PUBLICATIONS MATHÉMATIQUES DE BESANÇON

Algèbre et Théorie des nombres

Elvira Lupoian

Computing the Cuspidal Subgroup of the Modular Jacobian $J_H(p)$

2025, p. 97-113.

https://doi.org/10.5802/pmb.63

PRESSE UNIVERSITAIRE DE FRANCHE-COMTÉ

Les Publications mathématiques de Besançon *sont membres du Centre Mersenne pour l'édition scientifique ouverte*
http://www.centre-mersenne.org/
e-ISSN : 2592-6616

Publications mathématiques de Besançon – 2025, 97-113

COMPUTING THE CUSPIDAL SUBGROUP OF THE MODULAR JACOBIAN $J_H(p)$

by

Elvira Lupoian

Abstract. — For a fixed prime p congruent to 1 modulo 4 we define the modular curve $X_H(p)$ associated to the subgroup of non-zero squares modulo p. In this paper we compute the cuspidal group for all such curves of genus g, $2 \leq g \leq 10$ and compare this with the torsion group of the Jacobian $J_H(\mathbb{Q}(\sqrt{p}))_{\text{tors}}$.

Résumé. — Soit p un nombre premier, égal à 1 mod 4, et $X_H(p)$ la courbe modulaire correspondant au groupe des carrés mod p. Dans cet article, nous calculons le groupe cuspidal de $X_H(p)$ et le comparons au groupe de torsion de la Jacobienne $J_H(p)(\mathbb{Q}(\sqrt{p})_{\text{tors}}$.

1. Introduction

For any positive integer N let $X_0(N)$ be the canonical model of the modular curve attached to the congruence subgroup $\Gamma_0(N)$ and let $J_0(N)$ be its Jacobian. The famous Mordell–Weil theorem tells us that $J_0(N)(\mathbb{Q})$ is a finitely generated group, that is,

$$J_0(N)(\mathbb{Q}) \simeq J_0(N)(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$$

for some integer $r \geq 0$ called the *rank*, and a finite group $J_0(N)(\mathbb{Q})_{\text{tors}}$, known as the rational *torsion subgroup* of $J_0(N)$. The rank of $J_0(N)$ over $\mathbb{Q}$ can be analysed using the decomposition of $J_0(N)$ as a product of abelian varieties of GL_2-type; for details see [17]. Due to the additional structure of the modular curve, many things can also be said about the torsion subgroup $J_0(N)(\mathbb{Q})_{\text{tors}}$. For prime level $N \geq 5$, this group is completely understood due to the work of Mazur [9].

***Theorem* (Mazur).** — *For a prime $N \geq 5$, $J_0(N)(\mathbb{Q})_{\text{tors}}$ is a cyclic subgroup of order the numerator of $\frac{N-1}{12}$, and it is generated by the linear equivalence class of the difference of the two cuspidal points of $X_0(N)$.*

2020 ***Mathematics Subject Classification.*** — 11Y99, 11G10.
Key words and phrases. — Modular Jacobians, Cuspidal Subgroup.
Acknowledgements. — During the completion of this work the author was supported by the EPSRC studentship EP/V520226/1.

There is a natural generalisation of this question for non-prime level. Let N be a positive integer and write C_N for the subgroup of $J_0(N)$ generated by linear equivalences of differences of cusps of $X_0(N)$, which we call the *cuspidal group* of $J_0(N)$. We denote by $C_N(\mathbb{Q})$ the elements of C_N which are invariant under the action of the absolute Galois group $G_{\overline{\mathbb{Q}}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. The theorems of Manin [7] and Drinfeld [2] show that the difference of any two cusps is torsion and hence

$$C_N(\mathbb{Q}) \subseteq J_0(N)(\mathbb{Q})_{\mathrm{tors}}.$$

Conjecture 1.1 **(Generalised Ogg Conjecture).** — *For any positive integer N*

$$C_N(\mathbb{Q}) = J_0(N)(\mathbb{Q})_{\mathrm{tors}}.$$

There is plenty of evidence supporting this conjecture; some of which is computational, including for $N \in \{11, 14, , 15, 17, 19, 20, 21, 24, 27, 32, 36, 49\}$ by Ligozat [5], for $N = 125$ by Poulakis [12] and for $N \in \{34, 38, 44, 45, 51, 52, 54, 56, 64, 82\}$ by Ozman and Siksek [11].
There are also a number of theoretical result supporting this conjecture. For instance, Ohta [8] proved that for square-free N and any prime $p \nmid 6N$, the p-primary parts of $J_0(N)(\mathbb{Q})_{\mathrm{tors}}$ and $C_N(\mathbb{Q})$ coincide. This result was later recovered by Ribet and Wake [14] using a different method. Many other similar results have been proved, see for instance [6] when N is a prime power and [21] when N is an arbitrary positive integer.
Naturally we can ask the same question for curves corresponding to other subgroups of $\mathrm{SL}_2(\mathbb{Z})$. For any modular curve corresponding to a congruence subgroup, the equivalence class of the difference of cusps has finite order on the Jacobian (due to the theorems of Manin and Drinfeld), and hence the cuspidal group is a subgroup of the K-rational torsion points of the Jacobian, where K is the field of definition of the cusps. We ask whether this inclusion is in fact an equality. A first step usually involves understanding the size and structure of the cuspidal group; a problem that has been studied by many authors. For instance,the size of the cuspidal group of $X_0(N)$ and $X_1(N)$ has been studied in many cases, see [19], [20] and [22] for a few examples. The size of the subgroup of the cuspidal group generated by equivalence classes of divisors fixed by the Galois action for some modular curves of prime level lying between $X_0(N)$ and $X_1(N)$ has been studied by Chen [1]. The structure of the rational cuspidal group of $X_0(N)$ was studied by Yoo [21]. These questions are often difficult to study as they involve computing the group (or some specific subgroup) of the modular units of the modular curve. An overview of the general classical method used to study cuspidal groups is given by Gekeler [3].
In this paper we study the cuspidal group and its relations to the larger torsion subgroup in which it lies in the case of some intermediate modular curves. Let p be an odd prime and H a subgroup of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$. Let $\Gamma_H(p)$ be the congruence subgroup associated to H, $X_H(p)$ the associated modular curve and $J_H(p)$ the Jacobian variety of the curve, see Section 2 for precise definitions. Let $C_H(p)$ be the subgroup of $J_H(p)$ generated by linear equivalence classes of differences of cusps; we call this the *cuspidal group* as before. In this paper, we take H to be subgroup of squares modulo p, where p is additionally congruent to 1 modulo 4, and we explicitly investigate the above question. Note that for primes $p \equiv 3 \mod 4$, the two curves $X_H(p)$ and $X_0(p)$ coincide, and hence the above inclusion is an equality by the Mazur's theorem. The main result proved in Section 4 is the following.

Theorem. — *Let $p \geq 5$ be a prime such that the genus g of $X_H(p)$ satisfies $1 \leq g \leq 10$. Then*

$$C_H(p)(\mathbb{Q}) = J_H(p)(\mathbb{Q})_{\text{tors}}.$$

Furthermore, if additionally $p \equiv 1 \mod 4$, that is $p \in \{29, 37, 41, 53, 61, 73\}$, then

$$C_H(p) = J_H(p)(\mathbb{Q}(\sqrt{p}))_{\text{tors}} \simeq (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}) \quad C_H(p)(\mathbb{Q}) = J_H(p)(\mathbb{Q})_{\text{tors}} \cong (\mathbb{Z}/m\mathbb{Z})$$

where n is positive integers depending on the level p,

p	n	m
29	*3*	*21*
37	*5*	*15*
41	*8*	*40*
53	*7*	*91*
61	*11*	*55*
73	*22*	*66*

and m is the lowest common multiple of n and the numerator of $\frac{p-1}{12}$.

The `MAGMA` code used for our computations can be found in the `GitHub` repository:

`https://github.com/ElviraLupoian/XHSquares`

The main motivation for studying the modular curves $X_H(p)$ is their moduli interpretation. As with the classical modular curves, non-cuspidal points of the $X_H(p)$ parameterise elliptic curves with certain p-torsion information. In particular, non-cuspidal points of $X_H(p)$ represent isomorphism classes (depending on H) of elliptic curves E with a p-level structure. Moreover for such a point, if $j(E) \neq 0, 1728$, the image of the mod p Galois representation attached to E is of the form

$$\bar{\rho}_{E,p} \sim \left(\begin{smallmatrix} *\in H & * \\ 0 & * \end{smallmatrix}\right)$$

up to conjugation. For a summary of this see [16].

Acknowledgments. — The author sincerely thanks Samir Siksek and Damiano Testa for many helpful conversations, and the anonymous referee for their suggestions and corrections. This work was completed whilst the author was a student at the University of Warwick and was supported by EPSRC studentship EP/V520226/1.

