{\partial X}\right|_{P_0} &\equiv -9c \pmod{27}, \\ \left.\frac{\partial F}{\partial Y}\right|_{P_0} &\equiv 9(c-d) \pmod{27}, \\ \left.\frac{\partial F}{\partial Z}\right|_{P_0} &\equiv 9(2c-d) \pmod{27}. \end{aligned}$$

For P_0 to be a singular point, we would have to have $c \equiv d \equiv 0 \pmod{3}$, which is not possible since $(c, d) = 1$. Thus P_0 is non-singular and we can lift to find solutions.

Case 2: $\dfrac{2b'}{N(\gamma)} \equiv -(6c - 3d) \pmod{27}$.

We claim that $P_0 = (1, -1, -1)$ is a non-singular solution modulo 27. To see this notice

$$\begin{aligned} F_{u'}(1,-1,-1) &= 3(2a) - \frac{2b'}{N(\gamma)} - 6c + 3d \\ &\equiv -(-6c + 3d) - 6c + 3d \pmod{27} \\ &\equiv 0 \pmod{27} \end{aligned}$$

and

$$\begin{aligned}
\left.\frac{\partial F}{\partial X}\right|_{P_0} &\equiv -9c \pmod{27} \\
\left.\frac{\partial F}{\partial Y}\right|_{P_0} &\equiv 9(c-d) \pmod{27} \\
\left.\frac{\partial F}{\partial Z}\right|_{P_0} &\equiv 9\,(2c-d) \pmod{27}.
\end{aligned}$$

For P_0 to be a singular point, we would have to have $c \equiv d \equiv 0 \pmod{3}$, which is not possible since $(c,d) = 1$. Thus P_0 is non-singular and we can lift to find solutions.

The reverse direction requires a series of calculations in MATLAB to exhaust all possibilities. These show that whenever we have a solution, one of the above conditions is satisfied.

3. Assume $v_3(2a) = 1$.

   (a) In addition, assume $v_3(d) \geq 2$. Then since $v_3(N(\gamma)) = 0$, we know that $v_3(c) = 0$. Note that the equation modulo 3 becomes

$$F_{u'}(X,Y,Z) = \frac{2b}{N(\gamma)}Z^3.$$

   It is easy to see that $(1,1,0)$ is the only solution modulo 3, however it is singular. So we will look modulo 9. Now, reducing modulo 9 the equation is of the form

$$F_{u'}(X,Y,Z) = 2aX^2Z - 2aXYZ + 2aY^2Z + \frac{2b'}{N(\gamma)}Z^3 - 3cXY^2 + 3cX^2Y.$$

It is not hard to see that $P_0 = (1, 1, 0)$ is a solution modulo 9 and since

$$\begin{aligned} \left.\frac{\partial F}{\partial Z}\right|_{P_0} &\equiv 2a - 2a + 2a \pmod 9 \\ &\not\equiv 0 \pmod 9, \end{aligned}$$

P_0 is non-singular so we can lift to find solutions.

(b) Now assume $v_3(d) = v_3\left(2a + \dfrac{2b'}{N(\gamma)}\right) = 1$. Again, we can deduce that $v_3(c) = 0$. In addition, since 3 divides $2a$ exactly once and 3 divides $2a + \dfrac{2b'}{N(\gamma)}$ exactly once, it follows that $v_3\left(\dfrac{2b'}{N(\gamma)}\right) = 1$. Now, we can easily see that every term of $F_{u'}(X, Y, Z)$ is divisible by 3, so finding a solution to $F_{u'}(X, Y, Z) = 0$ is equivalent to finding a solution to $\dfrac{1}{3}F_{u'}(X, Y, Z) = 0$.
Let $a = 3\overline{a}$, $b' = 3\overline{b}$ and $d = 3\overline{d}$. Then the modified equation becomes

$$2\overline{a}X^2Z - 2\overline{a}XYZ + 2\overline{a}Y^2Z + \frac{2\overline{b}}{N(\gamma)}Z^3 - \overline{d}X^3 - \overline{d}Y^3 - cXY^2 + cX^2Y = 0.$$

There are two cases we need to consider.
Case 1: $2\overline{a} + \dfrac{2\overline{b}}{N(\gamma)} \equiv \overline{d} \pmod 3$
In this case, we claim that $P_0 = (0, 1, 1)$ is a non-singular solution modulo 3 to the modified equation. To see this, notice that we have

$$\begin{aligned} 2\overline{a}(1^2)(1) + \frac{2\overline{b}}{N(\gamma)}(1^3) - \overline{d}(1^3) &\equiv \overline{d} - \overline{d} \pmod 3 \\ &\equiv 0 \pmod 3, \end{aligned}$$

and

$$\left.\frac{\partial F}{\partial X}\right|_{P_0} = -2\overline{a}(1)(1) \not\equiv 0 \pmod 3 .$$

Thus we can lift to find solutions.

