5-7-2013

Siegel Functions, Modular Curves, and Serre's Uniformity Problem

Harris B. Daniels
harris.daniels@gmail.com

Siegel Functions, Modular Curves, and Serre's Uniformity Problem

Harris B. Daniels, Ph.D.

University of Connecticut, 2013

ABSTRACT

Serre's uniformity problem asks whether there exists a bound k such that for any $p > k$, the Galois representation associated to the p-torsion of an elliptic curve $E/\mathbb{Q}$ is surjective independent of the choice of E. Serre showed that if this representation is not surjective, then it has to be contained in either a Borel subgroup, the normalizer of a split Cartan subgroup, the normalizer of a non-split Cartan subgroup, or one of a finite list of "exceptional" subgroups. We will focus on the case when the image is contained in the normalizer of a split Cartan subgroup. In particular, we will show that the only elliptic curves whose Galois representation at 11 is contained in the normalizer of a split Cartan have complex multiplication. To prove this we compute $X_s^+(11)$ using modular units, use the methods of Poonen and Schaefer to compute its jacobian, and then use the method of Chabauty and Coleman to show that the only points on this curve correspond to CM elliptic curves.

Siegel Functions, Modular Curves, and Serre's Uniformity Problem

Harris B. Daniels

M.S. University of Connecticut

B.S. Trinity College

A Dissertation

Submitted in Partial Fulfillment of the

Requirements for the Degree of

Doctor of Philosophy

at the

University of Connecticut

2013

APPROVAL PAGE

Doctor of Philosophy Dissertation

Siegel Functions, Modular Curves, and Serre's Uniformity Problem

Presented by

Harris B. Daniels, B.S. Math., M.S. Math.

Major Advisor _____
Álvaro Lozano-Robledo

Associate Advisor _____
Keith Conrad

Associate Advisor _____
Kyu-Hwan Lee

University of Connecticut

2013

ACKNOWLEDGMENTS

Though only my name appears on the cover of this dissertation, a great many people have played a role in its creation. I owe much gratitude to all those people who have made this dissertation possible.

It is difficult to overstate my gratitude to my Ph.D. advisor, Dr. Álvaro Lozano-Robledo, without whom this dissertation would not have been possible. It was his patience, vision, support, and advice that laid the ground work for me to successfully proceed through the doctoral program and complete my dissertation. I could not imagine having a better advisor, academic role model, and friend.

I would also like to thank Dr. Keith Conrad, whose many classes and expository papers have served as the underpinning for my graduate education in mathematics. Without him I would not be half the mathematician that I am today.

Special thanks to Dr. Kyu-Hwan Lee for his many helpful comments throughout the research and writing process. I cannot thank him enough for his willingness to be on my committee.

The work in this thesis was done during my time in the Department of Mathematics at the University of Connecticut. There are many people at the University of Connecticut that are owed thanks for supporting me throughout this difficult process. In particular, I would like to thank Alex Baldenko, Chris Buechler and Leland Aldridge for always giving me (and allowing me to be) a distraction.

I also owe a debt of gratitude to Dr. Amit Savkar, whose door was always open to

speak about the difficulties and subtleties of teaching mathematics. He is one of the most dedicated teachers that I have met in my time in academia and I am a better teacher for having met him.

I am extremely indebted to Monique Roy for all of the help that she has provided me. Never have I met someone so patient and willing to lend a hand. Monique is a major reason that the University of Connecticut Department of Mathematics is such a warm and friendly place to work and study.

Of course, none of this would be possible without the love and support of my family. Specifically, I would like to thank my mother and father. Throughout my entire life my parents have placed my well-being ahead of their own. It is because of this that I have had the opportunities that have led me here. I can unequivocally say that without their unfaltering support and encouragement I never would have made it as far as I have.

Finally, and most importantly, I would like to thank Marcy. Her ability to tolerate my occasional sour moods and frequent bad jokes is a testament to her unyielding love and devotion. Her unwavering empathy and affection is the foundation on which this dissertation has been built. Her willingness to stand by my side through this process makes me the luckiest man in the world.

Contents

Chapter 1

Introduction

1.1 Background

It is a classical result that the points of an elliptic curve E over a number field K (a smooth projective genus one curve with at least one K-rational point) defined over a number field K can be given the structure of an abelian group. In fact, it is known from the Mordell-Weil theorem, that this group is finitely generated. Therefore, we have that

$$E(K) \cong E_{\text{tor}}(K) \times \mathbb{Z}^r$$

where $E_{\text{tor}}(K)$ is the torsion subgroup of $E(K)$ and r is the rank of $E(K)$. There are many interesting questions about the rank of an elliptic curve that are still open, but the focus of this thesis is on the torsion part of $E(K)$.

Since $E(K)$ can be viewed as a $\mathbb{Z}$-module, we know that the endomorphism group, $\text{End}(E)$, contains a subgroup isomorphic to $\mathbb{Z}$. The map that corresponds to multi-

plication by m is denoted $[m]$. Any elliptic curve whose endomorphism ring contains more than just a copy of $\mathbb{Z}$ is said to have complex multiplication.

Definition 1.1.1. Let E be an elliptic curve and $m \in \mathbb{Z}$, $m \neq 0$. The **m-torsion subgroup of** E, denoted $E[m]$, is the set of points of order m in E:

$$E[m] = \{P \in E(\overline{K}) : [m]P = O\},$$

where O is the identity element of $E(K)$.

For an elliptic curve, E, defined over a number field K, $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. One should note here that this is not saying that the m-torsion is fully defined over the base field K. When we say $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, we are considering the points of E that are defined over $\overline{K}$ and not just K. For example, there are many examples of elliptic curves defined over $\mathbb{Q}$ whose 2-torsion is not fully defined over $\mathbb{Q}$, but is defined over some number field (and hence $\overline{\mathbb{Q}}$).

For a fixed elliptic curve E over a number field K, there are two points in $E[m]$ defined over $\overline{K}$, P and Q, such that

$$E[m] = \{[a]P + [b]Q : a = 0, 1, 2, \ldots, m-1 \text{ and } b = 0, 1, 2, \ldots, m-1\}.$$

There is a natural action of $\mathrm{Gal}(\overline{K}/K)$ on $E(K)$ that maps $E[m]$ to $E[m]$. If $\sigma \in \mathrm{Gal}(\overline{K}/K)$, then we define $\sigma(P)$ to be the point given by letting σ act each component of P. Since σ is a field automorphism, we know that $\sigma([m]R) = [m]\sigma(R)$ for all R in $E(\overline{K})$ and σ can be thought of as an element of $\mathrm{Aut}(E[m])$. With a basis of $E[m]$ fixed as above we get an isomorphism from $E[m]$ to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, giving a map from $\mathrm{Gal}(\overline{K}/K)$ to $\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. This map depends on

the choice of basis and is *not* canonical.

Theorem 1.1.2. [Ser72] *If E is an elliptic curve over $\mathbb{Q}$ that does not have complex multiplication, then there exists a constant $C_E > 0$ such that for every prime $p > C_E$, the mod-p Galois representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ is surjective.*

Having answered this, Serre then asked the next natural question: can C_E be chosen independently of E?

Question 1.1.3 (Serre's Uniformity Problem)**.** *There exists a constant $C > 0$ such that $\rho_{E,p}$ is surjective for all $p > C$ and all E without complex multiplication.*

In [Ser72], Serre also shows that there are five possible cases for what the image of $\rho_{E,p}$ could be. There is an $\mathbb{F}_p$-basis of $E[p]$ such that one of the following happens:

1. $\rho_{E,p}$ is surjective;
2. The image of $\rho_{E,p}$ is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$;
3. The image of $\rho_{E,p}$ is contained in the normalizer of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$;
4. The image of $\rho_{E,p}$ is contained in the normalizer of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$;
5. The image of $\rho_{E,p}$ is contained in one of a finite list of "exceptional" subgroups.

Therefore if one were able to prove that cases 2-5 can only happen for "small" primes, then Serre's question would be answered positively. In case 3 (respectively 4) we say that E has split (respectively non-split) representation at p.

Case five was actually done by Serre himself. He showed the exceptional groups are not subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ for p greater than 13. Case two was proven by Mazur [Maz78] where he showed that if p is greater than 37, and E does not have CM, then the image of $\rho_{E,p}$ cannot be contained in a Borel subgroup. Case three was finished recently by Bilu and Parent [BP11] and uses results of Momose [Mom84].

This just leaves the case when the image of $\rho_{E,p}$ is contained in the normalizer of a non-split Cartain subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. In this case, the arguments used by Mazur [Maz78], and Bilu and Parent [BP11], fail and a different tactic must be taken.

In all of these cases the major objects of interest are the modular curves whose points correspond to elliptic curves, E, with a fixed basis for $E[p]$ whose corresponding representation falls into cases 2 through 5. To better understand these elliptic curves we will compute models for them.

1.2 My Results

1.2.1 Modular Units for $X(\Gamma)$

In Chapter 4, we use the work of Kubert and Lang in [KL81], to generate modular functions for $X(\Gamma) = \Gamma\backslash\mathcal{H}^*$ where $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ is any congruence subgroup of level $p \neq 2, 3$. To do this, we start by taking products of Siegel functions over a fixed set of lifts of $\overline{\Omega} = \Gamma/\Gamma^*(p)$, where

$$\Gamma^*(p) = \begin{cases} \{\pm I\} \cdot \Gamma(p) & \text{if } -I_2 \in \Gamma \\ \Gamma(p) & \text{if } -I_2 \notin \Gamma. \end{cases}$$

Throughout this section we will let Ω be a *fixed* set of lifts of $\overline{\Omega}$ to Γ. One might hope that precomposing these functions with elements in Γ only permutes the order of this product. The idea to use these products to generate modular units was first used in [CC04] in the case when $\Gamma = \Gamma_{ns}^{+}(11)$.

Definition 1.2.1. For $\mathbf{a} \in \left(\frac{1}{N}\mathbb{Z}\right)^2$ and $\mathbf{a} \notin \mathbb{Z}^2$, let $v_{\mathbf{a}}(\tau)$ be the scalar multiple of

$$\prod_{\gamma \in \Omega} g_{\mathbf{a}\gamma}(\tau)$$

whose q-expansion has leading coefficient is one.

The q-expansion of $v_{\mathbf{a}}(\tau)$ does not depend on the choice of Ω, so these functions are well defined. Once this is established, I am able prove my first main result:

Theorem 1.2.2 (Theorem 4.2.7, Corollary 4.2.14)**.** (D.) *Let* $\mathbf{a}, \mathbf{b} \in \left(\frac{1}{p}\mathbb{Z}/\mathbb{Z}\right)^2$*, with* $\mathbf{a}, \mathbf{b} \notin \mathbb{Z}^2$*. Let* $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ *be a congruence group of level* $p \neq 2, 3$*. The functions*

$$\frac{v_{\mathbf{a}}(\tau)}{v_{\mathbf{b}}(\tau)} \text{ and } \left(v_{\mathbf{a}}(\tau)\right)^{2c}$$

are modular for $X(\Gamma)$*, where* c *is the smallest positive integer such that* $\#\Omega \cdot c \equiv 0 \bmod 12$.

Remark 1.2.3. For a specific Γ, we expect that the exponent $2c$ should be able to be made smaller by analyzing the structure of the group $\overline{\Omega}$.

The potential usefulness of this result is that it works for *any* congruence subgroup of level p not equal to 2 or 3. The hope is that once a number of these functions are computed, the Riemann-Roch theorem can be used to find a relationship that gives an explicit equation for $X(\Gamma)$ and its j-map.

In particular, I am interested in the curves $X_s^+(p)$ and $X_{ns}^+(p)$, whose points correspond to elliptic curve with split or non-split representations at p. The congruence groups for these curves are $\Gamma_s^+(p)$ and $\Gamma_{ns}^+(p)$, and they are defined as the pull back of split (or non-split) Cartan subgroups of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ under the standard reduction map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$.

1.2.2 The case of $X_{ns}^+(11)$

In 2003 Chen and Cummins published a paper [CC04] where they computed $X_{ns}^+(11)$ using Siegel functions. They were able to show that $X_{ns}^+(11)$ is isomorphic to the elliptic curve $y^2 + y = x^3 - x^2 - 7x + 10$. This elliptic curve is known to have rank 1 and so after calculating the j-map from $X_{ns}^+(11)$ to the upper-half plane they were able to construct an infinite family of elliptic curves defined over $\mathbb{Q}$ with non-split representation at 11.

There are a few hurdles that one must overcome if there is any hope to generalize this method to other non-split modular curves. One issue is that the models for $X_{ns}^+(p)$ that one might get using Siegel functions end up being defined over $\mathbb{Q}(\zeta_p)^+$. This is not an issue in the case when $X_{ns}^+(p)$ has genus one. In this case one can compute the j-invariant and use this to find a model defined over $\mathbb{Q}$. But $p = 11$ is the only time that $X_{ns}^+(p)$ has genus 1. We work through these issues in Section 5.1.

1.2.3 The case of $X_s^+(11)$

In Chapter 6, we turn our attention to the curve $X_s^+(11)$. The $\mathbb{Q}$-rational points of this curve correspond to elliptic curves $E/\mathbb{Q}$ that have a basis for $E[11]$ such that the image of $\rho_{E,11}$ is contained in the normalizer of a split Cartan subgroup of

$\mathrm{GL}_2(\mathbb{Z}/11\mathbb{Z})$. The main result of this section:

Theorem 1.2.4 (Theorem 9.4.1, Corollary 9.4.2)**.** (D.) *Any elliptic curve defined over* $\mathbb{Q}$ *whose associated Galois representation at* 11 *has image contained in the normalizer of a split Cartan subgroup of* $\mathrm{GL}_2(\mathbb{Z}/11\mathbb{Z})$ *has complex multiplication.*

To prove this we use the modular units obtained from Theorem 1.2.2 and the Riemann-Roch theorem to compute a model for $X_s^+(11)$:

$$X_s^+(11) : y^2 = x^6 - 6x^5 + 11x^4 - 8x^3 + 11x^2 - 6x + 1.$$

We also use these units to compute the map from $X_s^+(11)$ to $\overline{\mathbb{Q}}$ that gives the j-invariant of the elliptic curve corresponding to each point on $X_s^+(11)$. This is done by finding an algebraic combination of the functions x and y that gives the well known q-expansion of the j-map to a certain accuracy and then use Riemann-Roch to show that it must actually be the same function.

After all of this information is obtained we turn to the task of computing *all* of the $\mathbb{Q}$-points on $X_s^+(11)$. The idea is once all of the points on $X_s^+(11)(\mathbb{Q})$ are found and the corresponding elliptic curves can be computed, we can determine if there are any elliptic curves that do not have complex multiplication and whose representation at 11 is contained in the normalizer of a split Cartan subgroup. A naive point search yields six $\mathbb{Q}$-rational points: $(0, \pm 1)$, $(1, \pm 2)$, and two points at infinity. It is a classical result that $X_s^+(11)$ has one rational cusp, and using SAGE one can check that there are 5 elliptic curves with complex multiplication that have split representation at 11. So the task now is to determine if these are all of the $\mathbb{Q}$-rational points on $X_s^+(11)$

To show that these are the only points on $X_s^+(11)(\mathbb{Q})$, we start by performing a 2-descent on the jacobian of $X_s^+(11)(\mathbb{Q})$, denoted by $J_s^+(11)(\mathbb{Q})$, using the method

was developed by Poonen and Schaefer, first published in [PS97] and then outlined explicitly for hyperelliptic curves in [Sto]. The method relies on transforming questions about cohomology groups into questions about square classes in local fields. This work can be found in Chapter 8.

The initial hope was that $J_s^+(11)(\mathbb{Q})$ would have rank zero. If the rank was zero then I would be able to use the fact that $X_s^+(11)(\mathbb{Q})$ injects into $J_s^+(11)(\mathbb{Q})$, then determining the points on $X_s^+(11)(\mathbb{Q})$ would simply amount to computing the torsion part of $J_s^+(11)(\mathbb{Q})$ and determining which points on $J_s^+(11)(\mathbb{Q})$ aries as the image of a point on $X_s^+(11)$. Unfortunately, it turns out that the rank of $J_s^+(11)(\mathbb{Q})$ is actually one. In fact, I was able to compute explicit generators and show

$$J_s^+(11)(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}.$$

Since the rank of $J_s^+(11)(\mathbb{Q})$ is not zero, one has to find another way to show that there are only 6 points on $X_s^+(11)$. Since the rank of the jacobian of $X_s^+(11)$ is less than the genus of $X_s^+(11)$, we are able to use the method of Chabauty and Coleman [Col85], [Cha41], [MP] to get an upper bound on the size of $X_s^+(11)(\mathbb{Q})$. The method of Chaubaty and Coleman relies on embedding $X_s^+(11)(\mathbb{Q})$ inside of $J_s^+(11)(\mathbb{Q}_p)$ for an appropriate p. Next, one has to find a function that is given by a power series with coefficients in $\mathbb{Q}_p$ that vanishes on the p-adic closure of $X_s^+(11)(\mathbb{Q})$. One can then bound the number of zeros that a p-adic power series has, thus giving a bound for the size of $X_s^+(11)(\mathbb{Q})$. This bound is not always sharp since sometimes the p-adic closure may be bigger. Details about this can be found in Chapter 9.

In this case the bound obtained by this method was eight, while we expect 6 $\mathbb{Q}$-points. I was able to use some of the added symmetries of $X_s^+(11)$ to show that

having one more $\mathbb{Q}$-rational point on this curve contradicted this bound. With this we knew that the there are only 6 points on $X_s^+(11)(\mathbb{Q})$ and plugging them into the j-map gives the following table:

P	$j(P)$
$(0,1)$	8000
$(0,-1)$	cusp
$(1,2)$	-3375
$(1,-2)$	16581375
∞_+	-884736
∞_-	-88473600

Thus, we have classified the $\bar{\mathbb{Q}}$-isomorphism classes of elliptic curves with split representation at 11. Comparing this to the table in [Sil94, Appendix A §3], we get that all of these curves have CM, thus giving us Theorem 1.2.4.

Chapter 2

Divisors and the Riemann Roch Theorem

2.1 Introduction

In this chapter, we will lay out the basic definitions that will be needed. The goals of this chapter are the statement of the Riemann-Roch theorem and the definition of an elliptic curve. This chapter follows the structure laid out in chapter 2 of [Sil09].

Throughout this chapter, when we say curve, we will always mean a 1-dimensional smooth projective variety. Here we will also assume that K is a perfect field.

2.2 Divisors

Definition 2.2.1. The divisor group of a curve C, denoted $\mathrm{Div}(C)$, is the free abelian group generated by points on $C(\bar{K})$. Therefore a divisor on a curve C can be written

as

$$D = \sum_{P \in C} n_P(P)$$

where $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many points $P \in C$. The degree of D is defined to be

$$\deg(D) = \sum_{P \in C} n_P.$$

The divisors of degree zero form a subgroup of $\mathrm{Div}(C)$ denoted $\mathrm{Div}^0(C)$.

If C is defined over a field K, then there is a natural action of $\mathrm{Gal}(\bar{K}/K)$ on $\mathrm{Div}(C)$ and $\mathrm{Div}^0(C)$. For $\sigma \in \mathrm{Gal}(\bar{K}/K)$ and $D = \sum n_P P \in \mathrm{Div}(C)$,

$$\sigma(D) = \sum n_P \cdot (\sigma(P)),$$

where σ acts on points of C by action on each coordinate.

Definition 2.2.2. A divisor, D, is defined over K if $\sigma(D) = D$ for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$.

Remark 2.2.3. If $D = n_{P_1}(P_1) + n_{P_2}(P_2) + \cdots + n_{P_n}(P_n)$ with $n_{P_i} \neq 0$, saying that D is defined over K does not necessarily mean that P_i is in $C(K)$ for all i.

For the rest of this chapter, we will let C be a smooth projective curve and let $\bar{K}(C)$ be the function field of C defined over $\bar{K}$. For any $f \in \bar{K}(C)^*$, we can associate a divisor to $\mathrm{div}(f)$, given by

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f)(P).$$

Definition 2.2.4. A divisor $D \in \mathrm{Div}(C)$ is *principal* if there is some $f \in \bar{K}(C)^*$ such that $D = \mathrm{div}(f)$. Two divisors, D_1 and D_2, are *linearly equivalent*, written $D_1 \sim D_2$

if there exists a function $f \in \bar{K}(C)^*$ such that $D_1 - D_2 = \mathrm{div}(f)$. The *divisor class group of* C, denoted $\mathrm{Pic}(C)$, is the quotient of $\mathrm{Div}(C)$ by the subgroup of principal divisors. Let $\mathrm{Pic}_K(C)$ be the subgroup of $\mathrm{Pic}(C)$ fixed by $\mathrm{Gal}(\bar{K}/K)$.

Proposition 2.2.5. [Sil09, Chapter 2, 3.1] *Let C be a smooth curve and let $f \in \bar{K}(C)^*$.*

1. $\mathrm{div}(f) = 0$ *if and only if* $f \in \bar{K}^*$.
2. $\deg(\mathrm{div}(f)) = 0$.

2.3 Differentials

Definition 2.3.1. Let C be a smooth curve. The space of meromorphic differentials on C, denoted Ω_C, is the $\bar{K}$-vector space generated by symbols of the form dx with $x \in \bar{K}(C)$, subject to the following relations:

1. $d(x+y) = dx + dy$ for all $x, y \in \bar{K}(C)$.
2. $d(xy) = xdy + ydx$ for all $x, y \in \bar{K}(C)$.
3. $da = 0$ for all $a \in \bar{K}$.

Proposition 2.3.2. [Sil09, Chapter 2, 4.2] *Let C be a curve.*

1. *Ω_C is a one dimensional $\bar{K}(C)$-vector space.*
2. *Let $x \in \bar{K}(C)$. Then dx generates Ω_C over $\bar{K}(C)$ if and only if $\bar{K}(C)/\bar{K}(x)$ is a finite separable extension.*

Proposition 2.3.3. [Sil09, Chapter 2, 4.3] *Let C be a curve, let $P \in C$, and let $t_P \in \bar{K}(C)$ be a uniformizer at P.*

1. *For every $\omega \in \Omega_C$ there exists a unique function $g \in \bar{K}(C)$, depending on ω and t_P, satisfying*

$$\omega = g\, dt_P.$$

   We denote g by ω/dt_P.

2. *Let $\omega \in \Omega_C$ with $\omega \neq 0$. The quantity $\mathrm{ord}_P(\omega/dt_P)$ depends only on ω and P. That is to say, it is independent of the choice of uniformizer t_P. We denote this quantity simply by $\mathrm{ord}_P(\omega)$.*

3. *Let $\omega \in \Omega_C$ with $\omega \neq 0$. Then $\mathrm{ord}_P(\omega) = 0$ for all but finitely many $P \in C$.*

Definition 2.3.4. Let $\omega \in \Omega_C$. The divisor associated to ω is

$$\mathrm{div}(\omega) = \sum_{P \in C} \mathrm{ord}_P(\omega)(P)$$

Remark 2.3.5. Because Ω_C is a 1-dimensional $\bar{K}(C)$-vector space for any two differentials, $\omega_1, \omega_2 \in \Omega_C$, $\mathrm{div}(\omega_1) = \mathrm{div}(\omega_2)$ in $\mathrm{Pic}(C)$.

Definition 2.3.6. The *canonical divisor class* on C, denoted K_C, is the image in $\mathrm{Pic}(C)$ of $\mathrm{div}(\omega)$ for any nonzero differential $\omega \in \Omega_C$. Any divisor in this divisor class is called a canonical divisor.

2.4 Riemann-Roch Theorem

Definition 2.4.1. A divisor $D = \sum n_P(P)$ is *positive* (or *effective*), denoted $D \geq 0$, if $n_P \geq 0$ for every $P \in C$. For two divisors, D_1, $D_2 \in \mathrm{Div}(C)$, we write $D_1 \geq D_2$ to indicate that $D_1 - D_2$ is positive.

Definition 2.4.2. Let $D \in \mathrm{Div}(C)$. Let $\mathscr{L}(D)$ denote the set of functions whose divisors plus D are positive, along with the zero function. That is to say,

$$\mathscr{L}(D) = \{f \in \bar{K}(C)^* : \mathrm{div}(f) \geq -D\} \cup \{0\}.$$

Clearly, $\mathscr{L}(D)$ is a $\bar{K}$ vector space, so we let $\ell(D) = \dim_{\bar{K}} \mathscr{L}(D)$.

