A CLASSIFICATION OF LOW GENUS MODULAR CURVES

ERAY KARABIYIK

Abstract. Let G be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ satisfying $\det(\mathsf{G}) = \widehat{\mathbb{Z}}^\times$ and $-\mathsf{I} \in \mathsf{G}$. Associated to G, there is a modular curve X_G defined over $\mathbb{Q}$, which parametrizes elliptic curves with G-level structure. Fixing a non-negative integer g, we give a classification of modular curves of genus g. In particular, we show that all modular curves of genus g lie in finitely many families of $\mathbb{Q}^{\mathrm{ab}}$-twists of modular curves. We also describe an algorithm for computing all families of modular curves of a fixed genus g and use this to compute projective models for these modular curves. This algorithm has been implemented for $g \leqslant 12$.

1. Introduction

Let E be a non-CM elliptic curve defined over the rational numbers. Fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Let $\mathrm{Gal}_\mathbb{Q} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ denote the absolute Galois group of $\mathbb{Q}$. For any positive integer N, let $\mathsf{E}[\mathsf{N}]$ be the N-torsion of $\mathsf{E}(\overline{\mathbb{Q}})$, it is a free $(\mathbb{Z}/\mathsf{N}\mathbb{Z})-$module of rank 2. The group $\mathrm{Gal}_\mathbb{Q}$ acts naturally on $\mathsf{E}[\mathsf{N}]$ and respects the group structure. This gives rise to a Galois representation

$$\rho_{\mathsf{E},\mathsf{N}}\colon \mathrm{Gal}_\mathbb{Q} \to \mathrm{Aut}(\mathsf{E}[\mathsf{N}]) \cong \mathrm{GL}_2(\mathbb{Z}/\mathsf{N}\mathbb{Z}).$$

Fixing compatible bases for $\mathsf{E}[\mathsf{N}]$ for all $\mathsf{N} \geqslant 1$, and taking the inverse limit, one gets the adelic representation

$$\rho_\mathsf{E}\colon \mathrm{Gal}_\mathbb{Q} \longrightarrow \mathrm{Aut}(\mathrm{E}_{\mathrm{tors}}) \cong \mathrm{GL}_2(\widehat{\mathbb{Z}})$$

where $\widehat{\mathbb{Z}}$ is the profinite completion of $\mathbb{Z}$. The image of ρ_E is uniquely determined up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. The group $\rho_\mathsf{E}(\mathrm{Gal}_\mathbb{Q})$ is a closed subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ with respect to the profinite topology. In [Ser72], Serre proved that $\rho_\mathsf{E}(\mathrm{Gal}_\mathbb{Q})$ is an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

Let $\chi_{\mathrm{cyc}} : \mathrm{Gal}_\mathbb{Q} \to \widehat{\mathbb{Z}}^\times$ be the cyclotomic character. Using the Weil pairing on E, one can show that $\det \circ \rho_\mathsf{E}$ agrees with χ_{cyc}, and hence the image of ρ_E has full determinant i.e, $\det(\rho_\mathsf{E}(\mathrm{Gal}_\mathbb{Q})) = \widehat{\mathbb{Z}}^\times$. Let G be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ such that $\det(\mathsf{G}) = \widehat{\mathbb{Z}}^\times$ and $-\mathsf{I} \in \mathsf{G}$. Associated to G, there is a modular curve X_G that parametrizes elliptic curves with G-structure, which will be explicitly defined in §2.

Let g be a non-negative integer. In Theorem 1.4, we show that all modular curves X_G of genus g lie in finitely many families of $\mathbb{Q}^{\mathrm{ab}}$-twists. We also describe an algorithm that computes projective models of modular curves of genus g. This classification in terms of families has been computed for modular curves of genus at most 24, and the algorithm has been implemented for modular curves of genus at most 12. A `Magma` [BCP97] package implementing the algorithm can be found at [Kar25]. When X_G is a geometrically non-hyperelliptic modular curve of genus at least 2, our implementation computes the image of the canonical map. During Summer 2025, this `Magma` package has been used by LMFDB [LMF]

2010 *Mathematics Subject Classification.* Primary 14K15; Secondary 11F80.

to compute projective models for more than one million modular curves in their modular curves database.

1.1. **Modular curves.** Let $\mathsf{G} \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ be an open subgroup such that $\det(\mathsf{G}) = \widehat{\mathbb{Z}}^\times$ and $-I \in \mathsf{G}$. We will define the associated modular curve X_G in §2. It is a smooth, projective, geometrically irreducible curve defined over $\mathbb{Q}$. An inclusion $G \subseteq G' \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$, induces a morphism of curves $X_G \to X_{G'}$. For the group $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, we have $X_{\mathrm{GL}_2(\widehat{\mathbb{Z}})} \cong \mathbb{P}^1_{\mathbb{Q}} = \mathbb{A}^1_{\mathbb{Q}} \cup \{\infty\}$. Taking $G' = \mathrm{GL}_2(\widehat{\mathbb{Z}})$, we have the associated j-map

$$\pi\colon X_G \longrightarrow \mathbb{P}^1_{\mathbb{Q}}.$$

Let $\rho_E^*\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$ be the dual representation of ρ_E defined by $\rho_E^*(\sigma) = \rho_E(\sigma^{-1})^\intercal$. The curve X_G has the following property, cf. [Zyw22, Proposition 3.5].

Proposition 1.1. Let G be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ that satisfies $\det(G) = \widehat{\mathbb{Z}}^\times$ and $-I \in G$. Let E be any elliptic curve defined over $\mathbb{Q}$ with j-invariant $j_E \notin \{0, 1728\}$. Then $\rho_E^*(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ to a subgroup of G if and only if j_E is an element of $\pi_G(X_G(\mathbb{Q})) \subseteq \mathbb{Q} \cup \{\infty\}$.

Throughout the paper, by the genus of an open subgroup $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$, we mean the genus of the associated modular curve X_G.

In §2, we will describe a method, developed in [Zyw22], to compute a model for the modular curve X_G using certain spaces of modular forms. In §7, using a twisting argument, we will describe an algorithm to compute the model of any modular curve X_G, whose genus is at most a fixed integer g. Our algorithm reduces this problem to a collection of group theory and linear algebra computations.