Case 2: $2\overline{a} + \dfrac{2\overline{b}}{N(\gamma)} \equiv -\overline{d} \pmod 3$

In this case, we claim that $P_0 = (0, 1, -1)$ is a non-singular solution modulo 3 to the modified equation. To see this, notice that we have

$$2\overline{a}1^2(-1) + \frac{2\overline{b}}{N(\gamma)}(-1)^3 - \overline{d}(1^3) \equiv \overline{d} - \overline{d} \pmod 3 \equiv 0 \pmod 3 ,$$

and

$$\left.\frac{\partial F}{\partial X}\right|_{P_0} = -2\overline{a}(1)(-1) \not\equiv 0 \pmod 3 .$$

Thus we can lift to find solutions.

(c) In this case, we will assume $v_3(d) = 0$ and $\left(2a + \dfrac{2b'}{N(\gamma)}\right)/d$ is a cube modulo 9. This implies that there exists $k \in \mathbb{Z}$ such that $\left(2a + \dfrac{2b'}{N(\gamma)}\right)/d \equiv k^3 \pmod 9$ and $(k, 9) = 1$. Reducing the equation modulo 3, we have

$$F_{u'}(X, Y, Z) \equiv \frac{2b'}{N(\gamma)}Z^3 - dX^3 - dY^3 \pmod 3 ,$$

which clearly has the solution $(1, -1, 0)$. It is easy to see that every solution

modulo 3 is singular. So again, we will look for solutions modulo 9.

If $k^3 \equiv 1 \pmod 9$, then this implies that $2a + \dfrac{2b'}{N(\gamma)} \equiv d \pmod 9$. It is not hard to see that $P_0 = (k, 0, k)$ is a solution modulo 9. Running Maple code, one can check that in all cases P_0 will be a non-singular solution. Hence we can lift to find solutions.

If $k^3 \equiv -1 \pmod 9$, then this implies that $2a + \dfrac{2b'}{N(\gamma)} \equiv -d \pmod 9$. Again, it is not hard to see that $P_0 = (-k, 0, k)$ is a solution modulo 9. Running Maple code, one can again check that in all cases P_0 will be a non-singular solution. Hence we can lift to find solutions.

(d) Now assume $v_3(d) = 0$, $v_3\left(\dfrac{2b'}{N(\gamma)}\right) = 1$ and there exists $s \in \{\pm 1\}$ such that $(d - 2c) \equiv s\left(\dfrac{2b'}{3N(\gamma)} + 2a\right) \pmod{27}$ and $s(2c - d) \equiv 2a/3 \pmod 3$. A tedious calculation in MATLAB shows that in this case, we will always have a solution.

If we assume there is a solution, then one can show that the equation always satisfies one of the situations listed above.

□

Appendix E Proof of Lemma 53

Lemma 101. *Suppose (S_1, S_2, S_3) is a partition of $V(G)$. Let*

$$u_1 = \prod_{p_i \in S_1} p_i \quad \text{and} \quad u_2 = \prod_{p_j \in S_2} p_j.$$

Then the homogeneous equation

$$u_1 X^3 + u_2 Y^3 + \frac{2b}{u_1 u_2} Z^3 - 2aXYZ = 0 \tag{8}$$

has a solution in every local field $\mathbb{Q}_p$ if and only if $3 \nmid a$ and (S_1, S_2, S_3) is three-balanced or if $3 \,||\, a$ and (S_1, S_2, S_3) is three-quasi-balanced at 3 or if $9 \mid a$ and (S_1, S_2, S_3) is three-quasi-balanced at 9.

