SIEGEL FUNCTIONS, MODULAR CURVES, AND SERRE'S UNIFORMITY PROBLEM

HARRIS B. DANIELS

1. Introduction

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) 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

$$E(K) \cong E_{\mathrm{tor}}(K) \times \mathbb{Z}^{r_K}$$

where $E_{\mathrm{tor}}(K)$ is the torsion subgroup of $E(K)$ and $r = r_K$ 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 paper is on the torsion part of $E(K)$.

Let p be a prime number, and let $E[p]$ be the $\mathbb{F}_p$-vector space of p-torsion points on $E(\overline{K})$, where $\overline{K}$ is a fixed algebraic closure of K. The natural Galois action of $\mathrm{Gal}(\overline{K}/K)$ on $E[p]$ induces a Galois representation $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(E[p])$, and if we choose a $\mathbb{Z}/p\mathbb{Z}$-basis of $E[p]$, then we obtain a Galois representation $\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. The image of $\rho_{E,p}$ was extensively studied by Serre in [15].

Theorem 1.1. [15] *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.*

Serre asked the next natural question: can the constant C_E be chosen independently of E?

Question 1.2 (Serre's Uniformity Problem, [15], §4.3)**.** Does there exist a constant $C > 0$ such that $\rho_{E,p}$ is surjective for all $p > C$ and all E without complex multiplication?

In [15], 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.

Serre showed the exceptional groups, as in case (5) above, are not subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ for p greater than 13. The uniformity question in case (2) was proven by Mazur [11] 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. Bilu, Parent, and Bilu, Parent, and Rebolledo [3] (also using results of Momose [12]) have shown that if $p \geq 11$, $p \neq 13$, and E is not CM, then case (3) cannot occur. 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 [11], and Bilu and Parent [2], fail and a different tactic must be taken. The focus of this paper is on the split case for the case of $p = 11$.

Date: April 22, 2015.
1991 *Mathematics Subject Classification.* Primary 14H52; Secondary 11F80.
Key words and phrases. Elliptic Curves, Modular Curves, Galois Representations.

Theorem 1.3 (Theorem 5.5, Corollary 5.6)**.** *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.*

As mentioned above, Theorem 1.3 has already been proven. It is the simplest case of [13, Theorem 1.1] and in fact was probably even known before that. Here, the main goal is to prove the result by analyzing completely the arithmetic of the modular curve, $X_s^+(11)$, that parametrizes elliptic curves over $\mathbb{Q}$ with $\rho_{E,11}$ having split Cartan image. In the proof of Parent, the author shows a bound on the height of the j-invariant of any elliptic curve in the split case (3) above, and then run an exhaustive calculation that proves that none of the curves up to that bound have split Cartan image and are not CM, therefore proving the desired result. Our methods work directly on $X_s^+(11)$, in that we calculate all the rational points on $X_s^+(11)$, and in doing so, we compute the structure of the jacobian of the modular curve, and determine its rational points.

More concretely, the main theorem of this article is the following.

Theorem 1.4. *Let X be the modular curve $X_s^+(11)$ and let J be its associated jacobian variety. Then:*

(1) *X has a model $y^2 = x^6 - 6x^5 + 11x^4 - 8x^3 + 11x^2 - 6x + 1$, and the j-map $X \to \mathbb{P}^1(\mathbb{Q})$ can be calculated explicitly.*

(2) *$X(\mathbb{Q})$ contains exactly 6 points, two of which are points at infinity ∞_+ and ∞_-, and one is a cusp $(0, -1)$. The points, together with the j-invariant of the elliptic curve associated to each non-cuspidal point are given in the following table:*

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

(3) *$J(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}$. The torsion subgroup of $J(\mathbb{Q})$ is generated by $[(0,1) - \infty_-]$, while $[\infty_+ - \infty_-]$ is a generator of infinite order.*