Proposition 2.4.3. [Sil09, Chapter 2, 5.2] *Let $D \in \mathrm{Div}(C)$.*

1. *If $\deg(D) < 0$, then $\mathscr{L}(D) = \{0\}$ and $\ell(D) = 0$.*
2. *$\mathscr{L}(D)$ is a finite-dimensional $\bar{K}$-vector space.*
3. *If $D' \in \mathrm{Div}(C)$ is linearly equivalent to D, then $\mathscr{L}(D) \cong \mathscr{L}(D')$ and thus $\ell(D) = \ell(D')$.*

Theorem 2.4.4 (Riemann-Roch)**.** *Let C be a smooth projective curve. There exists an integer $g \geq 0$ such that for all divisors $D \in \mathrm{Div}(C)$,*

$$\ell(D) - \ell(K_C - D) = \deg(D) - g + 1.$$

The integer g is called the genus of C.

Corollary 2.4.5. [Sil09, Chapter 2,5.5] *Let C be a smooth projective curve of genus g, and let $D \in \mathrm{Div}(C)$.*

1. $\ell(K_C) = g$,

2. $\deg(K_C) = 2g - 2$

3. *If* $\deg(D) \geq 2g - 1$, *then* $\ell(D) = \deg(D) - g + 1$.

Chapter 3

The Modular Curve $X_{ns}^{+}(n)$

3.1 Normalizers of Non-Split Cartan Subgroups

For this section, we fix a positive integer n. Let A be a finite free commutative $\mathbb{Z}/n\mathbb{Z}$-algebra of rank two with unit discriminant. Let p be a prime divisor of n. By Galois theory, the $\mathbb{F}_p$-algebra A/pA is either equal to $\mathbb{F}_p \times \mathbb{F}_p$ or $\mathbb{F}_{p^2}$. In the first case A is said to be *split* at p and in the second A is said to be *non-split.*

Fixing a $\mathbb{Z}/n\mathbb{Z}$-basis for A, we can use the action of $A^\times$ on A to get an embedding $A^\times \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.

Definition 3.1.1. A *Cartan subgroup* of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ is a subgroup that arises as the image of such a group $A^\times$ as above. If A is non-split (respectively split) at every prime dividing n then the subgroup is called a *non-split* (respectively *split*)Cartan subgroup.

Now we construct a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Suppose $n = \prod p^{e_p}$,

let $\mathcal{O}$ be a quadratic order with discriminant prime to n and suppose that every prime factor of n is inert in $\mathcal{O}$. We know that infinitely many such orders exist by Dirichlet's theorem on primes in arithmetic progressions. The algebra $\mathcal{O}/n\mathcal{O}$ is a finite commutative $\mathbb{Z}/n\mathbb{Z}$-algebra with unit discriminant. We know that $\mathcal{O}$ has a $\mathbb{Z}$-basis of the form $\{1, \alpha\}$ where α has minimal polynomial $p(x) = x^2 + bx + c \in \mathbb{Z}[x]$. Then $A = \mathcal{O}/n\mathcal{O}$ has $\{1, \alpha\}$ as a $\mathbb{Z}/n\mathbb{Z}$-basis. The group $A^\times = (\mathcal{O}/n\mathcal{O})^\times$ embeds into $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ and the image is a non-split Cartan subgroup. We will denote the image of $A^\times$ in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ as $C_{ns}(n)$. All other non-split Cartan subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ are conjugate to $C_{ns}(n)$.

For every prime p that divides n, there exists a unique ring automorphism σ_p of $\mathcal{O}/n\mathcal{O}$ such that

$$\sigma_p(\alpha) \equiv u - \alpha \bmod p^{e_p} \text{for some } u \in (\mathcal{O}/n\mathcal{O})^\times, \text{ and}$$
$$\sigma_p \equiv \text{identity map mod } \frac{n}{p^{e_p}}.$$

Using the $\mathbb{Z}/n\mathbb{Z}$-basis $\{1, \alpha\}$, we represent σ_p by $S_p \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. The ring automorphisms σ_p have order two and they commute with each other, and so do the matrices S_p.

Proposition 3.1.2. [Bar10, Proposition 2.3] *The normalizer of $C_{ns}(n)$ in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ is equal to*

$$C_{ns}^+(n) = \langle C_{ns}(n), S_p \text{ for } p|n \rangle.$$

3.2 Classical Modular Curves

We start by letting $\mathscr{H}^* = \mathscr{H} \cup \mathbb{P}^1(\mathbb{Q})$ where $\mathscr{H}$ is the upper half-plane, and we add the rational points on the real axis and a point at infinity at the top of the imaginary axis. We will sometimes denote the point at infinity by $i\infty$. These extra points are added to $\mathscr{H}$ for topological reasons that we will see later on.

In $\mathscr{H}^*$ a basis for the open sets containing $r \in \mathbb{Q}$ are the circles tangent to the real axis at r together with the point r, while a basis for the open sets containing the points at infinity are of the form $U_C = \{x + iy : y > C\} \cup \{i\infty\}$ for some $C \in \mathbb{R}^+$.

There is an action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathscr{H}^*$ given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d}$$

for $\tau \in \mathscr{H}^*$. We define

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} i\infty = \frac{a}{c},$$

and we write $\gamma r = i\infty$ if $c\tau + d = 0$. The fact that $\det \gamma = 1$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ is enough to ensure that $\mathrm{Im}(\gamma\tau) > 0$.

Definition 3.2.1. Let $N \in \mathbb{Z}^+$, then let

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

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : c \equiv 0 \bmod N \text{ and } a \equiv d \equiv 1 \bmod N \right\},$$

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : c \equiv b \equiv 0 \bmod N \text{ and } a \equiv d \equiv 1 \bmod N \right\}.$$

Definition 3.2.2. A subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is a *congruence subgroup* if $\Gamma(N) \subset \Gamma$ for some $N \in \mathbb{Z}^+$. When N is the smallest such positive integer, we say that Γ is a congruence subgroup of *level* N.

Proposition 3.2.3. [DS05, p.13] *For any positive integer N, the index of $\Gamma(N)$ inside of $\mathrm{SL}_2(\mathbb{Z})$ is finite. In particular,*

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)] = N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right).$$

Any congruence subgroup can be thought of as acting on $\mathscr{H}^*$ and we can mod out by that action. To do this, for a congruence subgroup Γ, we say that τ and τ' are equivalent if and only if there exists $\gamma \in \Gamma$ such that $\gamma\tau = \tau'$ for $\tau, \tau' \in \mathscr{H}^*$. What is left after we take a quotient by a congruence subgroup is a Riemann surface.

Definition 3.2.4. For $N \in \mathbb{Z}^+$,

$$X_0(N) = \Gamma_0(N)\backslash\mathscr{H}^*,$$
$$X_1(N) = \Gamma_1(N)\backslash\mathscr{H}^*,$$
$$X(N) = \Gamma(N)\backslash\mathscr{H}^*.$$

Further, for any congruence subgroup Γ, we let $X(\Gamma) = \Gamma\backslash\mathscr{H}^*$.

Notice that the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathscr{H}^*$ sends points in $\mathbb{P}^1(\mathbb{Q})$ back to points in $\mathbb{P}^1(\mathbb{Q})$. That is to say that if $\tau \in \mathscr{H}^*$ and $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, then $\gamma\tau \in \mathbb{P}^1(\mathbb{Q})$ if and only if $\tau \in \mathbb{P}^1(\mathbb{Q})$.

Definition 3.2.5. For a congruence subgroup Γ, the equivalence classes of $\Gamma\backslash\mathbb{P}^1(\mathbb{Q})$ inside of $\Gamma\backslash\mathscr{H}^*$ are called the *cusps* of $X(\Gamma)$.

Lemma 3.2.6. [DS05, Lemma 2.4.1] For any congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$, the curve $X(\Gamma)$ has finitely many cusps.

Proposition 3.2.7. [DS05, Proposition 2.4.2] *For any congruence subgroup* Γ *the curve* $X(\Gamma)$ *is Hausdorff, connected, and compact where* $X(\Gamma)$ *is given the quotient topology.*

3.3 Non-Split Modular Curves

Definition 3.3.1. For $N \in \mathbb{Z}^+$, let $\Gamma_{ns}^+(N)$ be the subset of $\mathrm{SL}_2(\mathbb{Z})$ made of matrices such that when you reduce each entry mod N, the resulting matrix is contained in $C_{ns}^+(N) \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Here we let $\overline{\Gamma_{ns}^+(N)} = C_{ns}^+(N) \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

Clearly, $\Gamma_{ns}^{+}(N)$ contains $\Gamma(N)$ since the identity matrix is in $C_{ns}^{+}(N) \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. With this in mind we define a new modular curve.

Definition 3.3.2. For $N \in \mathbb{Z}^{+}$, let $X_{ns}^{+}(N) = X(\Gamma_{ns}^{+}(N)) = \Gamma_{ns}^{+}(N) \backslash \mathscr{H}^{*}$.

For this thesis we will primarily be interested in the case when N is an odd prime greater than 3.

Proposition 3.3.3. [Bar10, 7.10] *For p an odd prime and $r \in \mathbb{Z}^{+}$, the curve $X_{ns}^{+}(p^r)$ has $\frac{\varphi(p^r)}{2}$ cusps.*

In [Ser89, Appendix 5], Serre shows that the cusps of $X_{ns}^{+}(p)$ are all conjugate over the maximal real subfield of $\mathbb{Q}(\zeta_p)$, where ζ_p is a primitive pth root of unity. Thus, except in the case when the curve has only one cusp, none of the cusps are rational. Next, we give a formula for the genus of the curve $X_{ns}^{+}(p^r)$.

Theorem 3.3.4. [Bar10, Theorem 7.2] *For p an odd prime and $r \in \mathbb{Z}^{+}$, the genus of the curve $X_{ns}^{+}(p^r)$ is given by*

$$g = 1 + \frac{(p^r - 6)\varphi(p^r)}{24} - \frac{\beta_3(p^r)}{3} - \frac{p^r}{8} \cdot B(p^r),$$

where

$$\beta_3(p^r) = \begin{cases} 1 & \text{if } p \equiv 2 \bmod 3, \\ 0 & \text{otherwise,} \end{cases}$$

and

$$B(p^r) = \begin{cases} 1 - \frac{1}{p} & \text{if } p \equiv 1 \bmod 4, \\ 1 + \frac{1}{p} + \frac{2}{p^r} & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

One of the reasons that these curves are of interest is that the non-cuspidal rational points on $X_{ns}^{+}(p)$, correspond to elliptic curves over $\mathbb{Q}$ whose Galois representation $\rho_p : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ has its image contained in $C_{ns}^{+}(p)$. Thus, if one wishes to understand all such elliptic curves, one needs to understand all of the rational points on $X_{ns}^{+}(p)$ but, to do this one would first wi will try to find explicit formulas for this curve. At this point in time there are very few non-split modular curves whose equations are known. In an attempt to find more models, we will first try and compute some functions on these curves.

Chapter 4

Klein Forms, Siegel Functions, and Modular Units

4.1 Klein Forms and Siegel Functions

In this section we follow the notation and terminology laid out in section 1 and 2 of chapter two of [KL81]. In these sections, the authors give explicit methods for computing units in the function field of the modular curve $X(N)$. These functions are units because they only have poles and zeros at the cusps, and so when we consider the functions only on the non-cuspidal points, they are invertible. Before diving in, we need to recall the definition of what it means to be modular for a given congruence subgroup.

Definition 4.1.1. A modular function for a congruence subgroup Γ is a meromorphic function on the compact Riemann surface $\Gamma\backslash\mathscr{H}^*$.

Often, modular functions are considered as meromorphic functions on $\mathscr{H}^*$ that

are invariant under the action of Γ. From this perspective a modular function for Γ is a function that satisfies the following conditions:

1. $f(\tau)$ is invariant under the Γ. That is, $f(\gamma\tau) = f(\tau)$ for all $\gamma \in \Gamma$;

2. $f(\tau)$ is meromorphic in $\mathscr{H}$;

3. $f(\tau)$ is meromorphic at the cusps.

Let L be a lattice in the complex plane and let $\mathfrak{f}(z, L)$ be the Klein form attached to L. This is a function which takes a complex variable z and a lattice L as its arguments. These functions are homogeneous of degree 1; that is to say that $\mathfrak{f}(\lambda z, \lambda L) = \lambda \mathfrak{f}(z, L)$ for $\lambda \in \mathbb{C}$.

Let $W = \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \in \mathbb{C}^2$ such that $\frac{\omega_1}{\omega_2} \notin \mathbb{R}$. Take $L = L(W) = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, and let $z = z(\mathbf{a}, w) = a_1\omega_1 + a_2\omega_2$ with $\mathbf{a} = (a_1, a_2) \in \mathbb{R}^2$. Now, we can create a new function that takes as its arguments a vector $\mathbf{a} \in \mathbb{R}^2$ instead of $z \in \mathbb{C}$ and a vector $W \in \mathbb{C}^2$ whose entries are linearly independent over $\mathbb{R}$ by $\mathfrak{f}_{\mathbf{a}}(W) = \mathfrak{f}(z, L)$. In [KL81, Chapter 2], the authors show that these function have the following properties:

K0. $\mathfrak{f}_{\mathbf{a}}(\lambda W) = \lambda \mathfrak{f}_{\mathbf{a}}(W)$.

K1. For $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, $\mathfrak{f}_{\mathbf{a}}(\alpha W) = \mathfrak{f}_{\mathbf{a}\alpha}(W)$.

K2. If $\mathbf{b} = (b_1, b_2) \in \mathbb{Z}^2$, then $f_{\mathbf{a}+\mathbf{b}}(W) = \varepsilon(\mathbf{a}, \mathbf{b})\mathfrak{f}_{\mathbf{a}}(W)$, where

$$\varepsilon(\mathbf{a}, \mathbf{b}) = (-1)^{b_1 b_2 + b_1 + b_2} e^{-\pi i(b_1 a_2 - b_2 a_1)}.$$

K3. If $\alpha \in \Gamma(N)$, and $\mathbf{a} = (a_1, a_2) \in \mathbb{Q}^2$ such that the denominators of a_1 and a_2

divide N, then

$$\mathfrak{f}_{\mathbf{a}}(\alpha W) = \mathfrak{f}_{\mathbf{a}\alpha}(W) = \varepsilon(\alpha)\mathfrak{f}_{\mathbf{a}}(W)$$

where $\varepsilon(\alpha)$ is a $2N$th root of unity. If we let $\mathbf{a} = \left(\frac{r}{N}, \frac{2}{N}\right)$, $\varepsilon(\alpha)$ is given by

$$\varepsilon(\alpha) = \varepsilon_{\mathbf{a}}(\alpha) = -(-1)^{\left(\frac{a-1}{N}r + \frac{c}{N}s + 1\right)\left(\frac{b}{N}r + \frac{d-1}{N}s + 1\right)} e^{2\pi i(br^2 + (b-1)rs - cs^2)2N^2}.$$

Definition 4.1.2. For $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ and $\tau \in \mathscr{H}$, let $j(\alpha, \tau)$ be the factor of automorphy given by

$$j(\alpha, \tau) = c\tau + d.$$

The Klein functions may be considered as functions on the upper half plane, as follows: let $\tau \in \mathscr{H}$ and define $\mathfrak{f}_{\mathbf{a}}(\tau) = \mathfrak{f}_{\mathbf{a}}(W_\tau)$, where $W_\tau = \begin{pmatrix} \tau \\ 1 \end{pmatrix}$.

Proposition 4.1.3. *For* $\alpha \in \mathrm{SL}_2(\mathbb{Z})$

$$\mathfrak{f}_{\mathbf{a}\alpha}(\tau) = j(\alpha, \tau)\mathfrak{f}_{\mathbf{a}}(\alpha\tau).$$

PROOF: Using properties **K0** and **K1** we see that for

$$\begin{aligned}
\mathfrak{f}_{\mathbf{a}\alpha}(\tau) = \mathfrak{f}_{\mathbf{a}\alpha}(W_\tau) &= \mathfrak{f}_{\mathbf{a}}(\alpha W_\tau) \\
&= \mathfrak{f}_{\mathbf{a}}\left(\begin{pmatrix} a\tau+b \\ c\tau+d \end{pmatrix}\right) \\
&= \mathfrak{f}_{\mathbf{a}}\left((c\tau+d)\begin{pmatrix} \frac{a\tau+b}{c\tau+d} \\ 1 \end{pmatrix}\right) \\
&= j(\alpha,\tau)\mathfrak{f}_{\mathbf{a}}(\alpha\tau).
\end{aligned}$$

■

Definition 4.1.4. The *Siegel function associated to* $\mathbf{a} \in \mathbb{R}^2$, $g_{\mathbf{a}}(\tau)$, is a function on $\mathscr{H}$ defined by

$$g_{\mathbf{a}}(\tau) = \mathfrak{f}_{\mathbf{a}}(\tau)\eta(\tau)^2,$$

where $\eta(\tau)^2 = q^{\frac{1}{12}}\prod_{n=1}^{\infty}(1-q^n)^2$ is the Dedekind eta function and $q = e^{2\pi i\tau}$.

Notice that property **K2** says that if we are normalizing our functions to have leading coefficient 1, then $\mathbf{a} \in \mathbb{R}^2$ only matters modulo $\mathbb{Z}$. That is, we can actually take $\mathbf{a} \in (\mathbb{R}/\mathbb{Z})^2$. In fact, for the rest of the paper we are going to restrict ourselves, for the sake of simplicity, to considering functions where $\mathbf{a} \in (\mathbb{Q}/\mathbb{Z})^2$.

Before we continue, let us recall a theorem about the Dedekind eta function.

Proposition 4.1.5. [Apo90, page 51] *If* $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, *then*

$$\eta(\alpha\tau) = \xi(\alpha)\cdot\sqrt{j(\alpha,\tau)}\eta(\tau),$$

where $\xi(\alpha)$ *is a* 24*th root of unity.*

Remark 4.1.6. The observant reader might ask about how the square root above is chosen and does the choice depend on τ? We will ignore this question for now and see in the proof of 4.1.8 that this ambiguity can be ignored.

For our purposes, we will only be interested in $\mathbf{a} = (a_1, a_2) \in (\mathbb{Q}/\mathbb{Z})^2$ and we let $z = a_1\tau + a_2$ and $q_z = e^{2\pi i z}$.

Theorem 4.1.7. [KL81, p. 29] *For each* $\mathbf{a} \in (\mathbb{Q}/\mathbb{Z})^2$*, the Siegel function* $g_{\mathbf{a}}(\tau)$ *can be given by the following q-expansion:*

$$g_{\mathbf{a}}(\tau) = -q_\tau^{(1/2)\mathbf{B}_2(a_1)} e^{2\pi i a_2(a_1-1)/2}(1-q_z)\prod_{n=1}^{\infty}(1-q_\tau^n q_z)(1-q_\tau^n/q_z)$$

where $\mathbf{B}_2(x) = x^2 - x + \frac{1}{6}$ *is the second Bernoulli polynomial.*

Theorem 4.1.8. *If* $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ *as above and* $a \in (\mathbb{Q}/\mathbb{Z})^2$*, then*

$$g_{\mathbf{a}}(\alpha\tau) = \zeta(\alpha)\cdot g_{\mathbf{a}\alpha}(\tau)$$

where $\zeta(\alpha)$ *is a* 12*th root of unity that depends only on* α*.*

Proof:

$$\begin{aligned} g_{\mathbf{a}}(\alpha\tau) &= \mathfrak{f}_{\mathbf{a}}(\alpha\tau)(\eta(\alpha\tau))^2 \\ &= j(\alpha,\tau)^{-1}\mathfrak{f}_{\mathbf{a}\alpha}(\tau)\left(\xi(\alpha)\cdot\sqrt{j(\alpha,\tau)}\eta(\tau)\right)^2 \text{ from Propositions 4.1.3 and 4.1.5} \\ &= \xi(\alpha)^2\mathfrak{f}_{\mathbf{a}\alpha}(\tau)\eta(\tau)^2 = \zeta(\alpha)g_{\mathbf{a}\alpha}(\tau). \end{aligned}$$

Here $\zeta(\alpha) = \xi(\alpha)^2$ and since $\xi(\alpha)$ is a 24th root of unity, $\zeta(\alpha)$ is a 12th root of unity and since $\sqrt{j(\alpha,\tau)}$ appears inside the square, which square root we choose doesn't matter. ∎

In [KL81], Kubert and Lang develop sufficient conditions for products of the $g_{\mathbf{a}}$'s to be modular of level N. These conditions are more difficult to state if N is not prime to 6, and also not of interest to us, so we will only state conditions for $(N, 6) = 1$.

Theorem 4.1.9. [KL81, 3.5.2] *Let $N \in \mathbb{N}$ such that $(N, 6) = 1$. Let A be the set of all $\mathbf{a} = \left(\frac{r_1}{N}, \frac{r_2}{N}\right) \in \left(\frac{1}{N}\mathbb{Z}\right)^2$ and $\mathbf{a} \notin \mathbb{Z}^2$. Let*

$$g(\tau) = \prod_{\mathbf{a} \in A} g_{\mathbf{a}}^{m(\mathbf{a})}(\tau).$$

Then g is modular of level N if and only if the family $\{m(\mathbf{a})\}$ satisfies the following:

(1) $\sum_{\mathbf{a} \in A} m(\mathbf{a}) r_1^2 \equiv \sum_{\mathbf{a} \in A} m(\mathbf{a}) r_2^2 \equiv \sum_{\mathbf{a} \in A} m(\mathbf{a}) r_1 r_2 \equiv 0 \bmod N$, *and*

(2) $\sum_{\mathbf{a} \in A} m(\mathbf{a}) \equiv 0 \bmod 12$.

In general, we will always assume that an element $\mathbf{a} = (a_1, a_2) \in (\mathbb{Q}/\mathbb{Z})^2$ is normalized so that $0 \leq a_1 < 1$ and $0 \leq a_2 < 1$. If we wish to remove this assumption then we will always use the notation $\langle a_1 \rangle$ and $\langle a_2 \rangle$ to mean the fractional part of a_1 and a_2.

Lemma 4.1.10. [KL81, p. 31] For $\mathbf{a} = (a_1, a_2) \in (\mathbb{Q}/\mathbb{Z})^2$ we have

$$\operatorname{ord}_{q_\tau} g_{\mathbf{a}}(\tau) = \operatorname{ord}_{i\infty} g_{\mathbf{a}}(\tau) = \frac{1}{2}\mathbb{B}_2\Big(\langle a_1 \rangle\Big).$$

With this lemma we will be able to compute the divisor of any Siegel function we want. This will be important in section 5.1 when we use Riemann-Roch to compute models of curves.

4.2 Modular Units for Congruence subgroups of Level p

In this section we generalize the methods used in [CC04] to find a class of explicitly computable modular units for an arbitrary congruence subgroup of prime level $p \neq 2, 3$. For the rest of this section let Γ be a congruence subgroup of level $p \neq 2, 3$.

Definition 4.2.1. Let

$$\Gamma^*(p) = \begin{cases} \Gamma(p) & \text{if } -I_2 \notin \Gamma, \\ \langle \Gamma(p), -I_2 \rangle & \text{if } -I_2 \in \Gamma. \end{cases}$$

Also, let $\overline{\Omega} = \Gamma/\Gamma^*(p)$, and let Ω be a **fixed** set of representatives of $\overline{\Omega}$ in Γ.

Remark 4.2.2. Notice that Ω and $\overline{\Omega}$ are finite since Γ is a congruence subgroup of level p.

