Quadratic Points on Non-Split Cartan Modular Curves

Philippe Michaud-Rodgers

September 17, 2020

Pour Papé

Abstract

In this project we study quadratic points on the non-split Cartan modular curves $X_{ns}(p)$, for $p = 7, 11$, and 13. In [38], Siksek proves that all quadratic points on $X_{ns}(7)$ arise as pullbacks of rational points on $X_{ns}^{+}(7)$. Using similar techniques for $p = 11$, and employing a version of Chabauty for symmetric powers of curves for $p = 13$, we show that the same holds for $X_{ns}(11)$ and $X_{ns}(13)$. As a consequence, we prove that certain classes of elliptic curves over quadratic fields are modular.

Contents

1 Introduction

Modular curves play a crucial role in modern mathematics. They have deep and wide-ranging applications in Number Theory and beyond. Modular curves allow us to understand and study families of elliptic curves, and are a very powerful tool for doing this. As examples, the proofs of both Fermat's Last Theorem and Mazur's Torsion Theorem rely heavily on the theory of modular curves.

Of particular interest are rational points and points of low degree on modular curves. Rational points on many classes of modular curves have been, and continue to be, studied extensively. Recently, there has been an increased interest in quadratic points on modular curves. Quadratic points on $X_1(N)$ are well understood: Kamienny proved in [21] that there are no quadratic points on $X_1(N)$ for $N \geq 17$. Also, due to several recent papers [31, 5, 8], much progress has been made in understanding quadratic points on $X_0(N)$: all quadratic points on $X_0(N)$ have been classified for genus $2, 3, 4$, and 5. In this project, we aim to understand quadratic points on some non-split Cartan modular curves; namely $X_{ns}(p)$, for $p = 7, 11$, and 13.

Quadratic points on algebraic curves often arise due to the existence of a degree 2 map to a curve with rational points. In fact, a well known result of Harris and Silverman [20, p. 352] states that a curve of genus ≥ 2 can have infinitely many quadratic points only if it is hyperelliptic or bielliptic. The curve $X_{ns}(p)$ comes equipped with a degree 2 map to the modular curve $X_{ns}^+(p)$. Rational points on $X_{ns}^+(p)$ therefore provide a source of quadratic points on $X_{ns}(p)$. Any quadratic point that does *not* arise in this way is said to be *exceptional*.

Theorem 1.1 (Main theorem)**.** *There are no exceptional quadratic points on $X_{ns}(p)$ for $p = 7, 11,$ or 13.*

Moreover, as the rational points on the curves $X_{ns}^{+}(p)$ for $p = 7, 11$, and 13 are understood, this result provides a full classification of the quadratic points on $X_{ns}(p)$ for these primes. The main consequence of this result is the following.

Corollary 1.2. *Let E be an elliptic curve defined over a quadratic field K such that $\overline{\rho}_{E,p}(Gal(\overline{K}/K)) \subseteq C_{ns}(p)$ for $p = 7, 11,$ or 13. Then $j(E) \in \mathbb{Q}$. Thus E is modular.*

Here, $C_{ns}(p)$ is a non-split Cartan subgroup, and $\overline{\rho}_{E,p}$ is the mod p Galois representation attached to E. These types of modularity results play a key role in the study of Diophantine equations. For example, quadratic points on certain modular curves are studied to prove that all elliptic curves over real quadratic fields are modular [19]. Non-split Cartan curves also play an important role here.

We present here the outline for the rest of the project. In Section 2 we introduce the framework to study modular curves, starting from subgroups of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. In Section 3 we focus on non-split Cartan modular curves. We look at Serre's uniformity conjecture and Gauss' class number one problem, and the role that non-split Cartan curves play. In Section 4 we follow the proof of Siksek [38] to show that Theorem 1.1 holds in the case $p = 7$. We apply similar ideas in Section 5 to show the theorem also holds for $p = 11$. However, for $p = 13$, matters are more complicated. We describe in Section 6 the method of Chabauty for symmetric powers of curves and apply this to the curve $X_{ns}(13)$ in Section 7.

I would like to express my sincere gratitude to Samir Siksek and Damiano Testa for supporting me throughout the whole year, keeping me motivated, and always answering my seemingly never-ending list of questions and queries!

2 Modular Curves

2.1 Modular Curves from subgroups of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$

Modular curves are classically constructed by starting with a congruence subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ and adjoining cusps to the Riemann surface $\Gamma\backslash\mathbb{H}$. This gives a compact Riemann surface to which we associate an algebraic curve. For the classical congruence subgroups $\Gamma(N), \Gamma_0(N)$, and $\Gamma_1(N)$ we have a natural moduli interpretation of the corresponding modular curves as parametrising equivalence classes of elliptic curves, with extra torsion data in the case of $X_0(N)$ and $X_1(N)$. The theory of these classical modular curves is extensively covered in [12].

We would like to interpret this construction in a slightly different way and generalise this moduli interpretation, as well as link modular curves with mod p representations of elliptic curves. We will associate modular curves to subgroups of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Our exposition is based on that of [37].

Given a group $H \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ we associate a congruence subgroup, Γ_H, to H as follows. We write

$$\Gamma_H \coloneqq \{A \in \mathrm{SL}_2(\mathbb{Z}) : (A \bmod N) \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \cap H\}.$$

We see that $\Gamma_H \supseteq \Gamma(N)$. We then define the open modular curve $Y_H \coloneqq \Gamma_H \backslash \mathbb{H}$, and its compactification by adjoining cusps $X_H \coloneqq \Gamma_H \backslash \mathbb{H}^*$, where $\mathbb{H}^* \coloneqq \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ denotes the extended upper half plane. Then X_H is a compact Riemann surface and so it corresponds to an algebraic curve. If H_1, H_2 are conjugate subgroups of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ then $X_{H_1} \cong X_{H_2}$.

To recover the classical modular curves $X_0(N)$ and $X_1(N)$ we can consider the subgroups $B_0(N)$ and $B_1(N)$ respectively, where

$$B_0(N) \coloneqq \left\{ \left(\begin{smallmatrix} \alpha & \beta \\ 0 & \delta \end{smallmatrix} \right) \;\middle|\; \beta \in \mathbb{Z}/N\mathbb{Z},\ \alpha, \delta \in (\mathbb{Z}/N\mathbb{Z})^* \right\},$$

$$B_1(N) \coloneqq \left\{ \left(\begin{smallmatrix} 1 & \beta \\ 0 & \delta \end{smallmatrix} \right) \;\middle|\; \beta \in \mathbb{Z}/N\mathbb{Z},\ \delta \in (\mathbb{Z}/N\mathbb{Z})^* \right\}.$$

We have $X_{B_0(N)} = X_0(N)$ and $X_{B_1(N)} = X_1(N)$.

The following important result tells us over which field the curve X_H is defined. A proof can be found in [12, pp. 291-294].

Proposition 2.1. *As an algebraic curve, X_H is defined over $\mathbb{Q}(\zeta_N)^{\det(H)}$. In particular, if $\det : H \mapsto (\mathbb{Z}/N\mathbb{Z})^*$ is surjective then X_H is defined over $\mathbb{Q}$.*

Here $\det(H) \subseteq (\mathbb{Z}/N\mathbb{Z})^* \cong \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$, and so it makes sense to talk about the fixed subfield of $\mathbb{Q}(\zeta_N)$ under the action of $\det(H)$. From now on, *we will assume the determinant map is surjective* so that X_H is an algebraic curve defined over $\mathbb{Q}$, as this will be the case for the subgroups H of interest to us.

2.2 Moduli Interpretation

Continuing with the same notation, we would like to understand how X_H parametrises elliptic curves. The basic idea is that the non-cuspidal points of X_H consist of pairs: an elliptic curve and a choice of basis for its N-torsion. The subgroup H will determine when two of these pairs are equivalent.

Definition 2.2. Let $E/\mathbb{C}$ be an elliptic curve and N a positive integer. A *level N structure* is an isomorphism[1] $\theta : E[N] \to (\mathbb{Z}/N\mathbb{Z})^2$. This is simply a choice of basis for $E[N]$.

[1] A level N structure is also sometimes defined as an isomorphism in the other direction: $(\mathbb{Z}/N\mathbb{Z})^2 \to E[N]$.

We consider pairs (E, θ) with E an elliptic curve and θ a level N structure. We want to define an equivalence relation on these pairs so that the non-cuspidal points of X_H parametrise them. For this we will require the elliptic curves to be isomorphic, as well as a matrix in H taking one basis to the other once the isomorphism has been applied. This is made precise by the following definition.

Definition 2.3. Two pairs, (E_1, θ_1) and (E_2, θ_2), are defined to be *H-isomorphic*, and we write $(E_1, \theta_1) \sim_H (E_2, \theta_2)$, if there is an isomorphism $\varphi : E_1 \to E_2$, and an element $h \in H$ making the following diagram commute:

$$\begin{array}{ccc} E_1[N] & \xrightarrow{\theta_1} & (\mathbb{Z}/N\mathbb{Z})^2 \\ {\scriptstyle\varphi}\downarrow{\scriptstyle\cong} & & \downarrow{\scriptstyle h} \\ E_2[N] & \xrightarrow[\theta_2]{} & (\mathbb{Z}/N\mathbb{Z})^2. \end{array}$$

Here $h : (\mathbb{Z}/N\mathbb{Z})^2 \to (\mathbb{Z}/N\mathbb{Z})^2$ is matrix-vector multiplication and is an isomorphism; it is a change-of-basis map.

A straightforward check shows that this is indeed an equivalence relation. We write $[(E, \theta)]_H$ for the equivalence class. The following proposition shows that Y_H parametrises H-isomorphism classes of elliptic curves.

Proposition 2.4. *Let N be a positive integer and let $H \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Denote by E_τ the elliptic curve $\mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}\tau)$. Write $\theta_\tau : E_\tau[N] \to (\mathbb{Z}/N\mathbb{Z})^2$ for the map $1/N \mapsto (1, 0)$ and $\tau/N \mapsto (0, 1)$. Then we have the following bijection:*

$$\begin{aligned} \big\{[(E_\tau, \theta)]_H : \tau \in \mathbb{H}\big\} &\longrightarrow Y_H(N) \\ [(E_\tau, \theta)]_H &\longmapsto \Gamma_H \tau. \end{aligned}$$

Proof. The proof follows the argument of [12, pp. 39-40] where it is shown that $X_1(N)$ parametrises classes of elliptic curves with an N-torsion point. □

Along with this moduli interpretation, the usual j-map behaves as one might expect; writing c for a cusp, we have:

$$\begin{aligned} j : X_H &\longrightarrow X(1) \cong \mathbb{P}^1 \\ [(E_\tau, \theta)]_H &\longmapsto j(\tau) \\ c &\longmapsto \infty, \end{aligned}$$

So the cusps of X_H are precisely the set $j^{-1}\{\infty\}$. Moreover, for non-cuspidal points, $j\big([(E, \theta)]_H\big) = j(E)$, the j-invariant of the elliptic curve.

Inclusion of subgroups leads to maps between the corresponding modular curves: if $H_1 \leq H_2 \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, then we have a degeneracy map

$$\begin{aligned} \varrho : X_{H_1} &\longrightarrow X_{H_2} \\ \Gamma_{H_1}\tau &\longmapsto \Gamma_{H_2}\tau \\ \Gamma_{H_1}c &\longmapsto \Gamma_{H_2}c. \end{aligned}$$

In terms of the moduli interpretation, for non-cuspidal points we have $\varrho\big([E,\theta]_{H_1}\big) = [E,\theta]_{H_2}$. The image of a point uses a coarser equivalence relation.

Remark 2.5. From now on we will identify the Riemann surface $\Gamma_H\backslash\mathbb{H}^*$ with the corresponding algebraic curve over $\mathbb{Q}$. So if we ask a question such as: "*is* $[(E,\theta)]_H$ *a rational point on* X_H*?*" we are really asking whether the image of this pair under the analytic isomorphism between the Riemann surface and algebraic curve is a rational point.

2.3 Rationality and mod p Representations of Elliptic Curves

We will be interested in rational and quadratic points, so given a point $[(E,\theta)]_H \in X_H$ we would like to understand over which field it is defined. We can do this directly by looking at the action of the Galois group on this point. Later we will see a way of reframing this in terms of the mod N representation of the elliptic curve E. We will then briefly consider the case of cusps. Write $G_{\mathbb{Q}} \coloneqq \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Definition 2.6. Let $\sigma \in G_{\mathbb{Q}}$ and let (E,θ) be an elliptic curve over $\overline{\mathbb{Q}}$ with level N structure θ. Then we define an action

$$(E,\theta)^\sigma \coloneqq (E^\sigma, \theta\circ\sigma^{-1}).$$

This action respects H-isomorphisms of pairs, and so we obtain an induced action on $Y_H(\overline{\mathbb{Q}})$.

Moreover, this action respects our analytic isomorphism between the Riemann surface and the algebraic curve, so $[(E,\theta)]_H \in X_H(\overline{\mathbb{Q}})$ is a rational point if and only if $[(E,\theta)]_H^\sigma = [(E,\theta)]_H$ for all $\sigma \in G_{\mathbb{Q}}$. Spelling this out, this holds if and only if E is defined over $\mathbb{Q}$ and for all $\sigma \in G_{\mathbb{Q}}$ there exist $h_\sigma \in H$ and $\varphi_\sigma \in \mathrm{Aut}(E)$ such that the following diagram commutes:

$$\begin{array}{ccc} E[N] & \xrightarrow{\theta} & (\mathbb{Z}/N\mathbb{Z})^2 \\ {\scriptstyle\varphi_\sigma}\downarrow & & \uparrow{\scriptstyle h_\sigma} \\ E[N] & \xrightarrow{\theta\circ\sigma^{-1}} & (\mathbb{Z}/N\mathbb{Z})^2. \end{array} \tag{1}$$

The following useful lemma tells us that given a point $[(E,\theta)]_H \in X_H(\overline{\mathbb{Q}})$, we can replace E by any elliptic curve isomorphic to it and obtain the same point as long as we choose the new level N structure appropriately.

Lemma 2.7. *Let $[(E_1, \theta_1)]_H \in X_H(\overline{\mathbb{Q}})$. Suppose $E_2/\overline{\mathbb{Q}}$ is an elliptic curve with $\varphi : E_1 \to E_2$ an isomorphism. Then $[(E_2, \theta_2)]_H = [(E_1, \theta_1)]_H$ where $\theta_2 = \theta_1 \circ \varphi$.*

The lemma holds simply by choosing $I \in H$ in Definition 2.3. It follows that if $[(E, \theta)]_H \in X_H(\mathbb{Q})$ then $E \cong E^\sigma$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, so $j(E) \in \mathbb{Q}$.

We now investigate the rationality of non-cuspidal points in terms of Galois representations of elliptic curves. We briefly recall the definition of the mod N representation of an elliptic curve. A more in-depth account can be found in [40, pp. 221-229].

Let $E/\mathbb{Q}$ be an elliptic curve and N a positive integer. Then $E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$ and is preserved by the action of $G_\mathbb{Q}$, so each $\sigma \in G_\mathbb{Q}$ can be viewed as a map from $E[N]$ to itself. In fact, $\sigma \in \mathrm{Aut}(E[N])$, so we have a map, $\overline{\rho}_{E,N}$, that assigns to each $\sigma \in G_\mathbb{Q}$ an element of $\mathrm{Aut}(E[N])$. This is known as the *mod N Galois representation* attached to E. After choosing a basis for $E[N]$ we can view this representation as a map

$$\overline{\rho}_{E,N} : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \cong \mathrm{Aut}(\mathbb{Z}/N\mathbb{Z}).$$

We are interested in $\overline{\rho}_{E,N}(G_\mathbb{Q})$, the image of this representation. This image depends on the choice of basis made for $E[N]$. A different choice of basis will lead to the image being a conjugate subgroup of the original image. So the image is only defined up to conjugation.

An important conjecture concerning mod N (in particular mod p for a prime p) Galois representations is *Serre's uniformity conjecture.*

Conjecture 2.8 (Serre's Uniformity Conjecture Version 1)**.** Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. Then $\overline{\rho}_{E,p}$ is surjective for all primes $p > 37$.

We will see in Section 3 how this conjecture can be rephrased in terms of modular curves.

Proposition 2.9. *Let E be an elliptic curve defined over $\mathbb{Q}$ and suppose that $\overline{\rho}_{E,N}(G_\mathbb{Q}) \subseteq H$ (up to conjugation). Then $[(E, \theta)]_H \in X_H(\mathbb{Q})$ for an appropriate choice of level N structure θ.*

Note that since conjugate subgroups give rise to isomorphic modular curves the statement of the proposition is well-defined.

Proof. Suppose $\overline{\rho}_{E,N}(G_\mathbb{Q})) \subseteq H$. Saying this means that we have already made a choice of basis. Write θ for the corresponding level N structure. Given $\sigma \in G_\mathbb{Q}$, write $h_\sigma = \overline{\rho}_{E,N}(\sigma)$ so that $\theta(P^\sigma) = h_\sigma(\theta(P))$. So $\theta = h_\sigma \circ \theta \circ \sigma^{-1}$. Then setting $\varphi_\sigma := id \in \mathrm{Aut}(E)$ makes Diagram 1 commute, meaning that $(E, \theta) \in X_H(\mathbb{Q})$. □

As for the cusps, we say a cusp is rational if it corresponds to a rational point on a model of the algebraic curve defined over $\mathbb{Q}$. In certain cases it is possible to describe this action concretely (for example if the Fourier coefficients of the q-expansions of the function field generators are rational; as is the case for $X_0(N)$ and $X_1(N)$). However, more generally, we do know that the cusps of X_H are always all defined over $\mathbb{Q}(\zeta_N)$. [43, pp. 12-14].

3 Non-Split Cartan Modular Curves

3.1 Non-Split Cartan Subgroups

We would like to consider certain special subgroups of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and the modular curves associated to them. We start by defining non-split Cartan subgroups and their normalisers. We then start investigating the modular curves associated to them and discuss quadratic points. We also see how non-split Cartan curves relate to Gauss' class number one problem and Serre's uniformity conjecture.

Let p be an odd prime and choose $\lambda \in \mathbb{F}_p$ a quadratic nonresidue. We define a *non-split Cartan subgroup* as

$$C_{ns}(p) \coloneqq \left\{ \begin{pmatrix} \alpha & \beta\lambda \\ \beta & \alpha \end{pmatrix} : (\alpha, \beta) \in \mathbb{F}_p^2 \setminus \{(0,0)\} \right\} \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

This subgroup is defined up to conjugation: a different choice of λ will lead to a conjugate subgroup. The normaliser of $C_{ns}(p)$ in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is denoted by $C_{ns}^+(p)$ and is given by

$$C_{ns}^+(p) \coloneqq \left\{ \begin{pmatrix} \alpha & \beta\lambda \\ \beta & \alpha \end{pmatrix}, \begin{pmatrix} \alpha & \beta\lambda \\ -\beta & -\alpha \end{pmatrix} : (\alpha, \beta) \in \mathbb{F}_p^2 \setminus \{(0,0)\} \right\} \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

This subgroup is again defined up to conjugation. For further information on non-split Cartan subgroups and their normalisers, as well as their definitions for composite n, we refer to [2, pp. 2754-2756]. As both $C_{ns}(p)$ and $C_{ns}^+(p)$ are defined up to conjugation, we can associate modular curves to these subgroups. Following the notation of the previous section, we have

$$X_{ns}(p) \coloneqq X_{C_{ns}(p)} \qquad \text{and} \qquad X_{ns}^+(p) \coloneqq X_{C_{ns}^+(p)}.$$

We will refer to both these modular curves, rather lazily, as *non-split Cartan modular curves*. We refer to the prime p as the *level* of the curve. Since for both of these subgroups the determinant map is surjective, the modular curves $X_{ns}(p)$ and $X_{ns}^+(p)$ are both defined over $\mathbb{Q}$.

Since $[C_{ns}^+(p) : C_{ns}(p)] = 2$, we see that the degeneracy map

$$\varrho : X_{ns}(p) \longrightarrow X_{ns}^+(p)$$

has degree 2. The curve $X_{ns}(p)$ comes with an automorphism, called the *modular involution*, which we denote w_p. This is the map that interchanges

the points of $\varrho^{-1}(P)$ for each $P \in X_{ns}^+(p)$. The curve $X_{ns}^+(p)$ is $X_{ns}(p)/\langle w_p \rangle$, and ϱ is the quotient map.