2. Preliminaries

In this section we give an overview of some basic facts and constructions related to modular curves. For a comprehensive overview we refer the reader to [15, Chapter 1] or [18, Chapter 1]. Fix a congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$. This group acts on the upper half plane $\mathbb{H} = \{z \in \mathbb{C} \,|\, \mathrm{Im}(z) > 0\}$ via fractional linear transformations

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot \tau = \frac{a\tau + b}{c\tau + d} \quad \text{for any } \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma, \tau \in \mathbb{H}$$

and the resulting quotient $Y(\Gamma) = \Gamma/\mathbb{H}$ is a complex Riemann surface, which can be compactified by adding finitely many points. We denote the compact surface by $X(\Gamma)$ and refer to the points of $X(\Gamma) \setminus Y(\Gamma)$ as the cusps of $X(\Gamma)$. Note that $X(\Gamma)$ is a compact Riemann surface, and hence an algebraic curve, and the cusps are in fact orbits of $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$ under the natural extension of the action of Γ to this set.

Let N be a positive integer. We recall the definitions of some standard congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$;

$$\Gamma(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : a, d \equiv 1 \bmod N \text{ and } b, c \equiv 0 \bmod N\},$$
$$\Gamma_1(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : a, d \equiv 1 \bmod N \text{ and } c \equiv 0 \bmod N\},$$
$$\Gamma_0(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \bmod N\}.$$

The associated modular curves $X(\Gamma(N))$, $X(\Gamma_1(N))$ and $X(\Gamma_0(N))$ are denoted by $X(N)$, $X_1(N)$ and $X_0(N)$ respectively. It can be shown that $X_1(N)$ and $X_0(N)$ have canonical models over $\mathbb{Q}$, see [15].
Let H be any subgroup of the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^*$. Corresponding to H, one can define the following congruence subgroup

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

We write $X_H(N)$ for the modular curve associated to $\Gamma_H(N)$. The $X_H(N)$ has a model over a subfield of $\mathbb{Q}(\zeta_N)$ depending on H.

Remark 2.1. — As $-I$ and I act the same on $\mathbb{H}$, $X_{\langle \pm 1, H\rangle}(N) = X_H(N)$ and thus we assume without loss of generality that $-1 \in H$.

The classical curves $X_1(N)$ and $X_0(N)$ can be recovered by taking $H = \{\pm 1\}$ and $H = (\mathbb{Z}/N\mathbb{Z})^*$ respectively. The above definitions show that for any N and H, we have the following inclusions:

$$\Gamma(N) \subseteq \pm\Gamma_1(N) \subseteq \Gamma_H(N) \subseteq \Gamma_0(N)$$

and these inclusions induce natural Galois coverings of curves:

$$X(N) \longrightarrow X_1(N) \longrightarrow X_H(N) \longrightarrow X_0(N)$$

where the above maps are simply quotient maps. We use the above to compute the genus of $X_H(N)$.
For any divisor d of N, let π_d be the projection map

$$(\mathbb{Z}/N\mathbb{Z})^* \longrightarrow (\mathbb{Z}/\operatorname{lcm}(d, N/d)\mathbb{Z})^*.$$

The following theorem is proved in [13].

Theorem. — *The genus of $X_H(N)$ is*

$$g_H(N) = 1 + \frac{\mu(N,H)}{12} - \frac{\nu_2(N,H)}{4} - \frac{\nu_3(N,H)}{3} - \frac{\nu_\infty(N,H)}{2}$$

where

$$\mu(N,H) = N\prod_{p|N}(1+1/p)\varphi(N)/|H|;$$
$$\nu_2(N,H) = |\{b \bmod N \in H \mid b^2+1 \equiv 0 \bmod N\}|\varphi(N)/|H|;$$
$$\nu_3(N,H) = |\{b \bmod N \in H \mid b^2-b+1 \equiv 0 \bmod N\}|\varphi(N)/|H|;$$
$$\nu_\infty(N,H) = \sum_{d|N}\frac{\varphi(d)\varphi(N/d)}{|\pi_d(H)|};$$

and φ denotes the usual Euler totient function.

From now on, we assume $N = p$ is prime, $p \geq 5$ and H is the subgroup of non-zero squares modulo p. We additionally assume that p is congruent to 1 modulo 4, in order to ensure that $-1 \in H$. Note that such curves have models over $\mathbb{Q}$.

Proposition 2.2. — *With p and H as above, the genus $g_H(p)$ of $X_H(p)$ is:*

$$g_H(p) = \begin{cases} \frac{p-5}{6} & \text{if } p \equiv 5 \bmod 24 \\ \frac{p-1}{6} - 3 & \text{if } p \equiv 1 \bmod 24 \\ \frac{p-17}{6} + 1 & \text{if } p \equiv 17 \bmod 24 \\ \frac{p-13}{6} & \text{if } p \equiv 13 \bmod 24 \end{cases}$$

Proof. — Applying the theorem above in our case, it is an elementary exercise to prove

$$\nu_2(p, H) = \begin{cases} 4 & \text{if } p \equiv 1 \bmod 8; \\ 0 & \text{otherwise;} \end{cases}$$

$$\nu_3(p, H) = \begin{cases} 4 & \text{if } p \equiv 1 \bmod 12; \\ 2 & \text{if } p \equiv 7 \bmod 12; \\ 0 & \text{otherwise;} \end{cases}$$

$$\nu_\infty(p, H) = \begin{cases} 4 & \text{if } p \equiv 1 \bmod 4; \\ 2 & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

□

The cusps of all modular curves considered can be described abstractly. We only consider the case $N = p$ prime and drop the standing assumption that p is congruent to 1 modulo 4 for our initial description. For arbitrary level N, see Ogg's classical description of cusps [10].
A cusp of $X(p)$ can be represented by a vector $\pm \left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$ with $x, y \in \mathbb{Z}/p\mathbb{Z}$ and $\gcd(x, y, p) = 1$. The cusps are rational over $\mathbb{Q}(\zeta_p)$, with the Galois group $(\mathbb{Z}/p\mathbb{Z})^*$ operating as $\left(\begin{smallmatrix} 1 & 0 \\ 0 & \sigma \end{smallmatrix}\right)$, where $\sigma \in (\mathbb{Z}/p\mathbb{Z})^*$ represents the automorphism $\zeta_p \mapsto \zeta_p^\sigma$, hence

$$\sigma \left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \sigma \end{smallmatrix}\right) \left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) = \left(\begin{smallmatrix} x \\ \sigma y \end{smallmatrix}\right).$$

The cusps of $X_1(p)$ are orbit classes under the action of $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, or equivalently, they are equivalence classes with respect to the relation

$$\pm \left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) \sim \pm \left(\begin{smallmatrix} x+ry \\ y \end{smallmatrix}\right) \quad \text{for } r \in \mathbb{Z}.$$

For each class, we may take a normalized representative $\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$ with

- $0 \leq y < p$,
- $0 \leq x < \gcd(p, y)$.

This splits the cusps of $X_1(p)$ into two natural groups, which can be parameterised using any generator α of $(\mathbb{Z}/p\mathbb{Z})^*/\{\pm 1\}$:

(C1) Cusps of the form $\left(\begin{smallmatrix} \alpha^k \\ 0 \end{smallmatrix}\right)$ with $k = 0, \ldots, \frac{p-1}{2} - 1$;

(C2) Cusps of the form $\left(\begin{smallmatrix} 0 \\ \alpha^k \end{smallmatrix}\right)$ with $k = 0, \ldots, \frac{p-1}{2} - 1$.