Now that we have defined these basic objects, we can define the basic functions that we are going to be interested in:

Definition 4.2.3. For $\mathbf{a}, \mathbf{b} \in \left(\frac{1}{p}\mathbb{Z}/\mathbb{Z}\right)^2$ with $\mathbf{a}, \mathbf{b} \notin \mathbb{Z}^2$ let

$$v_{\mathbf{a}}(\Gamma, \tau) = v_{\mathbf{a}}(\tau) = \Theta_{\mathbf{a}}(\Omega) \prod_{\gamma \in \Omega} g_{\mathbf{a}\gamma}(\tau)$$

where $\Theta_{\mathbf{a}}(\Omega) \in \mathbb{C}^\times$ is defined so that the leading term of the q-expansion of $v_{\mathbf{a}}(\tau)$ is 1. Also, let

$$w_{\mathbf{a},\mathbf{b}}(\Gamma, \tau) = w_{\mathbf{a},\mathbf{b}}(\tau) = \frac{v_{\mathbf{a}}(\tau)}{v_{\mathbf{b}}(\tau)},$$

and

$$u_{\mathbf{a}}(\Gamma,\tau) = u_{\mathbf{a}}(\tau) = v_{\mathbf{a}}(\Gamma,\tau)^c = \Theta_{\mathbf{a}}(\Omega)^c \prod_{\gamma\in\Omega} g_{\mathbf{a}\gamma}(\tau)^c$$

where c is the smallest positive integer such that $c \cdot \#\Omega \equiv 0 \bmod 12$. In each case, when the congruence subgroup is obvious, we will use the notation that omits Γ.

Lemma 4.2.4. For $\delta \in \Gamma^*(p)$, $\mathbf{a} \in \left(\frac{1}{p}\mathbb{Z}/\mathbb{Z}\right)^2$, $\mathbf{a} \notin \mathbb{Z}^2$, we have $g_{\mathbf{a}\delta}(\tau) = \varepsilon(\delta) g_{\mathbf{a}}(\tau)$, where $\varepsilon(\delta)$ is the $2p$-th root of unity in **K3**.

Proof: Suppose $\delta \in \Gamma(p)$ and $\mathbf{a}$ is as above, then

$$g_{\mathbf{a}\delta}(\tau) = \mathfrak{f}_{\mathbf{a}\delta}(\tau)(\eta(\tau))^2 \overset{\mathbf{K3}}{=} \varepsilon(\delta)\mathfrak{f}_{\mathbf{a}}(\tau)(\eta(\tau))^2 = \varepsilon(\delta) g_{\mathbf{a}}(\tau).$$

Now, recall that

$$-I_2\tau = \frac{-1\cdot\tau + 0}{0\tau - 1} = \frac{-\tau}{-1} = \tau,$$

and

$$j(-I_1,\tau) = 0\tau - 1 = -1.$$

This means

$$g_{\mathbf{a}\cdot(-I_2)}(\tau) = j(-I_2,\tau) g_{\mathbf{a}}(-I_2\cdot\tau) = -g_{\mathbf{a}}(\tau).$$

Thus, for any element of the form $-\delta$ with $\delta \in \Gamma(P)$,

$$g_{\mathbf{a}(-\delta)}(\tau) = g_{\mathbf{a}(-I_2\cdot\delta)}(\tau) = g_{(\mathbf{a}(-I_2))\cdot\delta}(\tau) = \varepsilon(\delta) g_{\mathbf{a}(-I_2)}(\tau) = -\varepsilon(\delta) g_{\mathbf{a}}(\tau),$$

and since $\varepsilon(\delta)$ is a $2p$-th root of unity, so is $-\varepsilon(\delta)$ and the result follows. ∎

Proposition 4.2.5. *Let $\Omega = \{\gamma_i\}_{i=1}^{\#\Omega}$ and $\Omega' = \{\gamma_i'\}_{i=1}^{\#\Omega}$ be two different choices of lifts*

for $\overline{\Omega}$ ordered so that there exists a $\delta_i \in \Gamma^*(p)$ such that $\gamma_i = \gamma_i'\delta_i$. Then

$$\prod_{i=1}^{\#\Omega} g_{\mathbf{a}\gamma_i}(\tau) = \kappa \cdot \prod_{i=1}^{\#\Omega} g_{\mathbf{a}\gamma_i'}(\tau)$$

where $\kappa = \prod_{i=1}^{\#\Omega} \varepsilon(\delta_i)$. Further,

$$\Theta_{\mathbf{a}}(\Omega') = \Theta_{\mathbf{a}}(\Omega) \cdot \kappa.$$

PROOF: Suppose that Ω and Ω' are as above. For any $\mathbf{a} \in \left(\frac{1}{p}\mathbb{Z}/\mathbb{Z}\right)^2$ such that $\mathbf{a} \notin \mathbb{Z}^2$, we have

$$\begin{aligned}
\prod_{i=1}^{\#\Omega} g_{\mathbf{a}\gamma_i}(\tau) &= \prod_{i=1}^{\#\Omega} g_{\mathbf{a}\gamma_i'\delta_i}(\tau) \\
&= \prod_{i=1}^{\#\Omega} \varepsilon(\delta_i) g_{\mathbf{a}\gamma_i'}(\tau) \\
&= \prod_{i=1}^{\#\Omega} \varepsilon(\delta_i) \cdot \prod_{i=1}^{\#\Omega} g_{\mathbf{a}\gamma_i'}(\tau) \\
&= \kappa \cdot \prod_{i=1}^{\#\Omega} g_{\mathbf{a}\gamma_i'}(\tau).
\end{aligned}$$

Therefore, we get that, if we choose a different set of lifts, we simply change our normalization constant by κ, more specifically, $\Theta_{\mathbf{a}}(\Omega') = \Theta_{\mathbf{a}}(\Omega) \cdot \kappa$. ∎

Corollary 4.2.6. *The q-expansion $v_{\mathbf{a}}$ is independent of choice of the representatives of Ω and thus so are the q-expansions of $u_{\mathbf{a}}(\tau)$ and $w_{\mathbf{a},\mathbf{b}}(\tau)$.*

PROOF: Follows immediately from Proposition 4.2.5

∎

Theorem 4.2.7. *Let* $\mathbf{a}, \mathbf{b} \in \left(\frac{1}{p}\mathbb{Z}/\mathbb{Z}\right)^2$, *with* $\mathbf{a}, \mathbf{b} \notin \mathbb{Z}^2$, *then for any* $\alpha \in \Gamma$,

$$w_{\mathbf{a},\mathbf{b}}(\alpha\tau) = w_{\mathbf{a},\mathbf{b}}(\tau).$$

PROOF: Recall that $\overline{\Omega} = \Gamma/\Gamma^*(p)$ and that Ω is a *fixed* set of lifts of $\overline{\Omega}$ to Γ. Fix $\alpha \in \Gamma$, $\overline{\alpha}$ its reduction to $\overline{\Omega}$. Let σ be the permutation of $\overline{\Omega}$ given by $\sigma(\overline{\beta}) = \overline{\beta} \cdot \overline{\alpha}$. For any $\gamma \in \Gamma$, we can write $\gamma\alpha = \gamma^\sigma \cdot \delta(\gamma, \alpha)$ where γ^σ is the unique lift of $\sigma(\overline{\gamma})$ into Ω and $\delta(\gamma, \alpha) \in \Gamma^*(p)$. By abuse of notation, we can let σ be a permutation of Ω by $\gamma \mapsto \gamma^\sigma$. Therefore,

$$g_{\mathbf{a}\gamma\alpha}(\tau) = g_{\mathbf{a}\gamma^\sigma\delta(\gamma,\alpha)}(\tau) = \varepsilon(\gamma, \alpha) g_{\mathbf{a}\gamma^\sigma}(\tau),$$

where $\varepsilon(\gamma, \alpha)$ is the $2p$-th root of unity from Lemma 4.2.4 that depends on $\delta(\gamma, \alpha)$. Let $\varepsilon_1(\alpha) = \prod_{\gamma \in \Omega} \varepsilon(\gamma, \alpha)$. Then

$$\begin{aligned} v_{\mathbf{a}}(\alpha\tau) &= \Theta_{\mathbf{a}}(\Omega) \prod_{\gamma \in \Omega} g_{\mathbf{a}\gamma}(\alpha\tau) = \Theta_{\mathbf{a}}(\Omega) \prod_{\gamma \in \Omega} \zeta(\alpha) \cdot g_{\mathbf{a}\gamma\alpha}(\tau) \\ &= \Theta_{\mathbf{a}}(\Omega) \cdot \zeta(\alpha)^{\#\Omega} \prod_{\gamma \in \Omega} \varepsilon(\gamma, \alpha) g_{\mathbf{a}\gamma^\sigma}(\tau) \\ &= \Theta_{\mathbf{a}}(\Omega) \cdot \zeta(\alpha)^{\#\Omega} \varepsilon_1(\alpha) \prod_{\gamma \in \Omega} g_{\mathbf{a}\gamma^\sigma}(\tau) \\ &= \zeta(\alpha)^{\#\Omega} \varepsilon_1(\alpha) v_{\mathbf{a}}(\tau). \end{aligned}$$

The last equality comes from the fact that σ can be thought of as a permutation of Ω as mentioned above, and so the product is just reordered. Since $\zeta(\alpha)$ and $\varepsilon_1(\alpha)$ only

depend on α and not $\mathbf{a}$ we have

$$w_{\mathbf{a},\mathbf{b}}(\alpha\tau) = \frac{\zeta(\alpha)^{\#\Omega}\varepsilon_1(\alpha)v_{\mathbf{a}}(\tau)}{\zeta(\alpha)^{\#\Omega}\varepsilon_1(\alpha)v_{\mathbf{b}}(\tau)} = w_{\mathbf{a},\mathbf{b}}(\tau).$$

■

Definition 4.2.8. Let $\varepsilon_1 : \Gamma^+_{ns}(p) \to \mathbb{C}^\times$ be the map given by $\varepsilon_1(\alpha) = \prod_{\gamma\in\Omega} \varepsilon(\gamma, \alpha)$.

Definition 4.2.9. For $\mathbf{a} = (a_1, a_2) = \left(\frac{r_1}{p}, \frac{r_2}{p}\right) \in \left(\frac{1}{p}\mathbb{Z}/\mathbb{Z}\right)^2$ and $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, let $(\mathbf{a}\alpha)_1$ and $(\mathbf{a}\alpha)_2$ be the integers such that $\mathbf{a}\alpha = \left(\frac{(\mathbf{a}\alpha)_1}{p}, \frac{(\mathbf{a}\alpha)_2}{p}\right)$.

Proposition 4.2.10. *If there exists an* $\mathbf{a} = (a_1, a_2) = \left(\frac{r_1}{p}, \frac{r_2}{p}\right) \in \left(\frac{1}{p}\mathbb{Z}/\mathbb{Z}\right)^2$ *such that*

$$\sum_{\gamma\in\Omega} c(\mathbf{a}\gamma)_1^2 \equiv \sum_{\gamma\in\Omega} c(\mathbf{a}\gamma)_2^2 \equiv \sum_{\gamma\in\Omega} c(\mathbf{a}\gamma)_1(\mathbf{a}\gamma)_2 \equiv 0 \bmod p,$$

then $u_{\mathbf{b}}(\tau)$ *is modular for any* $\mathbf{b} \in \left(\frac{1}{p}\mathbb{Z}/\mathbb{Z}\right)^2$ *such that* $\mathbf{b} \notin \mathbb{Z}^2$. *Further, in this case* $\left(\varepsilon_1(\delta)\right)^c = 1$ *for all* $\delta \in \Gamma^*(p)$.

Proof: Suppose that such an $\mathbf{a} \in \left(\frac{1}{p}\mathbb{Z}/\mathbb{Z}\right)^2$ exists. This means that the function $u_{\mathbf{a}}(\tau)$ is modular for $\Gamma^*(p)$ from Theorem 4.1.9. This implies

$$u_{\mathbf{a}}(\delta\tau) = u_{\mathbf{a}}(\tau)$$

for all $\delta \in \Gamma^*(p)$, but by the definition of $u_{\mathbf{a}}(\tau)$ in terms of $v_{\mathbf{a}}(\tau)$ this means

$$\left(\zeta(\delta)^{\#\Omega}\varepsilon_1(\delta)v_{\mathbf{a}}(\tau)\right)^c = v_{\mathbf{a}}(\tau)^c.$$

Since $\zeta(\delta)$ is a 12th root of unity and $c \cdot \#\Omega \equiv 0 \bmod 12$, it must be that $\varepsilon_1(\delta)^c = 1$ for all δ in $\Gamma^*(p)$, but ε_1 is independent of $\mathbf{a}$. Therefore, for *any* $\mathbf{b} \in \left(\frac{1}{p}\mathbb{Z}/\mathbb{Z}\right)^2$ and

$\delta \in \Gamma^*(p)$ we have

$$u_{\mathbf{b}}(\delta\tau) = \left(\zeta(\delta)^{\#\Omega}\varepsilon_1(\delta)v_{\mathbf{b}}(\tau)\right)^c = \varepsilon_1(\tau)^c v_{\mathbf{b}}(\tau)^c = v_{\mathbf{b}}(\tau)^c = u_{\mathbf{b}}(\tau).$$

The other conditions for modularity follow from the fact that these functions are products of Siegel functions and the work in [KL81]. ∎

Proposition 4.2.11. *Suppose the conditions of Proposition 4.2.10 are satisfied. The map $\chi : \overline{\Omega} \to \mathbb{C}^\times$ given by $\chi(\overline{\beta}) = \varepsilon_1(\beta)$, where $\overline{\beta}$ is the* unique *lift of β to Ω, gives a well-defined character on $\overline{\Omega}$.*

Proof: We start by checking that χ is multiplicative. We check multiplicativity first, because if χ is multiplicative, we know that χ is well-defined on $\overline{\Omega} = \Gamma/\Gamma^*(p)$ since ε_1 is trivial on $\Gamma^*(p)$ by Proposition 4.2.10. Notice that for any $\alpha_1, \alpha_2 \in \Gamma$ and $\mathbf{a} \in \left(\frac{1}{p}\mathbb{Z}/\mathbb{Z}\right)^2$,

$$u_{\mathbf{a}}(\alpha_1\alpha_2\tau) = \varepsilon_1(\alpha_1\alpha_2)^c u_{\mathbf{a}}(\tau)$$

and

$$u_{\mathbf{a}}(\alpha_1\alpha_2\tau) = \varepsilon_1(\alpha_1)^c u_{\mathbf{a}}(\alpha_2\tau) = \varepsilon_1(\alpha_1)^c\varepsilon_1(\alpha_2)^c u_{\mathbf{a}}(\tau).$$

Therefore, $\varepsilon_1^c(\alpha_1\alpha_2) = \varepsilon_1(\alpha_1)^c\varepsilon_1(\alpha_2)^c$ and so χ is multiplicative and well-defined. ∎

Corollary 4.2.12. *For any $\mathbf{a} \in \left(\frac{1}{p}\mathbb{Z}/\mathbb{Z}\right)^2$ such that $\mathbf{a} \notin \mathbb{Z}^2$ and $\alpha \in \Gamma$,*

$$u_{\mathbf{a}}(\alpha\tau) = \chi(\overline{\alpha})u_{\mathbf{a}}(\tau),$$

where $\overline{\alpha}$ is the reduction of α modulo $\Gamma^*(p)$.

Corollary 4.2.13. *If $e = \gcd\left(2p, \frac{\#\overline{\Omega}}{\#\left[\overline{\Omega},\overline{\Omega}\right]}\right)$, where $\left[\overline{\Omega},\overline{\Omega}\right]$ is the commutator of $\overline{\Omega}$, then for any $\alpha \in \Gamma$, $\varepsilon_1(\alpha)^c$ is an e-th root of unity.*

PROOF: Because χ is a 1-dimensional representation of the finite non-abelian group $\overline{\Omega}$, we know that it must be trivial on every element in the commutator of $\overline{\Omega}$. Thus χ can be regarded as a character on the quotient group $\overline{\Omega}/\left[\overline{\Omega},\overline{\Omega}\right]$. Thus the image of χ must be contained in the $\left(\frac{\#\overline{\Omega}}{\#\left[\overline{\Omega},\overline{\Omega}\right]}\right)$-th roots of unity. But we know from the previous computations that the image of ε_1 is in the $2p$-th roots of unity. The only way this can happen is if they $\varepsilon_{\mathbf{a}}(\alpha)^c$ is an e-th root of unity. ■

Corollary 4.2.14. *With notation as above, $u_{\mathbf{a}}(\tau)^e$ is a modular function for Γ.*

4.3 Modular Units for $X_{ns}^+(p)$

We start this section by giving a more concrete way to think about $C_{ns}^+(p)$. Let ε be an integer such that $\left(\frac{\varepsilon}{p}\right) = -1$, and let $\overline{\varepsilon}$ be the reduction of ε mod p. Then:

$$C_{ns}^+(p) = \left\{ \begin{pmatrix} \alpha & \overline{\varepsilon}\beta \\ \beta & \alpha \end{pmatrix}, \begin{pmatrix} \alpha & \overline{\varepsilon}\beta \\ -\beta & -\alpha \end{pmatrix} : (\alpha,\beta) \in (\mathbb{Z}/p\mathbb{Z})^2 \text{ and } (\alpha,\beta) \neq (0,0) \right\}$$

One should notice that the choice of ε does not change the group $C_{ns}^+(p)$, so we fix ε for the rest of the paper. Now, let $C = \{(\alpha,\beta) \in (\mathbb{Z}/p\mathbb{Z})^2 : \alpha^2 - \overline{\varepsilon}\beta^2 = 1\}$ and $C' = \{(\alpha,\beta) \in (\mathbb{Z}/p\mathbb{Z})^2 : \alpha^2 - \overline{\varepsilon}\beta^2 = -1\}$. Since we have seen that $\Gamma_{ns}^+(p)$ is a congruence subgroup of level p, all of the results from Section 4.2 follow. In particular, the functions $w_{\mathbf{a},\mathbf{b}}(\tau)$ are modular for $\Gamma_{ns}^+(p)$.

Lemma 4.3.1. There is a natural bijection between $C \cup C'$ and $\overline{\Gamma_{ns}^+(p)} \subseteq \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$

given by

$$(a,b) \mapsto \begin{cases} \begin{pmatrix} a & \overline{\varepsilon}b \\ b & a \end{pmatrix} & \text{if } (a,b) \in C, \\ \begin{pmatrix} a & \overline{\varepsilon}b \\ -b & -a \end{pmatrix} & \text{if } (a,b) \in C'. \end{cases}$$

Here we note that it is a standard number theory result that $\#C = \#C' = p+1$ and so $\#\overline{\Gamma^+_{ns}(p)} = 2(p+1)$. See [Bar00, Chapter 2].

Lemma 4.3.2. *Let $f(x,y)$ be a homogeneous polynomial of degree two, then $f(ix,iy) = -f(x,y)$ where $i = \sqrt{-1}$.*

PROOF: Since $f(x,y)$ is homogeneous of degree two we can write $f(x,y) = a_2x^2 + a_1xy + a_0y^2$. Therefore,

$$\begin{aligned} f(ix,iy) &= a_2(ix)^2 + a_1(ix)(iy) + a_0(iy)^2 = i^2a_2x^2 + i^2a_1xy + i^2a_0y^2 \\ &= i^2(a_2x^2 + a_1xy + a_0y^2) = -(a_2x^2 + a_1xy + a_0y^2) = -f(x,y). \end{aligned}$$

■

Let $\overline{\Omega} = \Gamma^+_{ns}(p)/\Gamma^*(p)$ where $\Gamma^*(p) = \langle \Gamma(p), -I_2 \rangle$, let Ω be a fixed set of lifts of $\overline{\Omega}$ to $\Gamma^+_{ns}(p)$ and notice that $\overline{\Omega} = \overline{\Gamma^+_{ns}(p)}/\{\pm I_2\}$.

Proposition 4.3.3. *For $\mathbf{a} = \left(\frac{r_1}{p}, \frac{r_2}{p}\right) = (\alpha_1, \alpha_2) \in \frac{1}{p}\mathbb{Z}^2$ and $\mathbf{a} \notin \mathbb{Z}^2$, $v_{\mathbf{a}}(\tau)$ satisfies condition (1) in Theorem 4.1.9. That is, if we write $\mathbf{a}\gamma = \left(\frac{(\mathbf{a}\gamma)_1}{p}, \frac{(\mathbf{a}\gamma)_2}{p}\right)$, then*

$$\sum_{\gamma \in \Omega} (\mathbf{a}\gamma)_1^2 \equiv \sum_{\gamma \in \Omega} (\mathbf{a}\gamma)_2^2 \equiv \sum_{\gamma \in \Omega} (\mathbf{a}\gamma)_1(\mathbf{a}\gamma)_2 \equiv 0 \bmod p. \tag{4.3.1}$$

PROOF: Because the sums in question are being considered mod p, we can actually consider the sum over $\overline{\Omega}$ instead of over Ω. Here it is worth noting that we can take the extra step of reducing mod $\{\pm I_2\}$ because each term in the sum is a homogeneous polynomial of degree two in the entries of γ. Thus, since these are even functions, changing γ by $-I_2$ won't change the value of the sum.

We also notice that for $\gamma = \begin{pmatrix} a & \varepsilon b \\ b & a \end{pmatrix}$

$$\mathbf{a}\gamma = (\alpha_1 a + \alpha_2 b\,,\ \alpha_1 \varepsilon b + \alpha_2 a)$$

Now, using the bijection from the lemma above and the symmetry of the sums, the first sum becomes

$$\sum_{C \cup C'} (r_1 a + r_2 b)^2.$$

To show that this sum is actually zero mod p, we will show that

$$\sum_{(a,b)\in C} (r_1 a + r_2 b)^2 \equiv - \sum_{(a,b)\in C'} (r_1 a + r_2 b)^2 \bmod p$$

CASE 1: $p \equiv 1 \bmod 4$

If $p \equiv 1 \bmod 4$ we know that $\left(\frac{-1}{p}\right) = 1$. Thus there exists an $i \in \mathbb{Z}/p\mathbb{Z}$ such that $i^2 \equiv -1 \bmod p$. Using this element, we can construct a bijection from C to C' by $(a, b) \mapsto (ia, ib)$. Using this we get that

$$\begin{aligned} \sum_{(a,b)\in C} (r_1 a + r_2 b)^2 \equiv i^4 \sum_{(a,b)\in C} (r_1 a + r_2 b)^2 &\equiv i^2 \sum_{(a,b)\in C} i^2 (r_1 a + r_2 b)^2 \\ \equiv - \sum_{(a,b)\in C} (r_1 (ia) + r_2 (ib))^2 &\equiv - \sum_{(c,d)\in C'} (r_1 c + r_2 d)^2 \bmod p. \end{aligned}$$

In fact, since each term in the sums are homogenous of degree two, we can use this bijection and Lemma 4.3.2 to see that all three sums in (4.3.1) must be zero mod p.