One important question concerns automorphisms of $X_{ns}(p)$. Is the modular involution the only non-trivial automorphism of this curve? This was recently answered in [17, p. 3] where it was shown that for all $p \geq 13$, $\mathrm{Aut}(X_{ns}(p)) = \langle w_p \rangle$ and $\mathrm{Aut}(X_{ns}^+(p)) = \{1\}$.

Next, we see that $X_{ns}(p)$ has no real points, let alone rational points.

Proposition 3.1. *Let $p \geq 3$, then $X_{ns}(p)(\mathbb{R}) = \emptyset$.*

Proof. First suppose $P = (E, \theta) \in Y_{ns}(\mathbb{R})$. Then replacing $\mathbb{Q}$ by $\mathbb{R}$ in Proposition 2.9, the same proof shows that $\overline{\rho}_{E,p}(G_{\mathbb{R}}) \subseteq C_{ns}(p)$ up to conjugation, where $G_{\mathbb{R}} \coloneqq \mathrm{Gal}(\mathbb{C}/\mathbb{R})$. Let $\sigma \in G_{\mathbb{R}}$ denote complex conjugation. Then $\overline{\rho}_{E,p}(\sigma) \in C_{ns}(p)$ has eigenvalues $+1$ and -1. However, since in the definition of $C_{ns}(p)$ the element λ is a quadratic non-residue, a simple check shows that no element of $C_{ns}(p)$ has characteristic polynomial $x^2 - 1$, a contradiction.

Then, since $Y_{ns}(\mathbb{R}) = \emptyset$ and we have finitely many cusps (which are smooth points), no cusp can be a real point, as otherwise $X_{ns}(p)(\mathbb{R})$ would be Zariski dense in $X_{ns}^+(p)(\mathbb{C})$ (see for example [41, p. 280]). It follows that $X_{ns}(p)(\mathbb{R}) = \emptyset$. □

In fact, $X_{ns}(p)$ has $p-1$ cusps and they form a single Galois orbit in $\mathbb{Q}(\zeta_p)$. The $(p-1)/2$ cusps of $X_{ns}^+(p)$ also form a single Galois orbit, but are all defined over the maximal real subfield $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ of $\mathbb{Q}(\zeta_p)$. [34, p. 195].

3.2 Jacobians and Chen's Isogenies

The Jacobians of the curves $X_{ns}(p)$ and $X_{ns}^+(p)$, which we denote $J_{ns}(p)$ and $J_{ns}^+(p)$ respectively, will play an important role in determining quadratic points. These Jacobians are related to the Jacobian of $X_0(p^2)$. This is useful as we understand this Jacobian well.

Given $N > 0$, write $f_1, \ldots, f_k$ for representatives of the Galois-conjugacy classes of Hecke eigenforms in the space of cuspforms $S_2(N)$. Write K_i for the Hecke eigenfield of f_i. This is a totally real number field, and we write d_i for its degree. To each f_i is associated a simple abelian variety $A_i/\mathbb{Q}$ of dimension d_i, with endomorphism algebra $\mathrm{End}(A_i) \otimes \mathbb{Q} = K_i$. In particular, the rank of A_i is a multiple of d_i. Each f_i arises from a newform at some level $M_i \mid N$. Write m_i for the number of divisors of N/M_i. Then

$$J_0(N) \sim A_1^{m_1} \times \cdots \times A_k^{m_k}.$$

It follows that $\mathrm{Rk}(J_0(N)) = \sum_{i=1}^k m_i \cdot \mathrm{Rk}(A_i)$. [29, p. 3481].

Although finding the rank of some A_i may not be feasible, it is sometimes possible to determine whether or not the rank is zero. Write $L(A_i, s)$ for the L-function of A_i. Then a theorem of Kolyvagin and Logachev [23]

asserts that if $L(A_i, 1) \neq 0$, then $\mathrm{Rk}(A_i) = 0$. Using the modular symbols algorithms of Cremona [11, pp. 29-31] and Stein [42, pp. 52-57], it is possible to check whether or not $L(A_i, 1)$ is zero. This is implemented in `Magma` as part of the 'modular abelian varieties package'.

Some of the abelian varieties in this decomposition are attached to the newforms at level N and the others come from oldforms. We denote by $J_0(N)_{\mathrm{new}}$ the product of those abelian varieties coming from newforms and we denote the product of the remaining abelian varieties (multiplicity included) by $J_0(N)_{\mathrm{old}}$, so that

$$J_0(N) \sim J_0(N)_{\mathrm{new}} \times J_0(N)_{\mathrm{old}}.$$

The following result links the Jacobians of non-split Cartan modular curves to the Jacobians of the curves $X_0(N)$ and $X_0^+(N) \coloneqq X_0(N)/\langle u_N \rangle$, where u_N denotes the Atkin-Lehner involution on $X_0(N)$ (we refer to [30, pp. 453-455] for a discussion of Atkin-Lehner involutions).

Proposition 3.2 (Chen's Isogenies [9, 14])**.** *Write $J_0(N)$ and $J_0^+(N)$ for the Jacobians of $X_0(N)$ and $X_0^+(N)$ respectively. Then*

$$J_{ns}(p) \sim J_0(p^2)_{\mathrm{new}},$$
$$J_{ns}^+(p) \sim J_0^+(p^2)_{\mathrm{new}}.$$

Note that $J_0^+(N) = J_0(N)/\langle u_N \rangle$, where we view u_N as an endomorphism of $J_0(N)$ under the inclusion $\mathrm{Aut}(X_0(N)) \hookrightarrow \mathrm{End}(J_0(N))$. Similarly, $J_{ns}^+(p) = J_{ns}(p)/\langle w_p \rangle$.

Of particular interest is the case when there are no newforms at level p, for example when $p = 13$. Since in this case, $J_{ns}(p) \sim J_0(p^2)_{\mathrm{new}} \sim J_0(p^2)$ and $J_{ns}^+(p) \sim J_0^+(p^2)_{\mathrm{new}} \sim J_0^+(p^2) \sim J_0(p^2)/\langle u_{p^2} \rangle$. Note that, as u_N is an involution,

$$J_0(N) \sim \frac{J_0(N)}{J_0^+(N)} \times J_0^+(N) \sim \ker(u_N + 1) \times \ker(u_N - 1).$$

So

$$\mathrm{Rk}(J_{ns}(p)) - \mathrm{Rk}(J_{ns}^+(p)) = \mathrm{Rk}(J_0(p^2)) - \mathrm{Rk}(J_0^+(p^2)) = \mathrm{Rk}(\ker(u_{p^2} + 1)).$$

By considering the L-function of the abelian variety $\ker(u_{p^2} + 1)$ as above, we can try and check whether or not $\mathrm{Rk}(\ker(u_{p^2} + 1)) = 0$. If this rank is zero, then $J_{ns}(p)$ and $J_{ns}^+(p)$ have equal rank, and it follows that $J_{ns}(p) = J_{ns}^+(p) \times \mathcal{A}$, for some abelian variety $\mathcal{A}$, with $\mathrm{Rk}(\mathcal{A}(\mathbb{Q})) = 0$.

3.3 Serre's Uniformity Conjecture

In Section 2 we saw Serre's uniformity conjecture stated in terms of mod p representations of elliptic curves (Conjecture 2.8). We would now like to reformulate this conjecture in terms of modular curves, and see the important role that $X_{ns}^+(p)$ plays.

Lemma 3.3. *Let $E/\mathbb{Q}$ be an elliptic curve and p a prime. If $\overline{\rho}_{E,p}(G_{\mathbb{Q}}) \supseteq \mathrm{SL}_2(\mathbb{F}_p)$, then $\overline{\rho}_{E,p}$ is surjective.*

Proof. From the properties of the Weil pairing, $\det \circ \overline{\rho}_{E,p} = \chi_p$, where χ_p is the mod p cyclotomic character, which is surjective on $G_{\mathbb{Q}}$. [12, p. 291]. So $\det : \overline{\rho}_{E,p}(G_{\mathbb{Q}}) \to (\mathbb{Z}/p\mathbb{Z})^*$ surjects. Since $\overline{\rho}_{E,p}(G_{\mathbb{Q}}) \supseteq \mathrm{SL}_2(\mathbb{F}_p)$, the kernel of this map is the whole of $\mathrm{SL}_2(\mathbb{F}_p)$, so by the first isomorphism theorem,

$$\big[\overline{\rho}_{E,p}(G_{\mathbb{Q}}) : \mathrm{SL}_2(\mathbb{F}_p)\big] = p - 1 = \big[\mathrm{GL}(\mathbb{F}_p) : \mathrm{SL}_2(\mathbb{F}_p)\big],$$

so $\overline{\rho}_{E,p}(G_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{F}_p)$. □

This means that we can replace surjectivity in Version 1 of Serre's conjecture by $\overline{\rho}_{E,p}(G_{\mathbb{Q}}) \supseteq \mathrm{SL}_2(\mathbb{F}_p)$. We would like to understand the possible images of $\overline{\rho}_{E,p}$ if its image does not contain $\mathrm{SL}_2(\mathbb{F}_p)$.

Theorem 3.4 (Dickson [24, pp. 712-722])**.** *Let H be a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ that does not contain $\mathrm{SL}_2(\mathbb{F}_p)$. Then up to conjugation, either $H \subseteq B_0(p)$, or $H \subseteq C_{ns}^+(p)$, or $H \subseteq C_s^+(p)$, or H is an exceptional subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$.*

Here, $C_s^+(p) \coloneqq \left\{ \left(\begin{smallmatrix} \alpha & 0 \\ 0 & \beta \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & \alpha \\ \beta & 0 \end{smallmatrix}\right) \middle| \alpha, \beta \in \mathbb{F}_p^* \right\}$ is the *normaliser of a split Cartan subgroup*, and an *exceptional subgroup of* $\mathrm{GL}_2(\mathbb{F}_p)$ is one whose image in $\mathrm{PGL}_2(\mathbb{F}_p)$ is isomorphic to A_4, S_4, or A_5. In order to prove the uniformity conjecture, it is enough to show that $\overline{\rho}_{E,p}(G_{\mathbb{Q}})$ does not lie in one of the subgroups appearing in Theorem 3.4.

Using Proposition 2.9, if $\overline{\rho}_{E,p}(G_{\mathbb{Q}}) = H$ then $(E, \theta) \in X_H(\mathbb{Q})$ for an appropriate choice of level structure θ. If E has complex multiplication then we call (E, θ) a *CM point*. So asking that, for example, $\overline{\rho}_{E,p}(G_{\mathbb{Q}}) \neq C_{ns}^+(p)$ for all elliptic curves $E/\mathbb{Q}$ without CM, is equivalent to saying that the only rational points on $X_{ns}^+(p)$ are either CM points or cusps. Using this idea and Theorem 3.4, we can reformulate Serre's conjecture.

Conjecture 3.5 (Serre's Uniformity Conjecture Version 2)**.** Let $p > 37$ be prime. Then all rational points of the modular curves $X_0(p)$, $X_s^+(p) \coloneqq X_{C_s^+(p)}$, $X_{ns}^+(p)$, and X_H with H exceptional are either cusps or CM points.

Much progress has been made with this conjecture. Serre himself proved [33, pp. 197-198] that if H is exceptional then $X_H(\mathbb{Q}) = \emptyset$ for $p \geq 17$. Mazur showed in [26] that $X_0(p)(\mathbb{Q})$ consists of cusps and CM points for $p > 37$, and in [1, 4] it has been shown that $X_s^+(p)(\mathbb{Q})$ consists of cusps and CM points for $p \geq 11$. The only case case remaining is that of $X_{ns}^+(p)(\mathbb{Q})$, and this is a famous open problem.

3.4 Class Number One Problem

One beautiful application of the theory of modular curves is to the seemingly unrelated Class Number One problem.

Theorem 3.6 (Class Number One)**.** *The imaginary quadratic field* $\mathbb{Q}(\sqrt{-d})$ *has class number one if and only if* $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$.

The class number one problem has a long and rich history as it remained unsolved for many years.

The following lemma reduces the problem to something fairly concrete.

Lemma 3.7. *Let* p *be a rational prime. If* p *is not inert in* $K \coloneqq \mathbb{Q}(\sqrt{-d})$*, and* $h(K) = 1$*, then* $d \leq 4p$*. In particular, there are only finitely many imaginary quadratic fields of class number one in which* p *is not inert.*

Proof. Based on [13, p. 2]. We first show that if $K = \mathbb{Q}(\sqrt{-d})$ is an imaginary quadratic field with $h(K) = 1$, then $d = 1, 2$, or $d = q \equiv 3 \pmod 4$, with q prime.

To see this, suppose $d > 2$ and $d \equiv 1$ or $2 \pmod 4$. Then 2 ramifies in K and so the prime above 2 has norm 2. However, this prime ideal is principal, so $a^2 + db^2 = 2$ for some $a, b \in \mathbb{Z}$, a contradiction.

If $d \equiv 3 \pmod 4$ and is composite, then let q be the smallest prime dividing d. Then q ramifies in K, so the prime above q has norm q. If this prime ideal is principal, then $a^2/4 + db^2/4 = q$ for some $a, b \in \mathbb{Z}$. As $d \geq 3$ and is composite, $d \geq 5q > 4q$, so $q > a^2/4 + b^2 q$, a contradiction.

Suppose now that p is not inert in K. If $d = 1$ or 2 the result holds, so we will assume d is a prime $q \equiv 3 \pmod 4$. Then if $p = q$ the result holds, so assume $p \neq q$ so that p splits in K, and we can write $p\mathcal{O}_K$ as a product of prime ideals, each principal of norm p. This means that $a^2/4 + qb^2/4 = p$ for some $a, b \in \mathbb{Z}$, from which we can deduce $q \leq 4p$. □

This lemma reduces the problem to finding the imaginary quadratic extensions in which a given prime p is inert. The crucial result which links this with modular curves is the following.

Theorem 3.8. *Let* p *be a rational prime, and let* K *be an imaginary quadratic field of class number one in which* p *is inert. Then the elliptic curve* $E_{\mathcal{O}_K} v \coloneqq \mathbb{C}/\mathcal{O}_K$ *gives rise to a CM integral point on* $X_{ns}^+(p)$.

Here, by an *integral* point, we mean a point $P \in X_{ns}^+(p)(\mathbb{Q})$ for which $j(P) \in \mathbb{Z}$. By this theorem, if we can list all the CM integral points on $X_{ns}^+(p)$, this will give us a finite list of imaginary quadratic fields by considering the CM fields of these points. We then know that if p is inert in an imaginary quadratic field of class number one, then this field must be contained in our list. This leaves us with a straightforward check.

We will see why Theorem 3.8 holds and then briefly describe how one can find all integral points on these curves.

We start by considering elliptic curves as quotients of the complex plane by a lattice. Let K be an imaginary quadratic field with ring of integers $\mathcal{O}_K$, and let $\mathfrak{a}$ be a fractional ideal of K. Then we can view $\mathfrak{a}$ as a lattice in

$\mathbb{C}$ and we write $E_{\mathfrak{a}} \coloneqq \mathbb{C}/\mathfrak{a}$ for the elliptic curve associated to $\mathfrak{a}$. Moreover, by the theory of complex multiplication, we have that

$$\mathrm{End}(E_{\mathfrak{a}}) \cong \{\alpha \in \mathbb{C} \mid \alpha\mathfrak{a} \subseteq \mathfrak{a}\} = \mathcal{O}_K,$$

with the last equality holding as $\mathfrak{a}$ is a fractional ideal. Saying that two fractional ideals are equal in $\mathrm{Cl}(K)$ is equivalent to saying that they are homothetic as lattices of $\mathbb{C}$, meaning they give rise to isomorphic elliptic curves. Conversely, if $E = \mathbb{C}/\Lambda$ is an elliptic curve with $\mathrm{End}(E) \cong \mathcal{O}_K$, then $\mathrm{End}(E) \cong \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\} \cong \mathcal{O}_K$, meaning that Λ is a fractional ideal of $\mathcal{O}_K$. This sets up the following bijection.

Proposition 3.9. *Write $\mathcal{E}(\mathcal{O}_K)$ for the set of elliptic curves over $\mathbb{C}$ with endomorphism ring $\mathcal{O}_K$ up to $\mathbb{C}$-isomorphism. Then there is a bijection*

$$\begin{aligned} \mu : \mathrm{CL}(K) &\longrightarrow \mathcal{E}(\mathcal{O}_K) \\ [\mathfrak{a}] &\longmapsto [E_{\mathfrak{a}}]. \end{aligned}$$

In particular, if $h(K) = 1$, then there is a unique elliptic curve over $\mathbb{C}$ (up to $\mathbb{C}$-isomorphism), $E_{\mathcal{O}_K}$, with endomorphism ring $\mathcal{O}_K$. Furthermore, when $h(K) = 1$, we have $j(E_{\mathcal{O}_K}) \in \mathbb{Z}$.

The only part of this Proposition not addressed by the discussion above is the fact that $j(E_{\mathcal{O}_K}) \in \mathbb{Z}$ when $h(K) = 1$. This can be demonstrated using elementary methods, but is somewhat lengthy, and so we refer to [39, pp. 140-151] for a proof (in fact many proofs).

Proof of Theorem 3.8. [13, pp. 28-29]. Proving the Theorem is reduced to showing that if p is inert in K, then there is an appropriate choice of level structure θ such that $[E_{\mathcal{O}_K}, \theta]_{C_{ns}^+(p)} \in X_{ns}^+(p)(\mathbb{Q})$, and by Proposition 2.9, it is enough to show that $\overline{\rho}_{E,p}(G_{\mathbb{Q}}) \subseteq C_{ns}^+(p)$ (up to conjugation).

As a lattice in $\mathbb{C}$, we can write $\mathcal{O} \coloneqq \mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\mu$, and as p is inert in K, $\lambda \coloneqq \mu^2$ is a quadratic nonresidue in $\mathbb{F}_p$ and can be chosen to define $C_{ns}(p)$. Now $E[p] \cong \mathcal{O}/p\mathcal{O} \cong \mathbb{F}_{p^2} = \mathbb{F}_p(\mu)$ because p is inert in K. The group $(\mathcal{O}/p\mathcal{O})^*$ acts on the 2-dimensional $\mathbb{F}_p$-vector space $\mathcal{O}/p\mathcal{O}$ by multiplication, and so we obtain a representation $\kappa : (\mathcal{O}/p\mathcal{O})^* \hookrightarrow \mathrm{GL}_2(\mathbb{F}_p)$. Explicitly, using the basis $\{1, \mu\}$ of $\mathcal{O}/p\mathcal{O}$, we have, for $a\mu + b \in (\mathcal{O}/p\mathcal{O})^*$,

$$\begin{aligned} (a + b\mu) \cdot 1 &= a \cdot 1 + b \cdot \mu, \\ (a + b\mu) \cdot \mu &= (b\lambda) \cdot 1 + a \cdot \mu. \end{aligned}$$

So $\kappa(a\mu + b) = \left(\begin{smallmatrix} a & b\lambda \\ b & a \end{smallmatrix}\right) \in C_{ns}(p)$. So $\kappa((\mathcal{O}/p\mathcal{O})^*) = C_{ns}(p)$.

Write $H \coloneqq \overline{\rho}_{E,p}(G_{\mathbb{Q}})$ and $N \coloneqq \overline{\rho}_{E,p}(G_K)$, where $G_K \coloneqq \mathrm{Gal}(\overline{K}/K) = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$. Since G_K fixes K, it also fixes $\mathcal{O}$, so the actions of G_K and $(\mathcal{O}/p\mathcal{O})^*$ on $E[p] \cong \mathcal{O}/p\mathcal{O}$ commute. It follows that N commutes with $C_{ns}(p)$, and a straightforward check shows that $C_{ns}(p)$ is its own centraliser

in $\mathrm{GL}_2(\mathbb{F}_p)$, so $N \subseteq C_{ns}(p)$. The kernel of the restriction map $G_{\mathbb{Q}} \to \mathrm{Gal}(K/\mathbb{Q})$ is G_K, so G_K is normal in G_Q, meaning that N is normal in H. So H lies in the normaliser of N, and $N \subseteq C_{ns}(p) \subseteq C_{ns}^+(p)$, the normaliser of $C_{ns}(p)$, so $H \subseteq C_{ns}^+(p)$, as required. □

It is also possible to prove Theorem 3.8 for all natural numbers n, not just for primes, by generalising the definition of a non-split Cartan subgroup. Baran, in [2], provides an in-depth account of what has been carried out for various $n \in \mathbb{N}$, thereby describing many possible routes for proving the class number one problem. In fact the original proof of the class number one problem by Heegner (which was formalised by Stark) is really a classification of the integral points on $X_{ns}^+(24)$, although it is not presented in this way.