The cusps of type (C1) are all rational, and the cusps of type (C2) form a single orbit under the action of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)^+/\mathbb{Q})$, where $\mathbb{Q}(\zeta_p)^+$ is the maximal real subfield of the cyclotomic field $\mathbb{Q}(\zeta_p)$.
The cusps of $X_0(p)$ are orbits of $G_0(p) = \Gamma_0(p)/\Gamma_1(p)$. We find that all cusps of type (C1) form a single orbit under this action and hence they map to a single cusp $c_\infty \in X_0(p)$, represented by $\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$. Similarly all cusps of type (C2) are identified by the above action and hence all map to a single cusp $c_0 \in X_0(p)$, represented by $\left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)$. Note that both cusps are defined over $\mathbb{Q}$.
Suppose that p is congruent to 1 modulo 4, and H is the subgroup of non-zero squares modulo p as before. The cusps of $X_H(p)$ are orbits of $G_H(p) = \Gamma_H(p)/\Gamma_1(p)$ and we find that cusps of type (C1) form two orbits under this action,

$$\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right), \left(\begin{smallmatrix}\alpha^2\\0\end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix}\alpha^{s-2}\\0\end{smallmatrix}\right) \quad \text{and} \quad \left(\begin{smallmatrix}\alpha\\0\end{smallmatrix}\right), \left(\begin{smallmatrix}\alpha^3\\0\end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix}\alpha^{s-1}\\0\end{smallmatrix}\right);$$

and as do the cusps of type (C2):

$$\left(\begin{smallmatrix}0\\1\end{smallmatrix}\right), \left(\begin{smallmatrix}0\\\alpha^2\end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix}0\\\alpha^{s-2}\end{smallmatrix}\right) \quad \text{and} \quad \left(\begin{smallmatrix}0\\\alpha\end{smallmatrix}\right), \left(\begin{smallmatrix}0\\\alpha^3\end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix}0\\\alpha^{s-1}\end{smallmatrix}\right).$$

Thus $X_H(p)$ has four cusps c_1, c_2, c_3, c_4, represented by $\left(\begin{smallmatrix}0\\1\end{smallmatrix}\right), \left(\begin{smallmatrix}0\\\alpha\end{smallmatrix}\right), \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}\alpha\\0\end{smallmatrix}\right)$, respectively. The cusps c_1 and c_2 are defined over $\mathbb{Q}$, whilst c_3 and c_4 are defined over $\mathbb{Q}(\sqrt{p})$, the unique degree 2 subfield of $\mathbb{Q}(\zeta_p)$, and they are Galois conjugate.

3. Computational Overview

Fix a prime p congruent to 1 modulo 4. Let H be the subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$ consisting of squares and consider the corresponding modular curve $X_H(p)$. Firstly, using the genus formulae given in the previous section we find that there are precisely 6 values of p as above for which the modular curve $X_H(p)$ has genus $g_H(p)$, with $2 \leq g_H(p) \leq 10$:

- $g_H(p) = 4 : p = 29, 37$;
- $g_H(p) = 5 : p = 41$;
- $g_H(p) = 8 : p = 53, 61$;
- $g_H(p) = 9 : p = 73$.

We begin our computations by finding canonical models for the curves $X_0(p)$ and $X_H(p)$ for p as above. This was done using Galbraith's method which is summarised in the following subsection. A concise summary of this method can be found in [16].

3.1. Models for Modular Curves: Galbraith's Method. — Let X be a modular curve of genus $g \geq 2$, corresponding to a congruence subgroup Γ. The space of holomorphic differentials $\Omega^1(X)$ and the space of weight 2 cups forms $S_2(\Gamma)$ on Γ are isomorphic as complex vector spaces. More explicitly, if $\{f_1(\tau), \ldots, f_g(\tau)\}$ is a basis for $S_2(\Gamma)$, then $\{f_1(\tau)\mathrm{d}\tau, \ldots, f_g(\tau)\mathrm{d}\tau\}$ is a basis for $\Omega^1(X)$. Thus, the canonical map is simply:

$$\phi : X \longrightarrow \mathbb{P}^{g-1}, \qquad \phi(\tau) = (f_1(\tau) : \ldots : f_g(\tau)).$$

The canonical map is an embedding if and only if the curve is not hyperelliptic. If X is hyperelliptic, the image of the canonical map is isomorphic to $\mathbb{P}^{g-1}$ and it is described by

$1/2(g-1)(g-2)$ quadrics. Thus we can determine whether the curve is hyperelliptic or not by computing the image of the canonical map.
If X is non-hyperelliptic, the image of the canonical map is a curve of degree $2g-2$ and it will be described by a set of projective equations of the form $\Phi(f_1,\dots,f_g)=0$. In the case that it is a complete intersection, the equations have degrees whose product is $2g-2$. We interpret each $\Phi(f_1,\dots,f_g)$ as a modular form of weight $2\cdot\deg(\Phi)$ which vanishes on the extended upper half plane. This gives a strategy for finding a model of the curve.
To find a defining set of equations for a non-hyperelliptic modular curve, take a basis $f_1,\dots,f_g$ for $S_2(\Gamma)$. For any degree d homogeneous polynomial $F\in\mathbb{Q}[x_1,\dots,x_g]$, $F(f_1,\dots,f_g)$ is a cusp form of weight $2d$ and level N. Let $I=[\mathrm{SL}_2(\mathbb{Z}):\Gamma]=N\prod_{p|N}(1+1/p)$.

***Theorem* (Sturm's theorem).** — *With notation as above, $F(f_1,\dots,f_g)=0$ if and only if, the q expansion satisfies $F(f_1,\dots,f_g)=O(q^r)$, where $r=\lfloor dI/6\rfloor+1$.*

Using the above result, we have reduced our problem to an elementary linear algebra computation, namely that of determining the vector space of all homogeneous F of degree d such that $F(f_1,\dots,f_g)=0$. This can be repeated for all divisors d of $2g-2$, resulting in a system of equations that cuts out a model for X in $\mathbb{P}^{g-1}$.
Suppose X is a hyperelliptic modular curve of genus $g\geq 2$. As before, there is an isomorphism $S_2(\Gamma)\cong\Omega^1(X)$. Let $f_1,\dots,f_g$ be a basis for $S_2(\Gamma)$, and since X is modular, we can choose a basis such that f_i has q-expansion of the form $q^i+\cdots$. As X is hyperelliptic, it has an affine model of the form

$$X: y^2=f(x)$$

with $f\in\mathbb{Q}[x]$, of degree $2g+1$ or $2g+2$. Then $\Omega^1(X)$ has a basis $\mathrm{d}x/y, x\mathrm{d}x/y,\dots,x^{g-1}\mathrm{d}x/y$. Note that this basis is not necessarily the same as the basis $f_1\mathrm{d}q/q,\dots,f_g\mathrm{d}q/q$. Changing coordinates if necessary, we can assume that the infinity cusp c_∞ of X(the class of $\infty\in\mathbb{H}^*$ in the analytic interpretation) is one of the points at infinity of the hyperelliptic curve in our affine model. Then q is a uniformiser at c_∞. To differentiate between the cases when f has degree $2g+2$ or $2g+1$ we use the following result.

Proposition 3.1. — *Suppose X is a hyperelliptic curve of genus $g\geq 2$, and has an affine model*

$$X: y^2=a_{2g+2}x^{2g+2}+\cdots+a_0 \quad \textit{with } a_{2g+2}\neq 0$$

and let ∞_+ be one of the points at infinity. Then

$$\mathrm{ord}_{\infty_+}(\mathrm{d}x/y)=g-1,\quad \mathrm{ord}_{\infty_+}(x\mathrm{d}x/y)=g-2,\quad \dots,\quad \mathrm{ord}_{\infty_+}(x^{g-1}\mathrm{d}x/y)=0.$$

If X has affine model

$$X: y^2=a_{2g+1}x^{2g+1}+\cdots+a_0 \quad \textit{with } a_{2g+1}\neq 0$$

and ∞ is the unique point at infinity on the above model then:

$$\mathrm{ord}_{\infty}(\mathrm{d}x/y)=2(g-1),\quad \mathrm{ord}_{\infty}(x\mathrm{d}x/y)=2(g-2),\quad \dots,\quad \mathrm{ord}_{\infty}(x^{g-1}\mathrm{d}x/y)=0.$$

Using the q-expansions of $f_1,\dots,f_g$, we determine if any linear combination of $f_1\mathrm{d}q/q,\dots,f_g\mathrm{d}q/q$ has order $2(g-1)$ at c_∞. If such a linear combination exists, then we have a degree $2g+1$ model; otherwise the polynomial in our affine model has degree $2g+2$.

From the above valuations and the q-expansions of $f_1, \ldots, f_g$, we have

$$\begin{aligned} \mathrm{d}x/y &= \alpha_g f_g(q)\mathrm{d}q/q \\ x\mathrm{d}x/y &= \beta_{g-1} f_{g-1}(q)\mathrm{d}q/q + \beta_g f_g(q)\mathrm{d}q/q \end{aligned}$$

for some constants $\alpha_g \neq 0$, $\beta_{g-1} \neq 0$ and β_g. The change of coordinates

$$x \longmapsto rx, \quad y \longmapsto sy$$

fixes the points at infinity, and scales the differentials as follows,

$$\begin{aligned} \mathrm{d}x/y &\longmapsto (r/s)\mathrm{d}x/y \\ x\mathrm{d}x/y &\longmapsto (r^2/s)x\mathrm{d}x/y \end{aligned}$$

and thus we may take $\alpha_g = \beta_{g-1} = 1$. The change of coordinates

$$x \longmapsto x + t, \quad y \longmapsto y$$

also fixes the points at infinity, and transforms the differentials as follows

$$\begin{aligned} \mathrm{d}x/y &\longmapsto \mathrm{d}x/y \\ x\mathrm{d}x/y &\longmapsto x\mathrm{d}x/y + t\mathrm{d}x/y \end{aligned}$$

and hence we may take $\beta_g = 0$. Thus we can assume

$$\begin{aligned} \mathrm{d}x/y &= f_g(q)\mathrm{d}q/q \\ x\mathrm{d}x/y &= f_{g-1}(q)\mathrm{d}q/q \end{aligned}$$

and hence

$$x = f_{g-1}(q)/f_g(q) \quad \text{and} \quad y = (\mathrm{d}x/\mathrm{d}q)(q/f_g(q)).$$

As in the previous case, we have reduced the problem to an elementary linear algebra exercise, as we now use these expressions to search for a polynomial $f \in \mathbb{Q}[x]$ of degree $2g+1$ or $2g+2$, such that

$$y^2 - f(x) = 0$$

using the q-expansions of $f_g(q)$ and $f_{g-1}(q)$ and Sturm's theorem.