Case 2: $p \equiv 3 \bmod 4$

In this case, we have that $\left(\frac{-1}{p}\right) = -1$, therefore we can let $\varepsilon = -1$. Now, we let $\sqrt{-1} = i$. In this case, $C = \{(a,b) \in \mathbb{Z}/p\mathbb{Z} : a^2 + b^2 = 1\}$ and $C' = \{(a,b) \in \mathbb{Z}/p\mathbb{Z} : a^2 + b^2 = -1\}$. If we consider the equality

$$(a + ib)(r_1 - ir_2) = (ar_1 + br_2) + i(br_1 - ar_2)$$

and take the norms on both sides, we see that

$$\begin{aligned}(a^2 + b^2)(r_1^2 + r_2^2) &\equiv N(a + ib) \cdot N(r_1 - ir_2) \\ &\equiv N\Big((ar_1 + br_2) + i(br_1 - ar_2)\Big) \\ &\equiv (ar_1 + br_2)^2 + (br_1 - ar_2)^2 \bmod p.\end{aligned}$$

Now, summing over $(a,b) \in C$ we get that

$$\begin{aligned}(p+1)(r_1^2 + r_2^2) &\equiv \sum_{(a,b)\in C} (ar_1 + br_2)^2 + (br_1 - ar_2)^2 \\ &\equiv \sum_{(a,b)\in C} (ar_1 + br_2)^2 + \sum_{(a,b)\in C} (br_1 - ar_2)^2 \bmod p.\end{aligned}$$

Now, if we use the fact that if $(a,b) \in C$ then we know that $(-b,a) \in C$ to get

$$(p+1)(r_1^2 + r_2^2) \equiv 2 \sum_{(a,b)\in C} (ar_1 + br_2)^2 \bmod p.$$

Summing over C' and applying the same trick we get

$$-(p+1)(r_1^2+r_2^2) \equiv 2 \sum_{(a,b)\in C'} (ar_1+br_2)^2 \bmod p$$

and thus

$$\sum_{(a,b)\in C} (ar_1+br_2)^2 \equiv - \sum_{(a,b)\in C'} (ar_1+br_2)^2.$$

The second sum in equation (4.3.1) sum follows by applying the same argument to

$$(a+ib)(r_2+ir_1) = (ar_2-br_1)+i(br_2+ar_1).$$

The last sum that must be dealt with is

$$\sum_{\bar{\Omega}} (ar_1+br_2)(ar_2-br_1).$$

Notice that the sum over $\bar{\Omega}$ is well defined since if you make both a and b negative, the value of the sum doesn't change. We show that this sum is zero mod p by showing that

$$\sum_{(a,b)\in C} (ar_1+br_2)(ar_2-br_1) \equiv \sum_{(a,b)\in C'} (ar_1+br_2)(ar_2-br_1) \equiv 0 \bmod p.$$

A little bit of algebra shows that

$$\begin{aligned}\sum_{(a,b)\in C} (ar_1+br_2)(ar_2-br_1) &= \sum_{(a,b)\in C} r_1r_2(a^2-b^2)+ab(r_2^2-r_1^2) \\ &= r_1r_2 \sum_{(a,b)\in C} (a^2-b^2) + (r_2^2-r_1^2) \sum_{(a,b)\in C} ab.\end{aligned}$$

Because we know that if (a, b) is in C then (b, a) is in C we know that

$$r_1 r_2 \sum_{(a,b)\in C} (a^2 - b^2) \equiv 0 \bmod p.$$

Now, we notice that if $a = 0$ or $b = 0$ then ab is already zero and if (a, b) is in C and neither are zero then $(-a, b)$ is in C. Using this we get that

$$(r_2^2 - r_1^2) \sum_{(a,b)\in C} ab \equiv 0 \bmod p.$$

Thus

$$\sum_{(a,b)\in C} (ar_1 + br_2)(ar_2 - br_1) \equiv 0 \bmod p$$

and the same argument shows that

$$\sum_{(a,b)\in C'} (ar_1 + br_2)(ar_2 - br_1) \equiv 0 \bmod p$$

and we are done. ■

Even without knowing anything about $\left[\overline{\Omega}, \overline{\Omega}\right]$, we can use the fact that $\#\overline{\Omega} = p+1$ to get the following proposition.

Proposition 4.3.4. *For $\Gamma = \Gamma_{ns}^+(p)$ and everything else as in Section 4.2, in particular $p > 3$, we have that for any $\alpha \in \Gamma_{ns}^+(p)$*

$$v_{\mathbf{a}}(\alpha\tau) = \pm v_{\mathbf{a}}(\tau).$$

PROOF: The proof follows from the fact that $\varepsilon_1(\alpha)^c$ is both a $2p$-th root of unity and a $(p + 1)$th root of unity with p not equal to 2 or 3. Thus by Proposition 4.2.10 and

Corollary 4.2.13, if we let $c = \gcd(2p, p+1) = 2$, then $u_{\mathbf{a}}(\tau) = (v_{\mathbf{a}}(\tau))^2$ is modular for Γ_{ns}^{+}. This gives us the above equality. ■

Chapter 5

Explicit computations for $X_{ns}^{+}(p)$

5.1 The case of $X_{ns}^{+}(11)$

In 2004 Chen and Cummins published a paper where they computed a model for $X_{ns}^{+}(11)$ and found an infinite family of elliptic curves whose associated Galois representations at 11 are contained in $C_{ns}^{+}(11)$. In their paper they apply the same arguments above to find Siegel functions that have poles of order two or three at infinity and use them to compute the model and the j-map. In this case, they use specific generators for Ω to show that the functions $u_{\mathbf{a}}(\tau) = v_{\mathbf{a}}(\tau)$ are modular for $\Gamma_{ns}^{+}(11)$.

In their paper, the authors omit showing that these functions *only* have poles at infinity. Since it is a delicate step that may not be obvious to the reader, we will include it here. To determine the order of vanishing of a function at a cusp that is not infinity, we first recall the fact that the curve $X(1) = \mathrm{SL}_2(\mathbb{Z})\backslash\mathscr{H}^*$ has only a single cusp. In other words, for every rational number r, there exists a $\gamma \in \mathrm{SL}_2(\mathbb{Z})$

such that $\gamma \cdot i\infty = r$. Using this we can see that

$$\operatorname{ord}_r g_{\mathbf{a}}(\tau) = \operatorname{ord}_{i\infty} g_{\mathbf{a}}(\gamma\tau) = \operatorname{ord}_{i\infty} \zeta g_{\mathbf{a}\gamma}(\tau) = \operatorname{ord}_{i\infty} g_{\mathbf{a}\gamma}(\tau),$$

for some constant ζ. Therefore, if

$$\mathbf{a} = (a_1, a_2) \quad \text{and} \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

such that $\gamma \cdot i\infty = r$ then $\operatorname{ord}_2 g_{\mathbf{a}}(\tau) = \frac{1}{2}\mathbb{B}_2\Big(\langle a_1 a + a_2 c\rangle\Big)$ by Lemma 4.1.10. Using this we can compute the divisors of modular units for $X_{ns}^+(11)$ once we know what the cusps are.

The easiest way to find representatives of the cusps of $X_{ns}^+(11)$ is to find representatives of the cusps of $X(11)$ and then see which ones are equivalent under the action of the matrices in Ω defined in the last section. Using SAGE, we get that the cusps of $X(11)$ can be represented by the following 60 elements of $\mathbb{P}^1(\mathbb{Q})$:

$$\Big[0, \tfrac{2}{11}, \tfrac{1}{5}, \tfrac{1}{4}, \tfrac{3}{11}, \tfrac{1}{3}, \tfrac{4}{11}, \tfrac{2}{5}, \tfrac{5}{11}, \tfrac{1}{2}, \tfrac{3}{5}, \tfrac{2}{3}, \tfrac{3}{4}, \tfrac{4}{5}, 1, \tfrac{6}{5}, \tfrac{5}{4}, \tfrac{4}{3}, \tfrac{7}{5}, \tfrac{3}{2}, \tfrac{8}{5}, \tfrac{5}{3}, \tfrac{7}{4}, \tfrac{9}{5}, 2,$$
$$\tfrac{11}{5}, \tfrac{9}{4}, \tfrac{7}{3}, \tfrac{5}{2}, \tfrac{8}{3}, \tfrac{11}{4}, 3, \tfrac{16}{5}, \tfrac{13}{4}, \tfrac{10}{3}, \tfrac{7}{2}, \tfrac{11}{3}, \tfrac{15}{4}, 4, \tfrac{21}{5}, \tfrac{17}{4}, \tfrac{9}{2}, \tfrac{14}{3}, \tfrac{19}{4}, 5,$$
$$\tfrac{21}{4}, \tfrac{11}{2}, \tfrac{17}{3}, 6, \tfrac{13}{2}, \tfrac{20}{3}, 7, \tfrac{15}{2}, 8, \tfrac{17}{2}, 9, \tfrac{19}{2}, 10, \tfrac{21}{2}, \infty\Big].$$

We check which of these cusps are equivalent under the action $\Gamma_{ns}^+(11)$, by taking a cusp of $X(11)$, call it c, and letting the lifts of $\Gamma_{ns}^+(11)/\Gamma^*(11)$ act on it. Then we can then check to see what cusps are now equivalent. We define a function in SAGE, that takes a cusp, c, of $X(11)$ and returns set of cusps in $X(11)$ that are equivalent to c under the action of $\Gamma_{ns}^+(11)$ using the following code:

```
def eqiv(c):
```

```
C = Gamma(11).cusps()
A1 = Matrix(QQ,[[-8,5],[-5,3]])
A2 = Matrix(QQ,[[-65,8],[8,-1]])
v = []
eqc = []
for a1 in [0,1,2,..,5]:
    for a2 in [0,1]:
        A = A1^a1*A2^a2
        if (A[1,0]*c + A[1,1]) == 0:
            v.append(Infinity)
        else:
            c1 = (A[0,0]*c + A[0,1])/(A[1,0]*c + A[1,1])
            v.append(c1)
for c0 in C:
    for c1 in v:
        if Gamma(11).are_equivalent(Cusp(c0),Cusp(c1)) == True:
            eqc.append(c0)
return eqc
```

For example, we see that the following cusps are equivalent to the cusp 0.

```
eqiv(0)
> [0, 1/3, 3/5, 8/5, 5/3, 7/4, 3, 10/3, 15/4, 17/3, 8, Infinity]
```

Remark 5.1.1. Notice, `equiv`(c) won't work for $c = \infty$ as it is defined now. This can be fixed, but is unnecessary to accomplish the goal of finding representatives for the cusps of $X_{ns}^{+}(11)$.

Remark 5.1.2. It turns out that the action of the lifts of $\Gamma^+_{ns}(p)/\Gamma^*(p)$ on the cusps of $X(p)$ is well-defined, transitive, and faithful. Therefore, we know that the number of cusps of $X^+_{ns}(p)$ is $\dfrac{\#\text{ cusps of } X(p)}{\#\Gamma^+_{ns}(p)/\Gamma^*(p)}$. It can be shown that if p is an odd prime, $X(p)$ has $\frac{1}{2}(p^2-1)$ cusps and $\#\Gamma^+_{ns}(p)/\Gamma^*(p) = p+1$. Therefore $X^+_{ns}(p)$ has exactly $\frac{p-1}{2}$ cusps.

So we start computing the equivalence classes until we have a partition of the set of cusps of $X(11)$. Doing this, we see that we can choose the following representatives for the cusps of $X^+_{ns}(11)$:

$$\left\{\infty, 1, 2, 5, \frac{5}{4}\right\}.$$

Using this information and the fact that $\mathrm{ord}_P(f\cdot g) = \mathrm{ord}_P(f) + \mathrm{ord}_P(g)$, we compute the following table:

	∞	1	2	5	5/4
$u_{(5/11,0)}$	-2	1	0	0	1
$u_{(3/11,0)}$	1	0	0	-2	1
$u_{(4/11,0)}$	1	0	-2	1	0
$\dfrac{u_{(5/11,0)}}{u_{(3/11,0)}}$	-3	1	0	2	0
$\dfrac{u_{(5/11,0)}}{u_{(4/11,0)}}$	-3	1	2	-1	1

Notice that both $\dfrac{u_{(5/11,0)}}{u_{(3/11,0)}}$ and $\dfrac{u_{(5/11,0)}}{u_{(4/11,0)}}$ have poles of order 3 at infinity, but $\dfrac{u_{(5/11,0)}}{u_{(4/11,0)}}$ has another pole at the cusp represented by 5. If you only look at the order vanishing at infinity, then it looks like the function $\dfrac{u_{(5/11,0)}}{u_{(4/11,0)}}$ might make a viable choice to be y in the typical Riemann-Roch argument. But now that we have computed the order of vanishing at the other cusps, we can see that this function will not work.

Since we have explicit formulas for each component of the $u_a(\tau)$'s, we can compute the q-expansions of each one and look for a relationship to find a Weirstrass equation for $X_{ns}^+(11)$. Each of these functions are defined over the maximal real subfield of $\mathbb{Q}(\zeta_{11})$, where ζ_{11} is a primitive 11th root of unity. Using SAGE and $x = u_{(5/11,0)}$ and $y = \dfrac{u_{(5/11,0)}}{u_{(3/11,0)}}$ we get that

$$\begin{aligned} & y^2 + (2\zeta_{11}^9 + 2\zeta_{11}^8 + 2\zeta_{11}^7 + 2\zeta_{11}^6 + 2\zeta_{11}^5 + 2\zeta_{11}^4 + 2\zeta_{11}^3 + 2\zeta_{11}^2 + 2)xy \\ & \quad + (-2\zeta_{11}^9 - 2\zeta_{11}^8 - \zeta_{11}^7 - \zeta_{11}^4 - 2\zeta_{11}^3 - 2\zeta_{11}^2)y \\ & \quad = x^3 + (2\zeta_{11}^9 + 2\zeta_{11}^8 + 2\zeta_{11}^7 + 2\zeta_{11}^4 + 2\zeta_{11}^3 + 2\zeta_{11}^2)x^2 \\ & \quad + (-2\zeta_{11}^9 - 3\zeta_{11}^8 - \zeta_{11}^7 + \zeta_{11}^6 + \zeta_{11}^5 - \zeta_{11}^4 - 3\zeta_{11}^3 - 2\zeta_{11}^2 + 2)x. \end{aligned}$$

Using SAGE again, we compute that the j-invariant of this elliptic curve is $-32768 = 2^{15}$. There is a rational model for $X_{ns}^+(11)$ given by the equation $y^2+y = x^3-x^2-7x+10$. This elliptic curve has rank 1 and no torsion points and so there are infinitely many elliptic curves whose representation at 11 has its image contained in the normalizer of a non-split Cartan subgroup.

In [CC04], they explicitly compute the j-map that takes points on $X_{ns}^+(11)$ and returns the j-invariants of the corresponding elliptic curves. To read more on this we point the reader to the third section of their paper.

5.2 Tables of Divisors for Functions of $X_{ns}^{+}(p)$

In this section we list the tables of the divisors of the functions that we have found for various values of p.

5.2.1 Tables for $X_{ns}^{+}(13)$

	∞	0	3	5	6	1/3
$v_{(1/13,0/13)}/v_{(2/13,0/13)}$	0	2	2	-1	-4	1
$v_{(1/13,0/13)}/v_{(4/13,0/13)}$	1	-2	4	-1	-2	0
$v_{(1/13,0/13)}/v_{(0/13,1/13)}$	-4	2	5	-1	0	-2
$v_{(1/13,0/13)}/v_{(0/13,2/13)}$	-2	2	4	-5	1	0
$v_{(1/13,0/13)}/v_{(0/13,2/13)}$	0	3	4	-3	0	-4
$v_{(2/13,0/13)}/v_{(4/13,0/13)}$	1	-4	2	0	2	-1
$v_{(2/13,0/13)}/v_{(0/13,1/13)}$	-4	0	3	0	4	-3
$v_{(2/13,0/13)}/v_{(0/13,2/13)}$	-2	0	2	-4	5	-1
$v_{(2/13,0/13)}/v_{(0/13,4/13)}$	0	1	2	-2	4	-5
$v_{(4/13,0/13)}/v_{(0/13,1/13)}$	-5	4	1	0	2	-2
$v_{(4/13,0/13)}/v_{(0/13,2/13)}$	-3	4	0	-4	3	0
$v_{(4/13,0/13)}/v_{(0/13,4/13)}$	-1	5	0	-2	2	-4
$v_{(0/13,1/13)}/v_{(0/13,2/13)}$	2	0	-1	-4	1	2
$v_{(0/13,1/13)}/v_{(0/13,4/13)}$	4	1	-1	-2	0	-2
$v_{(0/13,2/13)}/v_{(0/13,4/13)}$	2	1	0	2	-1	-4

5.2.2 Tables for $X_{ns}^{+}(17)$

	∞	0	1/2	1/3	1/4	1/7	1/11	2/11
$v_{(1/17,0/17)}/v_{(2/17,0/17)}$	-3	0	4	-3	3	-4	0	3
$v_{(1/17,0/17)}/v_{(3/17,0/17)}$	1	-2	6	-4	1	2	-6	2
$v_{(1/17,0/17)}/v_{(6/17,0/17)}$	-2	-6	6	-1	4	2	-2	-1
$v_{(1/17,0/17)}/v_{(0/17,1/17)}$	-8	2	6	-3	-1	5	-1	0
$v_{(1/17,0/17)}/v_{(1/17,1/17)}$	-2	0	5	-9	1	4	3	-2
$v_{(1/17,0/17)}/v_{(3/17,1/17)}$	-2	3	8	-5	1	1	0	-6
$v_{(1/17,0/17)}/v_{(4/17,1/17)}$	-4	-1	9	-3	-5	2	2	0
$v_{(2/17,0/17)}/v_{(3/17,0/17)}$	4	-2	2	-1	-2	6	-6	-1
$v_{(2/17,0/17)}/v_{(6/17,0/17)}$	1	-6	2	2	1	6	-2	-4
$v_{(2/17,0/17)}/v_{(0/17,1/17)}$	-5	2	2	0	-4	9	-1	-3
$v_{(2/17,0/17)}/v_{(1/17,1/17)}$	1	0	1	-6	-2	8	3	-5
$v_{(2/17,0/17)}/v_{(3/17,1/17)}$	1	3	4	-2	-2	5	0	-9
$v_{(2/17,0/17)}/v_{(4/17,1/17)}$	-1	-1	5	0	-8	6	2	-3
$v_{(3/17,0/17)}/v_{(6/17,0/17)}$	-3	-4	0	3	3	0	4	-3
$v_{(3/17,0/17)}/v_{(0/17,1/17)}$	-9	4	0	1	-2	3	5	-2
$v_{(3/17,0/17)}/v_{(1/17,1/17)}$	-3	2	-1	-5	0	2	9	-4
$v_{(3/17,0/17)}/v_{(3/17,1/17)}$	-3	5	2	-1	0	-1	6	-8
$v_{(3/17,0/17)}/v_{(4/17,1/17)}$	-5	1	3	1	-6	0	8	-2
$v_{(6/17,0/17)}/v_{(0/17,1/17)}$	-6	8	0	-2	-5	3	1	1
$v_{(6/17,0/17)}/v_{(1/17,1/17)}$	0	6	-1	-8	-3	2	5	-1
$v_{(6/17,0/17)}/v_{(3/17,1/17)}$	0	9	2	-4	-3	-1	2	-5
$v_{(6/17,0/17)}/v_{(4/17,1/17)}$	-2	5	3	-2	-9	0	4	1

	∞	0	1/2	1/3	1/4	1/7	1/11	2/11
$v_{(0/17,1/17)}/v_{(1/17,1/17)}$	6	-2	-1	-6	2	-1	4	-2
$v_{(0/17,1/17)}/v_{(3/17,1/17)}$	6	1	2	-2	2	-4	1	-6
$v_{(0/17,1/17)}/v_{(4/17,1/17)}$	4	-3	3	0	-4	-3	3	0
$v_{(1/17,1/17)}/v_{(3/17,1/17)}$	0	3	3	4	0	-3	-3	-4
$v_{(1/17,1/17)}/v_{(4/17,1/17)}$	-2	-1	4	6	-6	-2	-1	2
$v_{(3/17,1/17)}/v_{(4/17,1/17)}$	-2	-4	1	2	-6	1	2	6

Chapter 6

The modular Curve $X_s^+(11)$

6.1 Modular curves associated to Normalizers of Split Cartan Subgroups

We start this chapter by defining the basic groups that we will be interested.

Definition 6.1.1. A *split Cartan* subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ is a conjugate of the group of diagonal matrices;

$$C_s(p) = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in (\mathbb{Z}/p\mathbb{Z})^\times \right\}.$$

The normalizer of $C_s(p)$ is given by

$$C_s^+(p) = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, \begin{pmatrix} 0 & c \\ d & 0 \end{pmatrix} : a, b, c, d \in (\mathbb{Z}/p\mathbb{Z})^\times \right\}.$$

The congruence subgroup, $\Gamma_s^+(p)$, is the inverse image of $C_s^+(p) \cap \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ under the standard reduction map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$.

With these definitions we are now ready to define the modular curve $X_s^+(p)$.

Definition 6.1.2. Let $X_s^+(p)$ be the Riemann surface given by $\Gamma_s^+(p)\backslash\mathscr{H}^*$.

Theorem 6.1.3. [Che98, p. 4] *For $p > 3$, the genus of the curve $X_s^+(p)$ is given by*

$$g_s^+(p) = \frac{1}{24}\left(p^2 - 8p + 11 - 4\left(\frac{-3}{p}\right)\right).$$

Example 6.1.4.

p	$g_s^+(p)$
5	0
7	0
11	2
13	3
17	7
19	9
23	15
29	26

6.2 Curves of Genus Two

Using Theorem 6.1.3, we can see that the genus of $X_s^+(11)$ is equal to 2. Before we start looking at this curve in particular it would be worth it to better understand general genus 2 curves.

Proposition 6.2.1. *Every smooth projective curve of genus two, C, is birationally equivalent to a curve of the form:*

$$y^2 + yh(x) = f(x),$$

with $\deg(h) \leq 3$ *and* $\deg(f) \leq 5$.

PROOF: We prove this theorem by applying the Riemann-Roch theorem to multiples of the canonical divisor and look for a linear dependence. We build the following table:

TABLE 6.2.1

n	$\ell(nK_C)$	Basis for $\mathscr{L}(nK_C)$
1	2	$\langle 1, x \rangle$
2	3	$\langle 1, x, x^2 \rangle$
3	5	$\langle 1, x, x^2, x^3, y \rangle$
4	7	$\langle 1, x, x^2, x^3, y, x^4, xy \rangle$
5	9	$\langle 1, x, x^2, x^3, y, x^4, xy, x^5, x^2y \rangle$
6	11	$\langle 1, x, x^2, x^3, y, x^4, xy, x^5, x^2y, x^6, x^3y \rangle$

Here we notice that y^2 is also in $\mathscr{L}(6K_c)$, so we have 12 functions in an 11 dimensional vector space, so there must be a linear combination of the basis elements that gives y^2. After a little bit of algebra, we get a model for C described in the statement of the proposition. ■

Proposition 6.2.1 tells us that every genus two curve is hyperellyptic. In fact, if the base field of C is not of characteristic two, then C is birationally equivalent to a curve of the form $y^2 = f(x)$ where $\deg(f) = 5$ or 6. This model is obtained by completing the square on the left hand side and doing a change of variables.

Remark 6.2.2. Here we notice that it is impossible to embed a smooth genus two curve into $\mathbb{P}^2$. Indeed, if C is a smooth curve given as the vanishing set of a degree d homogeneous polynomial then its genus must be

$$g = \frac{(d-1)(d-2)}{2}.$$

A quick check shows that this formula never equals two since it is impossible for $(d-1)(d-2)$ to be 4. Therefore in regular projective space the models of these curves are always singular.

To combat this, when we consider a genus two curve given by a hyperelliptic equation, we are really thinking about them in weighted projective space. More specifically, we give x and z weight 1 and y weight 3. The reader will notice that the weight of each function corresponds to the multiple of K_C where the function first appears in the table 6.2.1. Therefore, when the models are homogenized they become $Y^2 + Yh(X,Z)) = f(X,Z)$ where $\deg(h) = 3$ and $\deg(f) = 6$, or $Y^2 = f(X,Z)$ with $\deg(f) = 6$.

6.3 Modular Units for $X_s^+(11)$

Now, we aim to find a model for $X_s^+(11)$ using a technique similar to the proof of Proposition 6.2.1. We start by computing the divisors of some modular units from last chapter. Doing so gives us the following table:

	$0/\infty$	1	2	3	4	5
$w_{(1/11,1/11),(0/11,1/11)}$	-5	1	3	1	0	0
$w_{(3/11,1/11),(0/11,1/11)}$	-5	1	0	3	1	0
$w_{(2/11,1/11),(0/11,1/11)}$	-5	3	0	0	1	1
$w_{(5/11,1/11),(0/11,1/11)}$	-5	0	1	0	3	1
$w_{(4/11,1/11),(0/11,1/11)}$	-5	0	1	1	0	3
$w_{(1/11,1/11),(3/11,1/11)}$	0	0	3	-2	-1	0
$w_{(3/11,1/11),(2/11,1/11)}$	0	-2	0	3	0	-1
$w_{(2/11,1/11),(5/11,1/11)}$	0	3	-1	0	-2	0
$w_{(5/11,1/11),(4/11,1/11)}$	0	0	0	-1	3	-2
$w_{(4/11,1/11),(1/11,1/11)}$	0	-1	-2	0	0	3
$w_{(4/11,1/11),(3/11,1/11)}$	0	-1	1	-2	-1	3
$w_{(1/11,1/11),(2/11,1/11)}$	0	-2	3	1	-1	-1
$w_{(3/11,1/11),(5/11,1/11)}$	0	1	-1	3	-2	-1
$w_{(2/11,1/11),(4/11,1/11)}$	0	3	-1	-1	1	-2
$w_{(5/11,1/11),(1/11,1/11)}$	0	-1	-2	-1	3	1

Remark 6.3.1. From Theorem 4.1.7 we know that the field of definition of the functions defined in Section 4.2 is the p-th cyclotomic field. In practice, the field of definition might actually be a subfield of the p-th cyclotomic field. In fact, using the Riemann-Roch Theorem, one can show that all of the functions above are actually defined over

the maximal real subfield of $\mathbb{Q}(\zeta_{11})$, usually denoted $\mathbb{Q}(\zeta_{11})^+$.