Finding all integral points on $X_{ns}^+(p)$ for a given p is itself a difficult problem. The curves $X_{ns}^+(5)$ and $X_{ns}^+(7)$ are of genus 0. The curves $X_{ns}^+(11)$ and $X_{ns}^+(13)$ are of genus 1 and 3 respectively. For $p = 5$ and $p = 7$, the basic strategy for listing all integral points on $X_{ns}^+(p)$ is to express the j-map, $j : X_{ns}^+(p) \to \mathbb{P}^1$ in terms of a *Hauptmodul* for $X_{ns}^+(p)$, which is an explicit isomorphism $\eta : X_{ns}^+(p) \to \mathbb{P}^1$. This is done by considering the ramification points of the j-map, and due to computational issues, passing through an intermediate curve (or curves). This was carried out for $p = 5$ by Chen in [10] and for $p = 7$ by Kenku in [22]. The integral points on $X_{ns}^+(11)$ are found in [32] using linear forms in elliptic logarithms. Finally, as we will see later, the case $p = 13$ was recently resolved [1].

3.5 Quadratic Points

We now turn our attention to quadratic points on $X_{ns}(p)$. We write $\varrho : X_{ns}(p) \to X_{ns}^+(p)$ for the degree 2 degeneracy map and w_p for the modular involution on $X_{ns}(p)$. We would like to describe all quadratic points on $X_{ns}(p)$. Since $X_{ns}(p)(\mathbb{R}) = \emptyset$ (Proposition 3.1), all quadratic points will come in pairs, defined over some imaginary quadratic field.

One way of obtaining quadratic points on $X_{ns}(p)$ is by pulling back rational points on $X_{ns}^+(p)$: if $P \in X_{ns}^+(p)(\mathbb{Q})$ then $\varrho^*(P)$ is a pair of quadratic points on $X_{ns}(p)$. We call such quadratic points *non-exceptional*. If on the other hand we have a quadratic point $Q \notin \varrho^* X_{ns}^+(p)(\mathbb{Q})$, then we say that Q is *exceptional*. The main theorem of this project is the following.

Theorem 1.1 (Main theorem)**.** *There are no exceptional quadratic points on $X_{ns}(p)$ for $p = 7, 11,$ or 13.*

As discussed in the introduction, quadratic points on the curves $X_0(N)$ of small genus are well understood. Due to the similarities between $X_0(p)$ and $X_{ns}(p)$, one might hope to be able to apply similar techniques to those in [31, 5] to study quadratic points on $X_{ns}(p)$. The equations for the curves $X_{ns}(7)$ and $X_{ns}(11)$ are relatively simple and Theorem 1.1 can be proved

for these curves fairly directly. For $p = 7$ we follow Siksek's proof [38], and use similar ideas for the case $p = 11$. The curve $X_{ns}(13)$ is of genus 8 and its equations are naturally much more complicated. For this case we use the method of Chabauty for symmetric powers of curves developed in [35]. The application of this method is similar to how it is used in [5]. The main difference in the case of $X_{ns}(13)$ is the inability to get a handle on the Mordell-Weil group of its Jacobian.

Corollary 1.2. *Let E be an elliptic curve defined over a quadratic field K such that $\overline{\rho}_{E,p}(Gal(\overline{K}/K)) \subseteq C_{ns}(p)$ for $p = 7, 11,$ or 13. Then $j(E) \in \mathbb{Q}$. Thus E is modular.*

Proof. The elliptic curve E gives rise to a non-cuspidal K-point (i.e. a non-cuspidal quadratic point), $[E, \theta]_{C_{ns}(p)}$, on $X_{ns}(p)$ by appropriate choice of level structure θ. Then $\varrho(E, \theta) = (E, \theta)$, now viewed as a point on $X^+_{ns}(p)$ which we know is rational by Theorem 1. Then $j(E) = j(E, \theta) \in \mathbb{Q}$ as the j-map is rational. We then know that E is modular by [12]. □

We note that Theorem 1.1 concerns only $p = 7, 11$, and 13. For $p \leq 5$, $X^+_{ns}(p)$ has genus 0, but what about for $p \geq 17$? Unfortunately, equations for $X_{ns}(p)$ (if any were known) would be far too complicated to carry out explicit computations using our methods. The genus grows quickly, with $X_{ns}(17)$ and $X_{ns}(19)$ having genera 15 and 20 respectively. Even equations for $X^+_{ns}(p)$ become difficult to compute and work with for $p \geq 17$. For example, in [28], a model for the genus 13 curve $X^+_{ns}(23)$ is computed, given by 55 equations. Given these computational issues, it seems as though a more general theoretical argument is needed.

4 Quadratic Points on $X_{ns}(7)$

The curve $X_{ns}(7)$ is of genus 1 and the curve $X^+_{ns}(7)$ is of genus 0. An affine model for $X_{ns}(7)$ is given in [44, p. 24] by the following equation:

$$y^2 = -(2x^4 - 14x^3 + 21x^2 + 28x + 7),$$

with the map $\varrho : X_{ns}(7) \to X^+_{ns}(7) \cong \mathbb{P}^1$ given by $(x, y) \mapsto x$. Homogenising gives the following model in weighted projective space $\mathbb{P}_{(1,2,1)}$:

$$Y^2 = -(2X^4 - 14X^3Z + 21X^2Z^2 + 28XZ^3 + 7Z^4).$$

We apply the change of coordinates

$$(X : Y : Z) \mapsto \left(\frac{3X}{2} : Y : -\frac{3X}{2} + 2Z\right)$$

to obtain a new model for $X_{ns}(7)$ in $\mathbb{P}_{(1,2,1)}$ with equation

$$Y^2 = -81X^4 + 189X^2Z^2 - 112Z^4.$$

The map ϱ in these new coordinates is given by $\varrho(X : Y : Z) = (3X/2 : -3X/2 + 2Z)$. Let $P := (u : v : w)$ be a quadratic point on this model. As the pair of points at infinity, which we denote ∞_+ and ∞_-, are non-exceptional, we can assume that $w = 1$. Then it will be enough to show that $u \in \mathbb{Q}$ to show that P is non-exceptional, as if $u \in \mathbb{Q}$, we have $\varrho(P) = (3u/2 : 3u/2 + 2) \in \mathbb{P}^1(\mathbb{Q}) \cong X_{ns}^+(7)(\mathbb{Q})$.

The reason for using this new model is that it is a double cover of the conic $\mathcal{C} \subseteq \mathbb{P}^2$ given by $Y^2 = -81X^2 + 189XZ - 112Z^2$. Note that $\mathcal{C}(\mathbb{Q}) = \emptyset$. We will use this to better understand $X_{ns}(7)$. We follow the proof of Siksek [38] to show that P is non-exceptional.

Lemma 4.1. *The group* $\mathrm{Pic}^0(X_{ns}(7)/\mathbb{Q}) = 0$.

Proof. Since X has genus 1, $J_{ns}(7)$ is an elliptic curve. By Chen's isogeny (Proposition 3.2), $J_{ns}(7) \sim J_0(49)_{\text{new}}$, so $J_{ns}(7)$ must be an elliptic curve of conductor 49. There are four elliptic curves of conductor 49, each of which has Mordell-Weil group $\mathbb{Z}/2\mathbb{Z}$, so we must have $J_{ns}(7)(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$. In fact one can verify that $J_{ns}(7)$ is the elliptic curve with Cremona reference 49A2.

From the inclusion $\mathrm{Pic}^0(X_{ns}(7)/\mathbb{Q}) \hookrightarrow J_{ns}(7)(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$, we know that $\mathrm{Pic}^0(X_{ns}(7)) = 0$ or $\mathbb{Z}/2\mathbb{Z}$. To prove that $\mathrm{Pic}^0(X_{ns}(7)) = 0$, we must show that the non-trivial rational divisor class of degree 0 cannot be represented by a rational divisor. We work on the affine patch $Z = 1$. Our model on this affine patch is given by the equation

$$y^2 = -81x^4 + 189x^2 - 112.$$

The non-trivial rational divisor class of degree 0 can be represented by the divisor $D := \infty_+ - \infty_-$, since a straightforward check shows that $\mathrm{div}(\mathrm{g}) = 2D$, where

$$g := 2y + 18ix^2 - 21i.$$

Note that i denotes $\sqrt{-1}$ here. Suppose for a contradiction that $D \sim D'$ with D' a rational degree 0 divisor. By Riemann-Roch, $D' + \infty_+ + \infty_-$ is lineary equivalent to an effective degree 2 rational divisor, say

$$D' + \infty_+ + \infty_- \sim Q + Q',$$

where Q is a quadratic point, and Q' its Galois conjugate. Then

$$Q + Q' - 2\infty_+ \sim D' - (\infty_+ - \infty_-) \sim D' - D \sim 0. \tag{2}$$

Since $\infty_+ \in X_{ns}(7)(\mathbb{Q}(i))$, by (2) there exists $f \in \mathbb{Q}(i)(X_{ns}(7))$ such that $\mathrm{div}(f) = Q + Q' - 2\infty_+$. So $f \in \mathcal{L}(2\infty_+)$ and $f(Q) = f(Q') = 0$. The elements $1, y + 9ix^2$ form a $\mathbb{Q}(i)$-basis for $\mathcal{L}(2\infty_+)$, so after rescaling we can write $h = y + 9ix^2 + \alpha$ for some $\alpha \in \mathbb{Q}(i)$. The vanishing locus of h on the curve X is given by

$$x^2 = \frac{-37}{6i\alpha - 63}, \qquad y = \frac{111i}{2i\alpha - 21} - \alpha.$$

So $x(Q)^2 = x(Q')^2$ and $y(Q) = y(Q')$. As Q and Q' are Galois conjugates, we must have that $x(Q)^2, y(Q) \in \mathbb{Q}$. This means that $(x(Q)^2, y(Q)) \in \mathcal{C}(\mathbb{Q})$, but $\mathcal{C}(\mathbb{Q}) = \emptyset$, a contradiction. □

Using this Lemma, the proof of Theorem 1.1 for $p = 7$ follows quickly. On the affine patch $Z = 1$, $P = (u, v)$, and we write $P' \coloneqq (u', v')$ for the quadratic conjugate of P. Then $D \coloneqq P + P'$ is a rational effective degree 2 divisor, and $\infty_+ + \infty_-$ is too. So $D - \infty_+ - \infty_- \sim 0$ because $\mathrm{Pic}^0(X_{ns}(7)/\mathbb{Q}) = 0$. It follows that there is an $h \in \mathcal{L}(\infty_+ + \infty_-)$ satisfying $h(P) = h(P') = 0$. Since X has genus 1, $l(\infty_+ + \infty_-) = 2$ and $\{1, x\}$ is a $\mathbb{Q}$-basis for this Riemann-Roch space. This means that we can write, after rescaling, $h = x + a$ for some $a \in \mathbb{Q}$. Then $0 = h(P) = u + a$, so $u = -a \in \mathbb{Q}$ as required.

5 Quadratic Points on $X_{ns}(11)$

The curve $X_{ns}(11)$ is of genus 4 and a model for this curve is given in [15, p. 97] by the following equations in $\mathbb{A}^3_{x,y,t}$:

$$\begin{aligned} y^2 + y &= x^3 - x^2 - 7x + 10, \\ t^2 &= -(4x^3 + 7x^2 - 6x + 19). \end{aligned}$$

Each of these two equations defines an elliptic curve in its own right. The first of the two equations is in fact the defining equation of $X^+_{ns}(11)$; that is, the curve $X^+_{ns}(11)$ is the elliptic curve defined by

$$y^2 + y = x^3 - x^2 - 7x + 10.$$

This curve has rank 1 and its rational points form an infinite cyclic group generated by the point $(4, -6)$.

The map $\varrho : X_{ns}(11) \to X^+_{ns}(11)$ is then given by $(x, y, t) \mapsto (x, y)$. This means that to verify Theorem 1.1 for $p = 11$, it will suffice to show that if $(u, v, w) \in X_{ns}(11)$ is a quadratic point, then $u, v \in \mathbb{Q}$; with the slight caveat that we must consider the points at infinity which are not on this affine patch, but a straightforward check shows that they are non-exceptional.

The way we show Theorem 1.1 holds for $p = 11$ is to use the maps from $X_{ns}(11)$ down to various elliptic curves, namely the elliptic curves over $\mathbb{Q}$ with conductor 121. By Chen's isogeny, we know that $J_{ns}(11) \sim J_0(11^2)_{\mathrm{new}}$. At level 121 there are four Galois-conjugacy classes of newforms, and to each of these is associated an elliptic curve of conductor 121, so

$$J_{ns}(11) \sim J_0(121)_{\mathrm{new}} \sim A_1 \times A_2 \times A_3 \times A_4,$$

the product of these four elliptic curves. Here, A_2 is the elliptic curve of rank 1 isomorphic to $X^+_{ns}(11)$, A_3 is the elliptic curve mentioned above with

defining equation

$$t^2 = -(4x^3 + 7x^2 - 6x + 19)$$

which has trivial Mordell-Weil group; we denote this curve by E. Finally A_1 and A_4 also have trivial Mordell-Weil group. Moreover, [15, pp. 100-101] gives the maps to these elliptic curves.

Lemma 5.1. *Let $P := (u, v, w) \in X_{ns}(11)$ be a quadratic point. Then $u \in \mathbb{Q}$.*

Proof. Write $\mathbb{Q}(P) = \mathbb{Q}(\sqrt{d})$ with d a squarefree integer, and write $P' = (u', v', w')$ for the quadratic conjugate of P.

To show $u \in \mathbb{Q}$, we consider the map $\psi : X_{ns}(11) \to E$ given by $(x, y, t) \mapsto (x, t)$. Write $D := P + P'$ for the rational effective degree 2 divisor on $X_{ns}(11)$, and $\psi(D) = (u, w) + (u', w')$ for its pushforward by ψ, which is a rational effective degree 2 divisor on the elliptic curve $E = A_3$. Since $E(\mathbb{Q}) = \{\infty_E\}$, $\mathrm{Pic}^0(E) = 0$, so $\left[\psi(D) - 2\infty_E\right] = [0]$. So $\psi(D) \sim 2\infty_E$. Now $\psi(D) \neq 2\infty_E$ because (u, w) is an affine point of the curve, so we have a non-constant function $h \in \mathbb{Q}(E)$ satisfying

$$\mathrm{div}(h) = \psi(D) - 2\infty_E.$$

So $h \in \mathcal{L}(2\infty_E)$ with $h(u, w) = h(u', w') = 0$. Now $1, x \in \mathcal{L}(2\infty_E)$ form a $\mathbb{Q}$-basis for this Riemann-Roch space, so we can write (after rescaling) $h = x - \alpha$ for some α in $\mathbb{Q}$. Then $0 = h(u, w) = u - \alpha$, so $u \in \mathbb{Q}$. □

Next we aim to show that $v \in \mathbb{Q}$. Since $E(\mathbb{Q}) = \{\infty_E\}$, we know that w cannot also be rational, so $w \in \mathbb{Q}(\sqrt{d})\backslash\mathbb{Q}$. As $\mathbb{Q}(P) = \mathbb{Q}(\sqrt{d})$ we must have $v \in \mathbb{Q}(\sqrt{d})$. Suppose for a contradiction that $v \notin \mathbb{Q}$. As $P \in X_{ns}(11)$, we know that v and w satisfy the following two equations; which we view as quadratic equations in v and w respectively:

$$v^2 + v - (u^3 - u^2 - 7u + 10) = 0$$
$$w^2 + (4u^3 + 7u^2 - 6u + 19) = 0.$$

Since $v, w \in \mathbb{Q}(\sqrt{d})\backslash\mathbb{Q}$, the discriminant of each of these equations is of the form da^2 for some non-zero integer a; say da_1^2 and da_2^2 for the first and second equations respectively. In particular, the product of the discriminants, $(da_1a_2)^2$, is a rational square, and so we have a rational point on the curve with affine equation

$$r^2 = (4s^3 - 4s^2 - 28s + 41)(-16s^3 - 28s^2 + 24s - 76).$$

Replacing r by $2r$, we have an affine rational point on the curve which we denote H, with affine equation

$$r^2 = -(4s^3 - 4s^2 - 28s + 41)(4s^3 + 7s^2 - 6s + 19).$$

The polynomial in s on the right-hand side of this equation has no repeated roots, so H is a hyperelliptic curve of genus 2. To obtain our desired contradiction it will be enough to show $H(\mathbb{Q}) = \emptyset$.

The hyperelliptic curve H is the same curve considered in [15, p. 100]. This curve appears as the maps from $X_{ns}(11)$ to both A_1 and A_4 factor through H. In particular we have maps from H to A_1 and A_4 defined over $\mathbb{Q}$. We need only consider one of these, say the map $\pi : H \to A_1$. Since $A_1(\mathbb{Q}) = \{\infty_{A_1}\}$, we know $H(\mathbb{Q}) \subseteq \pi^{-1}\{\infty_{A_1}\} = \{\infty_+, \infty_-\}$, where $\infty_+ = (4i : 1 : 0)$ and $\infty_- = (-4i : 1 : 0)$ are the two points at infinity on H, neither of which is rational, so we conclude that $H(\mathbb{Q}) = \emptyset$. So $v \in \mathbb{Q}$, meaning that $P \in \varrho^*(X_{ns}(11)(\mathbb{Q})$. This proves the theorem in the case $p = 11$.

6 Symmetric Chabauty and Sieve

6.1 Chabauty-Coleman

We recall here the basic idea of the standard Chabauty method for algebraic curves. A much more detailed account of this method can be found in [27]. We will then compare and contrast this method with the symmetric Chabauty method.

We start with a smooth projective curve C defined over $\mathbb{Q}$ with Jacobian $J = J(C)$ of rank r. Write g for the genus of C and assume $g \geq 2$. By Falting's theorem we know that $C(\mathbb{Q})$ is finite, but the proof of this result gives us no indication as to how one might find $C(\mathbb{Q})$. In order to apply the method of Chabauty-Coleman, we additionally require that $r < g$. This extra assumption gives rise to a strategy for finding $C(\mathbb{Q})$. Let p be a prime of good reduction for C. We suppose that we have a non-empty set of known rational points $\mathcal{L} \subseteq C(\mathbb{Q})$ so that $\mathcal{L} \twoheadrightarrow C(\mathbb{F}_p)$ surjects.

The basic idea is to bound, for each $P \in C(\mathbb{F}_p)$, the number of points of $C(\mathbb{Q})$ that lie above P. Given some point $Q \in C(\mathbb{Q})$ that reduces modulo p to P, we call the set of points that reduce to P the *mod p residue disc* of Q. If, for each $P \in C(\mathbb{F}_p)$, we can match the Chabauty bound by using points in $\mathcal{L}$, then $\mathcal{L} = C(\mathbb{Q})$. Even if this is not possible, it may be feasible to use a version of the Mordell-Weil sieve to conclude that $\mathcal{L} = C(\mathbb{Q})$.

Finding these Chabauty bounds relies on the following pairing:

$$\begin{aligned} \Omega_{C/\mathbb{Q}_p} \times J(\mathbb{Q}_p) &\longrightarrow \mathbb{Q}_p \\ \Big(\omega, \Big[\sum_i (P_i - Q_i)\Big]\Big) &\longmapsto \sum_i \int_{P_i}^{Q_i} \omega \end{aligned}$$

where $\Omega_{C/\mathbb{Q}_p}$ is the space of regular differentials on the curve C viewed as a curve over $\mathbb{Q}_p$. This pairing is $\mathbb{Q}_p$-linear on the left, $\mathbb{Z}$-linear on the right, and

its kernel on the right is $J(\mathbb{Q}_p)_{\text{tors}}$. The integrals are evaluated by expanding ω as a power series in a uniformiser.

The condition $r < g$ ensures the existence of an *annihilating differential*: a differential $\omega \in \Omega_{C/\mathbb{Q}_p}$ such that

$$\langle \omega, D \rangle = 0 \quad \text{for all} \quad D \in J(\mathbb{Q}_p).$$

Using this annihilating differential we can form an equation in terms of a uniformiser, allowing us to bound the number of points that reduce modulo p to a given point. This is how the Chabauty bounds are obtained.

6.2 Symmetric Chabauty

We now look into how the Symmetric Chabauty method works. We start with a set $\mathcal{L}$ of known quadratic points. This method is really a combination of two parts.

1. Chabauty step: for each known non-exceptional quadratic point Q, try and show, for various primes p, that there are no exceptional points in the mod p residue disc of Q.