3.2. The Quotient Map $X_H(p) \to X_0(p)$. — Suppose both curves $X_H(p)$ and $X_0(p)$ are not hyperelliptic. This is the case for $p = 53, 61$ and 73. Let $f_1, \ldots, f_g$ be a basis of $S_2(\Gamma_0(p))$. This can be extended to a basis $f_1, \ldots, f_g, f_{g+1} \ldots, f_{g_H}$ of $S_2(\Gamma_H(p))$. We compute models for the two curves with respect to the above bases and with coordinates $(x_1 : \ldots : x_{g_H}) = (f_1 : \ldots : f_{g_H})$. Then the degree 2 quotient map is simply the projection:

$$\begin{aligned} &\varphi : X_H(p) \longrightarrow X_0(p) \\ &\varphi(x_1, \ldots, x_{g_H}) = (x_1, \ldots, x_g). \end{aligned}$$

In the cases $p = 29, 37$ and 41, the curve $X_0(p)$ is hyperelliptic, whilst $X_H(p)$ is not. Take a basis $f_1, \ldots, f_g$ for $S_2(\Gamma_0(N))$, such that f_i has q-expansion of the form $q^i + \cdots$. As described in the previous subsection, we find an affine model of $X_0(p)$

$$X_0(p) : y^2 = f(x)$$

where $f \in \mathbb{Q}[x]$ has degree $2g+1$ or $2g+2$, and

$$x = f_{g-1}(q)/f_g(q) \quad \text{and} \quad y = (\mathrm{d}x/\mathrm{d}q)(q/f_g(q)).$$

The basis $f_1, \ldots, f_g$ can be extended to a basis of $S_2(\Gamma_H(p))$, $f_1, \ldots, f_{g_H}$, and we compute the canonical model of the non-hyperelliptic curve $X_H(p)$ with respect to this basis. The model of $X_H(p)$ will have coordinates

$$(x_1 : \ldots : x_{g-1} : x_g : \ldots : x_{g_H}) = (f_1 : \ldots : f_{g-1} : f_g : \ldots : f_{g_H})$$

and the degree 2 map $\varphi : X_H(p) \to X_0(p)$ is simply

$$(x_1 : \ldots : x_{g-1} : x_g : \ldots : x_{g_H}) \longmapsto (x(x_{g-1}, x_g), y(x_{g-1}, x_g))$$

where x and y are given by

$$x(x_{g-1}, x_g) = x_{g-1}/x_g \quad \text{and} \quad y = \sqrt{f(x(x_{g-1}, x_g))}.$$

3.3. The Cuspidal Group $C_H(p)$. — The cusps of $X_H(p)$, $c_1, \ldots, c_4$ are the inverse images of the cusps of $X_0(p)$ under the map φ. Then $C_H(p)$ is the group generated by these cusps

$$C_H(p) = \langle [c_2 - c_1], [c_3 - c_1], [c_4 - c_1] \rangle.$$

This is a subgroup of $J_H(p)(\mathbb{Q}(\sqrt{p}))_{\text{tors}}$ by the theorems of Manin [7] and Drinfeld [2]. To find a presentation of this group, and any relations amongst the cuspidal divisors, we reduce modulo a prime of good reduction in $\mathbb{Q}(\sqrt{p})$ and use the following result.

Lemma 3.2. — *Let $S = J_H(p)(\mathbb{Q}(\sqrt{p}))$, and let $\mathfrak{q}$ be any prime in $\mathbb{Q}(\sqrt{p})$, not lying above p or 2. Then reduction modulo $\mathfrak{q}$ induces an injection*

$$S \longrightarrow J_H(p)(\mathbb{F}_{\mathfrak{q}}).$$

Proof. — See [4]. □

By our choice of model (and notation), c_3 and c_4 are defined over $\mathbb{Q}(\sqrt{p})$ and Galois conjugate, and c_1, c_2 are rational. Thus the Galois action on $C_H(p)$ is clear and by taking Galois invariants we obtain the rational cuspidal subgroup $C_H(p)(\mathbb{Q})$.

3.4. Torsion Subgroup of $J_H(p)$. — For any prime ideal $\mathfrak{q}$ of $\mathcal{O}$, the ring of integers of $\mathbb{Q}(\sqrt{p})$, with norm is co-prime to p, reduction modulo $\mathfrak{q}$ induces an injection

$$J_H(p)(\mathbb{Q}(\sqrt{p}))_{\text{tors}} \longrightarrow J_H(p)(\mathbb{F}_{\mathfrak{q}}).$$

Reducing modulo multiple prime ideals, gives an upper bound on the size of $J_H(p)(\mathbb{Q}(\sqrt{p}))_{\text{tors}}$, and in our computations we found sufficiently many primes such that this bound matched to size of $C_H(p)$, and hence we were able to conclude $J_H(p)(\mathbb{Q}(\sqrt{p}))_{\text{tors}} = C_H(p)$.

4. Proof of the Main Theorem

The `MAGMA` code used to carry out the computations presented in this section can be found in the following online repository:

`https://github.com/ElviraLupoian/XHSquares`

4.1. Curves of Genus 4. — There are 2 primes for which $X_H(p)$ has genus 4, namely 29 and 37. Both curves $X_H(p)$ are not hyperelliptic, so their canonical model is the intersection of a quadric and a cubic in $\mathbb{P}^3$, and in both cases $X_0(p)$ has genus 2.

$p = 29$. — A canonical model of $X_H(29)$ is given by the zero locus of

$$C = x_1^2x_3 - 3x_1x_2x_3 - x_1x_3^2 - x_2^3 + x_2^2x_3 + x_2x_3^2 + 5x_2x_3x_4 - x_2x_4^2 + 4x_3^3 - 5x_3^2x_4 - 3x_3x_4^2;$$
$$Q = x_1x_4 - x_2x_3 + x_2x_4 + x_3^2 - 3x_3x_4 - 2x_4^2.$$

The cusps of $X_H(29)$ are

$$c_1 = (1:0:0:0), c_2 = (2:0:0:1);$$
$$c_3 = (3\sqrt{29} + 18 : \sqrt{29} + 5 : 1/2\sqrt{29} + 5/2 : 1);$$
$$c_4 = (-3\sqrt{29} + 18 : -\sqrt{29} + 5 : -1/2\sqrt{29} + 5/2 : 1).$$

The cuspidal subgroup $C_H(29) = \langle [c_2 - c_1], [c_3 - c_1], [c_4 - c_1] \rangle$ is isomorphic to $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/21\mathbb{Z})$, and in fact, $[c_3 - c_1]$ and $[c_4 - c_1]$ are sufficient to generate the entire group. Taking Galois invariants, the resulting rational cuspidal subgroup is

$$C_H(29)(\mathbb{Q}) = \langle [c_3 + c_4 - 2c_1] \rangle \cong (\mathbb{Z}/21\mathbb{Z})$$

An upper bound for $|J_H(29)(\mathbb{Q}(\sqrt{29}))_{\text{tors}}|$ resulting from reduction modulo multiple primes is exactly 63 and thus we conclude

$$J_H(29)(\mathbb{Q}(\sqrt{29}))_{\text{tors}} = C_H(29).$$

$p = 37$. — A canonical model of $X_H(37)$ is given by the zero locus of

$$C = 2x_1^2x_4 - 5x_1x_4^2 - 2x_2^3 + 2x_2^2x_3 - 2x_2x_3^2 + 6x_2x_3x_4 - 6x_2x_4^2 - 3x_3^3 + 8x_3^2x_4 - 9x_3x_4^2 + 6x_4^3;$$
$$Q = x_1x_3 - x_2^2 - 2x_3x_4.$$

The cusps of $X_H(37)$ are

$$c_1 = (1:0:0:0), c_2 = (2:0:1:1);$$
$$c_3 = (\sqrt{37} + 5 : 6 : \sqrt{37} - 1 : 2);$$
$$c_4 = (-\sqrt{37} + 5 : 6 : -\sqrt{37} - 1 : 2).$$