Example 6.3.2. Using SAGE, one can compute that the first few terms of the q-expansion of $w_{(2/11,1/11),(0/11,1/11)}(\tau)$ are given by

$$q^{-5} + (-\zeta_{11}^9 - \zeta_{11}^2 + 1)q^{-4} + (\zeta_{11}^8 + \zeta_{11}^7 + \zeta_{11}^6 + \zeta_{11}^5 + \zeta_{11}^4 + \zeta_{11}^3 + 4)q^{-3} +$$
$$(-2\zeta_{11}^9 - 2\zeta_{11}^2 + 4)q^{-2} + (-2\zeta_{11}^9 + \zeta_{11}^8 + \zeta_{11}^7 + \zeta_{11}^6 + \zeta_{11}^5 + \zeta_{11}^4 + \zeta_{11}^3 - 2\zeta_{11}^2 + 9)q^{-1} +$$
$$(-4\zeta_{11}^9 + \zeta_{11}^8 + 2\zeta_{11}^7 + \zeta_{11}^6 + \zeta_{11}^5 + 2\zeta_{11}^4 + \zeta_{11}^3 - 4\zeta_{11}^2 + 12) +$$
$$(-5\zeta_{11}^9 + 2\zeta_{11}^8 + 2\zeta_{11}^7 + 2\zeta_{11}^6 + 2\zeta_{11}^5 + 2\zeta_{11}^4 + 2\zeta_{11}^3 - 5\zeta_{11}^2 + 20)q +$$
$$(-8\zeta_{11}^9 + 2\zeta_{11}^8 + 2\zeta_{11}^7 + 2\zeta_{11}^6 + 2\zeta_{11}^5 + 2\zeta_{11}^4 + 2\zeta_{11}^3 - 8\zeta_{11}^2 + 27)q^2 +$$
$$(-9\zeta_{11}^9 + 5\zeta_{11}^8 + 5\zeta_{11}^7 + 5\zeta_{11}^6 + 5\zeta_{11}^5 + 5\zeta_{11}^4 + 5\zeta_{11}^3 - 9\zeta_{11}^2 + 43)q^3 +$$
$$(-16\zeta_{11}^9 + 5\zeta_{11}^8 + 5\zeta_{11}^7 + 5\zeta_{11}^6 + 5\zeta_{11}^5 + 5\zeta_{11}^4 + 5\zeta_{11}^3 - 16\zeta_{11}^2 + 57)q^4 +$$
$$(-19\zeta_{11}^9 + 7\zeta_{11}^8 + 7\zeta_{11}^7 + 7\zeta_{11}^6 + 7\zeta_{11}^5 + 7\zeta_{11}^4 + 7\zeta_{11}^3 - 19\zeta_{11}^2 + 84)q^5 + O(q^6)$$

If we have any hope to use these functions to compute a model for $X_s^+(11)$, we somehow have to use these functions to construct new functions that are defined over $\mathbb{Q}$ and apply the argument from Proposition 6.2.1 to them.

Proposition 6.3.3. *Let $K/\mathbb{Q}$ be a number field of degree n and let $\{e_1, e_2, \ldots, e_n\}$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$. Let $Gal(K/\mathbb{Q}) = \{\sigma_i\}_{i=1}^n$. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ such that the cusp of $X(\Gamma)$ at infinity is rational. Further, let $f(\tau) = \sum_k a_k\, q^k$ be the q-expansion of a modular function for Γ with coefficients in K. Let $a_k = a_{k,1}e_1 + \cdots + a_{k,n}e_n$ with $a_{i,j} \in \mathbb{Q}$. Then the function $f_k(\tau) = \sum_i a_{k,j}\, q^k$ is also modular for Γ. In particular, there are constants, $b_j \in K$ depending on k, such that $f_k = \sum_{j=1}^n b_j\, \sigma_j(f(\tau))$.*

PROOF: Using the fact that every element $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ is a field automorphism that fix $\mathbb{Q}$, for any $\alpha = \alpha_1\, e_1 + \cdots + \alpha_n\, e_n \in K$ we get

$$\begin{pmatrix} \sigma_1(e_1) & \sigma_1(e_2) & \dots & \sigma_1(e_n) \\ \sigma_2(e_1) & \sigma_2(e_2) & \dots & \sigma_2(e_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(e_1) & \sigma_n(e_2) & \dots & \sigma_n(e_n) \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} \sigma_1(\alpha) \\ \sigma_2(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{pmatrix}. \tag{6.3.1}$$

For convenience let A be the matrix on the left hand side of (6.3.1), and let A_i be the matrix obtained from replacing the i-th row of A with the column vector on the right hand side of (6.3.1). Applying Cramer's rule we get that

$$\alpha_i = \frac{\det A_i}{\det A}.$$

Now, if we let A_{ji} be the matrix obtained by deleting the j-th row and i-th column of A_i, we can compute the determinant of A_i by looking at the cofactor expansion of A_i along the i-th column. Doing this shows that:

$$\alpha_i = \frac{\det A_i}{\det A} = \frac{1}{\det A} \sum_{j=1}^{n} (-1)^{j+i} \sigma_j(\alpha) \det A_{ji}.$$

Letting $b_j = \dfrac{(-1)^{j+i} \det A_{ji}}{\det A}$ we have that

$$\alpha_i = \sum_{j=1}^{n} b_j\, \sigma_j(\alpha).$$

Notice that the definition of b_j does not depend on α because both determinants are polynomials in the $\sigma_i(e_k)$'s.

Now, if we assume that $X(\Gamma)$ has a rational cusp at infinity, then $\mathrm{Gal}(K/\mathbb{Q})$ acts on the q-expansion of a modular form $f = \sum_k a_k\, q^k$ simply by acting on the coefficients. Since the b_j's don't depend on anything other than the choice of basis for $\mathcal{O}_K$, we get that

$$f_k(\tau) = \sum_{j=1}^{n} b_j\, \sigma_j(f(\tau)),$$

and the modularity of $f_j(\tau)$ follows from the modularity of $\sigma_j(f(\tau))$. ■

Looking at the first 5 functions on our table, we see that they all have poles of order 5 at infinity and no where else. Now, since ord_p is a non-archemedian valuation on the functions of $X_s^+(11)$, and ∞ is a rational point, we know that taking linear combinations of the Galois conjugates won't introduce any other poles. With this in mind we let

$$X = \left[w_{(2/11,1/11),(0/11,1/11)}(\tau)\right]_1$$
$$Y = \left[w_{(1/11,1/11),(0/11,1/11)}(\tau)\right]_2$$
$$Z = \left[w_{(3/11,1/11),(0/11,1/11)}(\tau)\right]_0$$

where the subscript indicates which coefficients we are using to create the q-expantions. The q-expansions of these functions are given in Section 6.6. The important thing is that $\mathrm{ord}_\infty(X) = -3$, $\mathrm{ord}_\infty(Y) = -4$, and $\mathrm{ord}_\infty(Z) = -5$ and these functions don't have any poles anywhere else.

6.4 Computing a Model for $X_s^+(11)$

Now that we have computed some functions whose poles are concentrated at infinity, we need to find a polynomial relationship between them.

Proposition 6.4.1. *Let C be a smooth genus 2 curve. Let X, Y, and Z be in $K(C)$ the function field of C with poles of order 3, 4, and 5 respectively at ∞ and no where else. Then C can be mapped into $\mathbb{P}^2(K)$ as the vanishing set of a polynomials of degree at most 7.*

PROOF: We start by noticing that all the monomials of degree $d > 0$ in X, Y, and Z are contained in $\mathscr{L}(5d\infty)$. Using the Riemann-Roch theorem, we know that the dimension of this space is

$$\ell(5d(\infty)) = \deg(5d(\infty)) - g + 1 = 5d - 1.$$

The number of three variable monomials of degree d is given by $\binom{d+2}{2}$

So we build a table and see when the number of monomials of degree d becomes greater than the dimension of $\mathscr{L}(5d \cdot \infty)$.

d	$\ell(5d \cdot \infty)$	$\binom{d+2}{2}$
1	4	3
2	9	6
3	14	10
4	19	15
5	24	21
6	29	28
7	34	36

The table above shows that there must be a polynomial, p, of degree at most 7 such that $p(X, Y, Z) = 0$. ■

Lemma 6.4.2. Let C be a genus g curve. The only function without any poles and a zero at infinity is the zero function.

PROOF: Let f be a function that has no poles and a zero at ∞. This means that f is in $(-\infty)$, but by Proposition 2.4.3 part 1, we know that $\ell(-\infty) = 0$. Thus, f must be the zero function. ■

Now, we notice that since X, Y, and Z are functions whose only poles are at ∞, any polynomial in X, Y, and Z can also only have a pole at infinity. Thus, by Lemma 6.4.2, if we can find a polynomial in X, Y, and Z that has a zero at infinity, it must in fact be zero. Computing the q-expansions of X, Y, and Z to a reasonable

precision, it is easy to show that

$$0 = p(X,Y,Z) = 3\,X^2Y^3 + X^2Y^2Z - X^2YZ^2 + 2\,XY^4 - 2\,XY^2Z^2 + 2\,XYZ^3 + XZ^4 - Y^5 + 3\,Y^4Z - Y^3Z^2 - Y^2Z^3 + O(q^N).$$

for some $N \geq 1$ depending on the initial precision that was used to calculate X, Y, and Z. Unfortunately, this is not in the best model for the modular curve, first of all it is singular, and secondly it isn't written in hyperelliptic form.

A quick check show that if we use the change of variables

$$\begin{aligned}
X_1 &= Y^2Z^4 + \frac{1}{2}YZ^5 \\
Y_1 &= \frac{3}{2}XY^5Z^{12} - \frac{3}{2}Y^6Z^{12} + 2XY^4Z^{13} + \frac{1}{2}Y^5Z^{13} + \frac{3}{8}XY^3Z^{14} + \frac{5}{8}Y^4Z^{14}, \\
&\quad - \frac{3}{8}XY^2Z^{15} - \frac{1}{2}Y^3Z^{15} - \frac{1}{8}XYZ^{16} + \frac{1}{4}Y^2Z^{16} + \frac{1}{2}YZ^{17} + \frac{1}{8}Z^{18}, \\
Z_1 &= Y^2Z^4 - \frac{1}{2}YZ^5 - \frac{1}{2}Z^6.
\end{aligned}$$

and $x_1 = X_1/Z_1$ and $y_1 = Y_1/Z_1^3$, then we see that $X_s^+(11)$ is isomorphic to the hyperelliptic curve given by

$$y_1^2 + (x_1^3 + x_1^2 + x_1 + 1)y = -2x_1^5 + 2x_1^4 - 3x_1^3 + 2x_1^2 - 2x_1.$$

Here we note that we are working in weighted projective space where x_1 and z_1 have weight one and z_1 has weight three. While this model is minimal, it only has bad reduction at 11, it will not be convenient for us to use. In stead we will use its

simplified model:

$$\boxed{X_s^+(11) : y^2 = x^6 - 6x^5 + 11x^4 - 8x^3 + 11x^2 - 6x + 1.}$$

Here the change of variables from the initial curve is given by

$$\begin{aligned}
X_2 &= Y^2Z^4 + 1/2YZ^5 \\
Y_2 &= -3XY^5Z^{12} - Y^6Z^{12} - 4XY^4Z^{13} - Y^5Z^{13} - \frac{3}{4}XY^3Z^{14} + \frac{3}{4}Y^4Z^{14} \\
&\quad + \frac{3}{4}XY^2Z^{15} + \frac{1}{4}XYZ^{16} - \frac{5}{4}Y^2Z^{16} - \frac{3}{4}YZ^{17} - \frac{1}{8}Z^{18} \\
Z_2 &= Y^2Z^4 - 1/2YZ^5 - 1/2Z^6,
\end{aligned}$$

and again $x = X_2/Z_2$ and $y = Y_2/Z_2^3$. This model has bad reduction at two and eleven, but the extra prime of bad reduction will not cause any problems.

Remark 6.4.3. The minimal and simplified models for $X_s^+(11)$, along with the changes of variables were found using Magma and checked to work by hand.

6.5 Computing the j-map for $X_s^+(11)$

The last task for this chapter is to compute the map from $X_s^+(11)$ to $\overline{\mathbb{Q}}$, that takes a point on $X_s^+(11)$ and returns the j-invariant of the corresponding elliptic curve. Since we know that j must be a function in the function field of $X_s^+(11)$, it must be a rational function in x and y. Therefore, we know that there is a rational combination of the q-expansions of x and y that will give us the q-expansion of the j function.

Recall, we are using the nonstandard notation $q = e^{\frac{2\pi i\tau}{11}}$, then

$$j(\tau) = q^{-11} + 744 + 196884q^{11} + 21493760q^{22} + 864299970q^{33} + O(q^{44}).$$

Since x and y satisfy a hyperelliptic relationship, $y^2 = f(x)$ we know that the highest powers of y that can occur in numerator and denominator of our rational function is one. Further, if the denominator of our rational function is $C'y + D'$ with C' and D' in $\mathbb{Q}[x]$, we can multiply both the numerator and denominator by $C'y - D'$ to get the denominator to be completely in $\mathbb{Q}[x]$. Therefore we know that there must be $A,\ B$, and C in $\mathbb{Q}[x]$ such that

$$j = \frac{Ay + B}{C}.$$

This is equivalent to finding a solution to $Cj = Ay + B$. We do this by creating two vector spaces, one spanned by vectors made of the coefficients of the q-expansions of $V_1 = \{j, x \cdot j, x^2 \cdot j, \ldots, x^n \cdot j\}$, and the other spanned by $V_2 = \{1, x, xy, x^2, x^2y, \ldots, x^n, x^ny\}$ for various values of n. Then we look at the intersection of these two vector spaces, increasing n until there is a one dimensional intersection and we can use this to find j as a rational combination of x and y.

In the end, we find that A is a polynomial of degree 63, B is a polynomial of degree 66, and C is a polynomial of degree 66. Their explicit formulas can be found in the appendix to this chapter.

6.6 Appendix

Throughout this section we will be using the nonstandard notation $q = e^{\frac{2\pi i\tau}{11}}$.

The functions that give the singular model of $X_s^+(11)$.

$$X = \frac{1}{q^3} + \frac{1}{q} + 1 + 2q + 2q^2 + 5q^3 + 5q^4 + 7q^5 + 9q^6 + 13q^7 + 15q^8 + 21q^9 + 25q^{10} +$$
$$33q^{11} + 40q^{12} + 51q^{13} + 61q^{14} + 78q^{15} + 92q^{16} + 115q^{17} + 137q^{18} + 169q^{19} +$$
$$199q^{20} + 243q^{21} + 286q^{22} + 345q^{23} + 406q^{24} + 485q^{25} + 567q^{26} + 676q^{27} +$$
$$786q^{28} + 928q^{29} + 1080q^{30} + 1267q^{31} + 1468q^{32} + 1716q^{33} + 1981q^{34} + 2304q^{35} +$$
$$2654q^{36} + 3073q^{37} + 3529q^{38} + 4075q^{39} + 4665q^{40} + 5364q^{41} + 6131q^{42} +$$
$$7026q^{43} + 8008q^{44} + O(q^{45})$$
$$Y = \frac{1}{q^4} + \frac{1}{q^3} + \frac{2}{q^2} + \frac{3}{q} + 6 + 7q + 10q^2 + 14q^3 + 21q^4 + 26q^5 + 37q^6 + 49q^7 + 66q^8 +$$
$$85q^9 + 113q^{10} + 143q^{11} + 186q^{12} + 235q^{13} + 300q^{14} + 375q^{15} + 475q^{16} + 587q^{17} +$$
$$735q^{18} + 905q^{19} + 1120q^{20} + 1369q^{21} + 1683q^{22} + 2044q^{23} + 2493q^{24} + 3013q^{25} +$$
$$3649q^{26} + 4387q^{27} + 5286q^{28} + 6322q^{29} + 7574q^{30} + 9024q^{31} + 10756q^{32} +$$
$$12760q^{33} + 15146q^{34} + 17896q^{35} + 21153q^{36} + 24908q^{37} + 29325q^{38} + 34413q^{39} +$$
$$40377q^{40} + 47226q^{41} + 55224q^{42} + 64406q^{43} + 75075q^{44} + O(q^{45})$$

$$Z = \frac{1}{q^5} + \frac{1}{q^4} + \frac{3}{q^3} + \frac{4}{q^2} + \frac{8}{q} + 11 + 18q + 25q^2 + 38q^3 + 52q^4 + 77q^5 + 103q^6 +$$
$$145q^7 + 195q^8 + 267q^9 + 352q^{10} + 473q^{11} + 617q^{12} + 814q^{13} + 1052q^{14} +$$
$$1368q^{15} + 1750q^{16} + 2252q^{17} + 2855q^{18} + 3633q^{19} + 4574q^{20} + 5766q^{21} +$$
$$7205q^{22} + 9013q^{23} + 11188q^{24} + 13893q^{25} + 17144q^{26} + 21148q^{27} + 25949q^{28} +$$
$$31825q^{29} + 38845q^{30} + 47378q^{31} + 57558q^{32} + 69850q^{33} + 84469q^{34}$$
$$+ 102043q^{35} + 122876q^{36} + 147801q^{37} + 177281q^{38} + 212386q^{39} + 253797q^{40} +$$
$$302927q^{41} + 360717q^{42} + 429029q^{43} + 509201q^{44} + O(q^{45})$$

The functions that give the simplified model for $X_s^+(11)$.

$$x = -q - q^2 + q^4 + q^5 + q^6 + 2q^7 + 3q^8 + 2q^9 - 2q^{10} - 6q^{11} - 7q^{12} - 5q^{13} - 3q^{14} -$$
$$q^{15} + 4q^{16} + 13q^{17} + 21q^{18} + 20q^{19} + 8q^{20} - 9q^{21} - 24q^{22} - 36q^{23} - 46q^{24} -$$
$$47q^{25} - 26q^{26} + 23q^{27} + 83q^{28} + 124q^{29} + 127q^{30} + 93q^{31} + 27q^{32} - 78q^{33} -$$
$$218q^{34} - 345q^{35} - 373q^{36} - 242q^{37} + 27q^{38} + 355q^{39} + 663q^{40} + 884q^{41} +$$
$$908q^{42} + 582q^{43} - 168q^{44} - 1185q^{45} - 2094q^{46} - 2500q^{47} - 2162q^{48} -$$
$$994q^{49} + O(q^{50})$$

$$y = -1 - q - 2q^2 - 2q^3 - q^4 + q^5 + 4q^6 + 10q^7 + 18q^8 + 19q^9 + 4q^{10} - 24q^{11} -$$
$$47q^{12} - 56q^{13} - 60q^{14} - 61q^{15} - 23q^{16} + 94q^{17} + 253q^{18} + 335q^{19} + 254q^{20} +$$
$$59q^{21} - 154q^{22} - 405q^{23} - 782q^{24} - 1159q^{25} - 1099q^{26} - 259q^{27} + 1121q^{28} +$$
$$2348q^{29} + 2974q^{30} + 3072q^{31} + 2559q^{32} + 610q^{33} - 3499q^{34} - 8689q^{35} -$$
$$11944q^{36} - 10645q^{37} - 4805q^{38} + 3795q^{39} + 14242q^{40} + 26227q^{41} + 36012q^{42} +$$
$$34716q^{43} + 14446q^{44} - 22544q^{45} - 62983q^{46} - 92206q^{47} - 101718q^{48} -$$
$$84286q^{49} + O(q^{50})$$

Components of the j-map.

$$A = \frac{1}{2}(12x^4 - 18x^3 + 17x^2 - 7x + 1)^3(111x^6 - 170x^5 + 70x^4 - 2x^3 + 4x^2 - 5x + 1) \cdot$$
$$(x^7 + 7x^6 + 32x^5 - 64x^4 + 35x^3 - x^2 - 4x + 1) \cdot (32x^{12} + 120x^{11} - 1298x^{10} +$$
$$2948x^9 - 3168x^8 + 2827x^7 - 1727x^6 + 209x^5 + 253x^4 - 66x^3 - 22x^2 + 10x - 1) \cdot$$
$$(144x^{26} - 2256x^{25} + 18860x^{24} - 115940x^{23} + 574556x^{22} - 2329994x^{21} +$$
$$7758495x^{20} - 21308986x^{19} + 48397750x^{18} - 90908403x^{17} + 141194783x^{16} -$$
$$181604055x^{15} + 194211258x^{14} - 173809360x^{13} + 131248127x^{12} - 84357312x^{11} +$$
$$46486774x^{10} - 22039724x^9 + 8966083x^8 - 3098904x^7 + 894451x^6 - 210459x^5 +$$
$$39098x^4 - 5489x^3 + 545x^2 - 34x + 1)$$

$$B = -\frac{1}{2}(12x^4 - 18x^3 + 17x^2 - 7x + 1)^3(512512x^{54} - 4920960x^{53} +$$
$$8073824x^{52} + 32779472x^{51} + 575582832x^{50} - 11757298740x^{49} +$$
$$123153362046x^{48} - 1025903832074x^{47} + 7130112632786x^{46} -$$
$$41282109525668x^{45} + 200296029182722x^{44} - 822428489811719x^{43} +$$
$$2883161405954213x^{42} - 8692621889747421x^{41} + 22686370788241698x^{40} -$$
$$51569657533068960x^{39} + 102712628400692166x^{38} - 180262282831207631x^{37} +$$
$$280214886284970416x^{36} - 387584990364515294x^{35} + 478818483874641679x^{34} -$$
$$529823314147545769x^{33} + 526048866085233912x^{32} - 469013140571013349x^{31} +$$
$$375424845829986461x^{30} - 269524801566216518x^{29} + 173250531762163661x^{28} -$$
$$99487202053168339x^{27} + 50896310853946506x^{26} - 23124113010547420x^{25} +$$
$$9297706494276038x^{24} - 3295208796566316x^{23} + 1024310489156144x^{22} -$$
$$277371856580156x^{21} + 64920410256402x^{20} - 13195048116610x^{19} +$$
$$2489082153830x^{18} - 490065569397x^{17} + 58963068414x^{16} + 46761377446x^{15} -$$
$$43863985850x^{14} + 16410757861x^{13} + 227319892x^{12} - 4085480572x^{11} +$$
$$2813379669x^{10} - 1201174756x^9 + 376363296x^8 - 90993112x^7 + 17240015x^6 -$$
$$2554784x^5 + 291501x^4 - 24806x^3 + 1486x^2 - 56x + 1)$$
$$C = x^{11}(x^5 - 6x^4 - x^3 + 10x^2 - 6x + 1)^{11}$$

Chapter 7

The Modular Curves $X_s^+(5)$ and $X_s^+(7)$

From Theorem 6.1.3, we know that the curves $X_s^+(5)$ and $X_s^+(7)$ are both genus zero curves. It is a classical result that every genus zero curve with at least one point is isomorphic to $\mathbb{P}^1$. Since we know that there are elliptic curves with complex multiplication that have split representation at 5 and 7, we know that there must be points on both of these curves.

When $X_s^+(p)$ is a curve of genus zero, its function field is generated by a single function x (usually called the *Hauptmodul* of $X_s^+(p)$). In other words, the function field of $X_s^+(p)$ is of the form $\mathbb{Q}(x)$. Since the modular j-invariant function is a Hauptmodul for $X(1)$, the function field $\mathbb{Q}(x)$ is a finite extension of $\mathbb{Q}(j)$ and, therefore, x is algebraic over $\mathbb{Q}(j)$.

It is a classical result that the Hauptmodul of a genus zero curve is a function with a simple pole at one point (in particular ∞) and no other poles. Thus, if we can find the q-expansion of such a function, x, that only has a single pole, then we would

have found the Hauptmodul of our curve.