Proof. Let $u_3 = 2b/(u_1 u_2)$. We will begin by assuming that $3 \nmid a$ and (S_1, S_2, S_3) is a three-balanced partition. Note in this case, $3 \nmid \Delta'$. By Proposition 43, there are three things we need to show. First, for every prime $p \in S_\nu$, if p is only in S_ν and $p \mid \Delta'$, then $\chi_p(u_{\nu+1}/u_{\nu+2}) = 1$ where we cycle the indices. Second, for every $p \in S_\eta$ with $\eta = 1$ or 2 such that p is also in S_3 and $p \mid \Delta'$, we have $\chi_p(u_\eta/u_3) = 1$. Finally, we must also show that for every $p \in V(G') \setminus V(G)$, $\chi_p(u_1/u_2) = 1$.

Notice that for every $p \in S_\nu$, which is only in S_ν and $p \mid \Delta'$, we have

$$\begin{aligned}
\chi_p(u_{\nu+1}/u_{\nu+2}) &= \chi_p(u_{\nu+1})\,\chi_p(u_{\nu+2})^2 \\
&= \left(\prod_{p_j \in S_{\nu+1}} \chi_p(p_j)\right)\left(\prod_{p_k \in S_{\nu+2}} \chi_p(p_k)^2\right) \\
&= \left(\prod_{p_j \in S_{\nu+1}} \ell(p, p_j)\right)\left(\prod_{p_k \in S_{\nu+2}} \ell(p, p_k)^2\right) \\
&= 1
\end{aligned}$$

since (S_1, S_2, S_3) is three-balanced. In the case that $p \in S_\eta$, with $\eta = 1$ or 2 and p is also in S_3 and $p \mid \Delta'$, we have

$$\begin{aligned}
\chi_p\left(u_\eta/u_3\right) &= \chi_p\left(u'_\eta\right)\chi_p\left(u'_3\right)^2 \\
&= \left(\prod_{\substack{p_j \in S_\eta \\ p_j \neq p}} \chi_p(p_j)\right)\left(\prod_{\substack{p_k \in S_3 \\ p_k \neq p}} \chi_p(p_k)^2\right) \\
&= \left(\prod_{\substack{p_j \in S_\eta \\ p_j \neq p}} \ell(p, p_j)\right)\left(\prod_{\substack{p_k \in S_3 \\ p_k \neq p}} \ell(p, p_k)^2\right) \\
&= 1,
\end{aligned}$$

with $u_\eta = pu'_\eta$ and $u_3 = pu'_3$.

We also know that for every $p \in V(G') \setminus V(G)$,

$$\begin{aligned}
\chi_p\left(u_1/u_2\right) &= \chi_p\left(u_1\right)\chi_p\left(u_2\right)^2 \\
&= \left(\prod_{p_j \in S_1} \chi_p(p_j)\right)\left(\prod_{p_k \in S_2} \chi_p(p_k)^2\right) \\
&= \left(\prod_{p_j \in S_1} \ell(p, p_j)\right)\left(\prod_{p_k \in S_2} \ell(p, p_k)^2\right) \\
&= 1.
\end{aligned}$$

If $3 \mid\mid a$ and (S_1, S_2, S_3) is three-quasi-balanced at 3, then $3 \mid \Delta'$. Notice that we have checked most of the conditions already. So if $p = 3$ is only in one S_ν, then we only need to check that either $\chi_3\left(u_{\nu+1}/u_{\nu+2}\right) = 1$ or there exists $s_1, s_2 \in \{\pm 1\}$ such that $2a \equiv s_1\left(\prod_{p_i \in S_1} p_i\right) + s_2\left(\prod_{p_j \in S_2} p_j\right) + s_1 s_2\left(\prod_{p_k \in S_3} p_k\right) \pmod 9$. Otherwise we are guaranteed a solution.

If $p = 3$ is in only one S_ν, then either

$$\begin{aligned}
\chi_3\left(u_{\nu+1}/u_{\nu+2}\right) &= \chi_3\left(u_{\nu+1}\right)\chi_3\left(u_{\nu+2}\right)^2 \\
&= \left(\prod_{p_j \in S_{\nu+1}} \chi_3\left(p_j\right)\right)\left(\prod_{p_k \in S_{\nu+2}} \chi_3\left(p_k\right)^2\right) \\
&= \left(\prod_{p_j \in S_{\nu+1}} \ell(3,p_j)\right)\left(\prod_{p_k \in S_{\nu+2}} \ell(3,p_k)^2\right) \\
&= 1
\end{aligned}$$

or $2a \equiv s_1\left(\prod_{p_i \in S_1} p_i\right) + s_2\left(\prod_{p_j \in S_2} p_j\right) + s_1 s_2\left(\prod_{p_k \in S_3} p_k\right) \pmod 9$ for some $s_1, s_2 \in \{\pm 1\}$. In either case, by Proposition 44 we are guaranteed a solution in $\mathbb{Q}_3$.