Another main goal of this paper is to illustrate several important techniques in the computation of rational points on (hyperelliptic) curves. First, a model for $X = X_s^+(11)$ is computed using Siegel functions and modular units and compute the j-map that gives the j-invariant of the elliptic curve associated to each non-cuspidal point on the curve. The method used to compute a model for X should readily generalize to other modular curves of prime level. In order to be able to apply the method of Chabauty and Coleman to find a bound on the number of rational points on X, we first need to determine the rank of the jacobian variety (in particular, one needs to show that the rank of $J(\mathbb{Q})$ less than the genus of X, which is 2). The jacobian is studied by performing a 2-descent via the methods of Poonen, Schaefer, and Stoll, that allows us to determine the structure of $J(\mathbb{Q})$, and in particular show that the free rank is 1, less than the genus of X, as desired. The method of Chabauty and Coleman now produces a bound of 8 rational points on X, but a naive search for points only yields the 6 points listed in Theorem 1.4. Finally, we find several automorphisms of $X(\mathbb{Q})$ that allows us to conclude that if there was an additional point beyond the 6 we list, then there would be at least 10 points on X, contradicting the bound of 8. Hence, the ones we list are all the rational points on X.

The paper is organized as follows. In Section 2 Siegel functions, and modular units are defined. In Section 3 we construct a model for $X_s^+(11)$ using modular units built out of Siegel functions, and in Section 3.5 we go on to compute the j-map. The 2-descent on the jacobian variety is described in Section 4. Finally, the method of Chabauty and Coleman is summarized in Section 5 and Theorem 1.3 is proved in Section 5.4.

1.1. **Acknowledgments.** Much of the contents of this paper were originally written in partial fulfillment of the requirements for the degree of doctor of philosophy at the University of Connecticut in 2013. Without the help and guidance of my thesis advisor, Álvaro Lozano-Robledo, this paper would not have been possible.

2. Klein Forms, Siegel Functions, and Modular Units

2.1. **Klein Forms and Siegel Functions.** In this Section we follow the notation and terminology laid out in Section 1 and 2 of Chapter 2 of [10]. 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 2.1. *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 (see [10]). 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 [10, Chapter 2], the authors show that these functions 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

$$\varepsilon(\mathbf{a}, \mathbf{b}) = (-1)^{b_1b_2+b_1+b_2}e^{-\pi i(b_1a_2-b_2a_1)}.$$

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

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

where $\varepsilon_{\mathbf{a}}(\alpha)$ 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

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

Definition 2.2. *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 2.3. *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

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

■

Definition 2.4. *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 2.5. [1, 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 24th root of unity.

Remark 2.6. The observant reader might ask about how the square root above is chosen and whether the choice depend on τ. We will ignore this question for now and see in the proof of 2.8 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 2.7. [10, 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 2.8. *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 12th root of unity that depends only on α.

Proof: Using Propositions 2.3 and 2.5 we have,

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

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 [10], 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 2.9. [10, Chapter 3, Theorem 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) $\displaystyle\sum_{\mathbf{a}\in A} m(\mathbf{a})r_1^2 \equiv \sum_{\mathbf{a}\in A} m(\mathbf{a})r_2^2 \equiv \sum_{\mathbf{a}\in A} m(\mathbf{a})r_1r_2 \equiv 0 \bmod N$, *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 $0 \le a_1 < 1$ and $0 \le a_2 < 1$. 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 2.10. [10, 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 when we start to use these functions along with the Riemann-Roch theorem to compute models of curves.

2.2. **Modular Units for Congruence subgroups of Level p.** In this section we generalize the methods used in [6] 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 $p \neq 2, 3$. Let $\Gamma^*(p) = \langle -I_2, \Gamma(p) \rangle$ if $-I_2 \in \Gamma$, otherwise let $\Gamma^*(p) = \Gamma(p)$. Next, let $\overline{\Omega} = \Gamma/\Gamma^*(p)$, and let Ω be a **fixed** set of representatives of $\overline{\Omega}$ in Γ.