7.1 The j-map for $X_s^+(5)$

Computing a few of the functions from Chapter 4, we see that the function

$$\omega_5 = w_{(0/5,1/5),(1/5,1/5)}(\tau) = q^{-1} + (\zeta_5^3 + \zeta_5^2 + 2) + 4q + 5q^2 + 10q^3 + 16q^4 + 25q^5 + 36q^6 + 55q^7 + 75q^8 + 110q^9 + 150q^{10} + O(q^{11})$$

is a function with a simple pole at infinity and no other poles on $X_s^+(5)$. It turns out, in this case that ω_5 is actually defined over $\mathbb{Q}$ except for the constant term. So we don't even need Proposition 6.3.3 to make this function rational, but of course we could also take the ζ_5^0 coefficients to build our $\mathbb{Q}$-rational function. Instead, we subtract away the part of the constant term that is not defined over $\mathbb{Q}$. That is, we let

$$x = \omega_5 - \zeta_5^3 - \zeta_5^2.$$

Now, the function x has a simple pole at ∞ and no other poles.

Now, armed with a generator of our function field, x, we can use SAGE to find a rational combination of x that gives us the q-expansion for the modular j-function. This will be our j-map. Using the same argument as in the Lemma 6.4.2, one can show that

$$j_5(x) = \frac{(x+2)^3(x^2-6x+4)^3(x^2-x+4)^3}{(x^2-x-1)^5} + O(q^N),$$

for N large enough to show that these two functions are actually the same. Plugging in a few rational values of x, we get the following table:

t	$j_5(t)$	E with $j(E) = j(t)$	CM?
0	-32768	$y^2 + y = x^3 - x^2 - 7x + 10$	Yes
$\frac{1}{2}$	$-\frac{16875}{32}$	$y^2 = x^3 - \frac{3653656875}{1024}x + \frac{87896023441875}{16384}$	No
1	1728	$y^2 = x^3 + x$	Yes
$\frac{3}{2}$	$\frac{3131359847}{32}$	$y^2=x^3-\frac{29415724019189291091}{1024}x-\frac{3070319683074914617457068 5047}{16384}$	No
2	-884736	$y^2=x^3-2352859840512x+1390483697106419712$	Yes

7.2 The j-map for $X_s^+(7)$

Just like in the last section, we are looking for a function that has a simple pole at the point at infinity and nowhere else. Using the same techniques as before, one can show that

$$\omega_7 = w_{(0/7,1/7),(1/7,1/7)}(\tau) = q^{-1} + (-\zeta_7^5 - \zeta_7^4 - \zeta_7^3 - \zeta_7^2) + 2q + q^2 + 2q^3 + 3q^4 + 4q^5 + 5q^6 + 7q^7 + 8q^8 + 11q^9 + 13q^{10} + O(q^{11})$$

is such a function. Notice, ω_7 is defined over $\mathbb{Q}$ everywhere except the constant term. So we let,

$$x = \omega_7 + (\zeta_7^5 + \zeta_7^4 + \zeta_7^3 + \zeta_7^2),$$

and we have found a generator for the function field of $X_s^+(7)$. Using SAGE and the same Riemann-Roch argument as before, one can prove that the j-map from $X_s^+(7) \to \mathbb{P}^1$ is given as a rational function in x by

$$j_7(x) = \frac{(x+2)(x+3)^3(x^2-x-5)^3(x^2-x+2)^3(x^4+3x^3+2x^2-3x+1)^3}{(x^3+2x^2-x-1)^7}.$$

t	$j_7(t)$	E	CM?
0	54000	$y^2 = x^3 - 8468064000x - 295095094272000$	Yes
$\frac{1}{2}$	$\frac{2268945}{128}$	$y^2{=}x^3{-}\frac{13938771246435}{16384}x{-}\frac{9514424048790327345}{1048576}$	No
1	-12288000	$y^2{=}x^3{-}453048532992000x{+}3711895494180470784000$	Yes
2	$-\frac{68694048000}{62748517}$	$y^2{=}x^3{-}\frac{365019876190387261440000}{3937376385699289}x{+}\frac{43102395134904925795629685800960000}{24706452907345039270441 3}$	No

Chapter 8

The Mordell-Weil Group of the Jacobian of $X_s^+(11)$

8.1 Introduction

Given a curve C, one can construct an associated abelian variety J called its *jacobian*. As an abelian group, the jacobian is isomorphic to the Picard group of C. The Mordell-Weil theorem says that for any number field K, the K-rational points of the jacobian, $J(K)$, form a finitely generated abelian group. Therefore, it is non-canonically isomorphic to the product of a finite abelian group, $J(K)_{\text{tors}}$, and a free abelian group; i.e.,

$$J(K) \cong J(K)_{\text{tors}} \times \mathbb{Z}^r.$$

for some $r \in \mathbb{Z}_{\geq 0}$. In this case we say that $J(K)$ has rank r.

In this chapter we will be interested in computing the structure of $J(\mathbb{Q})$ for a fixed genus two curve. Computing $J(\mathbb{Q})_{\text{tors}}$ is not very difficult using the following

theorem.

Theorem 8.1.1. [HS00, Theorem C.1.4] *Let A be an abelian variety defined over a number field K, let v be a finite place of K at which A has good reduction, let $\widetilde{K}$ be the residue field of v, and let p be the characteristic of $\widetilde{K}$. Then for any $m \geq 1$ with $p \nmid m$, the reduction map*

$$A(K)[m] \to \widetilde{A}(\widetilde{K})$$

is injective, where $A(K)[m]$ denotes the m-torsion of $A(K)$. In other words, the reduction modulo v map is injective on the prime-to-p torsion subgroup of $A(K)$.

The basic idea for computing the rank of J is to try and compute the $\mathbb{F}_2$-dimension of the so-called weak Mordel-Weil group, $J(\mathbb{Q})/2J(\mathbb{Q})$. This is something that is easily done if one already knows the structure of $J(\mathbb{Q})$, but since we don't know the structure of this group we have to find another way to do this. We describe a method below, the 2-descent method, to bound the $\mathbb{F}_2$-dimension of $J(\mathbb{Q})/2J(\mathbb{Q})$ and therefore calculate a bound on the rank of $J(K)$. The method of 2-descent relies on the fact that we have the following short exact sequence of Galois modules

$$0 \longrightarrow J[2] \longrightarrow J \xrightarrow{[2]} J \longrightarrow 0$$

where $J[2]$ is the 2-torsion of J. Applying Galois cohomology to the above short exact sequence gives the following commutative diagram with exact rows.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & J(\mathbb{Q})/2J(\mathbb{Q}) & \longrightarrow & H^1(\mathbb{Q}, J[2]) & \longrightarrow & H^1(\mathbb{Q}, J)[2] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \prod_v \mathrm{res}_v} & \searrow^{\psi} & \downarrow{\scriptstyle \prod_v \mathrm{res}_v} & & \\
0 & \longrightarrow & \prod_v J(\mathbb{Q}_v)/2J(\mathbb{Q}_v) & \longrightarrow & \prod_v H^1(\mathbb{Q}_v, J[2]) & \longrightarrow & \prod_v H^1(\mathbb{Q}_v, J)[2] & \longrightarrow & 0
\end{array}$$

Above, the products are taken over all places of $\mathbb{Q}$.

If we could compute the kernel of the map $H^1(\mathbb{Q}, J[2]) \to H^1(\mathbb{Q}, J)[2]$ we would know the structure of $J(\mathbb{Q})/2J(\mathbb{Q})$. Unfortunately, it is not obvious how to do this, so instead, we define the following two groups

$$\mathrm{Sel}^{(2)}(\mathbb{Q}, J) = \ker \psi$$

$$Ш(\mathbb{Q}, J) = \ker \left(\prod_v \mathrm{res}_v : H^1(\mathbb{Q}, J) \to \prod_v H^1(\mathbb{Q}_v, J) \right)$$

The group $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$, is known as the *2-Selmer group*. This gives us the following short exact sequence.

$$0 \longrightarrow J(\mathbb{Q})/2J(\mathbb{Q}) \longrightarrow \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \longrightarrow Ш(\mathbb{Q}, J)[2] \longrightarrow 0$$

Using this sequence we can get a formula that involves the rank of $J(\mathbb{Q})$ and the $\mathbb{F}_2$-dimensions of the other groups that we defined.

$$\mathrm{rank}\, J(\mathbb{Q}) + \dim_{\mathbb{F}_2} J(\mathbb{Q})[2] + \dim_{\mathbb{F}_2} Ш(\mathbb{Q}, J)[2] = \dim_{\mathbb{F}_2} \mathrm{Sel}^{(2)}(\mathbb{Q}, J). \tag{8.1.1}$$

Using equation (8.1.1), we get the following computable upper bound on the rank

$$\mathrm{rank}\, J(\mathbb{Q}) \leq \dim_{\mathbb{F}_2} \mathrm{Sel}^{(2)}(\mathbb{Q}, J) - \dim_{\mathbb{F}_2} J(\mathbb{Q})[2]. \tag{8.1.2}$$

In order to calculate this upper bound we must compute the dimension of $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$. If it turns out that this bound is not sharp, which frequently happens, one would need to compute $Ш(\mathbb{Q}, J)[2]$. This is very subtle a task that lies outside of the scope of

this paper. The interested reader should consult either [Sto] or [Sil09] to read about computing $Ш(\mathbb{Q}, J)[2]$ or $Ш(\mathbb{Q}, J)$ in the case that X is elliptic or hyperelliptic.

8.2 The Two-Descent Procedure

The notation that we use in this section will follow that set out in [Sto]. Throughout the rest of this section we will focus on computing the dimension of the 2-Selmer group of the jacobian of a smooth projective curve given by an affine equation of the form

$$y^2 = f(x),$$

where f is squarefree and $\deg(f) = 6$. In this case, our curve is hyperelliptic of genus $g = 2$ with two points at infinity in the projective closure. Before we can compute the dimension of the 2-Selmer group, we must define a few objects of interest and examine some of their properties.

Remark 8.2.1. Almost all of what we do here will go through for $\deg(f) \geq 6$ with $\deg(f)$ even. We simply limit ourselves to this case for the sake of making this section cleaner. In fact, [PS97] considered the more general case of an equation of the form $y^p = f(x)$ with p a prime dividing $\deg(f)$. This is actually more difficult than the case when p does not divide $\deg(f)$.

Definition 8.2.2. For any field extension K of $\mathbb{Q}$, let $L_K = K[T]/(f(T))$ denote the algebra defined by f and N_K denote the norm map from L_K down to K.

Remark 8.2.3. We can denote $L_K = K[\theta]$, where θ is the image of T under the

reduction map $K[T] \to K[T]/(f(T))$, and L_K is a product of finite extensions of K:

$$L_K = L_{K,1} \times \cdots \times L_{K,m_K},$$

where m_K is the number of irreducible factors of $f(x)$ in $K[x]$. Here, the fields $L_{K,j}$ correspond to the irreducible factors of $f(x)$ in $K[x]$. Here $N_K : L_K \to K$ is just the product of the norms on each component. That is if $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_{m_K})$, then $N_K(\alpha) = \prod_{i=1}^{m_K} N_{L_{K,i}/K}(\alpha_i)$ where $N_{L_{K,i}/K} : L_{K,i} \to K$ is the typical field norm.

When $K = \mathbb{Q}$ we will drop the subscripts altogether and if $K = \mathbb{Q}_p$, we will just use the subscript p. This convention will apply to anything that has a field as a subscript throughout the paper, e.g., $L_p = \mathbb{Q}_p[T]/(f(T))$ and $L = \mathbb{Q}[T]/(f(T))$.

We will let $\mathcal{O}_K$, $I(K)$, and $\mathrm{Cl}(K)$ denote the ring of integers of K, the group of fractional ideals, and the ideal class group of K, respectively. We would like to define analogous objects for the algebra L_K, and we do so in the most natural way:

$$\begin{aligned}
\mathcal{O}_{L_K} &= \mathcal{O}_{L_{K,1}} \times \cdots \times \mathcal{O}_{L_{K,m_K}}, \\
I(L_K) &= I(L_{K,1}) \times \cdots \times I(L_{K,m_K}), \\
\mathrm{Cl}(L_K) &= \mathrm{Cl}(L_{K,1}) \times \cdots \times \mathrm{Cl}(L_{K,m_K}).
\end{aligned}$$

Definition 8.2.4. Let $I_p(L)$ denote the subgroup of $I(L)$ consisting of prime ideals in L with support above p a prime in $\mathbb{Q}$. For a finite set S of finite places, let

$$I_S(L) = \prod_{p \in S \smallsetminus \infty} I_p(L).$$

Definition 8.2.5. For any field extension K of $\mathbb{Q}$, let

$$H_K = \ker\left(N_K : L_K^\times/(L_K^\times)^2K^\times \to K^\times/(K^\times)^2\right).$$

For any place, v, of $\mathbb{Q}$, we let $\mathrm{res}_v : H \to H_v$ be the map induced by the natural inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_v$.

Remark 8.2.6. Notice that the norm map is well defined on $L_K^\times/(L_K^\times)^2K^\times$. Since the $\deg(f)$ is even, the dimension of L_K/K is even and $N(x) = x^{\deg(f)}$ is a square in K for all $x \in K$.

Definition 8.2.7. Let $\mathrm{Div}^\times(C)$ denote the group of degree-zero divisors on C with support disjoint from the principal divisor $\mathrm{div}(y)$.

Theorem 8.2.8. [CF96, Chapter 11] *For every K we get a homomorphism*

$$F_K : \mathrm{Div}^\times(C)(K) \to L_K^\times, \quad \sum_P n_P P \mapsto \prod_P (x(P) - \theta)^{n_p},$$

which induces a homomorphism

$$\delta_K : J(K) \to H_K.$$

Definition 8.2.9. Let

$$\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J) = \{\xi \in H : \mathrm{res}_v(\xi) \in \delta_v(J(\mathbb{Q}_v)) \text{ for all places } v\}.$$

We will call this group the fake 2-Selmer group.

The relationship between the fake 2-Selmer and the 2-Selmer group will be ad-

dressed in Corollary 8.2.22.

Remark 8.2.10. If we use this definition for $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J)$, in order to check if $\xi \in H$ is in $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J)$ we have to check that $\mathrm{res}_v(\xi) \in \delta_v(J(\mathbb{Q}_v))$ for ALL places v. In order to make this definition more tractable, we will need the following definition and proposition.

Definition 8.2.11. Let K be a finitely ramified algebraic extension of $\mathbb{Q}_p$ with maximal ideal $\mathfrak{p}_K$. We let $I_{\mathfrak{p}_K}(L_K)$ be the group of ideals in L_K and

$$I_K = \ker\left(N : I_{\mathfrak{p}_K}(L_K)^2/I_{\mathfrak{p}_K}(L_K)I_{\mathfrak{p}_K}(K) \to I_{\mathfrak{p}_K}(K)/I_{\mathfrak{p}_K}(K)^2\right).$$

For all primes p in $\mathbb{Q}$, let

$$I_p = \ker\left(N : I_p(L)/(I_p(L))^2 I_p(\mathbb{Q}) \to I_p(\mathbb{Q})/(I_p(\mathbb{Q}))^2\right).$$

We also have maps $\mathrm{val}_p : H_p \to I_p$. These maps, taken together, give us a map $\mathrm{val} : H \subset L^\times/(L^\times)^2 \to I(L)/(I(L))^2 I(\mathbb{Q})$. We denote $\widetilde{\mathrm{val}}$ the canonical map $L^\times/(L^\times)^2 \to I(L)/(I(L))^2$.

Remark 8.2.12. The notation I_p is not breaking with the subscript convention that we established at the beginning of this section since I_p is naturally isomorphic to $I_{\mathbb{Q}_p} = \ker\left(N : I_p(L_p)/I_p(L_p)^2 I_p(\mathbb{Q}) \to I_p(\mathbb{Q}_p)/I_p(\mathbb{Q}_p)^2\right)$.

Proposition 8.2.13. [Sto, Proposition 5.10] *If* $p \notin S = \{\infty, 2\} \cup \{p : p^2 | \operatorname{disc}(f)\}$, *then*

$$J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) \xrightarrow{\delta_p} H_p \xrightarrow{\mathrm{val}_p} I_p \longrightarrow 0$$

is exact.

Proposition 8.2.14. *If* $S = \{\infty, 2\} \cup \{p : p^2 | \operatorname{disc}(f)\}$

$$\operatorname{Sel}^{(2)}_{\text{fake}}(\mathbb{Q}, J) = \{\xi \in H : \operatorname{val}(\xi) \in I_S(L)/I_S(L)^2 I(\mathbb{Q}), \\ \textit{and } \operatorname{res}_v(\xi) \in \delta_v(J(\mathbb{Q}_v)) \textit{ for } v \in S\}.$$

Proof: Since

$$J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) \xrightarrow{\delta_p} H_p \xrightarrow{\operatorname{val}_p} I_p \longrightarrow 0$$

is exact for $p \notin S$, we know that $\operatorname{res}_p(\xi) \in \delta_p(J(\mathbb{Q}_p))$ if and only if $\operatorname{val}_p(\operatorname{res}_p(\xi))$ is the trivial class for $p \notin S$. Each $\xi \in L^\times/(L^\times)^2\mathbb{Q}^\times$ has a squarefree representative β in $\mathcal{O}_L$. Fix $\xi = [\beta] \in H \subseteq L^\times/(L^\times)^2\mathbb{Q}^\times$ with β normalized to be a squarefree element of $\mathcal{O}_L$. Using the fact that for $\xi = [\beta] \in H$, $\operatorname{res}_p(\xi) \in \delta_p$ if and only if $[(\beta)] = [(1)] \in I_p$. Using this we can rewrite Definition 8.2.9 as

$$\begin{aligned}
\operatorname{Sel}^{(2)}_{\text{fake}} &= \{\xi \in H : \operatorname{res}_v(\xi) \in \delta_v(J(\mathbb{Q}_v)) \text{ for all places } v\} \\
&= \{\xi \in H : \operatorname{val}_p(\operatorname{res}_v(\xi)) = [(1)] \text{ for } p \notin S, \text{ and } \operatorname{res}_v(\xi) \in \delta_v(J(\mathbb{Q}_v)) \text{ for } v \in S\} \\
&= \{\xi \in H : \operatorname{val}(\xi) \in I_S(L)/I_S(L)^2 I_S(\mathbb{Q}), \text{ and } \operatorname{res}_v(\xi) \in \delta_v(J(\mathbb{Q}_v)) \text{ for } v \in S\}.
\end{aligned}$$

■

Before exploring the relationship between $\operatorname{Sel}^{(2)}(\mathbb{Q}, J)$ and $\operatorname{Sel}^{(2)}_{\text{fake}}(\mathbb{Q}, J)$, we need to figure out when the kernel of δ is exactly $2J(\mathbb{Q})$.

Definition 8.2.15. We say that K satisfies condition (‡), if either of the following occurs:

(‡.a) $f(x)$ has a factor of odd degree in $K[x]$, or

(‡.b) f factors as $h\bar{h}$ over a quadratic extension K' of K, where $\bar{h}$ is the $\mathrm{Gal}(K'/K)$-conjugate of h.

Remark 8.2.16. Condition (‡.b) is equivalent to L_K containing a quadratic extension of K.

Lemma 8.2.17. [PS97, Theorem 11.2] *The kernel of δ_K is $2J(K)$ if K satisfies condition (‡), or if there is no K-rational divisor class of degree 1 on C. Otherwise, $2J(K)$ has index two in $\ker(\delta_K)$.*

Lemma 8.2.18. [Sto, Lemma 5.2] *Condition (‡) is satisfied in each of the following situations.*

1. *$K = \mathbb{R}$*
2. *K is a p-adic field, and the irreducible factors of f in $K[x]$ all define unramified extensions of K.*

Lemma 8.2.19. [Sto, Lemma 5.3] *Write $f(x) = \prod_{j=1}^{6}(x - \alpha_j)$, and let*

$$h(f) = \prod_{\sigma}(x - (\alpha_{\sigma(1)}\alpha_{\sigma(2)}\alpha_{\sigma(3)} + \alpha_{\sigma(4)}\alpha_{\sigma(5)}\alpha_{\sigma(6)})),$$

where the product is over left coset representative $\sigma \in S_6$ modulo the stabilizer of the partition $\{\{1,2,3\},\{4,5,6\}\}$. Then $h(f)$ has degree 10.

1. *For $a \in K$, (‡.b) holds for f if and only if it holds for $f(x+a)$.*
2. *If $h(f)$ has a simple root in K, then K satisfies (‡.b).*
3. *If $h(f)$ has no root in K, then K does not satisfy (‡.b).*

4. There are at most 45 values of $a \in K$ such that $h(f(x+a))$ is not squarefree.

Now, we answer the question about the relationship between $\mathrm{Sel}^{(2)}(K,J)$ and $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(K,J)$ with the following theorem.

Theorem 8.2.20. [PS97, Theorem 13.2] *There is an exact sequence*

$$\mu_2(K) \xrightarrow{\phi} \mathrm{Sel}^{(2)}(K,J) \xrightarrow{\epsilon} \mathrm{Sel}^{(2)}_{\mathrm{fake}}(K,J) \longrightarrow 0.$$

Moreover, the image of ϕ is trivial in $\mathrm{Sel}^{(2)}(K,J)$ if and only if K satisfies (‡).

Remark 8.2.21. Here the map ϵ is a map that is closely related to a generalization of the Weil pairing defined on $J[2] \times J[2]$. The map ϕ is the connecting homomorphism on the Galois cohomology groups induced from the short exact sequence

$$0 \longrightarrow J[2] \xrightarrow{\epsilon} \mu_2(L_{\overline{K}})/\mu_2(\overline{K}) \xrightarrow{\mathrm{Norm}} \mu_2(\overline{K}) \longrightarrow 0.$$

We use ϕ here only because δ has already been defined. We think of $\mu_2(\overline{K})$ living inside of $\mu_2(L_{\overline{K}})$ diagonally.

Corollary 8.2.22. *The relationship between the dimensions of $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(K,J)$ and $\mathrm{Sel}^{(2)}(K,J)$ is as follows:*

$$\dim_{\mathbb{F}_2} \mathrm{Sel}^{(2)}(K,J) = \begin{cases} \dim_{\mathbb{F}_2} \mathrm{Sel}^{(2)}_{\mathrm{fake}}(K,J) & \text{if } K \text{ satisfies (‡)} \\ \dim_{\mathbb{F}_2} \mathrm{Sel}^{(2)}_{\mathrm{fake}}(K,J) + 1 & \text{otherwise} \end{cases}$$

Now that we have the relationship between $\dim \mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q},J)$ and $\dim \mathrm{Sel}^{(2)}(\mathbb{Q},J)$, we need to compute $\dim \mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q},J)$. To make this possible we need to be able to

compute the image of δ_K for various K. To do this, we will use a theorem that tells us what the images of some specific divisors are.

Theorem 8.2.23. [PS97] *Let K be a field extension of $\mathbb{Q}$.*

1. *Suppose that the points $\infty_\pm$ at infinity on C are K-rational. Then for a point $P \in C(K)$ not in the support of $\mathrm{div}(y)$, we have $\delta_K(P - \infty_\pm) = x(P) - \theta \bmod (L_K^\times)^2 K^\times$.*

2. *To every monic polynomial $h \in K[x]$ of even degree such that h divides f, we can associate an element $P_h \in J(K)[2]$ such that:*

   (a) *The P_h generate $J(K)[2]$ and satisfy $\sum_j P_j = 0$, if $\prod_j h_j = f$.*

   (b) *Let $\widetilde{h}$ be the polynomial such that $f = h\widetilde{h}$. Then $\delta_K(P_h) = h(\theta) - \widetilde{h}(\theta) \bmod (L_K^\times)^2 K^\times$.*

3. *$\dim J(K)[2] = m_K - 1$, if all irreducible factors of f over K have even degree, and $\dim J(K)[2] = m_K - 2$ otherwise.*

Now that we know what the images of these divisors are, we want to compute the dimensions of these $\mathbb{F}_2$-vector spaces. This way, we can compute the images of "enough" divisors until we have a basis. To make things a little easier we define the following quantities:

Definition 8.2.24. For any field extension K of $\mathbb{Q}$, let:

- $t_K = 0$ if all the factors of f in $K[x]$ have even degree, and $t_K = 1$ otherwise,
- $u_K = 0$ if there is a quadratic extension of K contained in L_K, and $u_K = 1$ otherwise.