If $9 \mid a$ and (S_1, S_2, S_3) is three-quasi-balanced at 9, then we still have $3 \mid \Delta'$. Again, notice that most of the conditions have already been verified. If $v_3(2b) = 1$, then we are guaranteed a solution. Otherwise, if $v_3(2b) = 2$, then we need to check two things. First, if both copies of 3 are in S_3, then $\chi_3\left(u_1/u_2\right) = 1$. Otherwise if $3 \in S_\eta$, with $\eta = 1$ or 2, and $3 \in S_3$, then $\chi_3\left(u_\eta/u_3\right) = 1$.

If 3 is only in S_3, then

$$\begin{aligned}
\chi_3\left(u_1/u_2\right) &= \chi_3(u_1)\chi_3(u_2)^2 \\
&= \left(\prod_{p_j \in S_1} \chi_3\left(p_j\right)\right)\left(\prod_{p_k \in S_2} \chi_3\left(p_k\right)^2\right) \\
&= \left(\prod_{p_j \in S_1} \ell(3,p_j)\right)\left(\prod_{p_k \in S_2} \ell(3,p_k)^2\right) \\
&= 1.
\end{aligned}$$

If $3 \in S_\eta$ with $\eta = 1$ or 2 and $3 \in S_3$, then

$$\begin{aligned}
\chi_3\left(u_\eta/u_3\right) &= \chi_3\left(u'_\eta\right)\chi_3\left(u'_3\right) \\
&= \left(\prod_{\substack{p_j \in S_\eta \\ p_j \neq 3}} \chi_3(p_j)\right)\left(\prod_{\substack{p_k \in S_3 \\ p_k \neq 3}} \chi_3(p_k)^2\right) \\
&= \left(\prod_{\substack{p_j \in S_\eta \\ p_j \neq 3}} \ell(3,p_j)\right)\left(\prod_{\substack{p_k \in S_3 \\ p_k \neq 3}} \ell(3,p_k)^2\right) \\
&= 1,
\end{aligned}$$

where $u_\eta = 3u'_\eta$ and $u_3 = 3u'_3$. In either case, by Proposition 44, we have a solution in $\mathbb{Q}_3$.

Conversely, suppose if $3 \nmid a$, then (S_1, S_2, S_3) is not three-balanced or if $3 \,||\, a$, then (S_1, S_2, S_3) is not three-quasi-balanced at 3 or if $9 \mid a$, then (S_1, S_2, S_3) is not three-quasi-balanced at 9. There are a few cases we need to consider.

Case 1: These exists $p \in S_1 \cup S_2$ with $p^2 \mid 2b$ such that the additional copy of p is also in $S_1 \cup S_2$. Note in this case, we would either have that $(u_1, u_2) \neq 1$ or u_i not square-free for $i = 1$ and $i = 2$. These are both requirements for the equation (5.2).

Case 2: If we have $v_2(b) = 2$ and $2 \in S_1 \cup S_2$, then in this case we are guaranteed that the equation does not have a solution by Proposition 43.

Case 3: There exists p in some S_ν with $p \mid \Delta'$, $p \neq 3$ and p not in any other S_ν, such that

$$\left(\prod_{p_j \in S_{\nu+1}} \ell(p,p_j)\right)\left(\prod_{p_k \in S_{\nu+2}} \ell(p,p_k)^2\right) \neq 1.$$

Then

$$\begin{aligned}
\chi_p\left(u_{\nu+1}/u_{\nu+2}\right) &= \chi_p\left(u_{\nu+1}\right)\chi_p\left(u_{\nu+2}\right)^2 \\
&= \left(\prod_{p_j\in S_{\nu+1}}\chi_p(p_j)\right)\left(\prod_{p_k\in S_{\nu+2}}\chi_p(p_k)^2\right) \\
&= \left(\prod_{p_j\in S_{\nu+1}}\ell(p,p_j)\right)\left(\prod_{p_k\in S_{\nu+2}}\ell(p,p_k)^2\right) \\
&\neq 1,
\end{aligned}$$

where we cycle the indices. Hence by Proposition 43, equation (5.2) does not have a solution in Q_p.