The cuspidal subgroup $C_H(37) = \langle [c_2 - c_1], [c_3 - c_1], [c_4 - c_1] \rangle$ is isomorphic to $(\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/15\mathbb{Z})$, and it's also generated by $[c_3 - c_1]$ and $[c_4 - c_1]$ only. Taking Galois invariants gives

$$C_H(37)(\mathbb{Q}) = \langle [c_3 + c_4 - 2c_1] \rangle \cong (\mathbb{Z}/15\mathbb{Z}).$$

An upper bound for $|J_H(37)(\mathbb{Q}(\sqrt{37}))_{\text{tors}}|$ obtained from reducing modulo a number of primes is exactly 75, and hence:

$$J_H(37)(\mathbb{Q}(\sqrt{37}))_{\text{tors}} = C_H(37) \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}.$$

4.2. Curves of Genus 5. — There is a single prime congruent to 1 modulo 4 for which $X_H(p)$ has genus 5, namely 41. The curve $X_H(41)$ is not hyperelliptic, so its canonical model is the intersection of 3 quadrics in $\mathbb{P}^4$.
A canonical model of $X_H(41)$ is given by the zero locus of

$$Q_1 = x_1x_3 - x_2^2 + 2x_2x_4 + 2x_2x_5 - 2x_3^2 - x_3x_4 + x_3x_5 - 2x_4^2 - 2x_4x_5 - x_5^2;$$
$$Q_2 = x_1x_4 - x_2x_3 + x_2x_4 - x_3^2 + x_3x_4 + 2x_3x_5 - 2x_4^2 - 2x_4x_5;$$
$$Q_3 = x_1x_5 - x_2x_5 - x_3^2 + 2x_3x_4 + 2x_3x_5 - 2x_4^2 - x_4x_5 + x_5^2.$$

The cusps of $X_H(41)$ are

$$c_1 = (1:0:0:0:0), c_2 = (0:1:0:0:1);$$
$$c_3 = (18\sqrt{41}+114 : 6\sqrt{41}+54 : 6\sqrt{41}+42 : 3\sqrt{41}+21 : 12);$$
$$c_4 = (-18\sqrt{41}+114 : -6\sqrt{41}+54 : -6\sqrt{41}+42 : -3\sqrt{41}+21 : 12).$$

The cuspidal subgroup $C_H(41) = \langle [c_2 - c_1], [c_3 - c_1], [c_4 - c_1] \rangle$ is isomorphic to $(\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/40\mathbb{Z})$, and it's generated by $[c_3 - c_1]$ and $[c_4 - c_1]$ only. Taking Galois invariants, we find

$$C_H(41)(\mathbb{Q}) = \langle [c_3 + c_4 - 2c_1] \rangle \cong (\mathbb{Z}/40\mathbb{Z}).$$

An upper bound for $|J_H(41)(\mathbb{Q}(\sqrt{41}))_{\text{tors}}|$ obtained from reducing modulo multiple primes is 320, and so

$$C_H(41) = J_H(41)(\mathbb{Q}(\sqrt{41}))_{\text{tors}} \cong \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/40\mathbb{Z}.$$

4.3. Curves of Genus 8. — There are two primes congruent to 1 modulo 4 for which $X_H(p)$ has genus 8, namely 53 and 61. Both curves $X_H(p)$ are not hyperelliptic.

$p = 53$. — A canonical model of $X_H(53)$ is given by the zero locus of the following fifteen quadrics and one cubic.

$$\begin{aligned}
Q_1 &= 6x_1x_3 - 6x_2^2 + 15x_4x_6 + 5x_4x_7 - 23x_4x_8 - 15x_5^2 + 33x_5x_6 + 10x_5x_7 + 60x_5x_8 - 50x_6^2 \\
&\quad - 54x_6x_7 - 39x_6x_8 - 18x_7^2 + 37x_7x_8 + 15x_8^2; \\
Q_2 &= 6x_1x_4 - 6x_2x_3 - 6x_4^2 - 43x_4x_6 - 5x_4x_7 - 17x_4x_8 + 43x_5^2 - 13x_5x_6 - 10x_5x_7 \\
&\quad - 226x_5x_8 - 32x_6^2 + 68x_6x_7 + 205x_6x_8 + 32x_7^2 + 9x_7x_8 + 225x_8^2; \\
Q_3 &= 3x_1x_5 - 3x_3^2 - 16x_4x_6 - 28x_4x_8 + 16x_5^2 - x_5x_6 - 3x_5x_7 - 100x_5x_8 - 19x_6^2 + 23x_6x_7 \\
&\quad + 73x_6x_8 + 11x_7^2 + 13x_7x_8 + 144x_8^2; \\
Q_4 &= 3x_1x_6 - 3x_3x_4 + 3x_4^2 - 9x_4x_6 - 2x_4x_7 - 31x_4x_8 + 12x_5^2 - 6x_5x_6 + 2x_5x_7 - 66x_5x_8 \\
&\quad - 16x_6^2 + 3x_6x_7 + 48x_6x_8 + 6x_7^2 + 14x_7x_8 + 114x_8^2; \\
Q_5 &= 3x_1x_7 - 3x_4x_5 + 5x_4x_6 - 3x_4x_7 + 23x_4x_8 - 5x_5^2 - x_5x_6 + 38x_5x_8 + 14x_6^2 + 2x_6x_7 \\
&\quad - 23x_6x_8 - x_7^2 - 17x_7x_8 - 81x_8^2; \\
Q_6 &= 3x_1x_8 - 2x_4x_6 - x_4x_7 + 2x_4x_8 - x_5^2 + 4x_5x_6 + x_5x_7 + x_5x_8 - x_6^2 + x_6x_7 - 4x_6x_8 \\
&\quad + x_7^2 - 6x_7x_8 - 9x_8^2; \\
Q_7 &= 3x_2x_4 - 3x_3^2 - 3x_4x_5 - 5x_4x_6 - 3x_4x_7 + x_4x_8 + 5x_5^2 - 5x_5x_6 + 3x_5x_7 - 11x_5x_8 \\
&\quad + 10x_6^2 + 10x_6x_7 + 5x_6x_8 + 4x_7^2 - 10x_7x_8 + 3x_8^2; \\
Q_8 &= 3x_2x_5 - 3x_3x_4 - 11x_4x_6 + x_4x_7 - 3x_4x_8 + 14x_5^2 - 11x_5x_6 - 7x_5x_7 - 86x_5x_8 + 3x_6^2 \\
&\quad + 34x_6x_7 + 62x_6x_8 + 13x_7^2 - 11x_7x_8 + 75x_8^2; \\
Q_9 &= 3x_2x_6 - 3x_4^2 + 3x_4x_5 - 12x_4x_6 + 4x_4x_7 + 2x_4x_8 + 12x_5^2 - 6x_5x_6 - 10x_5x_7 - 75x_5x_8 \\
&\quad - 4x_6^2 + 30x_6x_7 + 57x_6x_8 + 9x_7^2 - 4x_7x_8 + 63x_8^2; \\
Q_{10} &= 3x_2x_7 + 3x_4x_6 - x_4x_7 + x_4x_8 - 6x_5^2 + 3x_5x_6 + x_5x_7 + 33x_5x_8 - 2x_6^2 - 15x_6x_7 \\
&\quad - 21x_6x_8 - 6x_7^2 + 4x_7x_8 - 27x_8^2;
\end{aligned}$$

$$\begin{aligned}
Q_{11} &= 3x_2x_8 + 2x_4x_6 + 2x_4x_8 - 2x_5^2 - x_5x_6 + 11x_5x_8 + 5x_6^2 - x_6x_7 - 11x_6x_8 - x_7^2 \\
&\quad - 2x_7x_8 - 18x_8^2; \\
Q_{12} &= 6x_3x_5 - 6x_4^2 + 5x_4x_6 + 13x_4x_7 + 43x_4x_8 - 5x_5^2 + 17x_5x_6 - 10x_5x_7 - 16x_5x_8 + 4x_6^2 \\
&\quad + 26x_6x_7 - 17x_6x_8 + 2x_7^2 - 51x_7x_8 - 57x_8^2; \\
Q_{13} &= 3x_3x_6 - 3x_4x_5 + 2x_4x_6 + x_4x_7 + 13x_4x_8 + x_5^2 + 2x_5x_6 + 2x_5x_7 - 4x_5x_8 + 4x_6^2 \\
&\quad + 5x_6x_7 - 11x_6x_8 + 2x_7^2 - 24x_7x_8 - 21x_8^2; \\
Q_{14} &= 3x_3x_7 - 2x_4x_6 - x_4x_7 - 10x_4x_8 + 2x_5^2 - 5x_5x_6 - 2x_5x_7 - 8x_5x_8 - 4x_6^2 - 5x_6x_7 \\
&\quad + 14x_6x_8 - 2x_7^2 + 15x_7x_8 + 30x_8^2; \\
Q_{15} &= 6x_3x_8 + 5x_4x_6 + x_4x_7 + x_4x_8 - 5x_5^2 + 5x_5x_6 + 2x_5x_7 + 20x_5x_8 - 2x_6^2 - 10x_6x_7 \\
&\quad - 23x_6x_8 - 4x_7^2 - 3x_7x_8 - 21x_8^2; \\
C &= 138x_1^2x_3 - 138x_1x_2^2 + 414x_4^3 - 1794x_4^2x_5 + 2346x_4x_5^2 + 636x_4x_7^2 - 7278x_4x_7x_8 \\
&\quad - 5148x_4x_8^2 - 2346x_5^3 + 2898x_5^2x_6 + 1978x_5^2x_7 + 2291x_5^2x_8 + 3036x_5x_6^2 \\
&\quad + 3643x_5x_6x_7 - 16010x_5x_6x_8 + 1548x_5x_7^2 - 12320x_5x_7x_8 + 31987x_5x_8^2 - 5152x_6^3 \\
&\quad - 9613x_6^2x_7 - 3888x_6^2x_8 - 1297x_6x_7^2 - 20654x_6x_7x_8 - 3220x_6x_8^2 + 1139x_7^3 \\
&\quad - 14602x_7^2x_8 + 46267x_7x_8^2 - 15816x_8^3.
\end{aligned}$$