Remark 2.11. 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 2.12. *For* $\mathbf{a} \in \left(\frac{1}{p}\mathbb{Z}/\mathbb{Z}\right)^2$ *with* $\mathbf{a} \notin \mathbb{Z}^2$ *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*

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

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 2.13. *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* $g_{\mathbf{a}\delta}(\tau) = \varepsilon_{\mathbf{a}}(\delta) g_{\mathbf{a}}(\tau)$, *where* $\varepsilon_{\mathbf{a}}(\delta)$ *is the* $2p$*-th root of unity in* **K3**.

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

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

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 $\delta \in \Gamma(P)$,

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

and since $\varepsilon_{\mathbf{a}}(\delta)$ is a $2p$-th root of unity, so is $-\varepsilon_{\mathbf{a}}(\delta)$ and the result follows. ■

Proposition 2.14. *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 $\kappa = \prod_{i=1}^{\#\Omega} \varepsilon_{\mathbf{a}\gamma_i'}(\delta_i)$. 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

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

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 2.15. *The q-expansion $v_{\mathbf{a}}$ is independent of choice of the representatives of Ω and thus so it the q-expansions of $u_{\mathbf{a}}(\tau)$.*

Proof: Follows immediately from Proposition 2.14

■

Theorem 2.16. *Let $\mathbf{a} \in \left(\frac{1}{p}\mathbb{Z}/\mathbb{Z}\right)^2$, with $\mathbf{a} \notin \mathbb{Z}^2$, then for any $\alpha \in \Gamma$,*

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

where $\varepsilon_1(\mathbf{a}, \alpha)$ is an explicitly computable $2p^{th}$-root of unity that depends on $\mathbf{a}$ and α and $\zeta(\alpha)$ is the 12^{th} root of unity in Theorem 2.8. Further, $\varepsilon_1(\mathbf{a}, \alpha) = 1$ if and only if the product of Siegel functions defining $v_{\mathbf{a}}$ satisfies condition (1) of Theorem 2.9. Similarly, $\zeta(\alpha)^{\#\Omega}$ is 1 if and only if the product of Siegel functions defining $v_{\mathbf{a}}$ satisfies condition (2) of Theorem 2.9.

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,

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

where $\varepsilon_{\mathbf{a}\gamma^\sigma}(\alpha, \gamma)$ is the $2p$-th root of unity from Lemma 2.13 that depends on $\mathbf{a}$ and $\delta(\gamma, \alpha)$. Let $\varepsilon_1(\mathbf{a}, \alpha) = \prod_{\gamma\in\Omega} \varepsilon_{\mathbf{a}\gamma}(\gamma, \alpha)$. Then

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

where the last equality follows from the fact that σ is a permutation of Ω, so the terms are simply being reordered.

Finally, we note that the content of the proof of [10, Chapter 3, Theorem 5.2] is exactly showing that $\varepsilon_1(\mathbf{a}, \alpha) = 1$ if and only if our product satisfies condition (1) of Theorem 2.9, while condition (2) ensures that $\zeta(\alpha)^{\#\Omega}$ would be 1. ■

Definition 2.17. *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 2.18. *For each* $\mathbf{a} = (a_1, a_2) = \left(\frac{r_1}{p}, \frac{r_2}{p}\right) \in \left(\frac{1}{p}\mathbb{Z}/\mathbb{Z}\right)^2$ *such that*

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

$u_{\mathbf{a}}(\tau)$ *is modular for* Γ*. Further, in this case* $\varepsilon_1(\mathbf{a}, \alpha) = 1$ *for all* $\alpha \in \Gamma$*, where* $\varepsilon_1(\mathbf{a}, \alpha)$ *is as defined in Theorem 2.16.*

Proof: Suppose that $\mathbf{a} \in \left(\frac{1}{p}\mathbb{Z}/\mathbb{Z}\right)^2$ such that