Case 4**:** There exists p in some S_η, with $p \mid \Delta'$ and $\eta = 1$ or 2, such that p is also in S_3 and $p \mid \Delta'$ and

$$\left(\prod_{p_j\in S_\eta}\ell(p,p_j)\right)\left(\prod_{p_k\in S_3}\ell(p,p_k)^2\right) \neq 1.$$

Then

$$\begin{aligned}
\chi_p\left(u_\eta/u_3\right) &= \chi_p\left(u'_\eta\right)\chi_p\left(u'_3\right)^2 \\
&= \left(\prod_{\substack{p_j\in S_\eta\\ p_j\neq p}}\chi_p(p_j)\right)\left(\prod_{\substack{p_k\in S_3\\ p_k\neq p}}\chi_p(p_k)^2\right) \\
&= \left(\prod_{\substack{p_j\in S_\eta\\ p_j\neq p}}\ell(p,p_j)\right)\left(\prod_{\substack{p_k\in S_3\\ p_k\neq p}}\ell(p,p_k)^2\right) \\
&\neq 1
\end{aligned}$$

with $u_\eta = pu'_\eta$ and $u_3 = pu'_3$. Hence by Proposition 43, equation (5.2) does not have a

solution in $\mathbb{Q}_p$.

Case 5**:** There exists a $p \in V(G') \setminus V(G)$

$$\left(\prod_{p_j \in S_1} \ell(p, p_j)\right)\left(\prod_{p_k \in S_2} \ell(p, p_k)^2\right) \neq 1.$$

Since

$$\begin{aligned}
\chi_p(u_1/u_2) &= \chi_p(u_1)\,\chi_p(u_2)^2 \\
&= \left(\prod_{p_j \in S_1} \chi_p(p_j)\right)\left(\prod_{p_k \in S_2} \chi_p(p_k)^2\right) \\
&= \left(\prod_{p_j \in S_1} \ell(p, p_j)\right)\left(\prod_{p_k \in S_2} \ell(p, p_k)^2\right) \\
&\neq 1,
\end{aligned}$$

it follows that (4.11) does not have a solution in $\mathbb{Q}_p$.

If $3 \,||\, a$ and (S_1, S_2, S_3) is not three-quasi-balanced at 3, then we have already covered every case except when $p = 3$ is only in one S_ν. For (S_1, S_2, S_3) not to be three-quasi-balanced at 3, this means that

$$\left(\prod_{p_j \in S_{\nu+1}} \ell(3, p_j)\right)\left(\prod_{p_k \in S_{\nu+2}} \ell(3, p_k)^2\right) \neq 1$$

where we cycle the indices of the partitions (i.e. $S_1 = S_4$, etc.) and for all $s_1, s_2 \in \{\pm 1\}$ we have

$$2a \not\equiv s_1\left(\prod_{p_i \in S_1} p_i\right) + s_2\left(\prod_{p_j \in S_2} p_j\right) + s_1 s_2\left(\prod_{p_k \in S_3} p_k\right) \pmod 9.$$

So for $3 \in S_\nu$,

$$\begin{aligned}
\chi_3\left(u_{\nu+1}/u_{\nu+2}\right) &= \chi_3\left(u_{\nu+1}\right)\chi_3\left(u_{\nu+2}\right)^2 \\
&= \left(\prod_{p_j \in S_{\nu+1}} \chi_3\left(p_j\right)\right)\left(\prod_{p_k \in S_{\nu+2}} \chi_3\left(p_k\right)^2\right) \\
&= \left(\prod_{p_j \in S_{\nu+1}} \ell(3,p_j)\right)\left(\prod_{p_k \in S_{\nu+2}} \ell(3,p_k)^2\right) \\
&\neq 1.
\end{aligned}$$

Hence by Proposition 44, there is no solution in $\mathbb{Q}_3$.