There are many equivalent definitions of the modular curve X_G. One can define X_G by explicitly defining its function field or as the general fiber of the coarse stack M_G defined over $\mathbb{Z}[1/N]$ that parametrizes elliptic curves with G-level structure, see [DR73] for details. One can also refer to [KM85] for the fine arithmetic of modular curves, where the level structure has a meaning over schemes where N is not invertible. We will opt to define X_G through a certain space of modular forms $M_{k,G}$, which is defined in §2.

1.2. **Agreeable groups.** Fix a non-negative integer g. Let G be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ that has full determinant and contains $-I$. For our classification of modular curves X_G, of genus g, we introduce a special kind of subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ that contains the group G.

Definition 1.2. An open subgroup $H \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ is agreeable if $\det(H) = \widehat{\mathbb{Z}}^\times$, H contains the scalar matrices, i.e. $\widehat{\mathbb{Z}}^\times \cdot I \subseteq H$, and the levels of H in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and $H \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ have the same odd prime divisors.

There exists a group $\mathcal{G}$, called the agreeable closure of G, which is minimal, with respect to inclusion, among all agreeable subgroups that contain G. The group G is normal in $\mathcal{G}$ and satisfies $[G, G] = [\mathcal{G}, \mathcal{G}]$ i.e., their commutator subgroups agree. Since there is a nonconstant map $X_G \to X_{\mathcal{G}}$, the genus of $\mathcal{G}$ is less than or equal to the genus of G.

The set of agreeable subgroups is closed under conjugation in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. We show in §5 that there are only finitely many agreeable subgroups of genus at most g up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

1.3. **Families attached to a pair.** Let $\mathcal{G} \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ be an agreeable subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. Fix a subgroup B of $\mathcal{G}$ such that $[\mathcal{G}, \mathcal{G}] \subseteq \mathsf{B} \subseteq \mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$.

Definition 1.3. The family attached to the pair $(\mathcal{G}, \mathsf{B})$ is the set of open subgroups G of $\mathcal{G}$ such that $\det(\mathsf{G}) = \widehat{\mathbb{Z}}^\times$ and $\mathsf{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = \mathsf{B}$. We denote the family by $\mathscr{F}(\mathcal{G}, \mathsf{B})$.

Assume $\mathscr{F}(\mathcal{G}, \mathsf{B})$ is nonempty and fix $\mathsf{G} \in \mathscr{F}(\mathcal{G}, \mathsf{B})$. In §4, we show that the family $\mathscr{F}(\mathcal{G}, \mathsf{B})$ consists of the groups

$$\mathsf{G}_\gamma := \{g \in \mathcal{G} \colon g \cdot \mathsf{G} = \gamma(\det(g))\} \tag{1.1}$$

where $\gamma \colon \widehat{\mathbb{Z}}^\times \longrightarrow \mathcal{G}/\mathsf{G}$ is a continuous homomorphism. Since the genus of an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ is determined by its intersection with $\mathrm{SL}_2(\widehat{\mathbb{Z}})$, all the groups in $\mathscr{F}(\mathcal{G}, \mathsf{B})$ have the same genus.

The families $\mathscr{F}(\mathcal{G}, \mathsf{B})$ were first introduced in [Zyw22]. The result of that paper can be given in terms of these families. We will inspect the family of modular curves in more detail in §4. For the remainder of the paper, by a *family of groups*, we mean a nonempty family attached to an arbitrary pair $(\mathcal{G}, \mathsf{B})$.

Clearly, G lies in the family $\mathscr{F}(\mathcal{G}, \mathsf{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}))$, where $\mathcal{G}$ is the agreeable closure of G. The family consists of groups of the form G_γ, where $\gamma \colon \widehat{\mathbb{Z}}^\times \to \mathcal{G}/\mathsf{G}$ is a continuous homomorphism. Consider the associated modular curve X_G and the natural map $\pi_\mathsf{G} \colon X_\mathsf{G} \to X_\mathcal{G}$. The group $\mathcal{G}$ acts on X_G, and the restricted action of G is trivial. Hence, there is an action of $\mathcal{G}/\mathsf{G}$ on X_G. We have $\mathrm{Aut}(X_\mathsf{G}/X_\mathcal{G}) \simeq \mathcal{G}/\mathsf{G}$, where $\mathrm{Aut}(X_\mathsf{G}/X_\mathcal{G})$ is the group of automorphisms f of the curve X_G that satisfy $\pi_\mathsf{G} \circ f = \pi_\mathsf{G}$. Precomposing γ with the cyclotomic character χ_{cyc}, we get a homomorphism $\xi \colon \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \longrightarrow \mathcal{G}/\mathsf{G}$, which can be viewed as a 1-cocycle of X_G. We will show in §6 that, by twisting the curve X_G with the cocycle ξ, we obtain a curve $(X_\mathsf{G})_\xi$ and $(X_\mathsf{G})_\xi = X_{\mathsf{G}_\gamma}$. Hence, a family $\mathscr{F}(\mathcal{G}, \mathsf{B})$ can be viewed as a family of twists of modular curves. In the rest of the paper, the terms *family of groups* and *family of curves* will be used interchangeably, and both will refer to a family of the form $\mathscr{F}(\mathcal{G}, \mathsf{B})$. Our main theorem is the following.

Theorem 1.4. Fix a non-negative integer g. Let G be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ of genus g with full determinant and $-I \in \mathsf{G}$.

(1) There are only finitely many families of modular curves of genus g. These families are effectively computable.

(2) There is an effective algorithm that takes as input the group G and outputs a projective curve $C_\mathsf{G} \subseteq \mathbb{P}^r_\mathbb{Q}$ for some $r > 0$ such that C_G is isomorphic to X_G.

Remark 1.5. For the implementation of the algorithm of Theorem 1.4, first, we compute the finitely many families of genus g, choose a representative group $\mathsf{H} \in \mathscr{F}(\mathcal{G}, \mathsf{B})$ for each family, and precompute a projective model for X_H. This reduces the computation of C_G to identifying a family $\mathscr{F}(\mathcal{G}, \mathsf{B})$ that contains G, computing the continuous homomorphism $\gamma : \widehat{\mathbb{Z}} \to \mathcal{G}/\mathsf{H}$ such that $\mathsf{G} = \mathsf{H}_\gamma$, and then twisting the projective model of X_H with respect to the cocycle $\gamma \circ \chi_{cyc}$. Computationally, twisting the model is equivalent to a collection of linear algebra and group theory computations which are easily handled on most computer algebra systems. Refer to §7 for a detailed exposition of our algorithm.