2. Sieve step: use the information obtained from the Chabauty step to sieve for unknown rational points.

Each of these steps could hypothetically be used separately to conclude that $\mathcal{L}$ consists of all quadratic points, but this is rare, and in practice it is the combination of the two parts that yields results. We note that there are in fact two variants of the Chabauty step. One is as described above, and considers non-exceptional quadratic points. This will be all we need to study $X_{ns}(13)$. However, if the curve has known exceptional quadratic points, then the method can be adapted [35, pp. 217-218] to attempt to show that an exceptional quadratic point is alone in its residue disc. We start by considering the Chabauty step. This method is developed in [35] with some adaptations (which we use) described in [5].

We first change how we view quadratic points. Given a smooth projective curve X over $\mathbb{Q}$, we write $X^{(2)}$ for its symmetric square. This is $(X \times X)/\sim$ where $(P_1, Q_1) \sim (P_2, Q_2)$ if $(P_1, Q_1) = \sigma(P_2, Q_2)$ for some $\sigma \in S_2$. The reason we consider $X^{(2)}$ is because we can view a pair of quadratic points $(P, \overline{P})$ on X as a *rational* point on $X^{(2)}$, and we can simply write $P \in X^{(2)}(\mathbb{Q})$. A simple way of representing this point is as a degree 2 effective rational divisor $D \coloneqq P + \overline{P} \in X^{(2)}(\mathbb{Q})$. From now on, when we speak of quadratic points, or rational points on $X^{(2)}$, or of degree 2 effective rational divisors, we really mean the same thing. We can rephrase Theorem 1.1 as $X_{ns}^{(2)}(p)(\mathbb{Q}) = \varrho^* X_{ns}^{+}(p)(\mathbb{Q})$ for $p = 7, 11$, or 13.

Ideally we would like to simply carry over the usual method of Chabauty to study $X^{(2)}(\mathbb{Q})$. This is not directly possible, but with some adaptations

we can apply similar techniques. We suppose we have an involution $w \in \mathrm{Aut}_{\mathbb{Q}}(X)$ with corresponding degree 2 map $\varrho : X \to C$, and that $C(\mathbb{Q}) \neq \emptyset$, so that $X^{(2)}(\mathbb{Q}) \neq \emptyset$. This gives us a basepoint, which we write as $\infty \in X^{(2)}(\mathbb{Q})$, for the Abel-Jacobi map

$$\begin{aligned} \iota : X^2(\mathbb{Q}) &\hookrightarrow J(\mathbb{Q}) \\ Q &\longmapsto \big[Q - \infty\big]. \end{aligned}$$

We then have a condition analogous to the condition $r < g$ from the previous subsection; we require

$$r_X - r_C < g_X - g_C,$$

where r_X and r_C are the ranks of $J(X)$ and $J(C)$, and g_X and g_C are the genera of X and C. Note that C may well have infinitely many rational points, as in the case $C = X^+_{ns}(11)$.

Write Ω_X and Ω_C for the spaces of holomorphic differentials on X and C respectively. Rather than simply looking for an annihilating differential as in the Chabauty-Coleman method, we need to look for holomorphic differentials, v, that are first of all annihilating, but also satisfy $\mathrm{Tr}(v) \coloneqq v + w^*v = 0$. Write V_0 for the space of such differentials on $X^{(2)}(\mathbb{Q})$. We use the same pairing described in the previous subsection.

Proposition 6.1. *Assume $r_X = r_C$, then $V_0 = (1 - w^*)(\Omega_X)$.*

Proof. Since w is an involution, $(1 - w^*)(\Omega_X) = \ker(1 + w^*)$. So $v \in (1 - w^*)(\Omega_X)$ if and only if $\mathrm{Tr}(v) = 0$. So $V_0 \subseteq (1 - w^*)(\Omega_X)$.

Next, as $r_X = r_C$, we have that $\varrho^*(J(C)(\mathbb{Q}))$ is a full rank subgroup of $J(X)(\mathbb{Q})$. Write N for its index. Let $D \in J(X)(\mathbb{Q})$. Then $ND \in \varrho^*(J(C)(\mathbb{Q})$ and we can write $ND = \varrho^*\Delta$ for some $\Delta \in J(C)(\mathbb{Q})$. Then for $v \in (1 - w^*)(\Omega_X)$

$$\int_0^D v = \frac{1}{N} \int_0^{\varrho^*\Delta} v = \frac{1}{N} \int_0^D \mathrm{Tr}(v) = 0.$$

So v annihilates $J(X)(\mathbb{Q})$. So $(1 - w^*)(\Omega_X) \subseteq V_0$. □

Corollary 6.2. *Assume $r_X = r_C$. Let p be a prime of good reduction for both X and C. Denote reduction mod p by $\sim$. Then $\widetilde{\Omega_X} = \Omega_{\tilde{X}}$, and*

$$\widetilde{V_0} = (1 - \widetilde{w}^*)(\Omega_{\tilde{X}}).$$

Proof. The fact that $\widetilde{\Omega_X} = \Omega_{\tilde{X}}$ follows from [5, p. 10] where it is shown that the reduction map is surjective on the space of holomorphic differentials.

Next, write $W_0 = (1 - \widetilde{w}^*)(\Omega_{\tilde{X}})$. Note that $W_0 = \ker(1 + \widetilde{w}^*)$. If $v \in V_0 = \ker(1 + w^*)$, then $\widetilde{v} \in \ker(1 + \widetilde{w}^*) = W_0$, so $\widetilde{V_0} \subseteq W_0$.

For the opposite inclusion, suppose $\mu \in W_0$ and choose $\eta \in \Omega_{\tilde{X}}$ such that $(1 - \widetilde{w}^*)(\eta) = \mu$. Choose $v \in \Omega_X$ satisfying $\widetilde{v} = \eta$. Write $u = (1 - w^*)v \in V_0$. Then $\widetilde{u} = (1 - \widetilde{w}^*)(\eta) = \mu$, so $W_0 \subseteq \widetilde{V_0}$. □

This gives us a concrete way of calculating the space $\widetilde{V_0}$ when $r_X = r_C$ (which will be the case for $X = X_{ns}(13)$).

We now come to the main result of this section which gives a way of testing whether a known non-exceptional quadratic point has any exceptional quadratic points in its mod p residue disc. The theorem uses the notion of a *well-behaved uniformiser* which has certain useful properties as discussed in [36, p. 771].

Theorem 6.3. *Let $Q \coloneqq Q_1 + Q_2 \in \varrho^*(C(\mathbb{Q})) \subseteq X^{(2)}(\mathbb{Q})$ be a non-exceptional quadratic point. Let p be a prime of good reduction for X and C, and moreover suppose either that $p > 3$, or that $p = 3$ and $\widetilde{Q_1} \neq \widetilde{Q_2} \mod 3$. Let t_{Q_1} be a well-behaved uniformiser at Q_1. If there exists some $v \in V_0$ satisfying*

$$\widetilde{a_0} \neq 0, \quad \text{where } a_0 \coloneqq \frac{v}{\mathrm{d}t_{Q_1}}\Big|_{t_{Q_1}=0}, \tag{3}$$

then Q has no exceptional points in its mod p residue disc.

Here, $a_0 = \frac{v}{\mathrm{d}t_{Q_1}}\Big|_{t_{Q_1}=0}$ is simply the constant term in the expansion of v as a power series in t_{Q_1}.

Proof. This is mainly a special case of the proof in [35, pp. 223-226]. Suppose $P = P_1 + P_2 \in X^{(2)}(\mathbb{Q})$ with $\widetilde{P} = \widetilde{Q}$. After reordering if necessary, we can assume that $\widetilde{Q_1} = \widetilde{P_1}$ and $\widetilde{Q_2} = \widetilde{P_2}$. Write

$$K \coloneqq \mathbb{Q}(Q_1), \quad M \coloneqq \mathbb{Q}(P_1), \quad L \coloneqq \mathbb{Q}(Q_1, P_1) = K \cdot M.$$

By the properties of Coleman integration, and the fact that $w^*v = -v$:

$$\begin{aligned} 0 = \int_Q^P v &= \int_{Q_1}^{P_1} v + \int_{Q_2}^{P_2} v = \int_{Q_1}^{P_1} v + \int_{w(w(Q_2))}^{w(w(P_2))} v \\ &= \int_{Q_1}^{P_1} v + \int_{w(Q_2)}^{w(P_2)} w^*v = \int_{Q_1}^{P_1} v + \int_{Q_1}^{w(P_2)} w^*v \\ &= \int_{Q_1}^{P_1} v - \int_{Q_1}^{w(P_2)} v = \int_{w(P_2)}^{P_1} v = -\int_{P_1}^{w(P_2)} v. \end{aligned}$$

Write $v = (a_0 + a_1 t_{Q_1} + a_2 t_{Q_1}^2 + \dots)\,\mathrm{d}t_{Q_1}$ as a power series expansion, and write $z_1 \coloneqq t_{Q_1}(P_1)$ and $z_2 \coloneqq t_{Q_1}(w(P_2))$. Since

$$\widetilde{w(P_2)} = \widetilde{w}(\widetilde{P_2}) = \widetilde{w}(\widetilde{Q_2}) = \widetilde{Q_1} = \widetilde{P_1},$$

we see that $w(P_2)$ and P_1 both share the same mod p residue class as Q_1. It follows that if $z_1 = z_2$ then $w(P_2) = P_1$, by injectivity of the well-behaved

uniformiser t_{Q_1} on the residue disc of Q_1. So it is enough to show that $z_1 = z_2$. From the above, we have

$$\begin{aligned} 0 &= \int_{P_1}^{w(P_2)} (a_0 + a_1 t_{Q_1} + a_2 t_{Q_1}^2 + \dots)\, \mathrm{d}t_{Q_1} \\ &= \Big[a_0 t_{Q_1} + \frac{a_1}{2} t_{Q_1}^2 + \frac{a_2}{3} t_{Q_1}^3 + \cdots \Big]_{P_1}^{w(P_2)} \\ &= a_0(z_2 - z_1) + \frac{a_1}{2}\big(z_2^2 - z_1^2\big) + \frac{a_2}{3}\big(z_2^3 - z_1^3\big) + \cdots \\ &= (z_2 - z_1) f(z_2, z_1), \end{aligned}$$

where $f(z_2, z_1) \coloneqq a_0 + \frac{a_1}{2}(z_2 + z_1) + \frac{a_2}{3}(z_2^2 + z_2 z_1 + z_1^2) + \cdots$.

In order to show that $z_2 = z_1$, we must show that $f(z_2, z_1) \neq 0$. To do this we let $\mathfrak{p}$ be a prime of L above p, and reduce f mod $\mathfrak{p}$. Denote this reduction by $\widetilde{f}$. Write $\mathfrak{p} = (\pi)$, so that π is a uniformiser for the corresponding valuation. Then $\pi \nmid a_0$ by assumption, but $\pi \mid z_2, z_1$. We want to show that $\pi \mid (f(z_2, z_1) - a_0)$. We have $\pi \mid a_1(z_2 + z_1)$, $\pi^2 \mid a_2(z_2^2 + z_2 z_1 + z_1^2)$, and so on. This means that the only issue is dealing with the denominators appearing in the expression. Note that for $i \geq 0$, $\mathrm{ord}_\pi(i+1) \leq e_{\mathfrak{p}/p}$ (the ramification index of p in L). As L is a compositum of quadratic fields, $e_{\mathfrak{p}/p} \leq 2$, with equality if and only if p ramifies in K or M (if it ramifies in both, then, as $p > 2$, $K = M = \mathbb{Q}(\sqrt{\pm p})$). Then for $p \geq 5$ and for all $i \geq 0$,

$$\mathrm{ord}_\pi(z_2^i + z_2^{i-1} z_1 + \cdots + z_1^i) > 2 \geq \mathrm{ord}_\pi(i+1). \tag{4}$$

So for $p \geq 5$ we have $\widetilde{f} - \widetilde{a_0} = 0$, so $\widetilde{f} = \widetilde{a_0} \neq 0$ as required.

For $p = 3$ the situation is more delicate. We have $\mathrm{ord}_\pi(z_2^2 + z_2 z_1 + z_1^2) \geq 2$ and $\mathrm{ord}_\pi(3) = 1$ or 2, with $\mathrm{ord}_\pi(3) = 2$ if and only if 3 ramifies in L. This means that if 3 is not ramified in L, then (4) holds for $p = 3$ and all $i \geq 0$, so $\widetilde{f} \neq 0$. If 3 ramifies in K, then the inertia group of a prime $\mathcal{P}$ above 3 in K is the full Galois group $\mathrm{Gal}(K/\mathbb{Q})$, so for $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$,

$$Q_2 = Q_1^\sigma \equiv Q_1 \pmod{\mathcal{P}},$$

meaning that $\widetilde{Q_1} = \widetilde{Q_2}$. Then if, as in the statement of the theorem, $\widetilde{Q_1} \neq \widetilde{Q_2}$, then 3 does not ramify in K. So if 3 ramifies in L, then it must ramify in M, so, by the same reasoning as above, $\widetilde{P_1} = \widetilde{P_2}$. But then $\widetilde{Q_1} = \widetilde{P_1} = \widetilde{P_2} = \widetilde{Q_2}$, a contradiction. So when $\widetilde{Q_1} \neq \widetilde{Q_2}$ mod 3, the relation (4) holds for all $i \geq 0$, meaning that $\widetilde{f} \neq 0$. □

We in fact use the following corollary to verify that a point contains no exceptional points in its mod p residue disc.

Corollary 6.4. *Let $Q = Q_1 + Q_2 \in \varrho^*(C(\mathbb{Q})) \subseteq X^{(2)}(\mathbb{Q})$ be a non-exceptional quadratic point. Let p be a prime of good reduction for X and C,*

and moreover suppose either that $p > 3$, or that $p = 3$ and $\widetilde{Q_1} \neq \widetilde{Q_2} \mod 3$. Let $t_{\widetilde{Q_1}}$ be a uniformiser at $\widetilde{Q_1}$. Let $\omega_1, \ldots, \omega_k$ be a basis for $\widetilde{V_0}$. If, for some $i \in \{1, \ldots, k\}$,

$$\frac{\omega_i}{\mathrm{d}t_{\widetilde{Q_1}}} \Big|_{t_{\widetilde{Q_1}}=0} \neq 0, \tag{5}$$

then Q has no exceptional points in its mod p residue disc.

Proof. We follow [5, p.11]. Choose $\omega = \omega_i$ satisfying (5), and write

$$\omega = (b_0 + b_1 t_{\widetilde{Q_1}} + b_2 t_{\widetilde{Q_1}}^2 + \ldots)\,\mathrm{d}t_{\widetilde{Q_1}}.$$

By assumption, $b_0 \neq 0$. Choose $v \in V_0$ so that $\widetilde{v} = \omega$. Let t_{Q_1} be a well-behaved uniformiser at Q_1 and write

$$v = (a_0 + a_1 t_{Q_1} + a_2 t_{Q_1}^2 + \ldots)\,\mathrm{d}t_{Q_1}.$$

By Theorem 6.3 it is enough to show $\widetilde{a_0} \neq 0$. Reducing this expression, we have

$$\omega = (\widetilde{a_0} + \widetilde{a_1}\widetilde{t_{Q_1}} + \widetilde{a_2}\widetilde{t_{Q_1}}^2 + \ldots)\,\mathrm{d}\widetilde{t_{Q_1}}.$$

Then $\widetilde{t_{Q_1}}$ is also a uniformiser at $\widetilde{Q_1}$ as t_{Q_1} is well-behaved, so $\widetilde{a_0} \neq 0$ since $b_0 \neq 0$. □

We have implemented this in `Magma` (Appendix B). Working with the space $\widetilde{V_0}$ is less computationally expensive than working with V_0, and also removes the issue of needing to work with a well-behaved uniformiser.

6.3 Sieve

We let X be a smooth projective curve over $\mathbb{Q}$ with Jacobian $J = J(X)$ of rank r. We start with a non-empty set $\mathcal{L} \subseteq X^{(2)}(\mathbb{Q})$ of known quadratic points, and a hypothetical unknown quadratic point $P \in X^{(2)}(\mathbb{Q})$. In order to apply the sieve we need the following data:

- A finite index subgroup $G \subseteq J(\mathbb{Q})$ with generators $D_1, \ldots, D_n$. We write $I \coloneqq [J(\mathbb{Q}) : G]$.
- A non-negative integer parameter, M.
- Primes $p_1, \ldots, p_k$ of good reduction for X so that the index I is coprime to $\#(J(\mathbb{F}_{p_i})/MJ(\mathbb{F}_{p_i}))$ for each $i \in \{1, \ldots, k\}$.

If the index I is known, or even if we know some integer $\hat{I}$ satisfying $\hat{I} \cdot J(\mathbb{Q}) \subseteq G$, then we can adapt the sieve and remove the coprimality assumption. This version of the sieve is described in [5, pp. 6-7]. However, usually, and in particular for $X_{ns}(13)$, we will not know the index, or such an integer

$\hat{I}$. In this case we use the p-saturation method described in the following subsection to determine primes that do not divide the index.

We present here an adaptation of the sieve used in [35, pp. 226-228]. For a more general introduction to this theory, and in particular its application to hyperelliptic curves, we refer to [6].

The coprimality condition allows us to choose an integer, I^*, so that for each $i \in \{1, \ldots, k\}$,

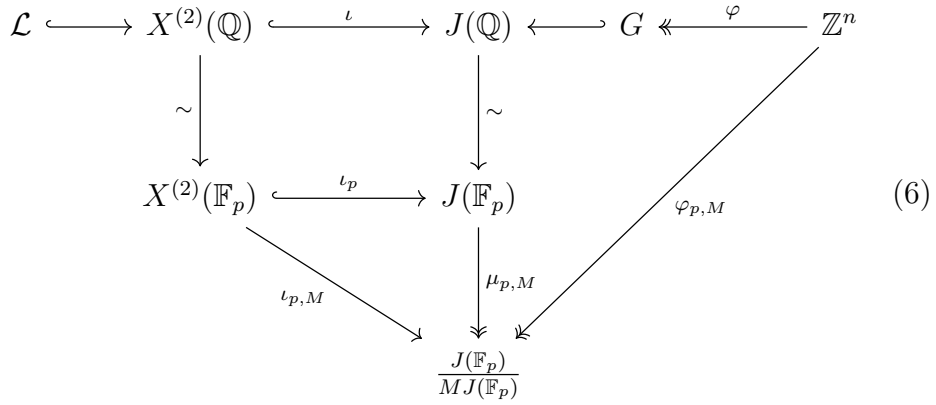
$$I^* I \equiv 1 \mod \#\big(J(\mathbb{F}_{p_i})/MJ(\mathbb{F}_{p_i})\big).$$

We write $\mu_{p_i,M} : J(\mathbb{F}_{p_i}) \to J(\mathbb{F}_{p_i})/MJ(\mathbb{F}_{p_i})$ for the natural quotient map. At the end of this section we discuss how one might choose M and the primes used in the sieve to maximise the chances of success. Here, 'success' means contradicting the existence of the unknown point P.

For the moment, we fix a prime $p := p_i$ for some i. Choose a base point, which we will denote $\infty \in X^2(\mathbb{Q})$, and write $\iota : X^2(\mathbb{Q}) \hookrightarrow J(\mathbb{Q})$ for the corresponding Abel-Jacobi map. Define

$$\begin{aligned} \varphi : \mathbb{Z}^n &\longrightarrow G \subseteq J(\mathbb{Q}) \\ (a_1, \ldots, a_n) &\longmapsto a_1 D_1 + \cdots + a_n D_n. \end{aligned}$$

We write $\varphi_{p,M}$ for the map obtained by first applying φ, then reducing modulo p, and then applying $\mu_{p,M}$. Denote reduction modulo p by $\sim$. The map ι_p is the Abel-Jacobi map on $X^{(2)}(\mathbb{F}_p)$ with basepoint $\widetilde{\infty}$. Finally $\iota_{p,M}$ is the composition of ι_p with the quotient map $\mu_{p,M}$. We obtain the following commutative diagram.