Finally, if $9 \mid a$ and (S_1, S_2, S_3) is not three-quasi-balanced at 9, then we have already covered every case except when $9 \mid 2b$. If $p = 3$ is only in S_3 and

$$\left(\prod_{p_j \in S_1} \ell(3,p_j)\right)\left(\prod_{p_k \in S_2} \ell(3,p_k)^2\right) \neq 1,$$

then

$$\begin{aligned}
\chi_3\left(u_1/u_2\right) &= \chi_3(u_1)\chi_{p_n}(u_2)^2 \\
&= \left(\prod_{p_j \in S_1} \chi_3\left(p_j\right)\right)\left(\prod_{p_k \in S_2} \chi_3\left(p_k\right)^2\right) \\
&= \left(\prod_{p_j \in S_1} \ell(3,p_j)\right)\left(\prod_{p_k \in S_2} \ell(3,p_k)^2\right) \\
&\neq 1.
\end{aligned}$$

If instead, $3 \in S_\eta$ with $\eta = 1$ or 2, $3 \in S_3$ and

$$\left(\prod_{\substack{p_j \in S_\eta \\ p_j \neq 3}} \ell(3, p_j) \right) \left(\prod_{\substack{p_k \in S_3 \\ p_k \neq 3}} \ell(3, p_k)^2 \right) \neq 1,$$

then

$$\begin{aligned} \chi_3 (u_\eta / u_3) &= \chi_3 \left(u'_\eta \right) \chi_3 \left(u'_3 \right) \\ &= \left(\prod_{\substack{p_j \in S_\eta \\ p_j \neq 3}} \chi_3(p_j) \right) \left(\prod_{\substack{p_k \in S_3 \\ p_k \neq 3}} \chi_3(p_k)^2 \right) \\ &= \left(\prod_{\substack{p_j \in S_\eta \\ p_j \neq 3}} \ell(3, p_j) \right) \left(\prod_{\substack{p_k \in S_3 \\ p_k \neq 3}} \ell(3, p_k)^2 \right) \\ &= 1, \end{aligned}$$

where $u_\eta = 3u'_\eta$ and $u_3 = 3u'_3$. So in either case, by Proposition 44 we would not have a solution in $\mathbb{Q}_3$. □

Bibliography

[1] Greg W. Anderson and Dinesh S. Thakur. Tensor powers of the Carlitz module and zeta values. Ann. of Math. (2), 132(1):159–191, 1990.

[2] Jeffrey Beyerl, Kevin James, Catherine Trentacoste, and Hui Xue. Products of nearly holomorphic eigenforms. The Ramanujan Journal, 27:377–386, 2012. 10.1007/s11139-011-9321-2.

[3] M. Bhargava and A. Shankar. Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. ArXiv e-prints, June 2010.

[4] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. II. J. Reine Angew. Math., 218:79–108, 1965.

[5] Morgan V. Brown, Neil J. Calkin, Kevin James, Adam J. King, Shannon Lockard, and Robert C. Rhoades. Trivial Selmer groups and even partitions of a graph. Integers, 6:A33, 17, 2006.

[6] L. Carlitz. On certain functions connected with polynomials in a galois field. Duke Math. J., 1:137–168, 1935.

[7] L. Carlitz. An analogue of the von Staudt-Clausen theorem. Duke Math. J., 3(3):503–517, 1937.

[8] L. Carlitz. An analogue of the Staudt-Clausen theorem. Duke Math. J., 7:62–67, 1940.

[9] L. Carlitz. An analogue of the Bernoulli polynomials. Duke Math. J., 8:405–412, 1941.

[10] L. Carlitz. Finite sums and interpolation formulas over $GF[p^n, x]$. Duke Math. J., 15:1001–1012, 1948.

[11] J. W. S. Cassels. Arithmetic on curves of genus 1. I. On a conjecture of Selmer. J. Reine Angew. Math., 202:52–99, 1959.

[12] Henri Cohen. Number theory. Vol. I. Tools and Diophantine equations, volume 239 of Graduate Texts in Mathematics. Springer, New York, 2007.

[13] Henri Cohen. Number theory. Vol. II. Analytic and modern tools, volume 240 of Graduate Texts in Mathematics. Springer, New York, 2007.

[14] Henri Cohen and Fabien Pazuki. Elementary 3-descent with a 3-isogeny. Acta Arith., 140(4):369–404, 2009.

[15] David Cox, John Little, and Donal O'Shea. Ideals, varieties, and algorithms. Undergraduate Texts in Mathematics. Springer, New York, third edition, 2007. An introduction to computational algebraic geometry and commutative algebra.