Theorem 1.4 will be proved in §5 and §6. Table 1 shows the number of families and agreeable subgroups for small g.

Genus	Families	Agreeable Groups
0	638	418
1	1753	1078
2	1209	885
3	3865	2244
4	1573	1151
5	6181	3659
$\leqslant 6$	15943	9998
$\leqslant 12$	48819	30233
$\leqslant 24$	166141	95981

TABLE 1. Number of families and agreeable groups up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ for small genus

1.4. **A family of quadratic twists.** For known families of modular curves ($X_0(N)$, $X_1(N)$, $X_{ns}(N)$, $X_{ns}^+(N)$,$X_s(N)$ and so on) there are many algorithms to compute models in the literature. On the other hand, for an arbitrary open subgroup $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ with $-I \in G$ and $\det(G) = \widehat{\mathbb{Z}}$, there are limited methods to compute a model for X_G. One such algorithm is the one implemented in [Zyw22] which we describe in §2.

Consider the family of modular curves $\mathscr{F}(\mathcal{G}, B)$ where $\mathcal{G}$ and B are given as

$$\mathcal{G} = \left\langle \left(\begin{smallmatrix} 3 & 10 \\ 6 & 5 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 6 \\ 6 & 15 \end{smallmatrix}\right), \left(\begin{smallmatrix} 7 & 2 \\ 2 & 9 \end{smallmatrix}\right), \left(\begin{smallmatrix} 5 & 0 \\ 9 & 3 \end{smallmatrix}\right) \right\rangle \subset \mathrm{GL}_2(\mathbb{Z}/16\mathbb{Z}),$$
$$B = \left\langle \left(\begin{smallmatrix} 7 & 0 \\ 0 & 7 \end{smallmatrix}\right) \right\rangle \subset \mathrm{SL}_2(\mathbb{Z}/8\mathbb{Z}).$$

We have precomputed a representative H in the family $\mathscr{F}(\mathcal{G}, B)$ given by

$$H = \left\langle \left(\begin{smallmatrix} 9 & 14 \\ 6 & 7 \end{smallmatrix}\right), \left(\begin{smallmatrix} 7 & 10 \\ 5 & 9 \end{smallmatrix}\right), \left(\begin{smallmatrix} 5 & 6 \\ 7 & 3 \end{smallmatrix}\right) \right\rangle \subset \mathrm{GL}_2(\mathbb{Z}/16\mathbb{Z}).$$

The group H has index 192 in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and has genus 5. There are 242 families of modular curves of genus 5 and index 192. The modular curve X_H has the following model $C_H \subseteq \mathbb{P}^4_{\mathbb{Q}}$ which we have precomputed:

$$\begin{aligned} -x_1x_4 - x_2^2 + x_3^2 &= 0 \\ -2x_1x_4 + 2x_2^2 + x_5^2 &= 0 \\ -2x_1^2 + 2x_3x_5 + x_4^2 &= 0. \end{aligned}$$

The agreeable closure $\mathcal{G}$ has index 96 in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and so $\mathcal{G}/H$ is isomorphic to the cyclic group of order 2. The model of X_H given above is the canonical model i.e., comes from the cusp forms $S_{2,H}$ (see §2) which is a $\mathbb{Q}$-vector space of dimension 5. The nontrivial element of $\mathcal{G}/H$ acts on $S_{2,H}$ (with respect to our choice of basis) via the matrix

$$M = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix}$$

Let $\gamma : \widehat{\mathbb{Z}} \to \mathcal{G}/H$ be a continuous homomorphism as in §1.3. Let H_γ be the corresponding group in $\mathscr{F}(\mathcal{G}, B)$. Since $\mathcal{G}/H$ is cyclic of order two, the curves X_H and X_{H_γ} are isomorphic over a quadratic number field which we denote by K_γ. In particular, the cocycle defining the twist X_{H_γ} of X_H is given by the map $\xi\colon \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}_5(K_\gamma)$, $\mathrm{id} \neq \sigma \mapsto M$.

Let $K_\gamma \simeq \mathbb{Q}(\sqrt{d})$ where d is a squarefree integer. A quick computation shows that the curve given by the equations

$$\begin{aligned} -x_1x_4 - dx_2^2 + x_3^2 &= 0 \\ -2x_1x_4 + 2dx_2^2 + x_5^2 &= 0 \\ -2x_1^2 + 2x_3x_5 + x_4^2 &= 0. \end{aligned}$$

is isomorphic to X_{H_γ}. Hence, the set of equations given above as we vary the squarefree integer d, corresponds to the family of modular curves $\mathscr{F}(\mathcal{G}, B)$. As a particular example, consider the following group.

$$G = \left\langle \left(\begin{smallmatrix} 429 & 214 \\ 270 & 211 \end{smallmatrix}\right), \left(\begin{smallmatrix} 633 & 548 \\ 824 & 505 \end{smallmatrix}\right), \left(\begin{smallmatrix} 425 & 275 \\ 630 & 871 \end{smallmatrix}\right), \left(\begin{smallmatrix} 663 & 909 \\ 610 & 913 \end{smallmatrix}\right) \right\rangle \subset \mathrm{GL}_2(\mathbb{Z}/944\mathbb{Z}).$$

The curves X_H and X_G are isomorphic over the number field $K := \mathbb{Q}(\sqrt{118}) \subset \mathbb{Q}(\zeta_{944})$. Using our implementation, we find the curve $C \subseteq \mathbb{P}^4_{\mathbb{Q}}$ given by the equations

$$\begin{aligned} -x_1x_4 - 118x_2^2 + x_3^2 &= 0 \\ -2x_1x_4 + 236x_2^2 + x_5^2 &= 0 \\ -2x_1^2 + 2x_3x_5 + x_4^2 &= 0. \end{aligned}$$

is isomorphic to X_G.