The cusps of $X_H(53)$ are

$$\begin{aligned}
c_1 &= (1:0:0:0:0:0:0:0); \\
c_2 &= (1:2:1:1:2:1:-1:1); \\
c_3 &= (6\sqrt{53}+46 : 4\sqrt{53}+34 : 3\sqrt{53}+25 : 3\sqrt{53}+23 : \sqrt{53}+13 : 2 : \sqrt{53}+5 : 2); \\
c_4 &= (-6\sqrt{53}+46 : -4\sqrt{53}+34 : -3\sqrt{53}+25 : -3\sqrt{53}+23 : -\sqrt{53}+13 : 2 : -\sqrt{53}+5 : 2).
\end{aligned}$$

The cuspidal subgroup $C_H(53) = \langle [c_2 - c_1], [c_3 - c_1], [c_4 - c_1] \rangle$ is isomorphic to $(\mathbb{Z}/7\mathbb{Z}) \times (\mathbb{Z}/91\mathbb{Z})$, and as in the previous cases it is generated by $[c_3 - c_1]$ and $[c_4 - c_1]$ only. Taking Galois invariants we find:

$$C_H(53)(\mathbb{Q}) = \langle [c_3 + c_4 - 2c_1] \rangle \cong (\mathbb{Z}/91\mathbb{Z}).$$

Reducing modulo multiple primes, we find that 637 is an upper bound for $|J_H(53)(\mathbb{Q}(\sqrt{53}))_{\mathrm{tors}}$ and hence

$$C_H(53) = J_H(53)(\mathbb{Q}(\sqrt{53}))_{\mathrm{tors}} \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/91\mathbb{Z}.$$

$p = 61$. — A canonical model of $X_H(61)$ is given by the zero locus of the following fifteen quadrics and one cubic.

$$\begin{aligned}
Q_1 &= 4x_1x_3 - 4x_2^2 - 404x_4x_6 + 427x_4x_7 - 329x_4x_8 + 408x_5^2 - 459x_5x_6 + 117x_5x_7 \\
&\quad + 219x_5x_8 + 240x_6^2 - 237x_6x_7 - 539x_6x_8 + 60x_7^2 + 469x_7x_8 - 475x_8^2; \\
Q_2 &= 4x_1x_4 - 4x_2x_3 + 16x_4x_6 - 9x_4x_7 + 23x_4x_8 - 4x_5^2 + 9x_5x_6 - 15x_5x_7 - 5x_5x_8 \\
&\quad - 28x_6^2 + 39x_6x_7 - 15x_6x_8 - 8x_7^2 + 5x_7x_8 + x_8^2;
\end{aligned}$$

$$
\begin{aligned}
Q_3 &= 4x_1x_5 - 4x_3^2 - 316x_4x_6 + 351x_4x_7 - 249x_4x_8 + 324x_5^2 - 347x_5x_6 + 73x_5x_7 \\
&\quad + 199x_5x_8 + 168x_6^2 - 169x_6x_7 - 455x_6x_8 + 44x_7^2 + 393x_7x_8 - 379x_8^2; \\
Q_4 &= 2x_1x_6 - 2x_3x_4 + 16x_4x_6 - 11x_4x_7 + 17x_4x_8 - 8x_5^2 + 11x_5x_6 - 5x_5x_7 - 9x_5x_8 \\
&\quad - 14x_6^2 + 13x_6x_7 + 13x_6x_8 - 2x_7^2 - 9x_7x_8 + 15x_8^2; \\
Q_5 &= 4x_1x_7 - 4x_4^2 - 216x_4x_6 + 237x_4x_7 - 175x_4x_8 + 228x_5^2 - 241x_5x_6 + 59x_5x_7 \\
&\quad + 129x_5x_8 + 128x_6^2 - 139x_6x_7 - 293x_6x_8 + 36x_7^2 + 267x_7x_8 - 253x_8^2; \\
Q_6 &= 2x_1x_8 - 2x_4x_5 + 34x_4x_6 - 39x_4x_7 + 25x_4x_8 - 36x_5^2 + 39x_5x_6 - 7x_5x_7 - 23x_5x_8 \\
&\quad - 16x_6^2 + 15x_6x_7 + 53x_6x_8 - 4x_7^2 - 45x_7x_8 + 45x_8^2; \\
Q_7 &= 4x_2x_4 - 4x_3^2 - 232x_4x_6 + 249x_4x_7 - 183x_4x_8 + 232x_5^2 - 237x_5x_6 + 51x_5x_7 \\
&\quad + 149x_5x_8 + 128x_6^2 - 135x_6x_7 - 309x_6x_8 + 36x_7^2 + 271x_7x_8 - 261x_8^2; \\
Q_8 &= 4x_2x_5 - 4x_3x_4 + 180x_4x_6 - 189x_4x_7 + 147x_4x_8 - 180x_5^2 + 197x_5x_6 - 51x_5x_7 \\
&\quad - 105x_5x_8 - 104x_6^2 + 103x_6x_7 + 245x_6x_8 - 24x_7^2 - 211x_7x_8 + 213x_8^2; \\
Q_9 &= 2x_2x_6 - 2x_4^2 - 44x_4x_6 + 49x_4x_7 - 37x_4x_8 + 44x_5^2 - 41x_5x_6 + 11x_5x_7 + 33x_5x_8 \\
&\quad + 26x_6^2 - 33x_6x_7 - 55x_6x_8 + 8x_7^2 + 53x_7x_8 - 47x_8^2; \\
Q_{10} &= x_2x_7 - x_4x_5 + 16x_4x_6 - 17x_4x_7 + 13x_4x_8 - 16x_5^2 + 20x_5x_6 - 5x_5x_7 - 7x_5x_8 \\
&\quad - 9x_6^2 + 8x_6x_7 + 22x_6x_8 - 3x_7^2 - 18x_7x_8 + 20x_8^2; \\
Q_{11} &= 4x_2x_8 - 16x_4x_6 + 15x_4x_7 - 13x_4x_8 + 12x_5^2 - 19x_5x_6 + 5x_5x_7 + 3x_5x_8 + 8x_6^2 \\
&\quad - 5x_6x_7 - 27x_6x_8 + 17x_7x_8 - 23x_8^2; \\
Q_{12} &= 2x_3x_5 - 2x_4^2 - 90x_4x_6 + 97x_4x_7 - 75x_4x_8 + 90x_5^2 - 97x_5x_6 + 25x_5x_7 + 53x_5x_8 \\
&\quad + 54x_6^2 - 57x_6x_7 - 119x_6x_8 + 14x_7^2 + 107x_7x_8 - 105x_8^2; \\
Q_{13} &= x_3x_6 - x_4x_5 - 22x_4x_6 + 23x_4x_7 - 18x_4x_8 + 22x_5^2 - 23x_5x_6 + 7x_5x_7 + 14x_5x_8 \\
&\quad + 15x_6^2 - 17x_6x_7 - 26x_6x_8 + 4x_7^2 + 24x_7x_8 - 23x_8^2; \\
Q_{14} &= 4x_3x_7 + 32x_4x_6 - 39x_4x_7 + 25x_4x_8 - 36x_5^2 + 39x_5x_6 - 5x_5x_7 - 19x_5x_8 - 8x_6^2 \\
&\quad + x_6x_7 + 67x_6x_8 - 57x_7x_8 + 51x_8^2; \\
Q_{15} &= x_3x_8 + 40x_4x_6 - 43x_4x_7 + 32x_4x_8 - 40x_5^2 + 42x_5x_6 - 10x_5x_7 - 25x_5x_8 - 23x_6^2 \\
&\quad + 24x_6x_7 + 53x_6x_8 - 6x_7^2 - 47x_7x_8 + 45x_8^2; \\
C &= 16256x_1^2x_3 - 16256x_1x_2^2 + 16256x_3x_4^2 - 130048x_4^3 + 113792x_4^2x_5 - 48768x_4x_5^2 \\
&\quad + 455620x_4x_7^2 + 934015x_4x_7x_8 + 378671x_4x_8^2 + 81280x_5^3 + 130048x_5^2x_6 \\
&\quad + 567328x_5^2x_7 + 1810692x_5^2x_8 - 1412640x_5x_6^2 - 710152x_5x_6x_7 - 3915151x_5x_6x_8 \\
&\quad + 499912x_5x_7^2 + 353577x_5x_7x_8 - 1485701x_5x_8^2 - 1474880x_6^3 + 3770532x_6^2x_7 \\
&\quad - 5789336x_6^2x_8 - 2251600x_6x_7^2 + 5914379x_6x_7x_8 - 7757003x_6x_8^2 + 294568x_7^3 \\
&\quad - 467500x_7^2x_8 + 3280949x_7x_8^2 - 3204251x_8^3.
\end{aligned}
$$