For a p-adic field K, let:

- Let $r_K = 0$ if all ramification indices of the field extensions $L_{K,j}/K$ are even, and $r_K = 1$ otherwise,
- Let $s_K = 0$ if all the residue class degrees of the field extensions $L_{K,j}/K$ are even and $s_k = 1$ otherwise,
- Let $d_K = [K : \mathbb{Q}_2]$ if $p = 2$ and $d_K = 0$ if p is odd.

With these definitions we can now compute the dimensions of most of the local groups we are interested in.

Lemma 8.2.25. [Sto, Lemma 5.7] *Let K be a p-adic field. Then*

1. $\dim J(K)/2J(K) = \dim J(K)[2] + d_K g = m_K - 1 - t_K + d_K \cdot g$.
2. $\dim I_K = m_K - r_K - s_K$.
3. $\dim H_K = 2 \dim I_K$ *if p is odd.*
4. *If p is odd and $r_K = 1$, then* $\mathrm{val}_p : H_p \to I_p$ *is onto.*

The last thing we need is to compute the dimensions of some of these same spaces over $\mathbb{R}$.

Lemma 8.2.26. [Sto, Lemma 4.8]

1. $\dim J(\mathbb{R})/2J(\mathbb{R}) = \dim \delta_\infty(J(\mathbb{R})) = \dim J(\mathbb{R})[2] - g$
2. $\delta_\infty(J(\mathbb{R}))$ *is generated by* $\delta_\infty(P + Q - \infty_+ - \infty_-)$ *with* $P, Q \in C(\mathbb{R})$, *and* $\delta_\infty(P + Q - \infty_+ - \infty_-)$ *only depends on the connected components of* $C(\mathbb{R})$ *contacting P and Q. Here $\infty_\pm$ are the two points at infinity on C.*

We have now translated the question of finding the dimension of $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ to finding the dimension of $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J)$, a finite subspace of $L^\times/(L^\times)^2\mathbb{Q}$. In order to compute $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J)$ as a finite subspace of $L^\times/(L^\times)^2\mathbb{Q}^\times$, we consider the following diagram. We want to define Ker, Sel_1, and Sel_2 so that the top and bottom row of the diagram become exact.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Ker} & \longrightarrow & \mathrm{Sel}_2 & \longrightarrow & \mathrm{Sel}_1 & \longrightarrow & \mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J) \longrightarrow 1 \\ & & \| & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & \mathrm{Ker} & \longrightarrow & \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 & \longrightarrow & L^\times/(L^\times)^2 & \longrightarrow & L^\times/(L^\times)^2\mathbb{Q}^\times \longrightarrow 1 \end{array} \tag{8.2.1}$$

In order for the bottom row to be exact, clearly we need

$$\mathrm{Ker} = \{d \in \mathbb{Q} : \sqrt{d} \in L^\times\}.$$

So now we need to find finite subgroups, Sel_1 and Sel_2, of $L^\times/(L^\times)^2$ and $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, respectively, that makes the top row of the diagram exact.

To determine exactly what Sel_1 and Sel_2 are, we need the following proposition:

Proposition 8.2.27. *Let G_p be the image of $J(\mathbb{Q}_p)$ in I_p (i.e. $G_p = \mathrm{val}_p \circ \delta_p(J(\mathbb{Q}_p))$). Recall that $r_p = 0$ if and only if all the fields $L_{p,j}$ have even ramification index. Let Sel_2 be the span in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ of $\{-1\} \cup S'$, where*

$$S' = \{p : \ r_p = 0 \text{ or } G_p \neq \{1\}\}.$$

Define

$$\widetilde{H} = \{\xi \in L^\times/(L^\times)^2 : \widetilde{\mathrm{val}}(\xi) \in I_{S'}(L)/I_{S'}(L)^2 \text{ and } \mathrm{val}_p(\xi) \in G_p \text{ for all } p \in S'\}$$

where $\widetilde{\mathrm{val}}_v$ *is the canonical map from* $L^\times/(L^\times)^2$ *to* $I(L)/I(L)^2$*. Then* $\widetilde{H}$ *is finite. Let* $S = S' \cup \{\infty, 2\}$ *and set*

$$\mathrm{Sel}_1 = \{\xi \in \widetilde{H} : \ \mathrm{res}_v(\xi) \in \delta_v(J(\mathbb{Q}_v)) \text{ for all } v \in S\}.$$

Then with these definitions of Sel_1 *and* Sel_2*, the top row of diagram (8.2.1) is exact.*

PROOF: For finiteness of $\widetilde{H}$ see [Sto, Lemma 4.9]

If p is a prime outside of S', then $G_p = 0$. This implies that $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J)$ is contained in

$$H' = \{L^\times/(L^\times)^2\mathbb{Q}^\times : \mathrm{val}(\xi) \in I_{S'}(L)/I_{S'}(L)^2 I_{S'}(Q), \ \mathrm{val}_p(\xi) \in G_p \text{ for all } p \in S'\}.$$

If p is odd and $r_p = 1$, we have that $\dim H_p = \dim \delta_p(J(\mathbb{Q}_p)) + \dim I_p$. We also have that $\mathrm{val}_p : H_p \to I_p$ is onto. Therefore, if $G_p = 0$, then $\delta_p(J(\mathbb{Q}_p)) = \ker \mathrm{val}_p$. Thus we have

$$\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J) = \{\xi \in H' : \ res_v(\xi) \in \delta_v(J(\mathbb{Q}_v)) \text{ for all } v \in S\}.$$

Since $\mathbb{Q}$ has trivial class gropup, $\widetilde{H}$ surjects onto H', and by definition Sel_1 is the inverse image of $\mathrm{Sel}^{(2)}_{\mathrm{fake}}$ in $\widetilde{H}$. The kernel of $\widetilde{H} \twoheadrightarrow H'$ is the intersection of $\widetilde{H}$ with the image of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ in $L^\times/(L^\times)^2$, which is easily seen to be Sel_2. ∎

With all of this, we finally have enough information to compute $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J)$ and $\dim_{\mathbb{F}_2} \mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ for a specific $f(x)$.

8.3 Explicit Computations

Now that we have laid the foundation we are ready to perform a 2-descent. The curve we will be working with is given by the affine equation

$$C : y^2 = f(x) = x^6 - 6x^5 + 11x^4 - 8x^3 + 11x^2 - 6x + 1.$$

In the projective closure, this curve has two points at infinity, call them $\infty_{\pm}$. Using SAGE, we compute $\mathrm{disc}(f) = -1 \cdot 2^{20} \cdot 11^3$ and that $f(x)$ is irreducible over $\mathbb{Q}$. We let $S = \{p : p^2 | \, \mathrm{disc}(f)\} \cup \{2, \infty\} = \{\infty, 2, 11\}$ and compute all of the basic information about the local groups associated to these places.

Using SAGE we can factor $f(x)$ over $\mathbb{Q}_p[x]$ to get the following table:

p	m_p	t_p	u_p	r_p	s_p	d_p
2	1	0	0	0	1	1
11	2	0	0	1	1	0
∞	3	–	–	–	–	–

From the information above and Lemmas 8.2.25 and 8.2.26 we have the following:

p	$\dim J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$	$\dim \delta_p(J(\mathbb{Q}_p))$	$\dim H_p$	$\dim I_p$
2	2	2	?	0
11	1	0	0	0
∞	0	0	–	–

Remark 8.3.1. Lemma 8.2.25 doesn't give us a formula for $\dim H_2$. We could compute it directly, but we will postpone its computation for now as we will need to compute all of H_2 later in the paper.

Next we use SAGE to compute $h(f)$ as in Lemma 8.2.19 in our case and we get

$$h(f) = x^{10}-7x^9+76x^8-696x^7+2800x^6-3328x^5-4464x^4+8256x^3+3712x^2-1280x-512.$$

Reducing $h(f)$ mod 17 we get

$$x^{10} + 10x^9 + 8x^8 + x^7 + 12x^6 + 4x^5 + 7x^4 + 11x^3 + 6x^2 + 12x + 15,$$

which is irreducible in $\mathbb{F}_{17}$. Thus we know that $h(f)$ is irreducible in $\mathbb{Q}[x]$ and so Lemma 8.2.19 tells us that in our case $\mathbb{Q}$ does not satisfy (‡). So, by Corollary 8.2.22, we have that

$$\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) = \dim \mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J) + 1,$$

and we now turn our attention to determining the dimension of $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J)$.

The first step to computing the dimension of $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J)$ is to find the subgroups Sel_1 and Sel_2 from Proposition 8.2.27. To do this we start by computing $\widetilde{H}$. Recall

that

$$\widetilde{H} = \{\xi \in L^\times/(L^\times)^2 : \widetilde{\mathrm{val}}(\xi) \in I_{S'}(L)/I_{S'}(L)^2 \text{ and } \mathrm{val}_p(\xi) \in G_p \text{ for all } p \in S'\}$$

where $S' = \{p : r_p = 0 \text{ or } G_p \neq \{1\}\}$. In this case we can see that we have that $S' = \{2\}$. Using SAGE, we find that the class number of L is one and that the prime factorization of the ideal $2\mathcal{O}_L = \mathfrak{p}_2^6 = (\beta_2)^6$.

This means that $I_{S'}/I_{S'}(L)^2 = \{[(1)], [(\beta_2)]\}$, and so ξ is in $\widetilde{H}$ only if it is equivalent modulo $(L^\times)^2$ to either a unit, or a unit multiple of β_2. Since G_2 is a subset of I_2, we only need to check if $\mathrm{val}_2(\beta_2)$ is in G_2. The table above gives us that $G_2 = \{[(1)]\}$ since it is a subgroup of $I_2 = \{[(1)]\}$. Therefore, we know that $\mathrm{val}_2(\beta_2)$ is not in G_2, since $[(\beta_2)] \neq [(1)]$. Hence the only classes modulo squares in $\widetilde{H}$ correspond to ones that are represented by units.

To find representatives of these classes we simply compute the fundamental units of L. Using SAGE, we find that $r_1 = 0$ and $r_2 = 3$ and so by Dirchlet's unit theorem we know that there are $r_1 + r_2 - 1 = 2$ fundamental units. Again using SAGE, one can check that the only roots of unity in L are ± 1. Therefore,

$$\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2 = \langle -1, u_1, u_2 \rangle$$

where

$$u_1 = \frac{53}{6455}\theta^5 - \frac{1334}{6455}\theta^4 + \frac{1729}{1291}\theta^3 + \frac{70491}{6455}\theta^2 + \frac{92264}{6455}\theta + \frac{4485}{1291},$$
$$u_2 = \frac{843}{71005}\theta^5 - \frac{21072}{71005}\theta^4 + \frac{132243}{71005}\theta^3 + \frac{238525}{14201}\theta^2 + \frac{1200429}{71005}\theta + \frac{235233}{71005}.$$

Recall that θ is the image of T under the map $K[T] \to K[T]/(f(T))$.

Before moving on we notice that with u_1 and u_2 defined as above, $2 = -u_1u_2\beta_2^6$ and so $2 \equiv -u_1u_2 \bmod (L^\times)^2$. Thus, $\widetilde{H} = \langle -1, u_1, u_2\rangle = \langle -1, 2, u_1\rangle$. Here we are suppressing the equivalence class notation to make things cleaner. From the work we did in the last section and to compute the tables at the beginning of the section, we know that $\mathrm{Sel}_2 = \langle -1, 2\rangle$ and since L does not satisfy (‡) we know that Ker $= \{1\}$. But using the fact that

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \langle -1, 2\rangle & \longrightarrow & \mathrm{Sel}_1 & \longrightarrow & \mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & & & \langle -1, 2, u_1\rangle & & & & \\
 & & & & \downarrow & & & & \\
1 & \longrightarrow & \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 & \longrightarrow & L^\times/(L^\times)^2 & \longrightarrow & L^\times/(L^\times)^2\mathbb{Q}^\times & \longrightarrow & 1
\end{array}$$

has exact rows, we know that $\mathrm{Sel}_1 \supseteq \langle -1, 2\rangle$. So the question becomes, is u_1 in Sel_1? From Proposition 8.2.27, this question amounts to checking if $\mathrm{res}_v(u_1) \in \delta_v(J(\mathbb{Q}_v))$ for all $v \in S$, where $S = \{2, 11, \infty\}$. We start by checking if $\mathrm{res}_2(u_1)$ is in $\delta_2(J(\mathbb{Q}_2))$ and hope that, in fact, $\mathrm{res}_2(u_1) \notin \delta_2(J(\mathbb{Q}_2))$, and therefore we are done.

In order to do this, we need to find explicit generators for $\delta_2(J(\mathbb{Q}_2))$. From the table above we know that $\dim \delta_2(J(\mathbb{Q}_2)) = 2$, so we just start looking for points $P \in C(\mathbb{Q}_2)$ and using Theorem 8.2.23 to compute the images of $P - \infty_+$ under δ_2.

Lemma 8.3.2. *For $f(x) = x^5 - 6x^5 + 11x^4 - 8x^8 + 11x^2 - 6x + 1$, the field $\mathbb{Q}_2$ does not satisfy* (‡).

PROOF: To prove this we just need to show that

$$h(f) = x^{10} + 10x^9 + 8x^8 + x^7 + 12x^6 + 4x^5 + 7x^4 + 11x^3 + 6x^2 + 12x + 15,$$

does not have a simple root in $\mathbb{Q}_2$. First, notice that since $h(f)$ is a monic polynomial, if it has a root in $\mathbb{Q}_2$, that root has to be in $\mathbb{Z}_2$. Next, if $h(f)$ has a root in $\mathbb{Z}_2$, then of course that root will reduce to a root in $\mathbb{F}_2$. So to show that $h(f)$ doesn't have a root in $\mathbb{Q}_2$ it is sufficient to show that the reduction of $h(f)$ modulo 2 doesn't have a root in $\mathbb{F}_2$. The reduction of $h(f)$ modulo 2 is

$$\overline{h(f)} = x^{10} + x^7 + x^4 + x^3 + 1.$$

Clearly zero isn't a root of $\overline{h(f)}$, and a quick check shows that one isn't a root of $\overline{h(f)}$ as well. Therefore since $\overline{h(f)}$ doesn't have a root in $\mathbb{F}_2$, we know that $h(f)$ doesn't have a root in $\mathbb{Q}_2$. ■

Lemma 8.3.3. *Two elements, a and b, in $L_2^\times$ are congruent modulo $(L_2^\times)^2\mathbb{Q}_2^\times$ if and only if there is an $r \in \mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 = \{\pm 1, \pm 2, \pm 5, \pm 10\}$ such that $\frac{a}{br}$ is a square in $L_2^\times$.*

PROOF: From Lemma 8.3.2 we know that L_2 does not contain a quadratic extension of $\mathbb{Q}_2$ and so we have the following exact sequence:

$$1 \longrightarrow \mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \xrightarrow{\psi} L_2^\times/(L_2^\times)^2 \xrightarrow{\phi} L_2^\times/(L_2^\times)^2\mathbb{Q}_2^\times \longrightarrow 1.$$

Therefore, $a \equiv b \bmod (L_2^\times)^2\mathbb{Q}_2^\times \Leftrightarrow \frac{a}{b} \equiv 1 \bmod (L_2^\times)^2\mathbb{Q}_2^\times$ if and only if $\frac{a}{b}$ is in the kernel of ϕ. Since we know that the kernel of ϕ is $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 = \{\pm 1, \pm 2, \pm 5, \pm 10\}$, if we want to check if $a \equiv b \bmod (L_2^\times)^2\mathbb{Q}_2^\times$, it is sufficient to check if $\frac{a}{b} \equiv r \bmod (L^\times)^2$ for

all representatives r of $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 = \{\pm 1, \pm 2, \pm 5, \pm 10\}$. Another way to say this is that $a \equiv b\ (L_2^\times)^2\mathbb{Q}_2^\times$ if and only if there is an $r \in \{\pm 1, \pm 2, \pm 5, \pm 10\}$ such that $\frac{a}{rb}$ is a square in $L_2^\times$. ■

Lemma 8.3.3 gives us an easy way to check if two elements are congruent modulo $(L_2^\times)^2\mathbb{Q}_2$ since Magma has a built in command that checks if an element of a field is a square or not. so we can check these equivalencies in Magma quite easily.

First, using Hensel's lemma, we can find that $P_1 = (2, 72512802334441 + O(2^{49}))$ is a point on $C(\mathbb{Q}_2)$ and from Theorem 8.2.23, we know that $\delta_2(P_1 - \infty_+) = 2 - \theta$. Using Lemma 8.3.3 we can check that $2 - \theta \not\equiv 1 \bmod (L_2^\times)^2\mathbb{Q}_2^\times$. Therefore, we only need to find one more non-trivial element in $\delta_2(J(\mathbb{Q}_2))$ that is not equivalent to $2-\theta \bmod (L_2^\times)^2\mathbb{Q}_2$. Next, we search for points on $C(\mathbb{Q}_2)$ using Magma and find that $P_2 = (151123620125253 \cdot 2 + O(2^{50}), 1)$ is also a point on $C(\mathbb{Q}_2)$ and $\delta_2(P_2 - \infty_+) = \alpha - \theta$ where $\alpha = 151123620125253 \cdot 2 + O(2^{50})$. We just need to know if if that $2-\theta \equiv \alpha-\theta \bmod (L_2^\times)^2\mathbb{Q}_2^\times$. Again using Lemma 8.3.3, we check this in Magma. The code used to do these computations can be found in the appendix of this section.

Remark 8.3.4. Here we note that $\mathrm{div}(y) = \sum_{i=1}^{6}(0, \alpha_i)$ where the α_i's are the roots of $f(x)$. Therefore none of the points we found are in the support of $\mathrm{div}(y)$.

Fortunately, it turns out that $2 - \theta \not\equiv \alpha - \theta \bmod (L_2^\times)^2\mathbb{Q}_2$. Thus we have two independent elements in a 2-dimensional $\mathbb{F}_2$-vector space and so we have generators for $\delta_2(J(\mathbb{Q}_2))$. One can directly check in Magma, using the same method as in Lemma

8.3.3, if $\mathrm{res}_2(u_1)$ is in $\delta_2(J(\mathbb{Q}_2))$. A few calculations later we see that

$$\mathrm{res}_2(u_1) \not\equiv 2-\theta \bmod L^\times/(L^\times)^2\mathbb{Q}$$
$$\mathrm{res}_2(u_1) \not\equiv \alpha-\theta \bmod L^\times/(L^\times)^2\mathbb{Q}$$
$$\mathrm{res}_2(u_1) \not\equiv (2-\theta)(\alpha-\theta) \bmod L^\times/(L^\times)^2\mathbb{Q}.$$

Again, the details of this computation can be found in the appendix to this section.

Thus we have that $u_1 \notin \mathrm{Sel}_1$ and $\mathrm{Sel}_1 = \langle -1, 2\rangle$. Using the top row in diagram 8.2.1 we know that $\mathrm{Sel}_1 = \mathrm{Sel}_2 = \langle -1, 2\rangle$ and $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J) = \{1\}$. Combining this with proposition 8.2.22 and equation (9.4.2) we get that the rank of $J(\mathbb{Q})$ is less than or equal to one.

8.4 Generators of $J(X_s^+(11))(\mathbb{Q})$

The method we will use to compute the generators of $J(X_s^+(11))(\mathbb{Q})$ will require the use of Magma. The reason we are going to need Magma is that it is able to compute the heights of points on the jacobian of a hyperelliptic curves of genus two. The interested reader can find more details about heights on abelian varieties in [HS00]. The method that Magma uses to compute the heights of points on the Jacobian of hyperelliptic curves was developed in [FS97] and improved in [Sto99].

We start by defining C to be the curve $X_s^+(11)$ and J its jacobian.

```
> _<x> := PolynomialRing(Rationals());
> C := HyperellipticCurve(x^6-6*x^5+11*x^4-8*x^3+11*x^2-6*x+1);
> J := Jacobian(C);
```

Now that we have defined all of the necessary curves, we do a naive search for points with height less than 1000.

```
> ptsC := Points(C : Bound:=1000); ptsC;
{@ (1 : -1 : 0), (1 : 1 : 0), (0 : -1 : 1), (0 : 1 : 1),
(1 : -2 : 1), (1 : 2 : 1) @}
```

Proposition 8.4.1. *The rank of J is exactly one.*

PROOF: Since we know that the rank of J is either zero or one, we look for a point of infinite order on J by using the map from C to J given by $P \mapsto P - \infty_-$. The first point we check is $[\infty_+ - \infty_-]$. We define

```
> PJ := J! [ ptsC[2], ptsC[1] ];
> Order(PJ);
0
```

We confirm that this point has infinite order, by computing its height; recall that if it were a torsion point, it would have height zero.

```
> Height(PJ);
0.17957031232138090665260618033O
```

This tells us that $PJ = [\infty_+ - \infty_-]$ has infinite order and that the rank of J is actually one. ∎

Proposition 8.4.2. *The point $[\infty_+ - \infty_-]$ generates J/J_{tors}.*

PROOF: The problem is that we only know that the point PJ generates a subgroup of finite index in J/J_{tors}. In order to show that PJ generates all of J/J_{tors}, we need

to show that there is no point QJ on J and a positive integer $m \geq 2$ such that $[m]QJ = PJ$. To this end, we recall that if there was such a point QJ on J, it must have height less than the height of PJ (See [HS00]). With this in mind, we compute an upper bound for the height of QJ and do a search for points on J of height less than this bound.

```
> heightconst := HeightConstant(J : Effort:=2, Factor);
> LogarithmicBound := Height(PJ) + heightconst;
> AbsoluteBound := Ceiling(Exp(LogarithmicBound));
> PtsUpToAbsBound := RationalPoints(J : Bound:=AbsoluteBound );
```

Now that we have computed all of the points with height less than the height of PJ, we need to find a generators for this set. Since the set of points less than the absolute bound we computed is a finite set, this is a finite computation. In fact, it is a computation that Magma has built in.

```
> RB := ReducedBasis(PtsUpToAbsBound ); RB;
[ (x - 1, -x^3 + 3, 2) ]


[0.17957031232138090666526061803291]
```

Next, we let QJ be the point that generates the set of points up to our bound and check the height of $PJ - QJ$. If it is zero, then we know that PJ in fact generates all of J/J_{tors} because $PJ - QJ$ has finite order.

```
> QJ:=RB[1];
> Height(PJ-QJ);
0.00000000000000000000000000000000
```

■

Proposition 8.4.3. *The torsion subgroup of J is isomorphic to $\mathbb{Z}/5\mathbb{Z}$.*

PROOF: We start by computing the size of the image of reduction mod p for two primes of good reduction.

```
> print #Points(BaseChange(J, GF(5)));
45
> print #Points(BaseChange(J, GF(7)));
80
```

From Theorem 8.1.1, the first computations shows that the prime to 5 torsion must be a subgroup of a group of size 45. This means that if there is a point of order prime to 5, it must have order dividing 9. The second computation shows that the prime to 7 torsion must be the subgroup of a group of size 80. Therefore, we know that if there is any nontrivial torsion point, it must have order dividing a 5. ■

Next we look for a point of order 5. The difference now is that we are looking for a point on J with height zero that is not the identity, $\mathcal{O}$. Fortunately this isn't too hard. Letting $TJ = [T - \infty_-]$ where $T = (0 : -1 : 1)$.

```
TJ:=J! [ ptsC[3], ptsC[1] ];
> Height(TJ);
0.00000000000000000000000000000000
```

Now, we just check that $[5]TJ = \mathcal{O}$ and $TJ \neq \mathcal{O}$.

```
> 5*TJ;
(1, 0, 0)
```

```
> 5*TJ eq TJ;
false
```

Corollary 8.4.4.

$$J(X_s^+(11))(\mathbb{Q}) = \langle TJ, PJ \rangle \cong \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}.$$

8.5 Appendix: Magma Code

We start by noting that one cannot directly define L_2 as $\mathbb{Q}_2$ adjoin the root of $f(x)$. Magma can only create totally ramified extensions of $\mathbb{Q}_p$ by adjoining the root of a polynomial that is Eisenstein at p. So we must first find a polynomial that is Eisensten at 2 that generates the same extension of $\mathbb{Q}_2$. Then we define L_2 to be $\mathbb{Q}_2(\pi)$ where π is a root of the Eisenstein polynomial. Next we can define θ to be a root of $f(x)$ in $L_2 = \mathbb{Q}_2(\pi)$.