On our machine, the precomputation of the family $\mathscr{F}(\mathcal{G}, B)$, the representative X_H, and the model C_H took 0.50 seconds. After this precomputation, our implementation took 0.41 seconds to compute the model C of X_G and the associated j-map $X_G \to \mathbb{P}^1_{\mathbb{Q}}$. On the same machine, Zywina's implementation took 22.79 seconds to compute a model for the modular curve X_G (without the j-map). For modular curves of higher level, the computation of j-maps is particularly time consuming, as it involves finding relations between the j-invariant and cusp forms whose coefficients lie in $\mathbb{Q}(\zeta_N)$, where N is the level of G. We avoid this step via twisting in our algorithm. As a result, our algorithm remains efficient even as the level of the input curve X_G increases. Although we do not compute q-expansions to find the models, it should be noted that the current implementation of our algorithm can still be used to compute certain subspaces of $M_{k,G}$ (for instance, $S_{2,G}$ in the above example) via twisting.

1.5. **An example of cubic twists.** Consider the the following group.

$$G = \left\langle \left(\begin{smallmatrix} 41 & 160 \\ 4 & 61 \end{smallmatrix}\right), \left(\begin{smallmatrix} 155 & 77 \\ 135 & 60 \end{smallmatrix}\right), \left(\begin{smallmatrix} 121 & 93 \\ 13 & 148 \end{smallmatrix}\right) \right\rangle \subset \mathrm{GL}_2(\mathbb{Z}/182\mathbb{Z}).$$

We find that G is conjugate to a group that lies in the family $\mathscr{F}(\mathcal{G}, B)$ where $\mathcal{G}$ and B are given as

$$\mathcal{G} = \left\langle \left(\begin{smallmatrix} 8 & 3 \\ 13 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 23 & 14 \\ 8 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 11 & 13 \\ 17 & 16 \end{smallmatrix}\right) \right\rangle \subset \mathrm{GL}_2(\mathbb{Z}/26\mathbb{Z}),$$

$$B = \left\langle \left(\begin{smallmatrix} 17 & 22 \\ 18 & 5 \end{smallmatrix}\right), \left(\begin{smallmatrix} 23 & 16 \\ 14 & 3 \end{smallmatrix}\right) \right\rangle \subset \mathrm{SL}_2(\mathbb{Z}/26\mathbb{Z}).$$

We have precomputed a representative H in the family $\mathscr{F}(\mathcal{G}, B)$ given by

$$H = \left\langle \left(\begin{smallmatrix} 13 & 4 \\ 22 & 23 \end{smallmatrix}\right), \left(\begin{smallmatrix} 15 & 18 \\ 6 & 25 \end{smallmatrix}\right) \right\rangle \subset \mathrm{GL}_2(\mathbb{Z}/26\mathbb{Z}).$$

G and H has index 84 in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and has genus 5. There are 178 families of modular curves of genus 5 and index 84. The modular curve X_H has the projective model $C_H \subseteq \mathbb{P}^4_{\mathbb{Q}}$ we have precomputed defined by the polynomials

$$f_1 = x_2x_4 + x_3x_5,$$

$$f_2 = -x_1^2 + x_1x_2 + x_1x_3 - x_1x_4 + x_1x_5 - x_2x_3 + x_2x_4 + x_4x_5,$$

$$f_3 = -x_1^2 + x_2^2 - x_2x_3 - x_2x_4 + x_2x_5 + x_3^2 - x_3x_4 + x_4^2 + x_4x_5 + x_5^2.$$

Using our implementation, we find the curve $C \subseteq \mathbb{P}^4_{\mathbb{Q}}$ defined by the polynomials

$$\begin{aligned} f_1' =& -4x_1^2 + 14x_1x_2 + 6x_1x_3 - 26x_1x_4 + 26x_1x_5 + 17x_2^2 - 42x_2x_3 \\ &+ 5x_2x_4 - 50x_2x_5 + 27x_3^2 + 24x_3x_4 + 21x_3x_5 + 5x_4^2 + 26x_4x_5 + 5x_5^2, \\ f_2' =& 4x_1^2 - 14x_1x_2 + 24x_1x_3 + 5x_1x_4 + 7x_1x_5 + 10x_2^2 + 3x_2x_3 \\ &- 11x_2x_4 + 8x_2x_5 + 6x_3x_4 - 24x_3x_5 + x_4^2 - 17x_4x_5 - 11x_5^2, \\ f_3' =& 6x_1^2 - 21x_1x_2 + 29x_1x_3 + 4x_1x_4 + 7x_1x_5 + 15x_2^2 + x_2x_3 \\ &- 13x_2x_4 + 5x_2x_5 + 2x_3x_4 - 29x_3x_5 - 2x_4^2 - 15x_4x_5 - 13x_5^2. \end{aligned}$$

is isomorphic to X_G. The curves X_H and X_G are isomorphic over the number field $K \subset \mathbb{Q}(\zeta_{182})$ with the defining polynomial $f(x) = x^3 + 5x^2 + 6x - 1$. The model of X_H given above is the canonical model i.e., comes from the cusp forms $S_{2,H}$ (see §2) which is a $\mathbb{Q}$-vector space of dimension 5. The agreeable closure $\mathcal{G}$ has index 28 in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and so $\mathcal{G}/G$ is isomorphic to the cyclic group of order 3. Choose a generator $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, and $g \in \mathcal{G}/G$ be its image under ξ (see §1.3). The generator g of $\mathcal{G}/G$ acts on $S_{2,H}$ (with respect to our choice of basis and generator) via the matrix

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & -1 & 1 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 1 & -1 & 0 & 0 & -1 \end{pmatrix}$$

The cocycle (which is a homomorphism) defining the twist X_G of X_H is given by the map $\mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}_5(K)$, $\sigma \mapsto M$. The matrix given by Hilbert 90 is

$$\begin{pmatrix} 1 & -1 & 0 & 1 & -1 \\ \frac{2z-1}{7} & \frac{3z^2-8z-2}{7} & 0 & \frac{3z^2-13z+11}{7} & \frac{-2z+1}{7} \\ \frac{2z-1}{7} & \frac{-2z+1}{7} & \frac{-3z^2+15z-12}{7} & \frac{2z-1}{7} & \frac{3z^2-8z-2}{7} \\ \frac{2z^2-6z-1}{7} & \frac{-2z^2+6z+1}{7} & \frac{3z^2-6z-3}{7} & \frac{2z^2-6z-1}{7} & \frac{4z^2-15z+10}{7} \\ \frac{2z^2-8z+7}{7} & \frac{z^2-7z+5}{7} & 0 & \frac{-4z^2+13z-2}{7} & \frac{-2z^2+8z-7}{7} \end{pmatrix}$$

where z is a root of $f(x)$. Hence, A encodes how to pass between two $\mathbb{Q}$-structures defined on $S_{2,H} \otimes_{\mathbb{Q}} K$ corresponding to $S_{2,H}$ and $S_{2,G}$. Consequently, we use the matrix A to twist the curve C_H and obtain the curve C.