The cusps of $X_H(61)$ are

$$\begin{aligned}
c_1 &= (1:0:0:0:0:0:0:0);\\
c_2 &= (-3:-2:0:-1:-1:-2:-1:1);\\
c_3 &= (6:\sqrt{61}+13:6:2:2:\sqrt{61}+7:\sqrt{61}+7:2);\\
c_4 &= (6:-\sqrt{61}+13:6:2:2:-\sqrt{61}+7:-\sqrt{61}+7:2).
\end{aligned}$$

The cuspidal subgroup $C_H(61) = \langle [c_2 - c_1], [c_3 - c_1], [c_4 - c_1] \rangle$ is isomorphic to $(\mathbb{Z}/11\mathbb{Z}) \times (\mathbb{Z}/55\mathbb{Z})$, and it is generated by $[c_3 - c_1]$ and $[c_4 - c_1]$ only. Taking Galois invariants, the resulting rational cuspidal subgroup is

$$C_H(61)(\mathbb{Q}) = \langle [c_3 + c_4 - 2c_1] \rangle \cong (\mathbb{Z}/55\mathbb{Z}).$$

Reducing modulo multiple primes, we find that 605 is an upper bound for $|J_H(61)(\mathbb{Q}(\sqrt{61}))_{\text{tors}}$ and hence

$$C_H(61) = J_H(61)(\mathbb{Q}(\sqrt{61}))_{\text{tors}} \cong \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/55\mathbb{Z}.$$

4.4. Curves of Genus 9. — There is single prime congruent to 1 modulo 4 for which $X_H(p)$ has genus 9, namely 73. The curve $X_H(73)$ is not hyperelliptic, so its canonical model is the intersection of 21 quadrics $\mathbb{P}^8$.

$$\begin{aligned}
Q_1 &= 2x_1x_3 - 2x_2^2 + 4x_3x_4 - 3x_4^2 - 6x_4x_5 + 29x_5^2 - 73x_5x_6 - 219x_5x_7 + 219x_5x_8\\
&\quad + 146x_5x_9 + 73x_6^2 + 438x_6x_7 - 438x_6x_8 - 292x_6x_9 + 584x_7^2 - 1314x_7x_8 - 876x_7x_9\\
&\quad + 657x_8^2 + 876x_8x_9 + 292x_9^2;\\
Q_2 &= 2x_1x_4 - 2x_2x_3 - 2x_3x_4 - 6x_4^2 + 7x_4x_5 + 15x_5^2 - 73x_5x_6 - 73x_5x_7 + 219x_5x_8\\
&\quad + 146x_5x_9 + 73x_6^2 + 146x_6x_7 - 438x_6x_8 - 292x_6x_9 + 73/2x_7^2 - 438x_7x_8 - 292x_7x_9\\
&\quad + 657x_8^2 + 876x_8x_9 + 292x_9^2;\\
Q_3 &= 4x_1x_5 - 4x_3^2 - 8x_3x_4 - 8x_4^2 + 16x_4x_5 - 12x_5^2 + 146x_5x_7 - 292x_6x_7 - 511x_7^2\\
&\quad + 876x_7x_8 + 584x_7x_9;\\
Q_4 &= 2x_1x_6 - 2x_3x_4 + 2x_4x_{5]} - 18x_4x_8 - 6x_5^2 + 13x_5x_6 + 59x_5x_7 + 27x_5x_8 + 32x_5x_9\\
&\quad - 15x_6^2 - 177x_6x_7 + 42x_6x_8 - 34x_6x_9 - 310x_7^2 + 411x_7x_8 + 172x_7x_9 + 27x_8^2\\
&\quad + 222x_8x_9 + 128x_9^2;\\
Q_5 &= 4x_1x_7 - 4x_4^2 + 8x_5^2 - 20x_5x_6 - 74x_5x_7 + 24x_5x_8 + 2x_5x_9 + 18x_6^2 + 188x_6x_7\\
&\quad - 72x_6x_8 - 10x_6x_9 + 280x_7^2 - 489x_7x_8 - 244x_7x_9 + 54x_8^2 - 42x_8x_9 - 52x_9^2;\\
Q_6 &= 3x_1x_8 - 3x_4x_5 - 12x_4x_8 + 6x_5^2 - 12x_5x_6 - 28x_5x_7 + 33x_5x_8 + 9x_5x_9 + 5x_6^2\\
&\quad + 60x_6x_7 - 24x_6x_8 + x_6x_9 + 75x_7^2 - 171x_7x_8 - 56x_7x_9 + 36x_8^2 - 9x_8x_9 - 26x_9^2;\\
Q_7 &= 4x_1x_9 + 6x_4x_8 - 4x_5^2 + 22x_5x_6 - 10x_5x_7 + 34x_5x_9 - 14x_6^2 - 40x_6x_7 + 24x_6x_8\\
&\quad - 66x_6x_9 - 18x_7^2 - 9x_7x_8 - 194x_7x_9 + 54x_8^2 + 330x_8x_9 + 196x_9^2;
\end{aligned}$$