The following code checks that $\delta_2(J(\mathbb{Q}_2)) = \langle 2-\theta, \alpha-\theta \rangle$. For the sake of brevity we let `alpha1` $= 2-\theta$ and `alpha2` $= \alpha - \theta$, where $\alpha = 151123620125253 \cdot 2$.

```
> Q2 := pAdicField(2,100);
> _<x1> := PolynomialRing(Q2);
> L2<pi> := ext<Q2 | x1^6 - 28*x1^5 + 244*x1^4 + 594*x1^3 + 452*x1^2 +
> 134*x1 + 14>;
> _<x> :=PolynomialRing(Q2);
> f := x^6-6*x^5+11*x^4-8*x^3+11*x^2-6*x+1;
> f1 := x^6-6*x^5+11*x^4-8*x^3+11*x^2-6*x+1-1^2;
> R := Roots(f, L2);
```

```
> R1 := Roots(f1,Q2);
> theta1 := R[1][1];
> alpha1 := 2-theta1;
> alpha2 := R[2][1]-theta1;
> u1 := 53/6455*pi^5 - 1334/6455*pi^4 + 1729/1291*pi^3
   + 70491/6455*pi^2 + 92264/6455*pi + 4485/1291;
> S:=[1,-1,2,-2,5,-5,10,-10];
> R:=[alpha1,alpha2,alpha1*alpha2];
> for x in S do
>     for y in R do
>         if IsSquare(x*y) eq true then
>             x,y;
>             break;
>          end if;
>     end for;
> end for;
```

To check that u_1 is not in Sel_1 we only need to make a small change to our code:

```
> for x in S do
>     for y in R do
>         if IsSquare(u1*x*y) eq true then
>             x,y;
>             break;
>          end if;
>     end for;
```

```
> end for;
```

Since none of these subroutines returns anything, we know that the assertions made in section 8.3 are correct.

Chapter 9

An Application of the Method of Chabauty and Coleman

9.1 Introduction

The moduli space of elliptic curves that have Galois representation contained in the normalizer of a split cartan subgroup at 11 is the genus two hyperelliptic curve given by the affine equation

$$X_s^+(11) : y^2 = x^6 - 6x^5 + 11x^4 - 8x^3 + 11x^2 - 6x + 1.$$

A naive search for $\mathbb{Q}$-rational points on $X_s^+(11)$ only turns up the points $(1, \pm 2)$, $(0, \pm 1)$, and the two points at infinity.

In this chapter we aim to show that

$$X_s^+(11)(\mathbb{Q}) = \{(0, \pm 1), (1, \pm 2), \infty_\pm\}. \tag{9.1.1}$$

One of these points corresponds to a rational cusp, while the other five points correspond to elliptic curves with complex multiplication.

Theorem 9.1.1 (Faltings' Theorem)**.** *Let K be a number field and let C/K be a non-singular curve defined over K of genus $g \geq 2$. Then the set of K-rational points on C is finite.*

Faltings' theorem tells us that there can only be finitely many rational points on $X_s^+(11)$, but it does not give us any way to show that (9.1.1) includes *all* of the points. In 1941, Claude Chabauty proved the following weaker version of Faltings' theorem:

Theorem 9.1.2 (Chabauty's Theorem [Cha41])**.** *Let X be a curve of genus $g \geq 2$ over $\mathbb{Q}$. Let J be the jacobian of X. Let p be a prime, and let $r' = \dim_{\mathbb{Q}_p} \overline{J(\mathbb{Q})}$ where $\overline{J(\mathbb{Q})}$ is the closure of $J(\mathbb{Q})$ with the p-adic topology. Suppose $r' < g$. Then $X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ is finite.*

Corollary 9.1.3. *If X is as in Chabauty's theorem, then $X(\mathbb{Q})$ is finite.*

The corollary follows because $X(\mathbb{Q})$ is inside of $X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ and thus it must be finite as well.

Clearly, Chabauty's theorem is weaker than Faltings' as it requires the assumption that $r' < g$, which is not always true.

As they are stated, neither Faltings' theorem nor Chabauty's theorem is effective. In 1985 Robert Coleman was able to apply the theory of Newton polygons to Chabauty's theorem to come up with an explicit bound on the size of $X(\mathbb{Q})$ in the case when r' is less then the genus of X.

To apply Coleman's method and get an upper bound on the number of points on $X_s^+(\mathbb{Q})$, we will use the fact that the rank of the jacobian of $X_s^+(11)$ is one, which

is less than its genus which is two in this case. It will turn out that the most naive bound is not sharp, but we will use some extra structure to show that the points in (9.1.1) are the only ones.

9.2 The p-adic Lie group $J(\mathbb{Q}_p)$

Before we continue we need to recall some information about the jacobians of algebraic varieties. The interested reader can find a more in depth treatment of jacobians in [Lan83], [Mum70], or [HS00]. Throughout this section we will follow the basic structure setup in [MP]. At this point, we also also fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$.

Given an algebraic variety $X/\mathbb{Q}$ of genus g, one can embed X into an abelian variety, J, of dimension g called its jacobian. The jacobian can be given as the vanishing set of explicit polynomials with coefficients in $\mathbb{Q}$, but there is a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-equivariant isomorphism between the $\overline{\mathbb{Q}}$-rational points of the jacobian and the group of linear equivalence classes of degree zero divisors on $X_{\overline{\mathbb{Q}}}$. Therefore, elements of $J(\mathbb{Q})$ or $J(\overline{\mathbb{Q}})$ can be represented by formal combinations of points in $X(\overline{\mathbb{Q}})$. An element of $J(\overline{\mathbb{Q}})$ is in $J(\mathbb{Q})$ if it is fixed by the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Let $J_{\mathbb{Q}_p}$ denote the variety J, base extended to $\mathbb{Q}_p$, $H^0(J_{\mathbb{Q}_p}, \Omega^1)$ is the g-dimensional $\mathbb{Q}_p$-vector space of regular 1-forms on $J_{\mathbb{Q}_p}$. Suppose that $\omega_J \in H^0(J_{\mathbb{Q}_p}, \Omega^1)$. Using the translation invariance of ω_J, one can show that ω_J has an "antiderivative" given by

$$\begin{aligned} \eta_J : J(\mathbb{Q}_p) &\to \mathbb{Q}_p \\ Q &\mapsto \int_0^Q \omega_J. \end{aligned}$$

This "antiderivative" is characterized by the fact that η_J is a homomorphism and that

there exists an open set $U \subseteq J(\mathbb{Q}_p)$ such that if $Q \in U$, then $\int_0^Q \omega_J$ can be computed by writing ω_J as a power series in local coordinates. Further, one can take this open set to be $J^1(\mathbb{Q}_p)$, the kernel of the reduction map $J(\mathbb{Q}_p) \to J(\mathbb{F}_p)$.

Letting Q and ω_J vary, we get a bilinear pairing

$$\begin{aligned} J(\mathbb{Q}_p) \times H^0(J_{\mathbb{Q}_p}, \Omega^1) &\to \mathbb{Q}_p \\ (Q, \omega_J) &\mapsto \int_0^Q \omega_J. \end{aligned}$$

If T is the dual vector space of $H^0(J_{\mathbb{Q}_p}, \Omega^1)$, then we can define a map

$$\begin{aligned} \log : J(\mathbb{Q}_p) &\to T \\ Q &\mapsto \left[\omega_J \mapsto \int_0^Q \omega_J\right]. \end{aligned}$$

Now, the tangent space of the p-adic Lie group $J(\mathbb{Q}_p)$ at zero and T can be identified with each other. Using this identification and the fact that for Q near 0, $\int_0^Q \omega_J$ can be computed by expanding ω_J as a power series in local coordinates, one can see that the derivative of log at 0 is the identity map $T \to T$. Thus, we have that log is a diffeomorphism.

Using the natural injection, $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, we have that $J(\mathbb{Q})$ injects into $J(\mathbb{Q}_p)$. We let $\overline{J(\mathbb{Q})}$ denote the closure of $J(\mathbb{Q})$ in $J(\mathbb{Q}_p)$ with its p-adic topology. We know that $\overline{J(\mathbb{Q})}$ is an analytic subgroup of $J(\mathbb{Q}_p)$ and so it has a dimension as a p-adic manifold.

Lemma 9.2.1. *If $r' = \dim_{\mathbb{Q}_p} \overline{J(\mathbb{Q})}$ and $r = \operatorname{rank}_{\mathbb{Z}} J(\mathbb{Q})$, then $r' \leq r$.*

Proof: Since log is a differentiable isomorphism of manifolds, we know that $r' = \dim \overline{J(\mathbb{Q})} = \dim \log \overline{J(\mathbb{Q})}$. Now, since $\overline{J(\mathbb{Q})}$ is a closed subset of a compact space, it is also compact. Using the fact that log is continuous $\log\left(\overline{J(\mathbb{Q})}\right) = \overline{\log(J(\mathbb{Q}))}$. But the closure of a subgroup in $\mathbb{Q}_p^{\oplus g}$ is simply its $\mathbb{Z}_p$-span. Thus,

$$r' = \operatorname{rank}_{\mathbb{Z}_p}(\mathbb{Z}_p \log J(\mathbb{Q})) \leq \operatorname{rank}_{\mathbb{Z}} \log J(\mathbb{Q}) = \operatorname{rank}_{\mathbb{Z}} J(\mathbb{Q}) = r. \tag{9.2.1}$$

The last non-trivial equality in (9.2.1) follows because log has a finite kernel. ∎

9.3 Chabauty's Theorem and Coleman's Method

Throughout this section we will assume that p is a prime number and that the curve X has good reduction at p. This means that the jacobian of X, also has good reduction at p and the injection $X \hookrightarrow J$ induces a mapping on the reduction as well. We will use the notation $X(\mathbb{F}_p)$ to indicate the set of $\mathbb{F}_p$-points on X, the reduction of X.

In fact, the requirement that X has good reduction at p is not necessary, but for our purposes it is all that we need and makes things clearer.

Theorem 9.3.1. [Mil86, Proposition 2.2] *The restriction map*

$$H^0(J_{\mathbb{Q}_p}, \Omega^1) \to H^0(X_{\mathbb{Q}_p}, \Omega^1)$$

induced by the injection $X \hookrightarrow J$ is an isomorphism of $\mathbb{Q}_p$-vector spaces.

Suppose that $\omega_J \in H^0(J_{\mathbb{Q}_p}, \Omega^1)$ such that ω_J restricts to $\omega \in H^0(X_{\mathbb{Q}_p}, \Omega^1)$. For $Q, Q' \in X(\mathbb{Q}_p)$ we define

$$\int_Q^{Q'} \omega = \int_0^{[Q'-Q]} \omega_J.$$

Using all of the properties we saw in section 9.2 we obtain

1) If $Q_i, Q_i' \in X(\mathbb{Q}_p)$ are such that $\left[\sum (Q_i' - Q_i)\right] \in J(\mathbb{Q}_p)$ is a torsion element, then $\sum \int_{Q_i}^{Q_i'} \omega = 0$.

2) If $Q, Q' \in X(\mathbb{Q}_p)$ have the same reduction in $X(\mathbb{F}_p)$, then $\int_Q^{Q'} \omega$ can be calculated by expanding ω as a power series in local coordinates.

Now, we can define an "antiderivative" of ω by

$$\eta : X(\mathbb{Q}_p) \to \mathbb{Q}_p$$
$$Q \mapsto \int_O^Q \omega.$$

Recall that we have a surjection $X(\mathbb{Q}_p) \twoheadrightarrow X(\mathbb{F}_p)$. With this in mind we give the following definition:

Definition 9.3.2. The preimage of a point of $X(\mathbb{F}_p)$ will be called a *residue class.*

Fix a residue class, C, above point $\widetilde{Q} \in X(\mathbb{F}_p)$ and let t be a rational function on X that reduces to a uniformizer on $X_{\mathbb{F}_p}$ at Q. In [**?**] the author shows the following:

i) The function t maps the residue class bijectively to $p\mathbb{Z}_p$.

ii) If we assume that ω is normalized by an element of $\mathbb{Q}_p^\times$ so that it reduces to a nonzero element $\widetilde{\omega} \in H^0(X_{\mathbb{F}_p}, \Omega^1)$, then ω on the residue class can be expressed as $w(t)dt$ for some power series $w(t) \in \mathbb{Z}_p[\![t]\!]$ such that $w(t) \bmod p$ is nonzero.

iii) The function η on the residue class is represented by a power series $I(t) \in \mathbb{Q}_p[\![t]\!]$ whose derivative is $w(t)$.

Now, we want a lemma that is purely about counting zeros of functions that satisfy the properties that $I(t)$ satisfies.

Lemma 9.3.3. *Suppose that $f(t) \in \mathbb{Q}_p[\![t]\!]$ such that $f'(t) \in \mathbb{Z}_p[\![t]\!]$. Let $m = \mathrm{ord}_{t=0}(f'(t) \bmod p)$. If $m < p-2$, then f has at most $m+1$ zeros in $p\mathbb{Z}_p$.*

Proof: We follow the proof laid out in [MP, Section 5.3].

Let $\nu : \mathbb{Q}_p \to \mathbb{Z} \cup \{\infty\}$ be the p-adic valuation. Write $f(t) = \sum a_i t^i$. The conditions on $f'(t)$ and m imply that $\nu(a_{m+1}) = 0$ and $\nu(a_i) \geq -\nu(i) > m+1-i$ for $i > m+1$.

So the Newton polygon of f has no slopes less than or equal to -1 to the right of $(m+1, 0)$. So by the theory of Newton polygons laid out in [Kob84, IV.4], f has at most $m+1$ zeros in $p\mathbb{Z}_p$. ■

Remark 9.3.4. The bound in the lemma above can be improved by giving stronger conditions on $f(t)$, but these bounds are sufficient for our purposes. The interested reader should see [MP, Section 8]

The next step is to find a linear functional λ that vanishes on $\log \overline{J(\mathbb{Q})} \subseteq T$. Using the duality between T and $H^0(J_{\mathbb{Q}_p}, \Omega^1)$, every $\omega \in H^0(J_{\mathbb{Q}_p}, \Omega^1)$ corresponds to a unique linear functional $\lambda_\omega : T \to \mathbb{Q}_p$. To find a linear functional that vanishes on $\log \overline{J(\mathbb{Q})}$, we simply need to find an appropriate holomorphic 1-form.

Clearly, we have an injection $\overline{J(\mathbb{Q})} \hookrightarrow J(\mathbb{Q}_p)$ and this injection induces a surjection $H^0(J(\mathbb{Q}_p), \Omega^1) \twoheadrightarrow H^0(\overline{J(\mathbb{Q})}, \Omega^1)$ via the restriction map. We know that $H^0(\overline{J(\mathbb{Q})}, \Omega^1)$ is at most an r' dimensional subspace of the g dimensional vector space of $H^0(J(\mathbb{Q}_p), \Omega^1)$. Hence, $\dim(\ker(\text{res})) \geq g - r'$, and so we know that the kernel of the restriction map is non-trivial when $r' < g$. In this case, we fix any non-trivial ω_J in the kernel of the restriction map and see that its corresponding linear functional on T must vanish on $\log \overline{J(\mathbb{Q})}$. From the above work, ω_J gives rise to corresponding η_J, ω, and η as before; but, by the definition of log, we know $\eta_J = \lambda_{\omega_J} \circ \log : J(\mathbb{Q}_p) \to T \to \mathbb{Q}_p$. So we now have a function, η_J, that vanishes on $\overline{J(\mathbb{Q})}$. It also follows that our particular ω satisfies

3) If $Q_i, Q_i' \in X(\mathbb{Q}_p)$ such that $\left[\sum (Q_i' - Q_i)\right] \in \overline{J(\mathbb{Q})}$, then $\sum \int_{Q_i}^{Q_i'} \omega = 0$.

Recall that from Theorem 9.3.1, we know that $H^0(J_{\mathbb{Q}_p}, \Omega^1) \cong H^0(X_{\mathbb{Q}_p}, \Omega^1)$. Therefore, this ω_J corresponds to a unique element ω in $H^0(X_{\mathbb{Q}_p}, \Omega^1)$.

Theorem 9.3.5 (Coleman's Theorem [Col85])**.** *Let X, J, p, r' be as in Theorem 9.1.2. Suppose that p is a prime of good reduction for X.*

a) Let ω be a non-zero 1-form in $H^0(X_{\mathbb{Q}_p}, \Omega^1)$ satisfying conditions 1-3. We scale ω by an element of $\mathbb{Q}_p^\times$ so that it reduces to a nonzero 1-form $\widetilde{\omega} \in H^0(X_{\mathbb{F}_p}, \Omega^1)$. Let $m = \mathrm{ord}_{\widetilde{Q}} \widetilde{\omega}$. If $m < p-2$, then the number of points in $X(\mathbb{Q})$ reducing to $\widetilde{Q}$ is at most $m+1$.

b) If $p > 2g$, then

$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + (2g-2).$$

9.4 Applying Coleman's Theorem

We now return to the question of computing all of the points on the genus 2 modular curve

$$X_s^+(11) : y^2 = f(x) = x^6 - 6x^5 + 11x^4 - 8x^3 + 11x^2 - 6x + 1. \tag{9.4.1}$$

We know that this curve has two points at infinity, call them ∞_- and ∞_+, and a naive search yielded four other points, $(1, \pm 2)$, and $(0, \pm 1)$. Now, we have seen that the group of rational points on the jacobian of $X_s^+(11)$ has rank 1. Thus we can apply Theorem 9.3.5 to get that

$$\#X_s^+(11)(\mathbb{Q}) \leq \#X_s^+(11)(\mathbb{F}_5) + (2 \cdot 2 - 2) = 6 + 2 = 8. \tag{9.4.2}$$

Unfortunately this bound is not sharp, there could still be two other points that we are missing. From the moduli interpretation, one expects that the six points in (9.1.1)

are in fact, the *only* ones on $X_s^+(11)(\mathbb{Q})$, but how do we show that these are the only points?

One could try something along the lines of Remark , studying the η_J corresponding to the holomorphic 1-form we used in Theorem 9.3.5. This turns out to be quite difficult in this case because all six of the points that we found are in unique residue classes for all odd p. Thus, computing the power series of ω in local coordinates is not a straightforward task since we cannot take our open set to be the kernel of the reduction map $J(\mathbb{Q}_p) \to J(\mathbb{F}_p)$.

Instead, we aim to exploit the symmetry of $f(x)$. Looking at the affine model of $X_s^+(11)$ given in (9.4.1), it becomes clear that there is a $\psi \in \mathrm{Aut}(X_s^+(11))$, given by $\psi((x,y)) = \left(\frac{1}{x}, \frac{y}{x^3}\right)$. Upon further inspection, the set

$$S = \{\infty_\pm, (0, \pm 1), (1, \pm 2)\}$$

is stable under ψ. In fact, S is also stable under the standard hyperelliptic "conjugation" automorphism that maps (x,y) to $(x,-y)$.

With this in mind, we can finally prove the following theorem:

Theorem 9.4.1. *The set of $\mathbb{Q}$-rational points on $X_s^+(11)$ is $S = \{\infty_\pm, (0, \pm 1), (1, \pm 2)\}$.*

Proof: The set S is stable under the automorphisms ψ and σ, so if P is a $\mathbb{Q}$-rational point not in S, the points $P,\ \sigma(P),\ \psi(P)$, and $\sigma(\psi(P))$ are all not in S.

Next we notice that the only points that are fixed by either ψ or σ have either x-coordinate 0 or 1, or y-coordinate 0, but these points are already in S. Thus the points $P,\ \sigma(P),\ \psi(P)$, and $\sigma(\psi(P))$ are actually distinct.

Therefore, if there is one $\mathbb{Q}$-rational point on $X_s^+(11)$ that is not in S then there must actually be four such points. But this would mean that there are at least

ten points in $X_s^+(11)(\mathbb{Q})$, contradicting the upper bound of eight that we found in equation (9.4.2).

■

We know that $X_s^+(11)$ has one rational cusp and one can check using SAGE that there are 5 $\bar{\mathbb{Q}}$-isomorphism classes of elliptic curves with complex multiplication and split representation at 11. Thus we get the following corollary.

Corollary 9.4.2. *The only elliptic curves whose Galois representation at 11 with image contained in the normalizer of a split Cartan subgroup have complex multiplication. Their j-invariants are:*

$$-3375 = -1 \cdot 3^3 \cdot 5^3,$$
$$16581375 = 3^3 \cdot 5^3 \cdot 17^3,$$
$$8000 = 2^6 \cdot 5^3,$$
$$-884736 = -1 \cdot 2^{15} \cdot 3^3,$$
$$-884736000 = -1 \cdot 2^{18} \cdot 3^3 \cdot 5^3.$$

PROOF: Plugging the points in S into the j-map from Chapter 6 Section 6.5 we get the following table.

P	$j(P)$
$(0,1)$	8000
$(0,-1)$	cusp
$(1,2)$	-3375
$(1,-2)$	16581375
∞_+	-884736
∞_-	-88473600

■

Bibliography

[Apo90] Tom M. Apostol. *Modular Functions and Dirichlet Series in Number Theory*. Springer, second edition, 1990.

[Bar00] Edward J. Barbeau. *Pell's Equation*. Springer-Verlag, 2000.

[Bar10] Burcu Baran. Normalizers of non-split cartan subgroups, modular curves, and the class number one problem. *Journal of Number Theory*, 130:2753–2772, 2010.

[BP11] Yuri Bilu and Pierre Parent. Serre's uniformity problem in the split cartan case. *Annals of Mathematics*, 173:569–584, 2011.

[CC04] I. Chen and C. Cummins. Elliptic curves with nonsplit mod 11 representations. *Mathematics of Computation*, 73:869–880, 2004.

[CF96] J. W. S. Cassels and E. V. Flynn. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*. Number 230 in London Mathematica Society Lecture Note Series. Cambridge University Press, 1996.

[Cha41] Claude Chabauty. Sur les points rationnels des courbes algebriques de genre superieur a lunite. *C. R. Acad. Sci.*, 212(882-885), 1941.

[Che98] Imin Chen. The Jacobians of non-split Cartan modular curves. *Proc. London Math. Soc. (3)*, 77(1):1–38, 1998.

[Col85] Robert Coleman. Effective Chabauty. *Duke Math Journal*, 54(3):765–770, 1985.

[DS05] Fred Diamond and Jerry Shurman. *A First Course in Modular Forms*. Springer, 2005.

[FS97] E.V. Flynn and N.P. Smart. Canonical heights on the jacobians of curves of genus 2 and the infinite descent. *Acta Arith.*, 1997.

[HS00] Marc Hindry and Joseph H. Silverman. *Diophantine Geometry: An Introduction*. Springer, 2000.

[KL81] Daniel S Kubert and Serge Lang. *Modular units*. Springer-Verlag, New York Springer, 1981.

[Kob84] Neal Koblitz. *p-adic numbers, p-adic analysis, and zeta-functions*. Graduate Texts in Mathematics. Springer, 2nd edition, 1984.

[Lan83] Serge Lang. *Abelian Varieties*. Springer, 1983.

[Maz78] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Inventiones Mathematicae*, 44(2):129–162, 1978.

[Mil86] J. S. Milne. Jacobian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 167–212. Springer, 1986.

[Mom84] Fumiyuki Momose. Rational points on the modular curves $X_{split}(p)$. *Compositio Mathematica*, 52:115–137, 1984.

[MP] Willaim McCallum and Bjorn Poonen. The method of Chabauty and Coleman. http://math.mit.edu/ poonen/papers/chabauty.pdf.

[Mum70] David Mumford. *Abelian Varieties*. Oxford University Press, 1970.

[PS97] Bjorn Poonen and Edward F. Schaefer. Explicit descent for jacobians of cyclic covers of the projective line. *J. Reine Angew. Math.*, pages 141–188, 1997.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones Mathematicae*, 15:259–331, 1972.

[Ser89] Jean-Pierre Serre. *Lectures on the Mordell-Weil theorem*. Aspects of Mathematics, E15. Friedr. Vieweg & Sohn, Braunschweig, 1989. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 2nd edition, 2009.

[Sto] Michael Stoll. Implementing 2-descents for jacobians of hyperellitpic curves.

[Sto99] Michael Stoll. On the height constant for curves of genus two. *Acta Arith.*, 1999.