1.6. **Motivation.** In [Maz77a], Mazur describes the following program which serves as motivation for computing projective models of modular curves and for classification problems related to modular curves:

Mazur's Program B. Given a number field K and a subgroup H of $\mathrm{GL}_2(\widehat{\mathbb{Z}}) = \prod_p \mathrm{GL}_2(\mathbb{Z}_p)$ classify all elliptic curves E/K whose associated Galois representation on torsion points maps $\mathrm{Gal}(\overline{K}/K)$ <u>into</u> $H \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$.

Let G_1 and G_2 be the groups $\pm\rho^*_{E_1}(\mathrm{Gal}_{\mathbb{Q}})$ and $\pm\rho^*_{E_2}(\mathrm{Gal}_{\mathbb{Q}})$, where E_1 and E_2 are elliptic curves with j-invariants $-7 \cdot 11^3$ and $-7 \cdot 137^3 \cdot 2083^3$, respectively. Note that these groups are well-defined up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

In [Zyw22], it is conjectured that if $G \subset \mathrm{GL}_2(\widehat{\mathbb{Z}})$ is an open subgroup with surjective determinant containing $-I$, and if X_G has genus at least 54, and G is not conjugate to G_1 or G_2 in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, then X_G contains no non-CM rational points over $\mathbb{Q}$. Hence, conjecturally, explicitly computing the families of modular curves up to genus 53, along with extending our algorithm to such families, allows us to compute a projective model for any modular curve over rationals that contains a non-CM rational point (except X_{G_1} and X_{G_2} whose rational points are understood).

Following the conjectures of Zywina, we suggest the following challenging program:

Program 1.6. One can consider the following steps to resolve Mazur's Program B:

(1) Prove Serre's uniformity problem.

(2) Classify all rational points on a finite number of special modular curves as described in Section 14 of [Zyw22].

(3) Classify all congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ (in the sense of [CP03]) up to genus 53 (or genus β as in Lemma 14.7 in [Zyw22]).

(4) Compute all families of modular curves up to the genus mentioned above, in the sense of §4.

(5) Investigate the behavior of rational points on the mentioned families.

Note that there has been much progress towards proving Serre's uniformity problem in which Serre asks whether for all primes $l > 37$, the mod l representation $\rho_{E,l}$ is surjective or not. If the image is not surjective, then E gives rise to a non-CM rational point on the modular curve X_G, where G is a maximal subgroup of $\mathrm{GL}_2(\mathbb{Z}/l\mathbb{Z})$. Mazur [Maz78, Maz77b] completely described the cases where G is the Borel subgroup or one of the exceptional subgroups of $\mathrm{GL}_2(\mathbb{Z}/l\mathbb{Z})$. Bilu, Parent and Rebolledo [BPR13] showed that when G is the normalizer of split Cartan subgroup, then X_G has no non-CM rational points. The only remaining case is the normalizer of non-split Cartan subgroups and the associated modular curves $X^+_{ns}(l)$. Using Chabauty methods, Balakrishnan et al. [BDM+19, BDM+23] determined rational points on $X^+_{ns}(l)$ for some small primes l.

1.7. **Related results.** There is a lot of work on modular curves and Galois representations attached to elliptic curves over $\mathbb{Q}$. Here, we mention some recent related results.

In [Zyw22], Zywina describes a practical algorithm that computes the image of ρ_E up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. Assuming some conjectures, they also give a complete classification of the groups $\rho_E(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$. The methods developed by Zywina to achieve this result include an algorithm to compute models of modular curves X_G. They also introduce the notion of a family of modular curves and interpret their results in this language. The notions and methods introduced by Zywina form an important basis for our paper. In [Zyw24], they describe an analogous algorithm that works for elliptic curves over number fields.

Rakvi [Rak24] has given a classification of genus 0 modular curves X_G over $\mathbb{Q}$ such that $X_G \cong \mathbb{P}^1_{\mathbb{Q}}$, in terms of families of abelian twists.

In [SZ17], authors determine all open subgroups G of prime power level for which $X_G(\mathbb{Q})$ is infinite. This work also provides a classification for possible images of l-adic Galois representations arising from elliptic curves for almost all j-invariants.

In [RZB15], Rouse, Zureick-Brown give a classification of possible 2-adic images of Galois representations associated to elliptic curves over $\mathbb{Q}$. [BBH+25] completed the classification of 3-adic images of Galois representations arising from elliptic curves, extending the work in [RZB15]. In [RSZB22], the authors investigate the l-adic images for $l = 3, 5, 7, 11$.

Most recently, [MR25] implemented an algorithm to provably compute the $\mathbb{Q}$-rationals points on modular curves X_G, which admits a non-trivial morphism to an elliptic curve of rank 0.

1.8. **Implementation.** The implementation of our algorithm can be found in the repository [Kar25]. All computations are done in `Magma` [BCP97].

In Section 7, we describe our algorithm including the precomputation part. While the precomputation part is computationally intense, it is only a one time computation and the rest of our algorithm is efficient.

1.9. **Acknowledgments.** I would like to thank David Zywina for his valuable suggestions and comments. I would like to thank David Roe for his help in computing family labels and his help in making the implementation of our algorithm faster and compatible with the LMFDB database. I would also like to thank Zachary Couvillion, Andrew Sutherland and Eran Assaf for fruitful mathematical discussions.