(6)

Consider $P \in X^{(2)}(\mathbb{Q}) \backslash \mathcal{L}$, our (hypothetical) unknown quadratic point. We see that $I \cdot \iota_p(P) \in G$, so we can write

$$I \cdot \iota_p(P) = a_1 D_1 + \cdots + a_n D_n = \varphi(a_1, \ldots, a_n),$$

for some $(a_1, \ldots, a_n) \in \mathbb{Z}^n$. Multiplying through by I^*, we have

$$(I^* I) \cdot \iota_p(P) = I^* a_1 D_1 + \cdots + I^* a_n D_n = \varphi(I^* a_1, \ldots, I^* a_n).$$

Reducing this expression modulo p and applying the quotient map $\mu_{p,M}$ gives, in the group $J(\mathbb{F}_{p_i})/MJ(\mathbb{F}_{p_i})$,

$$\mu_{p,M}\big((I^*I)\cdot\widetilde{\iota(P)}\big) = I^*a_1\mu_{p,M}(\widetilde{D_1}) + \cdots + I^*a_n\mu_{p,M}(\widetilde{D_n}).$$

Since Diagram 6 commutes, $\mu_{p,M}\big((I^*I)\cdot\widetilde{\iota(P)}\big) = (I^*I)\cdot\iota_{p,M}(\widetilde{P})$. Also, by our choice of I^*, we have $(I^*I)\cdot\iota_{p,M}(\widetilde{P}) = \iota_{p,M}(\widetilde{P})$ in $J(\mathbb{F}_{p_i})/MJ(\mathbb{F}_{p_i})$. So

$$\iota_{p,M}(\widetilde{P}) = I^*a_1\mu_{p,M}(\widetilde{D_1}) + \cdots + I^*a_n\mu_{p,M}(\widetilde{D_n}) = \varphi_{p,M}(I^*a_1,\ldots,I^*a_n).$$

We conclude that $\iota_{p,M}(\widetilde{P}) \in \varphi_{p,M}(\mathbb{Z}^n) = \mu_{p,M}(\widetilde{G})$.

From this, we obtain a set of points in $X^{(2)}(\mathbb{F}_p)$ that P could apriori reduce to modulo p, namely

$$\mathcal{S}_{p,M} \coloneqq \{D \in X^{(2)}(\mathbb{F}_p) : \iota_{p,M}(D) \in \mu_{p,M}(\widetilde{G})\}.$$

We now use the information obtained from the Chabauty step to eliminate as many of the points in $\mathcal{S}_{p,M}$ as possible. Write $\mathcal{H}_{p,M} \subseteq X^{(2)}(\mathbb{F}_p)$ for the reductions of points that pass the Chabauty test. Then $\widetilde{P} \neq \widetilde{Q}$ for any $\widetilde{Q} \in \mathcal{H}_{p,M}$ as otherwise P would be an exceptional point in the mod p residue disc of Q, contradicting $Q \in \mathcal{H}_{p,M}$. This leaves us with a set $\mathcal{T}_{p,M} \coloneqq \mathcal{S}_{p,M}\backslash\mathcal{H}_{p,M} \subseteq X^{(2)}(\mathbb{F}_p)$ of possibilities for $\widetilde{P}$. The more points that pass the Chabauty test the better, as this means we are eliminating more possibilities for $\widetilde{P}$. We can calculate $\mathcal{T}_{p,M}$ explicitly.

Since $\iota_{p,M}(\mathcal{T}_{p,M}) \subseteq \mu_{p,M}(\widetilde{G}) = \varphi(\mathbb{Z}^m)$, we obtain a set, $\mathcal{W}_{p,M}$, of $\mathcal{B}_{p,M} \coloneqq \ker(\varphi_{p,M})$ cosets:

$$\mathcal{W}_{p,M} \coloneqq \varphi_{p,M}^{-1}(\iota_{p,M}(\mathcal{T}_{p,M})).$$

This set of cosets, $\mathcal{W}_{p,M}$, encodes the list of possibilities for $I\cdot\iota(P)$; namely if $I\cdot\iota(P) = a_1D_1 + \cdots + a_nD_n$, then $(I^*a_1,\ldots,I^*a_n) \in u + \mathcal{B}_{p,M}$ for some $u + \mathcal{B}_{p,M} \in \mathcal{W}_{p,M}$.

Although $\mathcal{W}_{p,M}$ was obtained by investigating matters modulo p, the information it encodes is completely independent of p. This means that if we choose a different prime of good reduction, say p', then just as above, if $I\cdot\iota(P) = a_1D_1 + \cdots + a_nD_n$, then $(I^*a_1,\ldots,I^*a_n) \in u + \mathcal{B}_{p',M}$ for some $v + \mathcal{B}_{p',M} \in \mathcal{W}_{p',M}$. So $(I^*a_1,\ldots,I^*a_n) \in \mathcal{W}_{p,p',M} \coloneqq \mathcal{W}_{p,M} \cap \mathcal{W}_{p',M}$.

We then repeat this process for each prime p in our list $p_1,\ldots,p_k$ of primes of good reduction. We hope that $\mathcal{W}_{p_1,\ldots,p_k,M} = \emptyset$, as if this is the case, it follows that $I\cdot\iota(P)$ is not expressible as a linear combination of the D_i, and thus $I\cdot\iota(P) \notin G$, meaning that $P \notin X^2(\mathbb{Q})$, giving us our desired contradiction.

In this sieve we have two parameters: the primes we use and M. We briefly discuss how one might choose these. The integer M plays two roles. The first is crucial. We require I to be coprime to $\#(J(\mathbb{F}_{p_i})/MJ(\mathbb{F}_{p_i}))$ for

each i. If there is a prime $p \mid \#J(\mathbb{F}_{p_i})$ which is either not coprime to the index, or we cannot show it is coprime to the index, then by not including this prime as a factor of M, we have that $p \nmid \#(J(\mathbb{F}_{p_i})/MJ(\mathbb{F}_{p_i}))$. This allows us to remove any troublesome primes. For example in the case of $X_{ns}(13)$, we are unable to show whether or not $7 \mid I$. By choosing M such that $7 \nmid M$ we remove this issue. The downside to this is that we potentially lose information in the sieve. Secondly, M allows us to remove (in the quotient) any large primes appearing in the factorisation of $\#J(\mathbb{F}_{p_i})$. This can help avoid a combinatorial explosion due to the Chinese Remainder Theorem. Indeed, as we intersect the subgroups $\mathcal{B}_{p,M}$, the resulting subgroup can have very large index in $\mathbb{Z}^n$, which slows down calculations.

As for the primes we choose, although there is no set method, and this involves trial and error to a large degree, we can still offer some explanation as to which primes one might try and choose. As a guideline we look for a large overlap between the prime factors of $\#(J(\mathbb{F}_{p_i})/MJ(\mathbb{F}_{p_i}))$ as i varies. This means that we are more likely to obtain a smaller set $\mathcal{W}_{p_1,\dots,p_k,M}$, as it is more likely that we obtain contradictory information modulo these overlapping primes. More generally, heuristics for the choice of primes can be found in [5, p. 7] and [6, pp. 6-7].

6.4 Saturation

Continuing with the same notation, let $G = \langle D_1, \dots, D_n \rangle$ be an index I subgroup of $J(X)(\mathbb{Q})$. Write r for the rank of $J(X)$. Let p be a prime such that either $p \nmid \#(J(X)(\mathbb{Q})_{\text{tors}})$, or $J(X)(\mathbb{Q})_{\text{tors}} = 0$. We present here a strategy for showing that $p \nmid I$.

Lemma 6.5. *If $p \mid I$ then there exist $a_1, \dots, a_n \in \mathbb{Z}$, not all divisible by p, and $Q \in J(\mathbb{Q})$ such that*

$$a_1 D_1 + \cdots + a_n D_n = pQ.$$

Proof. Suppose $p \mid I$. Then $p \mid \#(J(\mathbb{Q})/G)$. So we can choose $Q + G \in J(\mathbb{Q})/G$ of order p. So $pQ \in G$, meaning that we can write $pQ = a_1 D_1 + \cdots + a_n D_n$ for some $a_i \in \mathbb{Z}$. If each a_i were divisible by p, then

$$p\big(Q - (a_1/p)D_1 + \cdots + (a_n/p)D_n\big) = 0.$$

Since, by assumption, either $p \nmid \#(J(X)(\mathbb{Q})_{\text{tors}})$, or $J(X)(\mathbb{Q})_{\text{tors}} = 0$, we must have that $Q = (a_1/p)D_1 + \cdots + (a_n/p)D_n \in G$, but then $Q + G = 0 \in J(\mathbb{Q})/G$, a contradiction, as $Q + G$ has order p. □

Choose a prime l. We define a map

$$\begin{aligned} \pi_l : (\mathbb{Z}/p\mathbb{Z})^n &\longrightarrow J(\mathbb{F}_l)/pJ(\mathbb{F}_l) \\ (b_1, \dots, b_n) &\longmapsto b_1\widetilde{D_1} + \cdots + b_n\widetilde{D_n}, \end{aligned}$$

where $\widetilde{D_i}$ is the image of D_i in $J(\mathbb{F}_l)/pJ(\mathbb{F}_l)$. Note that if $p \mid \#J(\mathbb{F}_l)$ then $J(\mathbb{F}_l)/pJ(\mathbb{F}_l) \neq 0$.

Theorem 6.6. *Choose a set $\mathcal{S} = \{l_1, \ldots, l_k\}$ of primes. If $\bigcap_{i=1}^{k} \ker(\pi_{l_i}) = 0$ then $p \nmid I$.*

Proof. Suppose for a contradiction that $p \mid I$, and choose $a_1, \ldots a_n \in \mathbb{Z}$, not all divisible by p, so that $a_1 D_1 + \cdots + a_n D_n = pQ$, for some $Q \in J(\mathbb{Q})$ (by Lemma 6.5). Choose some $l \in \mathcal{S}$. We note that

$$\pi_l(\widetilde{a_1}, \ldots, \widetilde{a_n}) = \widetilde{a_1}\widetilde{D_1} + \cdots + \widetilde{a_n}\widetilde{D_n} = p\widetilde{Q} = 0 \in J(\mathbb{F}_l)/pJ(\mathbb{F}_l).$$

So $(\widetilde{a_1}, \ldots, \widetilde{a_n}) \in \ker(\pi_l)$. Since l was chosen arbitrarily,

$$(\widetilde{a_1}, \ldots, \widetilde{a_n}) \in \bigcap_{i=1}^{k} \ker(\pi_{l_i}) = 0.$$

But then $p \mid a_i$ for each $i \in \{1, \ldots, n\}$, a contradiction. □

This gives a way of testing whether $p \nmid I$. We note that even if $p \nmid I$, the method is not guaranteed to show this. To have any chance of success, we must choose primes l so that $p \mid \#J(\mathbb{F}_l)$, as otherwise $\ker(\pi_l) = (\mathbb{Z}/p\mathbb{Z})^n$. We have implemented this method in `Magma`. The code is included in Appendix B.

7 Quadratic Points on $X_{ns}(13)$

7.1 Obtaining a New Model

We would now like to carry out the processes described in Section 6 for $X_{ns}(13)$. All the calculations and results are supported by the `Magma` code in Appendix B. Following the notation of the previous sections we write $X = X_{ns}(13)$, $C = X_{ns}^{+}(13)$, and $\varrho : X \to C$.

As a starting point we use the equations for X, C, and ϱ from [16]. A model for X is given by 15 degree 2 equations which cut out the curve in $\mathbb{P}^7$. It is a curve of genus 8. The equations are first obtained via the canonical embedding and then simplified to obtain small coefficients using an LLL algorithm.

A model for the genus 3 curve C is given by the following degree 4 equation in $\mathbb{P}^3$:

$$\begin{aligned}&(-Y - Z)X^3 + (2Y^2 + ZY)X^2 \\ &+ (-Y^3 + ZY^2 - 2(Z^2)Y + Z^3)X + (2Z^2Y^2 - 3Z^3Y) = 0.\end{aligned}$$

Finally,

$$\varrho : X_{ns}(13) \longrightarrow X_{ns}^{+}(13)$$
$$(x_1 : \cdots : x_8) \longmapsto (-3x_1 + 2x_2, -3x_1 + x_2 + 2x_4 - 2x_5, x_1 + x_2 + x_4 - x_5).$$

The curve C has precisely seven rational points. We know this from the important paper, [1], which uses a more general version of Chabauty to prove this. This means that, by pulling back these rational points, we have seven pairs of non-exceptional quadratic points on X. Note that $X(\mathbb{Q}) = \emptyset$ (since $X(\mathbb{R}) = \emptyset$ by Proposition 3.1).

Baran finds an explicit form for the j-map on C in [3, pp. 295-300]. Each of the seven points is a CM-point. The seven rational points along with the CM fields of the corresponding elliptic curves are displayed in Table 1. The CM fields of the rational points are precisely the quadratic fields over which their pullbacks are defined.

P	Coordinates	CM
P_1	$(0:1:0)$	-11
P_2	$(0:0:1)$	-67
P_3	$(-1:0:1)$	-7
P_4	$(1:0:0)$	-2
P_5	$(1:1:0)$	-19
P_6	$(0:3:2)$	-163
P_7	$(1:0:1)$	-7

Table 1: Rational points on $X_{ns}^{+}(13)$

We would first like to find the equations for the modular involution, w_{13}. We know that the modular involution interchanges each pair of quadratic points, and so we know the images of these fourteen points under w_{13}. Knowing nine of these images is enough to determine w_{13} as the standard simplex of $\mathbb{P}^8$ consists of nine points. This allows us to find the modular involution. As a matrix in PGL(8) it is given by

$$w_{13} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix}.$$

So as a map on the curve,

$$w_{13}(x_1 : \cdots : x_8) = \\ (x_1 : x_2 : x_1 - x_2 - x_3 : -x_5 : -x_4 : x_1 - x_6 : x_2 - x_7 : x_1 - x_8).$$

We would like to change coordinates so that our modular involution is in a nicer form. This is purely for computational purposes. To do this, we diagonalise the matrix and change coordinates appropriately. The matrix of w_{13} has eigenvalues 1 and -1, with multiplicities 3 and 5 respectively. Let T be the change of basis matrix satisfying $Tw_{13}T^{-1} = M$, where $M \coloneqq \mathrm{Diag}(1, 1, 1, -1, -1, -1, -1, -1)$. We then change coordinates with the matrix T^{-1}. The coordinate change induced by the matrix T^{-1} is

$$(x_1 : \cdots : x_8) \mapsto \\ \left(x_2 : x_3 : \frac{x_2 - x_3 - x_5}{2} : \frac{x_1 + x_8}{2} : \frac{-x_1 + x_8}{2} : \frac{x_2 - x_6}{2} : \frac{x_3 - x_7}{2} : \frac{x_2 - x_4}{2}\right).$$

As we can see from the denominators appearing in the coordinate change, this introduces 2 as a prime of bad reduction on our new model. This is not an issue as we will not need to use 2 in the sieving step. Applying this coordinate change to the equations of our curve and to the map φ gives us our new model and new map to C. These equations are displayed in Appendix A. Note that the model of the curve C is unchanged.

We now pull back the seven rational points on C to obtain seven pairs of quadratic points on X. These are listed in Table 2.

7.2 Applying Symmetric Chabauty to $X_{ns}(13)$

We start by considering the Jacobians of our curves. By [7, p. 56] we know that $J(C)(\mathbb{Q})$ has rank 3 and trivial torsion, with the divisors

$$\Delta_i \coloneqq [P_i - P_4], \qquad i = 1, 2, 3$$

generating a full rank subgroup which we denote $H \subseteq J(C)(\mathbb{Q})$. Writing u_{169} for the Atkin-Lehner involution on $X_0(169)$, we verify that the rank of $\ker(u_{169} + 1)$ is 0, so $J(X)(\mathbb{Q})$ also has rank 3 as there are no newforms at level 13 (see the discussion after Proposition 3.2). Therefore, pulling back the divisors Δ_i to $J(X)(\mathbb{Q})$ gives rise to a full rank subgroup, G, of this Jacobian (see the following Proposition). We note that

$$r_X - r_C = 0 < 5 = g_X - g_C,$$

meaning that the symmetric Chabauty criterion is satisfied.

We would like to use the p-saturation method to determine primes p not dividing the index, I, of G in $J(X)(\mathbb{Q})$. Rather than test saturation using G, we do so with the subgroup H due to the computational issues of working with X. This choice is justified by the following Proposition.

Q	θ^2	Coordinates	CM	$\varrho(Q)$
Q_1	-11	$\left(-\frac{5\theta}{13} : \frac{2\theta}{13} : \frac{3\theta}{13} : 0 : -1 : -2 : 1 : 1\right)$	-11	$(0:1:0)$
Q_2	-67	$\left(\frac{3\theta}{13} : \frac{4\theta}{13} : \frac{6\theta}{13} : 0 : 4 : -4 : -2 : 1\right)$	-67	$(0:0:1)$
Q_3	-7	$\left(\frac{7\theta}{13} : \frac{5\theta}{13} : \frac{\theta}{13} : -1 : 0 : -1 : 1 : 1\right)$	-7	$(-1:0:1)$
Q_4	-2	$\left(\frac{4\theta}{13} : \frac{\theta}{13} : -\frac{5\theta}{13} : 0 : 0 : 1 : 0 : 0\right)$	-2	$(1:0:0)$
Q_5	-19	$\left(\frac{\theta}{13} : -\frac{3\theta}{13} : \frac{2\theta}{13} : 1 : 1 : 1 : 0 : 1\right)$	-19	$(1:1:0)$
Q_6	-163	$\left(\frac{3\theta}{13} : \frac{2\theta}{91} : \frac{3\theta}{91} : -\frac{12}{7} : -\frac{5}{7} : -\frac{10}{7} : \frac{25}{7} : 1\right)$	-163	$(0:3:2)$
Q_7	-7	$\left(-\frac{\theta}{13} : \frac{3\theta}{13} : \frac{11\theta}{13} : 1 : 0 : -3 : -1 : 1\right)$	-7	$(1:0:1)$

Table 2: Quadratic points on $X_{ns}(13)$

Proposition 7.1. *Let $H \coloneqq \langle \Delta_1, \Delta_2, \Delta_3 \rangle \subseteq J(C)(\mathbb{Q})$ as above, and let $G \coloneqq \langle D_1, D_2, D_3 \rangle \subseteq J(X)(\mathbb{Q})$, where $D_i = \varrho^* \Delta_i$. Then G has finite index in $J(X)(\mathbb{Q})$. We write $I' = [J(C)(\mathbb{Q}) : H]$ and $I = [J(X)(\mathbb{Q}) : G]$. Then $I \mid 14I'$. In particular, if $p \nmid I'$ and $p \neq 2, 7$, then $p \nmid I$.*

Proof. We adapt the proof from [5, pp. 8-9]. Since $\deg \varrho = 2$, we have that

$$\varrho_* D_i = \varrho_* \varrho^* \Delta_i = 2\Delta_i. \tag{7}$$

It follows that D_1, D_2, D_3 are linearly independent, because if $a_1 D_1 + a_2 D_2 + a_3 D_3 = 0$ then applying ϱ_* gives $2a_1\Delta_1 + 2a_2\Delta_2 + 2a_3\Delta_3 = 0$, contradicting linear independence of the Δ_i. So G is a finite index subgroup of $J(X)(\mathbb{Q})$.

Furthermore, by (7) and the fact that $I'J(C)(\mathbb{Q}) \subseteq H$,

$$\varrho_* G = 2H \supseteq 2I'J(C)(\mathbb{Q}).$$

We claim that $14I'J(X)(\mathbb{Q}) \subseteq G$. Let $D \in J(X)(\mathbb{Q})$. Then

$$\varrho_*(2I'D) = 2I'\varrho_* D \in 2I'J(C)(\mathbb{Q}) \subseteq \varrho_* G.$$

So we can choose $D_G \in G$ satisfying $\varrho_*(2I'D) = \varrho_* D_G$. So $\varrho^*(2I'D - D_G) = 0$. Since $J(X)(\mathbb{Q})$ and $J(C)(\mathbb{Q})$ have equal rank, ϱ^* is injective modulo torsion, so $2I'D - D_G \in J(X)(\mathbb{Q})_{\text{tors}}$.

We find that (see Appendix A)

$$\#J(\mathbb{F}_5) = 3 \cdot 7 \cdot 11 \cdot 13^2 \cdot 29,$$
$$\#J(\mathbb{F}_{19}) = 2^2 \cdot 7 \cdot 83 \cdot 97 \cdot 113 \cdot 883,$$

so by injectivity on torsion, $J(X)(\mathbb{Q})_{\text{tors}} = 0$ or $\mathbb{Z}/7\mathbb{Z}$. So $14I'D = 7D_G \in G$. So $14I'J(X)(\mathbb{Q}) \subseteq G$. Moreover, as $J(X)(\mathbb{Q})_{\text{tors}} = 0$ or $\mathbb{Z}/7\mathbb{Z}$, it follows that $14I' \mid I$. □

Applying the p-saturation method to $H \subseteq J(C)(\mathbb{Q})$ we find that

$$3, 5, 13, 29, 41, 43, 83, 97, 113, 127 \nmid I' = [J(C)(\mathbb{Q}) : H].$$

This calculation is supported in the `Magma` code in Appendix B. It follows that these primes do not divide I either, as $I \mid 14I'$. This means that we can include these primes in our parameter M. We choose to set $M = 3^{10} \cdot 5^{10} \cdot 13^{10} \cdot 29^{10}$ (here, the exponent 10 is simply large enough to ensure we keep the corresponding factors in the quotient). Then

$$\#\big(J(\mathbb{F}_p)/MJ(\mathbb{F}_p)\big) \mid M,$$

so I is coprime to $\#\big(J(\mathbb{F}_p)/MJ(\mathbb{F}_p)\big)$ for all primes p (of good reduction).