[16] David A. Cox, John Little, and Donal O'Shea. Using algebraic geometry, volume 185 of Graduate Texts in Mathematics. Springer, New York, second edition, 2005.

[17] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll. Explicit n-descent on elliptic curves. I. Algebra. J. Reine Angew. Math., 615:121–155, 2008.

[18] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll. Explicit n-descent on elliptic curves. II. Geometry. J. Reine Angew. Math., 632:63–84, 2009.

[19] M.I. Rosen D. Goss, D.R. Hayes. The Arithmetic of Function Fields. Walter de Gruyter, 1992.

[20] Chantal David. Supersingular reduction of Drinfel′d modules. Duke Math. J., 78(2):399–412, 1995.

[21] Chantal David. Average distribution of supersingular Drinfel′d modules. J. Number Theory, 56(2):366–380, 1996.

[22] Chantal David. Frobenius distributions of Drinfeld modules of any rank. J. Number Theory, 90(2):329–340, 2001.

[23] Matt DeLong. A formula for the Selmer group of a rational three-isogeny. Acta Arith., 105(2):119–131, 2002.

[24] Fred Diamond and Jerry Shurman. A first course in modular forms, volume 228 of Graduate Texts in Mathematics. Springer-Verlag, New York, 2005.

[25] Javier Diaz-Vargas. Riemann hypothesis for $\mathbf{F}_p[T]$. J. Number Theory, 59(2):313–318, 1996.

[26] Javier Diaz-Vargas. On zeros of characteristic p zeta function. J. Number Theory, 117(2):241–262, 2006.

[27] Z. Djabri, Edward F. Schaefer, and N. P. Smart. Computing the p-Selmer group of an elliptic curve. Trans. Amer. Math. Soc., 352(12):5583–5597, 2000.

[28] V. G. Drinfel′d. Elliptic modules. Mat. Sb. (N.S.), 94(136):594–627, 656, 1974.

[29] W. Duke. When is the product of two Hecke eigenforms an eigenform? In Number theory in progress, Vol. 2 (Zakopane-Kościelisko, 1997), pages 737–741. de Gruyter, Berlin, 1999.

[30] Brad A. Emmons and Dominic Lanphier. Products of an arbitrary number of Hecke eigenforms. Acta Arith., 130(4):311–319, 2007.

[31] Bryan Faulkner and Kevin James. A graphical approach to computing Selmer groups of congruent number curves. Ramanujan J., 14(1):107–129, 2007.

[32] Keqin Feng and Maosheng Xiong. On elliptic curves $y^2 = x^3 - n^2x$ with rank zero. J. Number Theory, 109(1):1–26, 2004.

[33] Tom Fisher. Finding rational points on elliptic curves using 6-descent and 12-descent. J. Algebra, 320(2):853–884, 2008.

[34] Eknath Ghate. On monomial relations between Eisenstein series. J. Ramanujan Math. Soc., 15(2):71–79, 2000.

[35] D. Goss. Von-staudt for $f_q[t]$. Duke Math. J., 45:885–910, 1978.

[36] D. Goss. Modular forms for $f_r[t]$. J. reine angew. Math., 317:16–39, 1980.

[37] D. Goss. Basic Structures of Function Field Arithmetic. Springer-Verlag Berlin Heidelberg, 1998.

[38] D. Goss. ζ-phenomenology. In Workshop and Advanced Course on Drinfeld Modules and L-functions., 2010.

[39] Robin Hartshorne. Algebraic geometry. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[40] David R. Hayes. A brief introduction to Drinfel′d modules. In The arithmetic of function fields (Columbus, OH, 1991), volume 2 of Ohio State Univ. Math. Res. Inst. Publ., pages 1–32. de Gruyter, Berlin, 1992.

[41] D. R. Heath-Brown. The size of Selmer groups for the congruent number problem. Invent. Math., 111(1):171–195, 1993.

[42] D. R. Heath-Brown. The size of Selmer groups for the congruent number problem. II. Invent. Math., 118(2):331–370, 1994. With an appendix by P. Monsky.

[43] Dale Husemöller. Elliptic curves, volume 111 of Graduate Texts in Mathematics. Springer-Verlag, New York, second edition, 2004. With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen.