1.10. **Notation.** $\widehat{\mathbb{Z}}$ is the profinite group obtained by taking the inverse limit of $\mathbb{Z}/N\mathbb{Z}$ over all $N \in \mathbb{N}$. Similarly, $\mathbb{Z}_M$ is the profinite group obtained by taking the inverse limit of $\mathbb{Z}/M^s\mathbb{Z}$ where s ranges over $\mathbb{N}$ and $1 < M \in \mathbb{N}$. There are natural isomorphisms

$$\mathbb{Z}_M \cong \prod_{l|M} \mathbb{Z}_l \quad \text{and} \quad \widehat{\mathbb{Z}} \cong \prod_{l} \mathbb{Z}_l$$

where the product runs over the prime numbers l. The reduction modulo N homomorphism $\widehat{\mathbb{Z}} \to \mathbb{Z}/N\mathbb{Z}$ induces the homomorphisms $\pi_N : \mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. The level of an open subgroup G of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ is the smallest positive integer N such that G is the inverse image of the reduction modulo N map $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Similarly, the level of an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_M)$ is the smallest positive integer N that divides a power of M and such that G is equal to the inverse image of its image under the reduction modulo N map $\mathrm{GL}_2(\mathbb{Z}_M) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. The levels of an open subgroup of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ and $\mathrm{SL}_2(\mathbb{Z}_M)$ are defined similarly.

For $1 < N \in \mathbb{N}$, we let G_N be the image of G under the homomorphism $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}_N)$ arising from the natural projection map. We can interpret the *level* of G in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ as the smallest positive integer N for which we have $G = G_N \times \prod_{\ell \nmid N} \mathrm{GL}_2(\mathbb{Z}_\ell)$. We denote by $G(N)$ the image of G under the homomorphism $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

Unless stated otherwise, open subgroups G of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ are assumed to satisfy $\det(G) = \widehat{\mathbb{Z}}^\times$ and $-I \in G$.

1.11. **Overview of the paper.** In §2, we review the background material on modular curves and modular forms. In §3, we will discuss agreeable subgroups, define the agreeable closure of a subgroup G and discuss how to compute it. In §4, we define a family of groups associated to a pair $(\mathcal{G}, B)$, denoted by $\mathscr{F}(\mathcal{G}, B)$. In §5, we prove the finiteness of agreeable subgroups of a fixed genus and use this to deduce our main theorem, that modular curves over $\mathbb{Q}$ lie in finitely many families of abelian twists. In §6, we will describe the cocycles arising from families $\mathscr{F}(\mathcal{G}, B)$, show that $\mathscr{F}(\mathcal{G}, B)$ is a family of twists of modular curve and describe how to twist projective models of modular curves. In §7, we finally describe an algorithm for computing a model of any modular curve X_G of fixed genus g. In §8, we describe an algorithm to determine whether a geometrically hyperelliptic modular curve has $\mathbb{Q}$-gonality 2 or 4.

2. Modular Forms and Modular Curves

The goal of this section is to state some known facts about the theory of modular forms and introduce modular curves. We will mostly use the language of [Zyw22]. For the rest of the section, let $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ be an open subgroup. For any N divisible by the level of G, the projection $\pi_N : \mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ gives a group whose inverse image is the open subgroup G i.e., $G = \pi_N^{-1}(\pi_N(G))$. We will often abuse notation and denote by G both the open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and its image under π_N. Considering G as a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, we let Γ_G be the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ consisting of matrices that are modulo N congruent to an element of $G \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

2.1. **Setting the stage.** The group $\mathrm{SL}_2(\mathbb{Z})$ acts on the extended upper half-plane $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$ by linear fractional transformations. Fix a congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ such that $-I \in \Gamma$. For a positive integer N, define the primitive N-th root of unity $\zeta_N := e^{2\pi i/N}$ in $\mathbb{C}$.

The quotient $\mathcal{X}_\Gamma := \Gamma \backslash \mathcal{H}^*$ is a smooth compact Riemann surface [DS05, §2]. Let g be the genus of the Riemann surface $\mathcal{X}_\Gamma$. Let w be the width of the cusp ∞, i.e. the smallest positive integer such that $\left[\begin{smallmatrix} 1 & w \\ 0 & 1 \end{smallmatrix}\right] \in \Gamma$. Let $q_w := e^{2\pi i \tau/w}$.

Let $k \geqslant 0$ be a natural number. For a meromorphic function f on $\mathcal{H}$ and a matrix $\gamma \in \mathrm{GL}_2(\mathbb{R})$ with positive determinant, we define the *slash operator* of weight k on f by $(f|_k\gamma)(\tau) := \det(\gamma)^{k/2}(c\tau + d)^{-k} f(\gamma\tau)$. Let $P_1, \dots, P_r$ be the cusps of $\mathcal{X}_\Gamma$. Let $Q_1, \dots, Q_s$ be the elliptic points of $\mathcal{X}_\Gamma$ and denote their orders by $e_1, \dots, e_s$, respectively. Each e_i is either 2 or 3. Let ν_2 and ν_3 be the number of elliptic points of $\mathcal{X}_\Gamma$ of order 2 and 3, respectively.

2.2. **Modular forms.** A modular form of weight $k \geqslant 0$ with respect to Γ is a holomorphic function of $\mathcal{H}$ such that $f|_k\gamma = f$ for all $\gamma \in \Gamma$, and at the cusps it satisfies the usual growth condition. We denote the set of modular forms with respect to Γ by $M_k(\Gamma)$. It is a finite dimensional complex vector space. Let $f \in M_k(\Gamma)$ be a modular form. We have a unique q-expansion of f (at the cusp ∞) given by

$$f(\tau) = \sum_{n=0}^{\infty} a_n(f)\, q_w^n$$

where $a_n(f) \in \mathbb{C}$. The spaces of modular forms of different weights k form a graded $\mathbb{C}$-algebra denoted by

$$R_\Gamma := \bigoplus_{k \geqslant 0} M_k(\Gamma).$$

R_Γ is finitely generated as a $\mathbb{C}$-algebra. One can focus on modular forms f whose q-expansion (at the cusp ∞) has coefficients in a certain subring S of $\mathbb{C}$, which we denote by $M_k(\Gamma, S)$. It has a natural structure as an S-module.

In particular, consider the principal congruence subgroups $\Gamma(N)$ given by

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

The $\mathbb{Q}(\zeta_N)$-vector space $M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$ will be of special interest to us.