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

This means that the function $u_{\mathbf{a}}(\tau)$ is modular for $\Gamma^*(p)$ from Theorem 2.9. This implies $u_{\mathbf{a}}(\delta\tau) = u_{\mathbf{a}}(\tau)$ for all $\delta \in \Gamma^*(p)$, but by the definition $u_{\mathbf{a}}(\tau)$, this means that $\varepsilon_1(\mathbf{a}, \gamma)$ is also 1 since the product that defines it only depends on the $\delta(\gamma, \alpha)$'s which are elements in $\Gamma^*(p)$. Therefore, for all $\alpha \in \Gamma$,

$$u_{\mathbf{a}}(\alpha\tau) = \left(\zeta(\alpha)^{\#\Omega}\varepsilon_1(\mathbf{a}, \alpha)v_{\mathbf{a}}(\tau)\right)^c = \zeta(\alpha)^{\#\Omega \cdot c} \cdot 1^c \cdot v_{\mathbf{a}}(\tau)^c = v_{\mathbf{a}}(\tau)^c = u_{\mathbf{a}}(\tau),$$

and $u_{\mathbf{a}}(\tau)$ is modular for Γ. ■

3. The modular Curve $X_s^+(11)$

3.1. **Modular curves associated to Normalizers of Split Cartan Subgroups.**

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

Definition 3.1. *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 3.2. *Let* $X_s^+(p)$ *be the Riemann surface given by* $\Gamma_s^+(p)\backslash\mathscr{H}^*$.

Theorem 3.3. [7, 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 3.4.

p	5	7	11	13	17	19	23	29	31	37	41	43	47
$g_s^+(p)$	0	0	2	3	7	9	15	26	30	45	57	63	77

3.2. **Curves of Genus Two.** Using Theorem 3.3, 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 3.5. *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* $\deg(f) \leq 5$*.*

Proposition 3.5 tells us that every genus two curve is hyperelliptic. 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 3.6. 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. 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 $\deg(f) = 6$.

3.3. **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 3.5. We start noticing that in this case $\#\Omega = 12$ and so $c = 1$. Therefore in this case, have that $u_{\mathbf{a}} = v_{\mathbf{a}}$. To ease notation, we let

$$w_{\mathbf{a},\mathbf{b}} = \frac{v_{\mathbf{a}}}{v_{\mathbf{b}}}.$$

Using SAGE, we check that for every $\mathbf{a} \in \left(\frac{1}{11}\mathbb{Z}/\mathbb{Z}\right)^2$ the product defining $v_{\mathbf{a}}$ satisfies the condition in Proposition 2.18 and we compute the divisors of the modular units of the form $w_{\mathbf{a},\mathbf{b}}$. 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 3.7. From Theorem 2.7 we know that the field of definition of the functions defined in Section 2.2 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 3.8. *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*

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

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 3.5 to them.

Proposition 3.9. *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 fixes $\mathbb{Q}$, for any $\alpha = \alpha_1\, e_1 + \cdots + \alpha_n\, e_n \in K$ we get

$$\begin{pmatrix} \sigma_1(e_1) & \sigma_1(e_2) & \ldots & \sigma_1(e_n) \\ \sigma_2(e_1) & \sigma_2(e_2) & \ldots & \sigma_2(e_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(e_1) & \sigma_n(e_2) & \ldots & \sigma_n(e_n) \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} \sigma_1(\alpha) \\ \sigma_2(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{pmatrix}. \tag{3.1}$$

For convenience let A be the matrix on the left hand side of (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 (3.1). Applying Cramer's rule we get that $\alpha_i = \det A_i/\det A$. 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 $X = [w_{(2/11,1/11),(0/11,1/11)}(\tau)]_1$, $Y = [w_{(1/11,1/11),(0/11,1/11)}(\tau)]_2$, $Z = [w_{(3/11,1/11),(0/11,1/11)}(\tau)]_0$, where the subscript indicates which coefficients we are using to create the q-expansions. 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 other poles.

3.4. **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 3.10. *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 nowhere 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	1	2	3	4	5	6	7
$\ell(5d \cdot \infty)$	4	9	14	19	24	29	34
$\binom{d+2}{2}$	3	6	10	15	21	28	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 3.11. *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 $\mathscr{L}(-\infty)$, but by the Riemann-Roch Theorem, 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 3.11, 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

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

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

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

Here we note that we are working in weighted projective space where x_1 and z_1 have weight one and y_1 has weight three. While this model is minimal, it will not be the most convenient for us to use. Instead 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 3.12. 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.