As noted in the proof of Proposition 7.1, $J(X)(\mathbb{Q})_{\text{tors}} = 0$ or $\mathbb{Z}/7\mathbb{Z}$. Unfortunately we are unable to show whether or not $J(X)(\mathbb{Q})$ has a point of order 7. Using `Magma`, we compute that $7 \mid J(\mathbb{F}_p)$ for primes $2 \leq p \leq 97$, $p \neq 13$ (the data for $p \leq 73$ is included in Appendix A). This means that we are unable to rule out the possibility of 7-torsion. However, we are also unable to produce a point of $J(X)(\mathbb{Q})$ of order 7. As the behaviour of $X_{ns}(p)$ is often similar to that of $X_0(p)$, it would be natural to expect that a cuspidal divisor might produce a point of order 7 (perhaps over an extension of $\mathbb{Q}$, at which point we could consider Galois invariants as in [31, p. 13]). This is because in the case of $X_0(N)$, the Manin-Drinfeld Theorem [25, 18] asserts that $S_0(N) \subseteq J_0(N)(\overline{\mathbb{Q}})_{\text{tors}}$, where $S_0(N)$ is the subgroup generated by classes of differences of cusps. It follows that $S_0(N)(\mathbb{Q}) \subseteq J_0(N)(\mathbb{Q})_{\text{tors}}$. In fact the generalised Ogg conjecture (discussed for example in [31]) asserts that $S_0(N)(\mathbb{Q}) \subseteq J_0(N)(\mathbb{Q})_{\text{tors}}$. This has been checked for numerous values of N. [5, 31].

As stated at the end of Section 2, the 12 cusps of X form a single Galois orbit over $\mathbb{Q}(\zeta_{13})$. Over $\mathbb{Q}(\sqrt{13})$, this orbit splits, giving rise to two divisors defined over $\mathbb{Q}(\sqrt{13})$. Considering their difference gives a degree 0 cuspidal divisor defined over $\mathbb{Q}(\sqrt{13})$. Using `Magma` we find that the order of this divisor modulo the primes $3, 5, 7$, and 11, is 7; leading us to believe, especially given the above discussion, that the divisor also has order 7 in $J(X)(\mathbb{Q}\sqrt{13})$, but we are unable to verify this. Even if we assume this is the case, we are currently unable to rule out the possibility of a different (non-cuspidal) rational divisor producing a point of order 7 in $J(X)(\mathbb{Q})$. In any case, not completely understanding the structure of $J(X)(\mathbb{Q})_{\text{tors}}$ does not impede our progress.

We now exhibit some of the calculations carried out, using $p = 3$ as our primary example. Many of the calculations are too complicated to be carried out by hand, but we show as many intermediate steps as possible.

We first follow the Chabauty step to try and show that our quadratic points have no exceptional points in their mod 3 residue discs. For each point $Q_i = Q_{i,1} + Q_{i,2}$ we find that $\widetilde{Q_{i,1}} \neq \widetilde{Q_{i,2}}$ mod 3. This means, by Corollary 6.4, that we can obtain Chabauty information from the prime 3. We work with the quadratic point Q_2. Reducing mod 3 gives the following point on $X^{(2)}(\mathbb{F}_3)$:

$$\widetilde{Q_2} = (0 : t^2 : 0 : 0 : 1 : 2 : 1 : 1) + (0 : t^6 : 0 : 0 : 1 : 2 : 1 : 1),$$

where $t^2 + 2t + 2 = 0$.

We compute a basis for $\widetilde{V_0} = (1 - \widetilde{w_{13}}^*)(\Omega_{\tilde{X}})$, and for the first basis element, ω_1, we find that

$$\frac{\omega_1}{\mathrm{d}t_{\widetilde{Q_1}}} \Big|_{t_{\widetilde{Q_1}}=0} = t^3 \neq 0.$$

We conclude that there are no exceptional points in the mod 3 residue disc of Q_2. Repeating this process for the other six points yields the same outcome.

We now apply the sieving step with $p = 3$. Our aim is to calculate $\mathcal{W}_{3,M}$. To do this, we must first calculate $\mathcal{T}_{3,M}$. We find that $X^{(2)}(\mathbb{F}_3)$ consists of 27 points. By considering $\iota_{3,M}(R)$ for each $R \in X^{(2)}(\mathbb{F}_3)$, and seeing which of these lie in $\mu_{3,M}(\widetilde{G})$, we obtain the set $\mathcal{S}_{3,M}$ which consists of nine points. As each of our seven points satisfies the Chabauty criterion,

$$\mathcal{H}_{3,M} = \{\widetilde{Q_i} : i = 1, \ldots, 7\}.$$

Since $\widetilde{Q_2} = \widetilde{Q_6}$, $\#\mathcal{H}_{3,M} = 6$, and removing these six points from $\mathcal{S}_{3,M}$ gives

$$\begin{aligned}\mathcal{T}_{3,M} = \{&(0 : 0 : 0 : t^5 : t^5 : 2 : t^2 : 1) + (0 : 0 : 0 : t^3 : t^3 : 2 : t^6 : 1),\\ &(0 : 0 : 0 : t^3 : t^7 : t^7 : t^5 : 1) + (0 : 0 : 0 : t^5 : t : t : t3 : 1),\\ &(0 : 0 : 0 : t^5 : t^6 : t^5 : 1 : 0) + (0 : 0 : 0 : t^3 : t^2 : t^3 : 1 : 0)\}.\end{aligned}$$

Applying $\iota_{3,M}$ to this set, we obtain

$$\iota_{3,M}(\mathcal{T}_{3,M}) = \{(8, 8), (7, 7), (9, 9)\} \in \frac{J(\mathbb{F}_3)}{MJ(\mathbb{F}_3)} \cong \mathbb{Z}/13\mathbb{Z} \oplus \mathbb{Z}/13\mathbb{Z}.$$

Writing $\mathbb{Z}^3 \coloneqq \langle e_1, e_2, e_3\rangle$ with e_i the standard basis vectors, we find that

$$\begin{aligned}\mathcal{B}_{3,M} &= \ker(\varphi_{3,M}) = \langle e_1 + 7e_3, e_2 + 5e_3, 13e_3\rangle,\\ \mathcal{W}_{3,M} &= \{-3e_1 + \mathcal{B}_{3,M}, 4e_1 + \mathcal{B}_{3,M}, -2e_1 + \mathcal{B}_{3,M}\}.\end{aligned}$$

The index of $B_{3,M}$ in $\mathbb{Z}^3$ is 13. This completes the calculations for $p = 3$.

We now repeat these calculations for $p = 5$. This provides us with a group $\mathcal{B}_{5,M}$ and a set of $\mathcal{B}_{5,M}$ cosets, $\mathcal{W}_{5,M}$. We find that

$$\begin{aligned}\mathcal{B}_{5,M} &\coloneqq \langle e_1 + 6e_3, e_2 + 320e_3, 377e_3\rangle\\ \mathcal{W}_{5,M} &\coloneqq \{-57e_1 + \mathcal{B}_{5,M}, -165e_1 + \mathcal{B}_{5,M}, 28e_1 + \mathcal{B}_{5,M}\}.\end{aligned}$$

Although $\mathcal{W}_{3,M}$ and $\mathcal{W}_{5,M}$ were obtained from information modulo the corresponding prime, the information encoded is independent of the prime used. We now intersect $\mathcal{W}_{3,M}$ and $\mathcal{W}_{5,M}$ to find a new list of cosets, which will now be $\mathcal{B}_{3,5,M} \coloneqq \mathcal{B}_{3,M} \cap \mathcal{B}_{5,M}$ cosets. We obtain

$$\begin{aligned}
\mathcal{B}_{3,5,M} &\coloneqq \langle e_1 + 9e_2 + 247e_3, 13e_2 + 13e_3, 377e_3 \rangle, \\
\mathcal{W}_{3,5,M} &\coloneqq \{-165e_1 + \mathcal{B}_{3,5,M},\ 274e_1 - 5e_3 + \mathcal{B}_{3,5,M},\ -371e_1 + e_3 + \mathcal{B}_{3,5,M}, \\
&\qquad 445e_1 - 4e_3 + \mathcal{B}_{3,5,M},\ -1187e_1 + 6e_3 + \mathcal{B}_{3,5,M}, \\
&\qquad 29e_1 + 6e_3 + \mathcal{B}_{3,5,M},\ -475e_1 - 2e_3 + \mathcal{B}_{3,5,M}, \\
&\qquad 91e_1 + e_3 + \mathcal{B}_{3,5,M},\ -981e_1 + 5e_3 + \mathcal{B}_{3,5,M}\}.
\end{aligned}$$

Our list of cosets has grown, and so it may seem like we are worse off than we were before. However, these cosets are cosets of a much smaller subgroup: the index of $\mathcal{B}_{3,5,M}$ in $\mathbb{Z}^3$ is 4901. By continuing in this manner, we eventually find that

$$\mathcal{W}_{3,5,11,17,23,29,31,41,43,47,53,61,71,73,M} = \emptyset,$$

proving that there are no exceptional quadratic points on $X_{ns}(13)$.

We note that we have been somewhat crude with our choice of primes here. Given our choice of M, we have simply chosen all primes $p \leq 73$ for which $J(\mathbb{F}_p)/MJ(\mathbb{F}_p) \neq 0$. It is possible that a different choice of M and primes used in the sieve will reduce the computation time. However, the conclusion will of course be the same.

8 Bibliography

[1] J. Balakrishnan, N. Dogra, S. Müller, J. Tuitman, and J. Vonk. Explicit Chabauty—Kim for the split Cartan modular curve of level 13. *Annals of Mathematics*, 189(3):885–944, 2019.

[2] B. Baran. Normalizers of non-split Cartan subgroups, modular curves, and the class number one problem. *Journal of Number Theory*, 130 (12):2753–2772, 2010.

[3] B. Baran. An exceptional isomorphism between modular curves of level 13. *Journal of Number Theory*, 145:273–300, 2014.

[4] Y. Bilu, P. Parent, and M. Rebolledo. Rational points on $X_0^+(p^r)$. *Annales de l'Institut Fourier*, 63(3):957–984, 2013.

[5] J. Box. Quadratic points on modular curves with infinite Mordell–Weil group. *arXiv preprint arXiv:1906.05206* (to appear in *Mathematics of Computation*), 2019.

[6] N. Bruin and M. Stoll. The Mordell–Weil sieve: proving non-existence of rational points on curves. *LMS Journal of Computation and Mathematics*, 13:272–306, 2010.

[7] N. Bruin, B. Poonen, and M. Stoll. Generalized explicit descent and its application to curves of genus 3. *Forum of Mathematics, Sigma*, 4, 2016.

[8] P. Bruin and F. Najman. Hyperelliptic modular curves $X_0(n)$ and isogenies of elliptic curves over quadratic fields. *LMS Journal of Computation and Mathematics*, 18(1):578–602, 2015.

[9] I. Chen. The Jacobians of non-split Cartan modular curves. *Proceedings of the London Mathematical Society*, 77(1):1–38, 1998.

[10] I. Chen. On Siegel's modular curve of level 5 and the class number one problem. *Journal of Number Theory*, 74(2):278–297, 1999.

[11] J. Cremona. *Algorithms for Modular Elliptic Curves*. Cambridge University Press, 2nd edition, 1997.

[12] F. Diamond and J. Shurman. *A First Course in Modular Forms*. Springer-Verlag New York, 1st edition, 2005.

[13] M. Dickson. Modular curves and the class number one problem. `https://nms.kcl.ac.uk/martin.dickson/files/part_iii_essay.pdf`, 2011. Accessed: 2020-02-26.

[14] V. Dose. On the automorphisms of the non-split Cartan modular curves of prime level. *Nagoya Mathematical Journal*, 224(1):74–92, 2016.

[15] V. Dose, J. Fernández, J. González, and R. Schoof. The automorphism group of the non-split Cartan modular curve of level 11. *Journal of Algebra*, 417:95–102, 2014.

[16] V. Dose, P. Mercuri, and C. Stirpe. Double covers of Cartan modular curves. *Journal of Number Theory*, 195:96–114, 2019.

[17] V. Dose, G. Lido, and P. Mercuri. Automorphisms of Cartan modular curves of prime and composite level. *arXiv preprint arXiv:2005.09009*, 2020.

[18] V. Drinfeld. Two theorems on modular curves. *Funktsional'nyi Analiz i ego Prilozheniya*, 7(2):83–84, 1973.

[19] N. Freitas, B. Le Hung, and S. Siksek. Elliptic curves over real quadratic fields are modular. *Inventiones mathematicae*, 201(1):159–206, 2015.

[20] J. Harris and J. Silverman. Bielliptic curves and symmetric products. *Proceedings of the American Mathematical Society*, 112(2):347–356, 1992.

[21] S. Kamienny. Torsion points on elliptic curves and q-coefficients of modular forms. *Inventiones mathematicae*, 109(1):221–229, 1992.

[22] M. Kenku. A note on the integral points of a modular curve of level 7. *Mathematika*, 32(1):45–48, 1985.

[23] V. Kolyvagin and D. Logachëv. Finiteness of the Shafarevich–Tate group and the group of rational points for some modular abelian varieties. *Algebra i Analiz*, 1(5):171–196, 1989.

[24] S. Lang. *Algebra*. Springer-Verlag New York, 3rd edition, 2002.

[25] J. Manin. Parabolic points and zeta-functions of modular curves. *Mathematics of the USSR-Izvestiya*, 6(1):19, 1972.

[26] B. Mazur. Rational isogenies of prime degree. *Inventiones mathematicae*, 44(2):129–162, 1978.

[27] W. McCallum and B. Poonen. The method of Chabauty and Coleman. *Explicit Methods in Number Theory*, 36:99–117, 2012.

[28] P. Mercuri and R. Schoof. Modular forms invariant under non-split Cartan subgroups. *Mathematics of Computation*, 89(324):1969–1991, 2020.

[29] M. Murty and K. Sinha. Factoring newparts of Jacobians of certain modular curves. *Proceedings of the American Mathematical Society*, 138, 10:3481–3494, 2010.

[30] A Ogg. Hyperelliptic modular curves. *Bulletin de la Société Mathématique de France*, 102:449–462, 1974.

[31] E. Ozman and S. Siksek. Quadratic points on modular curves. *Mathematics of Computation*, 88(319):2461–2484, 2019. (Used arXiv:1806.08192v3).

[32] R. Schoof and N. Tzanakis. Integral points of a modular curve of level 11. *arXiv preprint arXiv:1107.2776*, 2011.

[33] J-P. Serre. Quelques applications du théorème de densité de Chebotarev. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 54(1):123–201, 1981.

[34] J-P. Serre. *Lectures on the Mordell-Weil Theorem*. Springer Vieweg, 1989.

[35] S. Siksek. Chabauty for symmetric powers of curves. *Algebra & Number Theory*, 3(2):209–236, 2009.

[36] S. Siksek. Explicit chabauty over number fields. *Algebra & Number Theory*, 7(4):765–793, 2013.

[37] S. Siksek. Explicit arithmetic of modular curves. `https://homepages.warwick.ac.uk/staff/S.Siksek/teaching/modcurves/lecturenotes.pdf`, 2019. Accessed: 2020-05-20.

[38] S. Siksek. Elliptic curves over quadratic fields with non-split Cartan mod 7 image. *Unpublished*, 2019.

[39] J. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer-Verlag New York, 1994.

[40] J. Silverman and J. Tate. *Rational Points on Elliptic Curves*. Springer, 2nd edition, 2015.

[41] F. Sottile. Real algebraic geometry for geometric constraints. *Handbook of Geometric Constraint Systems Principles, Discrete Math. Appl.(Boca Raton)*, pages 273–285, 2016.

[42] W. Stein. *Explicit approaches to modular abelian varieties*. PhD thesis, University of California, Berkeley, 2000.

[43] G. Stevens. *Arithmetic on Modular Curves*, volume 20. Springer Science & Business Media, 2012.

[44] D. Zywina. On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$. *arXiv preprint arXiv:1508.07660*, 2015.

Appendix A: Data

Structure of $J_{ns}(13)(\mathbb{F}_p)$

We list here the sizes of the Jacobians $J(X_{ns}(13))(\mathbb{F}_p)$ for primes up to 73 other than 2 and 13. The expression of $\#J(\mathbb{F}_p)$ reflects its group structure. For example, $J(\mathbb{F}_3) \cong \mathbb{Z}/182\mathbb{Z} \oplus \mathbb{Z}/182\mathbb{Z}$.

p	$\#J(\mathbb{F}_p)$
3	$2 \cdot 7 \cdot 13 \times 2 \cdot 7 \cdot 13$
5	$13 \times 3 \cdot 7 \cdot 11 \cdot 13 \cdot 29$
7	$2^3 \times 2^3 \cdot 7 \cdot 43 \cdot 659$
11	$2^2 \cdot 3 \times 2^2 \cdot 3 \cdot 7 \cdot 113 \cdot 3121$
17	$7 \times 7 \times 3 \cdot 5 \cdot 7 \cdot 127 \times 3 \cdot 5 \cdot 7 \cdot 127$
19	$2 \times 2 \cdot 7 \cdot 83 \cdot 97 \cdot 113 \cdot 883$
23	$2 \cdot 3^2 \cdot 7 \cdot 2381 \times 2 \cdot 3^2 \cdot 7 \cdot 2381$
29	$3^3 \cdot 7 \cdot 13 \cdot 293 \times 3^3 \cdot 7 \cdot 13 \cdot 293$
31	$2 \cdot 13 \times 2 \cdot 7 \cdot 11 \cdot 13 \cdot 23 \cdot 29 \cdot 97 \cdot 293$
37	$7 \cdot 37^2 \cdot 41 \cdot 83 \cdot 127 \cdot 953$
41	$7 \times 7 \times 3 \cdot 7 \times 3 \cdot 7 \cdot 193 \cdot 1217 \cdot 1723$
43	$7 \times 7 \cdot 13 \times 2^2 \cdot 7 \cdot 13 \cdot 97 \times 2^2 \cdot 7 \cdot 13^2 \cdot 97$
47	$2 \cdot 13 \times 2 \cdot 3 \cdot 7 \cdot 13 \cdot 43 \cdot 191 \cdot 281 \cdot 811$
53	$13 \times 13 \times 3 \cdot 7 \cdot 13 \cdot 19 \cdot 127 \times 3 \cdot 7 \cdot 13 \cdot 19 \cdot 127$
61	$7 \cdot 13 \cdot 29 \cdot 61 \cdot 83 \times 7 \cdot 13 \cdot 29 \cdot 61 \cdot 83$
67	$2 \times 2 \cdot 7 \cdot 43 \cdot 97 \cdot 449 \cdot 1153 \cdot 7307$
71	$2 \times 2 \cdot 3 \cdot 7 \cdot 443 \cdot 35531 \cdot 529747$
73	$13 \times 3 \cdot 13 \times 3 \cdot 13 \times 3 \cdot 7 \cdot 13 \cdot 29 \cdot 71 \cdot 181 \cdot 421$

Equations For New Model

We display here the 15 degree 2 equations for the new model obtained for $X_{ns}(13)$ as a curve in $\mathbb{P}^7$.