2.3. **Modular forms and differential forms.** Fix an even integer $k \geqslant 0$. Take any modular form $f \in M_k(\Gamma)$. By definition, f satisfies $f(\gamma\tau) = (c\tau + d)^k f(\tau)$ for all $\gamma \in \Gamma$, which is equivalent to $f(\gamma\tau) d(\gamma\tau)^{k/2} = f(\tau)(d\tau)^{k/2}$. Therefore, f gives a differential form

$$f(\tau)\,(d\tau)^{k/2} = \left(\frac{w}{(2\pi i)}\right)^{k/2} \left(\sum_{n=0}^{\infty} a_n(f)\, q_w^n\right) \left(\frac{dq_w}{q_w}\right)^{k/2} \tag{2.1}$$

on $\mathcal{H}$ and this induces a meromorphic differential $k/2$-form ω_f, associated to f, on $\mathcal{X}_\Gamma$. For details, see [DS05, §3.3].

Let $\mathcal{D}_k$ be the divisor

$$\sum_{i=1}^{r} k/2 \cdot P_r + \sum_{i=1}^{s} \lfloor k/2 \cdot (1 - 1/e_i) \rfloor \cdot Q_i \tag{2.2}$$

of $\mathcal{X}_\Gamma$ supported on cusps and elliptic points [Zyw22, §4.4]. For any modular form $f \in M_k(\Gamma)$, we have $\mathrm{div}(\omega_f) + \mathcal{D}_k \geqslant 0$. This defines a map of complex vector spaces

$$\psi_k \colon M_k(\Gamma) \to H^0(\mathcal{X}_\Gamma, \Omega^1(\mathcal{D}_k)^{\otimes k/2}).$$

sending f to ω_f.

Moreover, any differential form in $H^0(\mathcal{X}_\Gamma, \Omega^1(\mathcal{D}_k)^{\otimes k/2})$ pulls back to a differential form $f(\tau)(d(\tau))^{k/2}$ on $\mathcal{H}$ as in (2.1). The form f is holomorphic and satisfies the growth conditions at cusps (due to being in the space $H^0(\mathcal{X}_\Gamma, \Omega^1(\mathcal{D}_k)^{\otimes k/2})$). Therefore, the map ψ_k is an isomorphism of vector spaces.

The groups Γ that we consider contain $-I$, which means that $M_k(\Gamma) = 0$ when k is odd. Combining the isomorphisms ψ_k for even $k \in \mathbb{N}$, we get an isomorphism of $\mathbb{C}$ algebras:

$$\psi \colon R_\Gamma \xrightarrow{\sim} \bigoplus_{k \geqslant 0} H^0(\mathcal{X}_\Gamma, \Omega^1(\mathcal{D}_k)^{\otimes k/2}).$$

2.4. **Actions.** Fix positive integers k and N. The principal congruence subgroup $\Gamma(N)$ is normal in $\mathrm{SL}_2(\mathbb{Z})$ and the weight-k operator gives a right action of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ on $M_k(\Gamma(N))$. Let $f = \sum_{n=0}^{\infty} a_n(f) q_N^n$ be a modular form in $M_k(\Gamma(N))$. Let σ be a field automorphism of $\mathbb{C}$, it acts on the coefficients of f and gives rise to a unique weight-k modular form $\sigma(f)$, i.e. the q-expansion of $\sigma(f)$ is given by $\sum_{n=0}^{\infty} \sigma(a_n(f)) q_N^n$.

Consider the isomorphism $(\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$, $d \mapsto \sigma_d$, where $\sigma_d(\zeta_N) = \zeta_N^d$. The following lemma gives an action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on $M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$ viewed as a $\mathbb{Q}$-vector space.

Lemma 2.1. There is a unique right action $*$ of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on $M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$ such that the following hold:

- if $A \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, then $f * A = f|_k\gamma$, where γ is any matrix in $\mathrm{SL}_2(\mathbb{Z})$ that is congruent to A modulo N,
- if $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$, then $f * A = \sigma_d(f)$.

Proof. See [BN19, §3]. □

Combining the action of Lemma 2.1 for all k, we get a right action $*$ of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on the graded $\mathbb{Q}$-algebra $\bigoplus_{k\geqslant 0} M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$.

2.5. **The spaces $M_{k,G}$.** Fix a positive integer N. Let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ such that $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$. Define the $\mathbb{Q}$-vector space

$$M_{k,G} := M_k(\Gamma(N), \mathbb{Q}(\zeta_N))^G,$$

i.e. the subspace fixed by the G under the action $*$ from Lemma 2.1. Note that $M_{k,G} \subseteq M_k(\Gamma(N), \mathbb{Q}(\zeta_N))^{G\cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})} = M_k(\Gamma_G, \mathbb{Q}(\zeta_N))$.

Tensoring $M_{k,G}$ with $\mathbb{Q}(\zeta_N)$ and $\mathbb{C}$ give natural isomorphisms.

Lemma 2.2. The natural homomorphisms

$$M_{k,G} \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_N) \to M_k(\Gamma_G, \mathbb{Q}(\zeta_N)) \quad \text{and} \quad M_{k,G} \otimes_{\mathbb{Q}} \mathbb{C} \to M_k(\Gamma_G)$$

are isomorphisms for $k \neq 1$.

Proof. See Lemma 4.5 in [Zyw22]. □

2.6. **Modular curves.** Let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that satisfies $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$ and $-I \in G$. We have defined the $\mathbb{Q}$-vector spaces

$$M_{k,G} := M_k(\Gamma(N), \mathbb{Q}(\zeta_N))^G.$$

Note that when $-I \in G$, $M_{k,G}$ is trivial for odd integers k. Consider the graded $\mathbb{Q}$-algebra $\bigoplus_{k=0}^\infty M_{k,G}$.

Definition 2.3. The modular curve X_G associated to group G is the $\mathbb{Q}$-scheme $\mathrm{Proj}(\bigoplus_{k=0}^\infty M_{k,G})$. For open subgroups $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$, the modular curve X_G is defined using the image of G under the natural projection $\pi\colon \mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ where N is divisible by the level of G.

Remark 2.4. X_G is a smooth, projective and geometrically irreducible curve over $\mathbb{Q}$. This definition is independent of the choice of N.

When $G := \mathrm{GL}_2(\widehat{\mathbb{Z}})$, we have $X_G = \mathrm{Proj}(\bigoplus_{k=0}^\infty M_{k,G}) = \mathrm{Proj}(\mathbb{Q}[E_4, E_6])$. Its function field is $\mathbb{Q}(j)$, where j is the modular j-invariant. The first few terms of the q-expansion of j is given by

$$j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots$$

We can identify $X_{\mathrm{GL}_2(\widehat{\mathbb{Z}})}$ with $\mathbb{P}^1_{\mathbb{Q}}$. It is commonly called as the *j*-line.