3.5. **Computing the j-map for $X_s^+(11)$.** The last task for this section 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 section.

3.6. 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 $X_s^+(11)$.

$$X = \frac{1}{q^3} + \frac{1}{q} + 1 + 2q + 2q^2 + 5q^3 + O(q^4)$$

$$Y = \frac{1}{q^4} + \frac{1}{q^3} + \frac{2}{q^2} + \frac{3}{q} + 6 + 7q + 10q^2 + 14q^3 + O(q^4)$$

$$Z = \frac{1}{q^5} + \frac{1}{q^4} + \frac{3}{q^3} + \frac{4}{q^2} + \frac{8}{q} + 11 + 18q + 25q^2 + 38q^3 + O(q^4)$$

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

4.1. 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.

It turns out that computing $J(\mathbb{Q})_{\text{tors}}$ is not very difficult using the following theorem.

Theorem 4.1. [9, 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*

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

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

$$\begin{tikzcd} 0 \arrow[r] & J[2] \arrow[r] & J \arrow[r, "{[2]}"] & J \arrow[r] & 0 \end{tikzcd}$$

where $J[2]$ is the 2-torsion of J. Let $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ be the *2-Selmer group* as defined in [9]. This gives us the following short exact sequence.

$$\begin{tikzcd} 0 \arrow[r] & J(\mathbb{Q})/2J(\mathbb{Q}) \arrow[r] & \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \arrow[r] & Ш(\mathbb{Q}, J)[2] \arrow[r] & 0 \end{tikzcd}$$

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.

$$\text{rank}\, J(\mathbb{Q}) + \dim_{\mathbb{F}_2} J(\mathbb{Q})[2] + \dim_{\mathbb{F}_2} Ш(\mathbb{Q}, J)[2] = \dim_{\mathbb{F}_2} \mathrm{Sel}^{(2)}(\mathbb{Q}, J). \tag{4.1}$$

Using equation (4.1), we get the following computable upper bound on the rank

$$\operatorname{rank} J(\mathbb{Q}) \leq \dim_{\mathbb{F}_2} \operatorname{Sel}^{(2)}(\mathbb{Q}, J) - \dim_{\mathbb{F}_2} J(\mathbb{Q})[2]. \tag{4.2}$$

In order to calculate this upper bound we must compute the dimension of $\operatorname{Sel}^{(2)}(\mathbb{Q}, J)$. 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 a very subtle task that lies outside of the scope of this paper. The interested reader should consult either [17] or [16] to read about computing $Ш(\mathbb{Q}, J)[2]$ or $Ш(\mathbb{Q}, J)$ in the case that X is elliptic or hyperelliptic.

4.2. **The Two-Descent Procedure.**

The notation that we use in this section will follow that set out in [17]. 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, C, given by an affine equation of the form

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

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 4.2. 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, [14] 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 4.3. *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 4.4. 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 $\operatorname{Cl}(K)$ 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:

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

Definition 4.5. *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*

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

Definition 4.6. *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 4.7. 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 4.8. *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 4.9. [4, 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 4.10. *Let*

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

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

The link between the fake 2-Selmer and the 2-Selmer group will be explained in Corollary 4.23.

Remark 4.11. If we use this definition for $\mathrm{Sel}^{(2)}_{\text{fake}}(\mathbb{Q}, J)$, in order to check if $\xi \in H$ is in $\mathrm{Sel}^{(2)}_{\text{fake}}(\mathbb{Q}, J)$ 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 4.12. *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

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

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

Remark 4.13. 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

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

Proposition 4.14. [17, Proposition 5.10] *If $p \notin S = \{\infty, 2\} \cup \{p : p^2 | \operatorname{disc}(f)\}$, then*

$$\begin{tikzcd} J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) \arrow[r, "\delta_p"] & H_p \arrow[r, "\mathrm{val}_p"] & I_p \arrow[r] & 0 \end{tikzcd}$$

is exact.