$$-2x_1^2 + x_1x_2 - 3x_1x_3 + x_1x_4 - 4x_1x_5 - x_1x_7 + 3x_2^2 + 2x_2x_3 - x_2x_4$$

$$
\begin{aligned}
&+ 3x_2x_5 + x_2x_7 - x_2x_8 - x_3^2 - 2x_3x_4 + 2x_3x_7 + 5x_3x_8 - x_4x_5 + x_4x_7 \\
&- x_4x_8 - x_7^2 - x_7x_8 + 2x_8^2 = 0, \\
&- 3x_1x_2 + 2x_1x_3 - 4x_1x_4 + x_1x_5 + 2x_1x_6 - x_1x_7 + 2x_1x_8 - 3x_2^2 - x_2x_3 \\
&+ 3x_2x_4 + x_2x_5 + 2x_2x_6 + 2x_2x_7 - x_2x_8 + 2x_3^2 + x_3x_5 + 2x_3x_6 \\
&- 3x_3x_7 + 4x_3x_8 - x_4^2 - 3x_4x_6 + 2x_4x_8 + x_5x_6 - x_5x_7 + 3x_5x_8 - x_6x_7 \\
&+ x_7^2 - x_7x_8 - 2x_8^2 = 0, \\
&- 2x_1^2 - 2x_1x_2 - x_1x_3 + 3x_1x_4 + x_1x_5 + 2x_1x_7 - 2x_1x_8 + x_2x_3 - 4x_2x_4 \\
&+ x_2x_5 + 5x_2x_6 + 4x_2x_8 + x_3^2 - x_3x_4 + x_3x_5 + x_3x_6 - x_3x_7 + 7x_3x_8 \\
&- x_4^2 - 2x_4x_6 + x_4x_7 + x_4x_8 + x_5x_6 - x_5x_7 + x_5x_8 - 2x_7x_8 = 0, \\
&2x_1^2 - 2x_1x_2 - 5x_1x_3 + x_1x_4 + x_1x_6 + x_1x_7 + x_2x_3 - x_2x_4 + x_2x_6 - x_2x_7 \\
&+ 2x_2x_8 + 2x_3^2 - 2x_3x_4 + x_3x_6 - 2x_3x_7 + 3x_3x_8 - x_4^2 - x_4x_5 + x_4x_7 \\
&+ x_4x_8 - x_5^2 + x_5x_6 + 2x_5x_8 + 2x_6^2 - 2x_6x_7 - x_6x_8 + x_7^2 - x_7x_8 - 2x_8^2 \\
&= 0, \\
&- 3x_1^2 - 2x_1x_2 + x_2^2 + 4x_2x_3 + 3x_3^2 - x_4^2 + x_4x_5 - x_4x_6 + x_4x_7 + 4x_4x_8 \\
&+ x_5^2 - x_5x_6 + 2x_5x_8 + x_6x_7 - 4x_6x_8 - 2x_7x_8 - x_8^2 = 0, \\
&- x_1^2 + x_1x_3 - 4x_1x_4 + 2x_1x_5 - x_1x_7 + x_2^2 + 3x_2x_3 + 3x_2x_4 - 3x_2x_5 \\
&+ 2x_2x_7 - 2x_2x_8 + 2x_3^2 + x_3x_5 - 3x_3x_7 - 3x_3x_8 - x_4x_6 + x_5^2 - x_5x_6 \\
&- x_5x_7 + 2x_5x_8 + x_6x_7 - 2x_6x_8 - x_7x_8 + x_8^2 = 0, \\
&- 2x_1x_6 - 4x_1x_8 - 2x_2x_4 - 3x_2x_5 + 3x_2x_6 + 3x_2x_7 - 3x_3x_4 + 2x_3x_5 \\
&- x_3x_6 - 2x_3x_7 + 2x_3x_8 - x_4x_5 - x_4x_6 + 2x_5x_8 - x_6x_7 = 0, \\
&- 2x_1^2 - 2x_1x_2 - x_1x_3 - x_1x_4 - x_1x_5 + 2x_1x_6 + 2x_1x_8 + x_2x_3 + 2x_2x_4 \\
&- x_2x_5 - 3x_2x_6 - 2x_2x_7 + x_3^2 - 3x_3x_4 - x_3x_5 + x_3x_6 - 3x_3x_7 - x_3x_8 \\
&- x_4^2 - 2x_4x_6 + x_4x_7 + x_4x_8 + x_5x_6 - x_5x_7 + x_5x_8 - 2x_7x_8 = 0, \\
&- x_1^2 + x_1x_2 - 4x_1x_3 + x_1x_4 - 2x_1x_6 - 2x_1x_7 + 4x_1x_8 + 2x_2^2 - x_2x_3 \\
&+ 2x_2x_4 - 2x_2x_5 - 2x_2x_6 - 3x_2x_7 - 3x_2x_8 - 3x_3^2 - 4x_3x_4 - 3x_3x_5 \\
&- 2x_3x_6 + 3x_3x_7 - x_4x_5 + x_4x_6 + x_4x_7 - x_4x_8 - x_5^2 + x_5x_6 + x_5x_7 \\
&- 2x_5x_8 - x_6x_7 + 2x_6x_8 - x_7^2 + x_8^2 = 0, \\
&- 4x_1^2 - 4x_1x_2 - 2x_1x_3 + 2x_2x_3 + 2x_3^2 - 2x_4^2 + 2x_4x_5 - 2x_4x_6 + 2x_4x_7 \\
&+ 2x_4x_8 + 2x_5x_6 - 2x_5x_7 - 2x_5x_8 + 2x_6x_7 - 4x_7x_8 = 0, \\
&2x_1x_4 + 2x_1x_6 + 2x_1x_7 - 2x_2x_4 + 2x_2x_6 - 2x_2x_7 + 4x_2x_8 - 4x_3x_4 + 2x_3x_6 \\
&- 4x_3x_7 + 6x_3x_8 = 0, \\
&- x_1^2 + x_1x_2 - 4x_1x_3 + 3x_1x_4 + 2x_1x_5 + 2x_1x_7 + 2x_2^2 - x_2x_3 - 2x_2x_4 \\
&- 3x_2x_7 + 3x_2x_8 - 3x_3^2 + 2x_3x_4 - x_3x_5 + x_3x_7 - 2x_3x_8 - x_4x_5 \\
&+ x_4x_6 + x_4x_7 - x_4x_8 - x_5^2 + x_5x_6 + x_5x_7 - 2x_5x_8 - x_6x_7 + 2x_6x_8
\end{aligned}
$$

$$
\begin{aligned}
&\quad - x_7^2 + x_8^2 = 0,\\
&- 2x_1x_4 - x_1x_5 + x_1x_6 - x_1x_7 + 2x_1x_8 + 3x_2x_4 - x_2x_5 - 4x_2x_6 - x_2x_7\\
&\quad - 2x_2x_8 - x_3x_4 - x_3x_5 - x_3x_7 - 4x_3x_8 - 2x_4^2 - x_4x_5 + 2x_4x_6 + 2x_4x_7\\
&\quad - x_5^2 + x_5x_7 + x_5x_8 - x_6x_8 + 2x_7^2 - 3x_7x_8 + 2x_8^2 = 0,\\
&x_1^2 - x_1x_2 + 4x_1x_3 + x_1x_5 - 2x_1x_6 + x_1x_7 - 6x_1x_8 + 4x_2^2 + 6x_2x_3 - 3x_2x_4\\
&\quad - 2x_2x_5 + 3x_2x_6 + 4x_2x_7 + x_2x_8 - 3x_3^2 + 2x_3x_4 + 3x_3x_5 - x_3x_6\\
&\quad - x_3x_7 - 2x_3x_8 + 2x_4^2 + x_4x_6 - 2x_4x_7 + 3x_5^2 - 2x_5x_6 - x_5x_7 + x_5x_8\\
&\quad - 2x_6^2 - x_6x_7 - 4x_6x_8 - x_7^2 - x_7x_8 + x_8^2 = 0,\\
&- 2x_1x_2 + 10x_1x_3 - 3x_1x_4 + 3x_1x_5 - 2x_1x_6 - x_1x_7 - 2x_1x_8 + 3x_2^2\\
&\quad - 16x_2x_3 + x_2x_4 - 2x_2x_5 + 3x_2x_6 + 4x_2x_7 - 2x_2x_8 + 5x_3^2 + 3x_3x_4\\
&\quad + 2x_3x_5 - x_3x_6 - 2x_3x_8 + x_4^2 + x_4x_5 - 2x_4x_7 + x_4x_8 + x_5x_6 + 3x_5x_8\\
&\quad + 2x_6x_7 + 6x_6x_8 + x_7^2 - x_7x_8 + 6x_8^2 = 0.
\end{aligned}
$$

The equations for the map ϱ from this new model to the curve $X_{ns}^+(13)$ is given by

$$
\begin{aligned}
\varrho : X_{ns}(13) &\longrightarrow X_{ns}^+(13)\\
(x_1 : \cdots : x_8) &\longmapsto (-3x_2 + x_3, -2x_1 - 3x_1 + x_3, x_1 + x_2 + x_3).
\end{aligned}
$$

Appendix B: Magma Code

Testing saturation

```
// Defining XNS+(13).
S<X,Y,Z>:=PolynomialRing(Rationals(),3);
f:=(-Y-Z)*X^3+(2*Y^2+Z*Y)*X^2+(-Y^3+Z*Y^2-2*(Z^2)*Y+Z^3)*X+(2*Z^2*Y^2-3*Z^3*Y);
C:=Curve(ProjectiveSpace(S),f);

p := 41; // Primes to test

Zp3:=AbelianGroup([p,p,p]);
Kls:=[];
for i in [1,12,23,26] do //
    l:=NthPrime(i);
    Cl:=ChangeRing(C,GF(l));
    ClGrp,phi,psi:=ClassGroup(Cl);
    Z:=FreeAbelianGroup(1);
    degr:=hom<ClGrp->Z | [ Degree(phi(a))*Z.1 : a in OrderedGenerators(ClGrp)]>;
    JFl:=Kernel(degr);                  // Jacobian mod l as an abelian group
    JFlmodp,pi:=quo<JFl | p*JFl>;

    h1p:= Place(Cl ! [0,1,0]);
    h2p:= Place(Cl ! [0,0,1]);
    h3p:= Place(Cl ! [-1,0,1]);
    bp := Place(Cl ! [1,0,0]);
```

```
    Delta1p:=h1p-bp; Delta2p:=h2p-bp; Delta3p:=h3p-bp;  // Generators of H

    pil:=hom<Zp3->JFlmodp | [pi(psi(Delta1p)),pi(psi(Delta2p)),pi(psi(Delta3p))]>;
    Kl:=Kernel(pil);
    Kls:=Kls cat [Kl];
    print  "Calculations completed for l =", l;
end for;

IntKl:=&meet(Kls);  // Intersection Kernels
if #IntKl eq 1 then
print "Index not divisible by", p;
end if;
```

Computing a new model for $X_{ns}(13)$.

```
R<x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8> := PolynomialRing(Rationals(),8);
// Equations for XNS13 from Double Cover paper
Eq1:=x_1^2 - x_1*x_3 - x_1*x_4 - x_1*x_7 + x_1*x_8 + x_2*x_4 + x_2*x_5 + 2*x_3*x_4
- 2*x_3*x_5 - x_3*x_8 + 2*x_4*x_5 +x_4*x_7 + x_5*x_8 - x_7^2 + x_7*x_8;
Eq2:=-x_1*x_3 + 2*x_1*x_5 + x_1*x_8 - 2*x_3*x_4 - x_3*x_5 + x_3*x_6 - x_3*x_7
- x_4*x_5 - x_4*x_6 + x_4*x_7 + x_4*x_8 - x_5^2 + x_5*x_6 - 3*x_5*x_8 - x_6*x_7 -
3*x_6*x_8 + x_7^2 - x_8^2;
Eq3:=-x_1*x_3 + 2*x_1*x_4 + x_1*x_5 - 2*x_1*x_6 +
4*x_1*x_8 + x_2*x_4 + x_2*x_5 - x_3*x_4 + x_3*x_6 - x_3*x_7 - x_4^2 + x_4*x_5
- 2*x_4*x_8 + 2*x_5*x_7 + x_5*x_8 - 2*x_6*x_8 + x_7*x_8 - x_8^2;
Eq4:=x_1*x_3
+ x_1*x_4 + x_1*x_5 - 3*x_1*x_6 + x_1*x_7 + 2*x_1*x_8 - x_2*x_3 - x_2*x_4 + x_2*x_5
+ x_2*x_6 - x_3^2 - x_3*x_4 - x_3*x_5 + x_3*x_6 - x_3*x_8 - 2*x_4*x_5 - x_4*x_8
 + x_5*x_6 + x_5*x_7 + 2*x_6^2 - 2*x_6*x_7 + x_7^2 + x_7*x_8 - x_8^2;
Eq5:=x_1*x_2 - x_1*x_3 + x_1*x_5 + x_1*x_6 - x_1*x_7 + x_1*x_8 + x_2^2 + x_2*x_3
- x_2*x_4 - x_2*x_5 - x_2*x_6 + x_3^2 - x_3*x_4 - x_3*x_5 - x_3*x_6 + x_3*x_8
 - x_4^2 + x_4*x_5 + 2*x_4*x_6 + x_4*x_7 - 2*x_4*x_8 - x_5^2 + 2*x_5*x_6 + x_5*x_7
 - 2*x_5*x_8 + x_6*x_7 - x_6*x_8 + x_7*x_8 - x_8^2;
Eq6:=2*x_1*x_2 + x_1*x_3 - x_1*x_4 + x_1*x_6 - x_1*x_7 - x_1*x_8 + x_2*x_3 - 2*x_2*x_4
- x_2*x_5 - x_2*x_6 + x_2*x_7  +x_3^2 - 2*x_3*x_4 - x_3*x_6 - x_3*x_7 + x_4*x_5
+ x_4*x_6 + x_4*x_7 + 2*x_4*x_8 + x_5*x_6 - 2*x_5*x_8 + x_6*x_7 - x_6*x_8;
 Eq7:=-x_1^2 + x_1*x_2 + 2*x_1*x_3 + x_1*x_5 - x_1*x_6 - x_1*x_7 + 2*x_1*x_8 - x_2^2
 - x_2*x_3 + x_2*x_6 + x_2*x_7  +x_2*x_8 - x_3*x_4 - x_3*x_5 - x_3*x_8 - x_4^2 + x_4*x_6
+ x_5^2 - x_5*x_6 - x_6*x_7 - x_6*x_8;
Eq8:=-x_1^2 - x_1*x_2 + x_1*x_5 + 2*x_1*x_6 + x_1*x_7 + x_1*x_8 + x_2*x_3 - x_2*x_4
- x_2*x_5 + x_2*x_7 + x_2*x_8 - x_3*x_5 + x_3*x_6 - x_3*x_7 + x_4*x_5 - x_4*x_6
 + x_4*x_7 - x_5^2 + x_5*x_6 + x_5*x_7 - x_5*x_8 - 2*x_6*x_8 + x_7*x_8 - x_8^2;
Eq9:=-2*x_1*x_2 + 2*x_1*x_3 - x_1*x_4 - x_1*x_5 + x_1*x_7 - x_1*x_8 - x_2*x_4
+ 2*x_2*x_5 + 2*x_2*x_6 + x_2*x_8 - x_3^2 + x_3*x_4 + x_3*x_5 + x_3*x_6 + x_3*x_7
 - x_3*x_8 + x_4^2 + x_4*x_5 + x_4*x_7 - x_5^2 - 2*x_5*x_6 - x_5*x_7 + x_5*x_8
 - x_6*x_7 + x_6*x_8 - x_7^2+ x_7*x_8;
Eq10:=-2*x_1*x_3 - x_1*x_4 + x_1*x_5 - x_1*x_7 + 2*x_1*x_8 + x_2^2 + x_2*x_3
 - x_2*x_4 - x_2*x_7 + x_3*x_4 + x_3*x_5 + 2*x_3*x_6 - 2*x_3*x_7 + 2*x_3*x_8
 - x_4^2 + 2*x_4*x_5 + 2*x_4*x_7 - x_4*x_8 - x_5^2 + 2*x_5*x_7 - x_5*x_8
+ 2*x_6*x_7 - 2*x_6*x_8 + 2*x_7*x_8 - 2*x_8^2;
Eq11:=-x_1*x_2 + 2*x_1*x_4 - x_1*x_6 + x_1*x_7 + x_1*x_8 - x_2^2 + 2*x_2*x_4
```

```
+ x_2*x_5 - x_2*x_6 + 2*x_2*x_7  +2*x_2*x_8 - x_4*x_6 - x_4*x_7 - x_4*x_8 + x_5*x_6
 + x_5*x_7 + x_5*x_8;
 Eq12:=x_1*x_3 + 2*x_1*x_4 - x_1*x_5 - x_1*x_6 + x_1*x_7 + x_1*x_8 - x_2^2 - x_2*x_3
 - x_2*x_4 + x_2*x_5 + x_2*x_6 + x_2*x_7 - 2*x_2*x_8 - x_3^2 + 2*x_3*x_5 + x_3*x_6
+ x_3*x_7 - x_3*x_8 + x_4*x_5 - x_4*x_6 - x_4*x_7 - x_4*x_8 - x_5*x_6 + x_5*x_7
 + 2*x_5*x_8 - x_6*x_7 + x_6*x_8 - x_7^2 + x_7*x_8;
 Eq13:=-x_1^2 + x_1*x_2 + 2*x_1*x_3 - x_1*x_4 + x_1*x_6 - x_1*x_7 - x_2*x_3 - 2*x_2*x_4
 - 2*x_2*x_5 - x_2*x_7 - x_2*x_8 - x_3^2 - x_3*x_5 + x_3*x_7 - x_3*x_8 + x_4^2 + x_4*x_5
 + 2*x_4*x_7 + x_4*x_8 + x_5*x_6 + x_5*x_7 - x_5*x_8 +2*x_6*x_8 + 2*x_7^2 + 2*x_7*x_8 - 2*x_8^2;
 Eq14:=x_1^2 + 2*x_1*x_2 - x_1*x_3 - x_1*x_4 + x_1*x_6 - x_1*x_8 - x_2^2 + 2*x_2*x_3
- 2*x_2*x_5 + x_2*x_7 + 3*x_3^2 - x_3*x_4 - 2*x_3*x_6 - x_3*x_7 - x_4^2 + 3*x_4*x_6
+ 2*x_5^2 + x_5*x_6 + x_5*x_7 - 2*x_6^2 - x_6*x_7 + x_6*x_8 - x_7^2 - 2*x_7*x_8 + 2*x_8^2;
Eq15:=2*x_1^2 - 2*x_1*x_2 + x_1*x_4 + 3*x_1*x_5 - 2*x_1*x_6 - 2*x_1*x_7 - 2*x_1*x_8 + x_2^2
 - x_2*x_3 - 3*x_2*x_5 - x_2*x_7 -3*x_3*x_4 + x_3*x_6 + x_3*x_8 + x_4^2 + 3*x_4*x_5 - 2*x_4*x_6
+ x_4*x_7 + x_4*x_8 + 2*x_5^2 - 4*x_5*x_6 - 2*x_5*x_8 +2*x_6*x_7 + x_7^2 -2*x_7*x_8 + x_8^2;
eqns:=[Eq1,Eq2,Eq3,Eq4,Eq5,Eq6,Eq7,Eq8,Eq9,Eq10,Eq11,Eq12,Eq13,Eq14,Eq15];
XNS13:=Curve(ProjectiveSpace(R),eqns);  // The curve X_ns(13)

S<X,Y,Z>:=PolynomialRing(Rationals(),3);
f:=(-Y-Z)*X^3+(2*Y^2+Z*Y)*X^2+(-Y^3+Z*Y^2-2*(Z^2)*Y+Z^3)*X+(2*Z^2*Y^2-3*Z^3*Y);
XNSplus13:=Curve(ProjectiveSpace(S),f); // The curve X_ns^+(13),

Eqphi1:=-3*x_1+2*x_2;  // Equations for rho
Eqphi2:=-3*x_1+x_2+2*x_4-2*x_5;
Eqphi3:=x_1+x_2+x_4-x_5;
eqnsphi:=[Eqphi1,Eqphi2,Eqphi3];
phi:=map< XNS13->XNSplus13 | eqnsphi >;

SvnPts:=PointSearch(XNSplus13,100);

////////////////////////////////////////////////////////////////////////////////////////////

// Finding matrix of modular involution
T<x> := PolynomialRing(Integers());
QQ<d1,d2,d4,d5,d6,d7>:=ext<Rationals() | x^2+11,x^2+67,x^2+2,x^2+19,x^2+163,x^2+7>;
PQQ<u1,u2,u3,u4,u5,u6,u7,u8> := ProjectiveSpace(QQ,7);
ProjPts:=[];

for i in [1..7] do
    Ds:=[11,67,7,2,19,163,7];
    K:=NumberField(x^2+Ds[i]);
    XK:=ChangeRing(XNS13,K);
    XplK:=ChangeRing(XNSplus13,K);
    phiK:=map< XK->XplK| eqnsphi >;
    PK:=XplK ! Eltseq(SvnPts[i]);
    Pinv:=Points(PK @@ phiK);
    Qa:=Eltseq(Pinv[1]);
    Qb:=Eltseq(Pinv[2]);
    _,pi:=IsSubfield(K,QQ);
    PQa:= PQQ ! [pi(Qa[i]) : i in [1..8]];
    PQb:= PQQ ! [pi(Qb[i]) : i in [1..8]];
    ProjPts:=ProjPts cat [PQa,PQb];
end for;
```

```
Seq1:=[ProjPts[i] : i in [1,3,5,7,9,11,13,2,4]];  // 9 of our quadratic points...
Seq2:=[ProjPts[i] : i in [2,4,6,8,10,12,14,1,3]]; // ... and their conjugate points
T1 := TranslationOfSimplex(PQQ,Seq1);             // Map to standard simplex
T2 := TranslationOfSimplex(PQQ,Seq2);
TofS := T2^(-1)*T1;
EqTS:=DefiningEquations(TofS);

////////////////////////////////////////////////////////////////////////////////////////////

w:=map<XNS13->XNS13 | EqTS>;          // The modular involution on the curve
Mw:=Transpose((Matrix(w)));           // Matrix of the modular involution
Diag,T:=PrimaryRationalForm(Mw);
assert T*Mw*(T^-1) eq Diag;

Eqg:=[];                              // We use T^-1 to find our change of coordinate map
for i in [1..8] do
    ri:=&+[(T^-1)[i][j]*R.j : j in [1..8]];
    Eqg:=Eqg cat [ri];
end for;
g:=hom<R->R | Eqg>;                   // Change of coordinate map


////////////////////////////////////////////////////////////////////////////////////////////

// Apply our change of coordinates to each of the 15 equations
Neqns:=[];
for i in [1..15] do
    Neqn:=g(eqns[i]);
    Neqns:=Neqns cat [Neqn];
end for;

// Apply change of coordinates to obtain new equations for map (to same bottom curve)
Nphis:=[];
for i in [1..3] do
    Nphi:=g(eqnsphi[i]);
    Nphis:=Nphis cat [Nphi];
end for;

// We now have the following new data:
NX:=Curve(ProjectiveSpace(R),Neqns);                          // New model of our curve
Nw:=map<NX -> NX | [x_1,x_2,x_3,-x_4,-x_5,-x_6,-x_7,-x_8]>;  // New modular involution
Nphi:=map< NX -> XNSplus13 | Nphis >;                         // New equations for map

// Check that this new model is nonsingular at the primes used in (very long).
for p in [3,5,7,17,23,29,31,41,47,53,61,71,73] do
    print "Starting p =", p;
    NXp:=ChangeRing(NX,GF(p));
    assert IsNonsingular(NXp);
    print "Nonsingular mod", p;
end for;
```