$$\begin{aligned}
Q_8 &= 2x_2x_4 - 2x_3^2 - 2x_4^2 - 10x_4x_5 + 32x_5^2 - 73x_5x_6 - 219x_5x_7 + 219x_5x_8 + 146x_5x_9 \\
&\quad + 73x_6^2 + 438x_6x_7 - 438x_6x_8 - 292x_6x_9 + 1241/2x_7^2 - 1314x_7x_8 - 876x_7x_9 \\
&\quad + 657x_8^2 + 876x_8x_9 + 292x_9^2; \\
Q_9 &= x_2x_5 - x_3x_4 - 2x_4^2 - x_4x_5 + 11x_5^2 - 73/2x_5x_6 - 73x_5x_7 + 219/2x_5x_8 + 73x_5x_9 \\
&\quad + 73/2x_6^2 + 146x_6x_7 - 219x_6x_8 - 146x_6x_9 + 146x_7^2 - 438x_7x_8 - 292x_7x_9 \\
&\quad + 657/2x_8^2 + 438x_8x_9 + 146x_9^2; \\
Q_{10} &= x_2x_6 - x_4^2 - 9x_4x_8 + 2x_5^2 - 6x_5x_6 - x_5x_7 + 15x_5x_8 + 4x_5x_9 + 2x_6^2 + 1/2x_6x_7 \\
&\quad - 6x_6x_8 + 4x_6x_9 - 8x_7^2 - 6x_7x_8 + 30x_7x_9 - 18x_8x_9 - 16x_9^2; \\
Q_{11} &= 4x_2x_7 - 4x_4x_5 + 8x_5^2 - 20x_5x_6 - 50x_5x_7 + 24x_5x_8 + 2x_5x_9 + 18x_6^2 + 132x_6x_7 \\
&\quad - 72x_6x_8 - 10x_6x_9 + 184x_7^2 - 345x_7x_8 - 132x_7x_9 + 54x_8^2 - 42x_8x_9 - 52x_9^2; \\
Q_{12} &= 3x_2x_8 - 12x_4x_8 - 3x_5^2 + 12x_5x_6 + 34x_5x_7 - 42x_5x_8 - 39x_5x_9 - 19x_6^2 - 64x_6x_7 \\
&\quad + 120x_6x_8 + 97x_6x_9 - 73x_7^2 + 201x_7x_8 + 192x_7x_9 - 189x_8^2 - 297x_8x_9 - 122x_9^2; \\
Q_{13} &= 2x_2x_9 + 3x_4x_8 - 2x_5x_6 + 3x_5x_8 + 6x_5x_9 + 4x_6^2 - 2x_6x_7 - 18x_6x_8 - 18x_6x_9 \\
&\quad - 6x_7^2 - 3x_7x_8 - 11x_7x_9 + 18x_8^2 + 42x_8x_9 + 24x_9^2; \\
Q_{14} &= 2x_3x_5 - 2x_4^2 - 4x_4x_5 + 8x_5^2 - 73x_5x_7 + 146x_6x_7 + 292x_7^2 - 438x_7x_8 - 292x_7x_9; \\
Q_{15} &= 2x_3x_6 - 2x_4x_5 + 12x_4x_8 + 4x_5^2 - 10x_5x_6 - 41x_5x_7 - 6x_5x_8 - 17x_5x_9 + 15x_6^2 \\
&\quad + 121x_6x_7 - 54x_6x_8 + 13x_6x_9 + 185x_7^2 - 591/2x_7x_8 - 118x_7x_9 + 27x_8^2 \\
&\quad - 111x_8x_9 - 78x_9^2; \\
Q_{16} &= 2x_3x_7 - 2x_5^2 + 8x_5x_6 + 7x_5x_7 - 18x_5x_8 - 9x_5x_9 - 7x_6^2 - 14x_6x_7 + 36x_6x_8 \\
&\quad + 17x_6x_9 - 14x_7^2 + 69/2x_7x_8 + 10x_7x_9 - 45x_8^2 - 39x_8x_9 - 6x_9^2; \\
Q_{17} &= 6x_3x_8 + 18x_4x_8 - 6x_5x_6 - 22x_5x_7 - 30x_5x_8 - 28x_5x_9 + 16x_6^2 + 92x_6x_7 \\
&\quad - 36x_6x_8 + 12x_6x_9 + 140x_7^2 - 183x_7x_8 - 68x_7x_9 - 36x_8^2 - 156x_8x_9 - 80x_9^2; \\
Q_{18} &= 4x_3x_9 - 6x_4x_8 + 8x_5x_7 + 6x_5x_8 - 2x_5x_9 - 6x_6^2 - 16x_6x_7 + 18x_6x_8 \\
&\quad + 30x_6x_9 - 50x_7^2 + 39x_7x_8 + 66x_7x_9 - 54x_8x_9 - 36x_9^2; \\
Q_{19} &= 2x_4x_6 - 6x_4x_8 - 2x_5^2 + 8x_5x_6 + 15x_5x_7 - 6x_5x_8 - 3x_5x_9 - 11x_6^2 - 50x_6x_7 \\
&\quad + 42x_6x_8 + 15x_6x_9 - 53x_7^2 + 195/2x_7x_8 + 42x_7x_9 - 27x_8^2 + 3x_8x_9 + 14x_9^2; \\
Q_{20} &= x_4x_7 - x_5x_6 + x_5x_7 - 3x_5x_8 - 4x_5x_9 + x_6^2 + 2x_6x_7 + 6x_6x_9 + 2x_7^2 + 3x_7x_8 \\
&\quad + 16x_7x_9 - 9x_8^2 - 30x_8x_9 - 16x_9^2; \\
Q_{21} &= 2x_4x_9 + x_5x_7 - 3x_5x_9 - x_6^2 - 4x_6x_7 + 3x_6x_8 + 5x_6x_9 + x_7^2 - 3/2x_7x_8 + 10x_7x_9 \\
&\quad - 9x_8x_9 - 6x_9^2.
\end{aligned}$$

The cusps of $X_H(73)$ are

$c_1 = (1:0:0:0:0:0:0:0:0)$;

$c_2 = (3:0:0:0:0:-3:0:-1:0)$;

$$c_3 = \left(1:1:1:0:0 :: \frac{1}{73}(-11\sqrt{73}-73) : -\frac{2}{73}\sqrt{73} : -\frac{4}{219}\sqrt{73} : \frac{1}{146}(-11\sqrt{73}-73)\right);$$
$$c_4 = \left(1:1:1:0:0 :: \frac{1}{73}(11\sqrt{73}-73) : \frac{2}{73}\sqrt{73} : \frac{4}{219}\sqrt{73} : \frac{1}{146}(11\sqrt{73}-73)\right).$$

The cuspidal subgroup $C_H(73) = \langle [c_2 - c_1], [c_3 - c_1], [c_4 - c_1] \rangle$ is isomorphic to $(\mathbb{Z}/22\mathbb{Z}) \times (\mathbb{Z}/66\mathbb{Z})$, and as in the previous cases, $[c_3 - c_1]$ and $[c_4 - c_1]$ generate the entire group. Taking Galois invariants gives:

$$C_H(73)(\mathbb{Q}) = \langle [c_3 + c_4 - 2c_1] \rangle \cong (\mathbb{Z}/66\mathbb{Z}).$$

An upper bound for the size of $J_H(73)(\mathbb{Q}(\sqrt{73}))_{\text{tors}}$ is 1452, and hence

$$J_H(73)(\mathbb{Q}(\sqrt{73}))_{\text{tors}} = C_H(73) \cong \mathbb{Z}/22\mathbb{Z} \times \mathbb{Z}/66\mathbb{Z}.$$

References

[1] Y.-H. Chen, "Cuspidal $\mathbb{Q}$ Rational Torsion Subgroup of $J(\Gamma)$ of Level P", *Taiwanese J. Math.* **15** (2011), no. 3, p. 1305-1323.

[2] V. G. Drinfel′d, "Two theorems on modular curves", *Funkts. Anal. Prilozh.* **7** (1973), no. 2, p. 83-84.

[3] E.-U. Gekeler, "Cuspidal divisor class groups of modular curves", in *Algebraic number theory and Diophantine analysis (Graz, 1998)*, Walter de Gruyter, 2011, p. 163-189.

[4] N. M. Katz, "Galois properties of torsion points on abelian varieties", *Invent. Math.* **62** (1981), no. 3, p. 481-502.

[5] G. Ligozat, "Courbes modulaires de genre 1", *Bull. Soc. Math. Fr., Suppl., Mém.* **43** (1975), p. 80, supplément au Bull. Soc. Math. France, Tome 103, no. 3.

[6] D. J. Lorenzini, "Torsion points on the modular jacobian $J_0(N)$", *Compos. Math.* **96** (1995), no. 2, p. 149-172.

[7] Y. I. Manin, "Parabolic points and zeta functions of modular curves", *Izv. Akad. Nauk SSSR, Ser. Mat.* **36** (1972), p. 19-66.

[8] O. Masami, "Eisenstein ideals and the rational torsion subgroups of modular Jacobian varieties II", *Tokyo J. Math.* **37** (2014), no. 2, p. 273-318.

[9] B. Mazur, "Modular curves and the Eisenstein ideal", *Publ. Math., Inst. Hautes Étud. Sci.* **47** (1977), p. 33-186 (1978), with an appendix by Mazur and M. Rapoport.

[10] A. P. Ogg, "Rational points on certain elliptic modular curves", in *Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972)*, American Mathematical Society, 1973, p. 221-231.

[11] E. Ozman & S. Siksek, "Quadratic points on modular curves", *Math. Comput.* **88** (2019), no. 319, p. 2461-2484.

[12] D. Poulakis, "La courbe modulaire $X_0(125)$ et sa jacobienne", *J. Number Theory* **25** (1987), no. 1, p. 112-131.

[13] J. Quer, "Dimensions of spaces of modular forms for $\Gamma_H(N)$", *Acta Arith.* **145** (2010), p. 373-395.

[14] K. A. Ribet & P. Wake, "Another look at rational torsion of modular Jacobians", *Proc. Natl. Acad. Sci. USA* **119** (2022), no. 41, article no. e2210032119 (8 pages).

[15] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, 1971.

[16] S. Siksek, "Explicit arithmetic of modular curves", Summer school notes, 2019.

[17] W. A. Stein, "Explicit approaches to modular abelian varieties", PhD Thesis, University of California, Berkeley, 2000, 119 pages.

[18] G. Stevens, *Arithmetic on modular curves*, Progress in Mathematics, vol. 20, Springer, 2012.

[19] T. Takagi, "Cuspidal class number formula for the modular curves $X_1(p)$", *J. Algebra* **151** (1992), no. 2, p. 348-374.

[20] ———, "The Cuspidal Class Number Formula for the Modular Curves $X_0(M)$ with M Square-Free", *J. Algebra* **193** (1997), no. 1, p. 180-213.

[21] H. Yoo, "The rational cuspidal divisor class group of $X_0(N)$", *J. Number Theory* **242** (2023), p. 278-401.

[22] J. Yu, "A Cuspidal Class Number Formula for the Modular Curves $X_1(N)$.", *Math. Ann.* **250** (1980), p. 197-216.

Elvira Lupoian, Department of Mathematics, University College London, London, United Kingdom
E-mail : e.lupoian@ucl.ac.uk