Proposition 4.15. *If $S = \{\infty, 2\} \cup \{p : p^2 | \operatorname{disc}(f)\}$*

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

Proof: Since

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

is exact for $p \notin S$, we know that $\mathrm{res}_p(\xi) \in \delta_p(J(\mathbb{Q}_p))$ if and only if $\mathrm{val}_p(\mathrm{res}_p(\xi))$ 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 $\xi = [\beta] \in H$, $\mathrm{res}_p(\xi) \in \delta_p$ if and only if $[(\beta)] = [(1)] \in I_p$. Using this we can rewrite Definition 4.10 as

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

■

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

Definition 4.16. *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 4.17. Condition (‡.*b*) is equivalent to L_K containing a quadratic extension of K.

Lemma 4.18. [14, 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 4.19. [17, 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 4.20. [17, 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 4.21. [14, 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 4.22. 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

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

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

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

Now that we have the relationship between $\dim \mathrm{Sel}^{(2)}_{\text{fake}}(\mathbb{Q}, J)$ and $\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J)$, we need to compute $\dim \mathrm{Sel}^{(2)}_{\text{fake}}(\mathbb{Q}, J)$. 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 4.24. [14] *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 4.25. *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 4.26. [17, 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 4.27. [17, 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 $\mathrm{Sel}^{(2)}_{\text{fake}}(\mathbb{Q}, J)$, a finite subspace of $L^\times/(L^\times)^2\mathbb{Q}$. In order to compute $\mathrm{Sel}^{(2)}_{\text{fake}}(\mathbb{Q}, J)$ 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.

(4.3)

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Ker} \arrow[r] \arrow[d, equal] & \mathrm{Sel}_2 \arrow[r] \arrow[d] & \mathrm{Sel}_1 \arrow[r] \arrow[d] & \mathrm{Sel}^{(2)}_{\text{fake}}(\mathbb{Q}, J) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \mathrm{Ker} \arrow[r] & \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \arrow[r] & L^\times/(L^\times)^2 \arrow[r] & L^\times/(L^\times)^2\mathbb{Q}^\times \arrow[r] & 1
\end{tikzcd}$$

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 4.28. [17, Lemma 4.9] *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 (4.3) is exact.*

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

4.3. **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 4.26 and 4.27 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 4.29. Lemma 4.26 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 4.20 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 4.20 tells us that in our case $\mathbb{Q}$ does not satisfy (‡). So, by Corollary 4.23, we have that

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

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

The first step to computing the dimension of $\mathrm{Sel}^{(2)}_{\text{fake}}(\mathbb{Q}, J)$ is to find the subgroups Sel_1 and Sel_2 from Proposition 4.28. To do this we start by computing $\widetilde{H}$. Recall that

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

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

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

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 $\mathrm{Ker} = \{1\}$. But using the fact that

$$\begin{tikzcd}
1 \arrow[r] & \langle -1,2\rangle \arrow[r] \arrow[dd, hook] & \mathrm{Sel}_1 \arrow[r] \arrow[d, hook] & \mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J) \arrow[r] \arrow[dd, hook] & 1 \\
 & & \langle -1, 2, u_1\rangle \arrow[d, hook] & & \\
1 \arrow[r] & \mathbb{Q}^{\times}/(\mathbb{Q}^{\times})^2 \arrow[r] & L^{\times}/(L^{\times})^2 \arrow[r] & L^{\times}/(L^{\times})^2\mathbb{Q}^{\times} \arrow[r] & 1
\end{tikzcd}$$

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 4.28, 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 4.24 to compute the images of $P - \infty_+$ under δ_2.

Lemma 4.30. *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 4.31. *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 4.30 we know that L_2 does not contain a quadratic extension of $\mathbb{Q}_2$ and so we have the following exact sequence:

$$\begin{tikzcd}
1 \arrow[r] & \mathbb{Q}_2^{\times}/(\mathbb{Q}_2^{\times})^2 \arrow[r, "\psi"] & L_2^{\times}/(L_2^{\times})^2 \arrow[r, "\phi"] & L_2^{\times}/(L_2^{\times})^2\mathbb{Q}_2^{\times} \arrow[r] & 1.
\end{tikzcd}$$

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 4.31 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 4.24, we know that $\delta_2(P_1 - \infty_+) = 2 - \theta$. Using Lemma 4.31 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 $2 - \theta \equiv \alpha - \theta \bmod (L_2^\times)^2\mathbb{Q}_2^\times$. Again using Lemma 4.31, we check this in Magma.