Chabauty and Sieve computations.

```
// First recreate the new model
R<x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8>:=PolynomialRing(Rationals(),8);
Eq1:=x_1^2 - x_1*x_3 - x_1*x_4 - x_1*x_7 + x_1*x_8 + x_2*x_4 + x_2*x_5 + 2*x_3*x_4
- 2*x_3*x_5 - x_3*x_8 + 2*x_4*x_5 +x_4*x_7 + x_5*x_8 - x_7^2 + x_7*x_8;
Eq2:=-x_1*x_3 + 2*x_1*x_5 + x_1*x_8 - 2*x_3*x_4 - x_3*x_5 + x_3*x_6 - x_3*x_7
- x_4*x_5 - x_4*x_6 + x_4*x_7 + x_4*x_8 - x_5^2 + x_5*x_6 - 3*x_5*x_8 - x_6*x_7 -
3*x_6*x_8 + x_7^2 - x_8^2;
Eq3:=-x_1*x_3 + 2*x_1*x_4 + x_1*x_5 - 2*x_1*x_6 +
4*x_1*x_8 + x_2*x_4 + x_2*x_5 - x_3*x_4 + x_3*x_6 - x_3*x_7 - x_4^2 + x_4*x_5
- 2*x_4*x_8 + 2*x_5*x_7 + x_5*x_8 - 2*x_6*x_8 + x_7*x_8 - x_8^2;
Eq4:=x_1*x_3
+ x_1*x_4 + x_1*x_5 - 3*x_1*x_6 + x_1*x_7 + 2*x_1*x_8 - x_2*x_3 - x_2*x_4 + x_2*x_5
+ x_2*x_6 - x_3^2 - x_3*x_4 - x_3*x_5 + x_3*x_6 - x_3*x_8 - 2*x_4*x_5 - x_4*x_8
 + x_5*x_6 + x_5*x_7 + 2*x_6^2 - 2*x_6*x_7 + x_7^2 + x_7*x_8 - x_8^2;
Eq5:=x_1*x_2 - x_1*x_3 + x_1*x_5 + x_1*x_6 - x_1*x_7 + x_1*x_8 + x_2^2 + x_2*x_3
- x_2*x_4 - x_2*x_5 - x_2*x_6 + x_3^2 - x_3*x_4 - x_3*x_5 - x_3*x_6 + x_3*x_8
 - x_4^2 + x_4*x_5 + 2*x_4*x_6 + x_4*x_7 - 2*x_4*x_8 - x_5^2 + 2*x_5*x_6 + x_5*x_7
 - 2*x_5*x_8 + x_6*x_7 - x_6*x_8 + x_7*x_8 - x_8^2;
Eq6:=2*x_1*x_2 + x_1*x_3 - x_1*x_4 + x_1*x_6 - x_1*x_7 - x_1*x_8 + x_2*x_3 - 2*x_2*x_4
- x_2*x_5 - x_2*x_6 + x_2*x_7  +x_3^2 - 2*x_3*x_4 - x_3*x_6 - x_3*x_7 + x_4*x_5
+ x_4*x_6 + x_4*x_7 + 2*x_4*x_8 + x_5*x_6 - 2*x_5*x_8 + x_6*x_7 - x_6*x_8;
 Eq7:=-x_1^2 + x_1*x_2 + 2*x_1*x_3 + x_1*x_5 - x_1*x_6 - x_1*x_7 + 2*x_1*x_8 - x_2^2
 - x_2*x_3 + x_2*x_6 + x_2*x_7  +x_2*x_8 - x_3*x_4 - x_3*x_5 - x_3*x_8 - x_4^2 + x_4*x_6
+ x_5^2 - x_5*x_6 - x_6*x_7 - x_6*x_8;
Eq8:=-x_1^2 - x_1*x_2 + x_1*x_5 + 2*x_1*x_6 + x_1*x_7 + x_1*x_8 + x_2*x_3 - x_2*x_4
- x_2*x_5 + x_2*x_7 + x_2*x_8 - x_3*x_5 + x_3*x_6 - x_3*x_7 + x_4*x_5 - x_4*x_6
 + x_4*x_7 - x_5^2 + x_5*x_6 + x_5*x_7 - x_5*x_8 - 2*x_6*x_8 + x_7*x_8 - x_8^2;
Eq9:=-2*x_1*x_2 + 2*x_1*x_3 - x_1*x_4 - x_1*x_5 + x_1*x_7 - x_1*x_8 - x_2*x_4
+ 2*x_2*x_5 + 2*x_2*x_6 + x_2*x_8 - x_3^2 + x_3*x_4 + x_3*x_5 + x_3*x_6 + x_3*x_7
 - x_3*x_8 + x_4^2 + x_4*x_5 + x_4*x_7 - x_5^2 - 2*x_5*x_6 - x_5*x_7 + x_5*x_8
 - x_6*x_7 + x_6*x_8 - x_7^2+ x_7*x_8;
Eq10:=-2*x_1*x_3 - x_1*x_4 + x_1*x_5 - x_1*x_7 + 2*x_1*x_8 + x_2^2 + x_2*x_3
 - x_2*x_4 - x_2*x_7 + x_3*x_4 + x_3*x_5 + 2*x_3*x_6 - 2*x_3*x_7 + 2*x_3*x_8
 - x_4^2 + 2*x_4*x_5 + 2*x_4*x_7 - x_4*x_8 - x_5^2 + 2*x_5*x_7 - x_5*x_8
+ 2*x_6*x_7 - 2*x_6*x_8 + 2*x_7*x_8 - 2*x_8^2;
Eq11:=-x_1*x_2 + 2*x_1*x_4 - x_1*x_6 + x_1*x_7 + x_1*x_8 - x_2^2 + 2*x_2*x_4
+ x_2*x_5 - x_2*x_6 + 2*x_2*x_7  +2*x_2*x_8 - x_4*x_6 - x_4*x_7 - x_4*x_8 + x_5*x_6
 + x_5*x_7 + x_5*x_8;
 Eq12:=x_1*x_3 + 2*x_1*x_4 - x_1*x_5 - x_1*x_6 + x_1*x_7 + x_1*x_8 - x_2^2 - x_2*x_3
 - x_2*x_4 + x_2*x_5 + x_2*x_6 + x_2*x_7 - 2*x_2*x_8 - x_3^2 + 2*x_3*x_5 + x_3*x_6
+ x_3*x_7 - x_3*x_8 + x_4*x_5 - x_4*x_6 - x_4*x_7 - x_4*x_8 - x_5*x_6 + x_5*x_7
 + 2*x_5*x_8 - x_6*x_7 + x_6*x_8 - x_7^2 + x_7*x_8;
 Eq13:=-x_1^2 + x_1*x_2 + 2*x_1*x_3 - x_1*x_4 + x_1*x_6 - x_1*x_7 - x_2*x_3 - 2*x_2*x_4
 - 2*x_2*x_5 - x_2*x_7 - x_2*x_8 - x_3^2 - x_3*x_5 + x_3*x_7 - x_3*x_8 + x_4^2 + x_4*x_5
 + 2*x_4*x_7 + x_4*x_8 + x_5*x_6 + x_5*x_7 - x_5*x_8 +2*x_6*x_8 + 2*x_7^2 + 2*x_7*x_8 - 2*x_8^2;
 Eq14:=x_1^2 + 2*x_1*x_2 - x_1*x_3 - x_1*x_4 + x_1*x_6 - x_1*x_8 - x_2^2 + 2*x_2*x_3
- 2*x_2*x_5 + x_2*x_7 + 3*x_3^2 - x_3*x_4 - 2*x_3*x_6 - x_3*x_7 - x_4^2 + 3*x_4*x_6
+ 2*x_5^2 + x_5*x_6 + x_5*x_7 - 2*x_6^2 - x_6*x_7 + x_6*x_8 - x_7^2 - 2*x_7*x_8 + 2*x_8^2;
Eq15:=2*x_1^2 - 2*x_1*x_2 + x_1*x_4 + 3*x_1*x_5 - 2*x_1*x_6 - 2*x_1*x_7 - 2*x_1*x_8 + x_2^2
 - x_2*x_3 - 3*x_2*x_5 - x_2*x_7 -3*x_3*x_4 + x_3*x_6 + x_3*x_8 + x_4^2 + 3*x_4*x_5 - 2*x_4*x_6
+ x_4*x_7 + x_4*x_8 + 2*x_5^2 - 4*x_5*x_6 - 2*x_5*x_8 +2*x_6*x_7 + x_7^2 -2*x_7*x_8 + x_8^2;
```

```
eqns:=[Eq1,Eq2,Eq3,Eq4,Eq5,Eq6,Eq7,Eq8,Eq9,Eq10,Eq11,Eq12,Eq13,Eq14,Eq15]; // List of equations

// Change of coordinates map
g:=hom<R->R | x_2,x_3,1/2*x_2-1/2*x_3-1/2*x_5,1/2*x_1+1/2*x_8,-1/2*x_1+1/2*x_8,1/2*x_2-1/2*x_6,
1/2*x_3-1/2*x_7,1/2*x_2-1/2*x_4>;

Neqns:=[];
for i in [1..15] do
    Neqn:=g(eqns[i]);
    Neqns:=Neqns cat [Neqn];
end for;

NX:=Curve(ProjectiveSpace(R),Neqns);
Nw:=map<NX -> NX | [x_1,x_2,x_3,-x_4,-x_5,-x_6,-x_7,-x_8]>;

Eqphi1:=-3*x_1+2*x_2;  Eqphi2:=-3*x_1+x_2+2*x_4-2*x_5; Eqphi3:=x_1+x_2+x_4-x_5;
eqnsphi:=[Eqphi1,Eqphi2,Eqphi3];
Nphis:=[];  //
for i in [1..3] do
    Nphi:=g(eqnsphi[i]);
    Nphis:=Nphis cat [Nphi];
end for;

S<X,Y,Z>:=PolynomialRing(Rationals(),3);
f:=(-Y-Z)*X^3+(2*Y^2+Z*Y)*X^2+(-Y^3+Z*Y^2-2*(Z^2)*Y+Z^3)*X+(2*Z^2*Y^2-3*Z^3*Y);
XNSplus13:=Curve(ProjectiveSpace(S),f);

Nphi:=map< NX -> XNSplus13 | Nphis >;

SvnPts:=PointSearch(XNSplus13,100);

////////////////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////////////////


pinsieve:=[5,7,11,17,23,29,31,41,43,47,53,61,71,73];  // Primes to be used in sieve

M:=3^10*5^10*13^10*29^10;
A:=AbelianGroup([0,0,0]);

Ws:=[**];
Bs:=[**];

////////////////////////////////////////////////////////////////////////////////////////////

for p in pinsieve do

    redpL:={};    // Build up to list of known divisors reduced mod p
    divsp:=[];    // Build up to list of generators for G reduced mod p
    Rks:=[];      // Ranks of residue disc matrices
    TQ<x> := PolynomialRing(Integers());
    Fp:=GF(p);
    Xp:=ChangeRing(NX,Fp);
```

```
////////////////////////////////////////////////////////////////////////////////////////

    for i in [1..7] do
        Ds:=[11,67,7,2,19,163,7];
        K:=NumberField(x^2+Ds[i]);
        XK:=ChangeRing(NX,K);
        XplK:=ChangeRing(XNSplus13,K);
        phiK:=map< XK->XplK| Nphis >;   // Base change everything to new field
        PK:=XplK ! Eltseq(SvnPts[i]);

        Pinv:=Points(PK @@ phiK);       // Pullback of the point to the top curve
        Qa:=Eltseq(Pinv[1]);
        Qb:=Eltseq(Pinv[2]);             // The two quadratic points

        OK:=RingOfIntegers(K);
        dec:=Factorization(p*OK);
        pp:=dec[1][1];                   // A prime above the rational prime p
        f:=InertiaDegree(pp);
        Fpp<t>:= ResidueClassField(pp);  // Either GF(p) or GF(p^2) depending on inertia degree
        Xpp:=ChangeRing(NX,Fpp);

        unif:=UniformizingElement(pp);   // Use to reduce point modulo p
        m:=Minimum([Valuation(a,pp) : a in Qa | not a eq 0]);
        Qared:=[unif^(-m)*a : a in Qa];
        Qtaa:=Xpp![Evaluate(a,Place(pp)) : a in Qared]; // Reduction of quadratic point to Xpp
        Qta:=Xp(Fpp) ! Eltseq(Qtaa);
        plQtaa:=Place(Qtaa);
        plQta:=Place(Qta);

        m:=Minimum([Valuation(a,pp) : a in Qb | not a eq 0]); // Repeat with conjugate
        Qbred:=[unif^(-m)*a : a in Qb];
        Qtbb:=Xpp![Evaluate(a,Place(pp)) : a in Qbred];
        Qtb:=Xp(Fpp) ! Eltseq(Qtbb);
        plQtbb:=Place(Qtbb);
        plQtb:=Place(Qtb);

////////////////////////////////////////////////////////////////////////////

// Checking if there are exceptional points in residue disc of the point
        wpp:=map< Xpp->Xpp | [x_1,x_2,x_3,-x_4,-x_5,-x_6,-x_7,-x_8] >; // Modular involution
        V,phiD:=SpaceOfDifferentialsFirstKind(Xpp);  // Holomorphic differentials on Xpp
        t:=hom<V->V | [ (Pullback(wpp,phiD(V.i)))@@phiD -V.i  : i in [1..8] ]>;
        T:=Image(t);                                 // The space red(V_0)
        oms:=[phiD(T.i) : i in [1..Dimension(T)]];
        tQta:=UniformizingParameter(Qtaa);
        tQtb:=UniformizingParameter(Qtbb);
        Ata:=Matrix([[Evaluate(omega/Differential(tQta),plQtaa) : omega in oms]]);
        Atb:=Matrix([[Evaluate(omega/Differential(tQtb),plQtbb) : omega in oms]]);
        ra:=Rank(Ata);
        rb:=Rank(Atb);  // Rank 1 means no exceptional points in residue class
        if ra eq 0 then print "Point Not Lonely When i =", i; print"and p =", p; end if;
// An alert to say that there could potentially be an exceptional point in the residue class.
        Rks:=Rks cat [ra];
```

```
////////////////////////////////////////////////////////////////////////////

        if Degree(plQta) eq 1 then   // if a point is defined over Fp
           DivQ:=plQta+plQtb;        // then form a divisor from the point and its conjugate
        end if;
        if Degree(plQta) eq 2 then   // if a point is defined over Fp^2
           DivQ:=Divisor(plQta);     // then form the divisor of its place
        end if;

        redpL:=redpL join {DivQ};    // Include  divisors in the reductions of our known points

        if i in [1..3] then          // Reductions of generators for our subgroup G
           divsp:=divsp cat [DivQ];
        end if;
        if i eq 4 then
           bpp:=DivQ;                // Reduction of our base point
        end if;
    end for;  // End of loop for i = 1 to 7

////////////////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////////////////

    pls1p:=Places(Xp,1);   // The degree 1 places on Xp
    pls2p:=Places(Xp,2);   //  The degree 2 places on Xp
    //Degree 2 divisors on Xp
    degr2:={1*pl1 + 1*pl2 : pl1 in pls1p, pl2 in pls1p} join {1*pl : pl in pls2p};
    C,phi,psi:=ClassGroup(Xp);
    Z:=FreeAbelianGroup(1);
    degr:=hom<C->Z | [ Degree(phi(a))*Z.1 : a in OrderedGenerators(C)]>;
    JFp:=Kernel(degr);     // This is isomorphic to J_X(\F_p)

    JFpmodM,pi:=quo<JFp | M*JFp>;

    imGhat:=sub<JFpmodM | [pi(JFp!psi(divp-bpp)) : divp in divsp]>; // Image of G in JFpmodM
    poshat:={DD : DD in degr2 |pi((JFp!(psi(DD-bpp)))) in imGhat};  // Set S_{p,M}
    posP:={DD : DD in poshat | not DD in redpL};   // Remove reductions of all known points,
    for i in [1..7] do  // then add back in those that don't pass the Chabuaty test
        if Rks[i] eq 0 then posP := posP join {redpL[i]}; end if;
    end for;
    // posP is now T_{p,M}
    jposP:=Setseq({pi(JFp!(psi(DD-bpp))) : DD in posP});  // The set iota_{p,M}(T_{p,M}).

    h:=hom<A -> JFpmodM | [pi(JFp!psi(divp-bpp)) : divp in divsp]>; // The map phi_{p,M}.
    Bp:=Kernel(h);
    Bp,iAp:=sub<A|Bp>;
    Wp:={x@@h : x in jposP};

    Ws:=Ws cat [* Wp *];
    Bs:=Bs cat [* Bp *];
    print "Calculations completed for p =", p;
end for;

////////////////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////////////////
```

```
////////////////////////////////////////////////////////////////////////////////////////////

// We now intersect the coset lists W_{p,M}

B,iA:=sub<A|A>;
W:={0*A.1};

for i in [1..#pinsieve] do
    if Ws[1] eq {} then print true; end if;
    Bs[i],iAp:=sub<A | Bs[i]>;
    Bnew,iBp:=sub<Bs[i] | B meet Bs[i]>; // Now intersect Bp+Wp and B+W.
    iAnew:=iBp*iAp;
    A0,pi0:=quo<A | iAnew(Bnew)>;
    Ap,pi0p:=quo<A0 | pi0(iAp(Bs[i]))>;
    A1,pi01:=quo<A0 | pi0(iA(B))>;
    pi1:=pi0*pi01;
    pip:=pi0*pi0p;
    W:={x@@pi0 : x in {(pi1(y))@@pi01 +k : y in W, k in Kernel(pi01)} | pi0p(x) in pip(Ws[i])};

    B:=Bnew;
    iA:=iAnew;
    if W eq {} then print "true at i =", i; end if;
end for;
Wsieved:=W; // Output of the final sieved cosets
Bsieved:=B; // Wsieved are cosets in Z^3 of Bsieved
if Wsieved eq {} then print true; end if; // This means we have found all the quadratic points!
```