[44] Kenneth F. Ireland and Michael I. Rosen. A classical introduction to modern number theory, volume 84 of Graduate Texts in Mathematics. Springer-Verlag, New York, 1982. Revised edition of ıt Elements of number theory.

[45] Kevin James and Ken Ono. Selmer groups of quadratic twists of elliptic curves. Math. Ann., 314(1):1–17, 1999.

[46] Matthew Johnson. Hecke Eigenforms as Products of Eigenforms. Masters Thesis, 2008.

[47] Neal Koblitz. Introduction to Elliptic Curves and Modular forms. Springer, 1993.

[48] Serge Lang. Elliptic curves: Diophantine analysis, volume 231 of Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, Berlin, 1978.

[49] Serge Lang. Introduction to modular forms, volume 222 of Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, Berlin, 1995. With appendixes by D. Zagier and Walter Feit, Corrected reprint of the 1976 original.

[50] Dominic Lanphier. Combinatorics of Maass-Shimura operators. J. Number Theory, 128(8):2467–2487, 2008.

[51] Dominic Lanphier and Ramin Takloo-Bighash. On Rankin-Cohen brackets of eigenforms. J. Ramanujan Math. Soc., 19(4):253–259, 2004.

[52] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). Invent. Math., 44(2):129–162, 1978.

[53] J. Meher. Some Remarks on Rankin-Cohen Brackets of Eigenforms. ArXiv e-prints, November 2011.

[54] O. Ore. On a special class of polynomials. Trans. Amer. Math So., 35:559–584, 1933.

[55] Robert C. Rhoades. 2-Selmer groups and the Birch-Swinnerton-Dyer conjecture for the congruent number curves. J. Number Theory, 129(6):1379–1391, 2009.

[56] M. Rosen. Number Theory in Function Fields. Springer-Verlag, 2002.

[57] Karl Rubin and Alice Silverberg. Ranks of elliptic curves. Bull. Amer. Math. Soc. (N.S.), 39(4):455–474 (electronic), 2002.

[58] J.-P. Serre. A course in arithmetic. Springer-Verlag, New York, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

[59] Jeffrey T. Sheats. The Riemann hypothesis for the Goss zeta function for $\mathbf{F}_q[T]$. J. Number Theory, 71(1):121–157, 1998.

[60] Goro Shimura. The special values of the zeta functions associated with cusp forms. Comm. Pure Appl. Math., 29(6):783–804, 1976.

[61] Goro Shimura. Elementary Dirichlet series and modular forms. Springer Monographs in Mathematics. Springer, New York, 2007.

[62] Joseph H. Silverman. The arithmetic of elliptic curves, volume 106 of Graduate Texts in Mathematics. Springer, Dordrecht, second edition, 2009.

[63] Joseph H. Silverman and John Tate. Rational points on elliptic curves. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

[64] Ethan C. Smith. On Elliptic Curves, Modular Forms and Distribution of Primes. PhD thesis, Clemson University, 2009.

[65] Dinesh S. Thakur. Drinfel′d modules and arithmetic in the function fields. Internat. Math. Res. Notices, (9):185–197, 1992.

[66] Dinesh S. Thakur. On characteristic p zeta functions. Compositio Math., 99(3):231–247, 1995.

[67] Dinesh S. Thakur. Function field arithmetic. World Scientific Publishing Co. Inc., River Edge, NJ, 2004.

[68] Jaap Top. Descent by 3-isogeny and 3-rank of quadratic fields. In Advances in number theory (Kingston, ON, 1991), Oxford Sci. Publ., pages 303–317. Oxford Univ. Press, New York, 1993.

[69] Catherine M. Trentacoste. Construction of a dimension two rank one Drinfeld module. Master's thesis, Clemson University, 2009.

[70] Lawrence C. Washington. Introduction to cyclotomic fields, volume 83 of Graduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1997.

[71] Gang Yu. Average size of 2-Selmer groups of elliptic curves. II. Acta Arith., 117(1):1–33, 2005.

[72] Jing Yu. Transcendence and special zeta values in characteristic p. Ann. of Math. (2), 134(1):1–23, 1991.

[73] D. Zagier. Modular forms whose Fourier coefficients involve zeta-functions of quadratic fields. In Modular functions of one variable, VI (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), pages 105–169. Lecture Notes in Math., Vol. 627. Springer, Berlin, 1977.