Remark 4.32. 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 4.31, if $\mathrm{res}_2(u_1)$ is in $\delta_2(J(\mathbb{Q}_2))$. A few calculations later we see that

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

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 4.3 we know that $\mathrm{Sel}_1 = \mathrm{Sel}_2 = \langle -1, 2\rangle$ and $\mathrm{Sel}^{(2)}_{\text{fake}}(\mathbb{Q}, J) = \{1\}$. Combining this with proposition 4.23 and equation (5.3) we get that the rank of $J(\mathbb{Q})$ is less than or equal to one.

In fact, using Magma, one can show that the divisor class of $\infty_+ - \infty_-$ is of infinity order. Further we can show that

$$J(X_s^+(11))(\mathbb{Q}) = \langle [(0, -1) - \infty_-], [\infty_+ - \infty_-]\rangle \cong \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}.$$

5. Applying the Method of Chabauty and Coleman

5.1. Introduction to the method.

Theorem 5.1 (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 a curve of genus greater than or equal to 2, but it does not give us any way to show that a set of points on a curve is complete. In 1941, Claude Chabauty proved the following weaker version of Faltings' theorem:

Theorem 5.2 (Chabauty's Theorem [5]). *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 5.3. *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 a method for finding an explicit bound on the size of $X(\mathbb{Q})$ in the case when r' is less then the genus of X.

Theorem 5.4 (Coleman's Theorem [8]). *Let X, J, p, r' be as in Theorem 5.2. 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*

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

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 simplest bound obtained from Coleman's method is not sharp, but utilizing some extra structure of $X_s^+(11)$, we will be able to show that the only points on $X_s^+(11)$ are the ones found by a naive search. That is to say that

$$X_s^+(11)(\mathbb{Q}) = \{(0, \pm 1), (1, \pm 2), \infty_\pm\}. \tag{5.1}$$

5.2. **Applying Coleman's Theorem.** We now return to the question of computing all of the points on the genus 2 modular curve

$$X_s^+(11) : y^2 = f(x) = x^6 - 6x^5 + 11x^4 - 8x^3 + 11x^2 - 6x + 1. \tag{5.2}$$

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 5.4 to get that

$$\#X_s^+(11)(\mathbb{Q}) \leq \#X_s^+(11)(\mathbb{F}_5) + (2 \cdot 2 - 2) = 6 + 2 = 8. \tag{5.3}$$

Unfortunately this bound does not line up with the number of points that we found, there could still be two other points that we are missing. From the moduli interpretation, one expects that the six points in (5.1) 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 studying the η_J corresponding to the holomorphic 1-form we used in Theorem 5.4, but 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 (5.2), 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 5.5. *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 (5.3).

■

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

Corollary 5.6. *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, 16581375, 8000, -884736, -884736000.

PROOF: Plugging the points in S into the j-map from Section 3.5 we get the following table.

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

■

References

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

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

[3] Yuri Bilu, Pierre Parent, and Marusia Rebolledo. Rational points on $X_0^+(p^r)$. *Ann. Inst. Fourier (Grenoble)*, 63(3):957–984, 2013.

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

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

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

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

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

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

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

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

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

[13] Pierre Parent. Towards the triviality of $X_0^+(p^r)(\mathbb{Q})$ for $r > 1$. *Compositio Mathematica*, 141:561–572, 2005.

[14] 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.

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

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

[17] Michael Stoll. Implementing 2-descents for Jacobians of hyperelliptic curves. *Acta Arith.*, 98:245–277, 2001.

(Harris B. Daniels) DEPARTMENT OF MATHEMATICS AMHERST COLLEGE BOX 2239 P.O. 5000 AMHERST, MA 01002-5000

E-mail address: hdaniels@amherst.edu