Let $G \subseteq G' \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ be open subgroups. There is an inclusion $M_{k,G'} \subseteq M_{k,G}$, and so there is an induced map of curves $X_G \to X_{G'}$. When $G' = \mathrm{GL}_2(\widehat{\mathbb{Z}})$, we get the absolute j-map $\pi\colon X_G \to \mathbb{P}^1_{\mathbb{Q}}$.

2.6.1. *Compatibility with other definitions.* Consider the space of modular forms $M_k(\Gamma_G)$ as in §2.2. It is a finite dimensional complex vector space. The map ψ_k shows us that $M_k(\Gamma_G)$ is isomorphic to $H^0(\mathcal{X}_{\Gamma_G}, \Omega^1(\mathcal{D}_k)^{\otimes k/2})$, the global sections of the line bundle $\Omega^1(\mathcal{D}_k)^{\otimes k/2}$ on the Riemann surface $\mathcal{X}_{\Gamma_G}$. Let's consider the graded ring $R_{\Gamma_G} := \bigoplus_{k\geqslant 0} M_k(\Gamma_G)$. The graded $\mathbb{C}$-algebra R_{Γ_G} is isomorphic to the ring of sections of the line bundle $\Omega^1(\mathcal{D}_k)$, and since this line bundle is ample we have $\mathrm{Proj}(R_{\Gamma_G}) \cong \mathcal{X}_{\Gamma_G}$ where the latter is viewed as a scheme over $\mathbb{C}$ [VZB22, §1.1].

Similarly, the graded ring $R := \mathrm{Proj}(\bigoplus_{k=0}^{\infty} M_{k,G})$ is finitely generated over $\mathbb{Q}$. Lemma 2.2 shows that tensoring R with $\mathbb{C}$ gives the ring R_{Γ_G}. Using this equality we identify $X_G(\mathbb{C})$ with $\mathcal{X}_{\Gamma_G}$. Base changing the map $\pi\colon X_G \to \mathbb{P}^1_{\mathbb{Q}}$ to $\mathbb{C}$, we get the complex projection map $\mathcal{X}_{\Gamma_G} \to \mathbb{P}^1_{\mathbb{C}}$.

Let X_G be as in [Zyw22, §3.3], which is defined by explicitly describing its function field. Let $\mathcal{L}_k := \Omega^1(\mathcal{D}_k)$, the invertible sheaf on the Riemann surface $\mathcal{X}_{\Gamma_G}$ where $\mathcal{D}_k$ is the divisor defined in equation (4.3) in loc. cit. The divisor D_k is defined over $\mathbb{Q}$, so we can view it as a divisor on X_G. Define the invertible sheaf $\mathscr{L}_k := \Omega^1(\mathcal{D}_k)$ on X_G, which gives rise to $\mathcal{L}_k$ on $X_G(\mathbb{C}) = \mathcal{X}_{\Gamma_G}$. Between the global sections of $\mathcal{L}_k$ and $\mathscr{L}_k$, we have the inclusion $H^0(\mathcal{X}_G, \mathscr{L}_k) \subseteq H^0(X_{\Gamma_G}, \mathcal{L}_k) \simeq M_k(\Gamma_G)$. In particular, it is shown that the map ψ_k induces an isomorphism

$$M_{k,G} \xrightarrow{\sim} H^0(X_G, \mathscr{L}_k).$$

Since $\mathscr{L}_k$ is an ample invertible sheaf on X_G, there is an isomorphism $\mathrm{Proj}(\bigoplus_{k=0}^{\infty} M_{k,G}) \cong X_G$. Hence, our definition is compatible with Zywina's definition.

2.7. **Models of modular curves.** In this section, we briefly describe how to compute projective models of modular curves, as explained in [Zyw22, §5]. This method uses explicit q-expansions of modular forms in $M_{k,G}$.

Let G be as above, and let N be a positive integer divisible by the level of G. Let $\mathcal{X}_{\Gamma_G}$ be the Riemann surface associated to Γ_G which we identify with $X_G(\mathbb{C})$. Let $P_1, \cdots, P_r$ be the cusps of $X_G(\mathbb{C})$, which are defined over $\mathbb{Q}(\zeta_N)$. Let $E = \sum_{i=1}^{r} e_i P_i$ be a divisor on X_G defined over $\mathbb{Q}$ with $e_i \geqslant 0$. Let g be the genus of the curve X_G. Define:

$$V := \{f \in M_{k,G} : \nu_{P_i}(f) \geqslant e_i \text{ for all } 1 \leqslant i \leqslant r\}$$

Assume $\dim_{\mathbb{Q}} V = d \geqslant 2$ with $d \geqslant 1$, and let $f_0, \cdots, f_d$ be a basis of V over $\mathbb{Q}$. One can compute such a basis by computing Eisenstein series and multiplying them [Zyw22, Algorithm 4.14]. Note that the quotients f_j/f_i are rational functions of X_G. The modular forms $f_0, \cdots, f_d$ define a morphism

$$\varphi\colon X_G \to \mathbb{P}^d_{\mathbb{Q}}$$

via $\varphi(P) = [f_0(P), \ldots, f_d(P)]$ for all but finitely many P. Up to an automorphism of $\mathbb{P}^d_{\mathbb{Q}}$, the map φ does not depend on the choice of basis. Denote the image of X_G under ϕ in $\mathbb{P}^d_{\mathbb{Q}}$ by C. Let $I(C) \subseteq \mathbb{Q}[x_0, \ldots, x_d]$ be the homogeneous ideal of C. There is an algorithm to compute a basis for each graded part $I(C)_n$ [Zyw22, §5.3].

Let $\mathcal{F} := \mathscr{L}_k(-E)$ be the invertible sheaf associated to divisor E on X_G. The map $\psi_k :$ $M_{k,G} \xrightarrow{\sim} H^0(X_G, \mathscr{L}_k)$ restricts to an isomorphism between V and $H^0(X_G, \mathcal{F})$ as $\mathbb{Q}$-vector spaces. The degree of the invertible sheaf $\mathscr{L}_k$ is $k/2 \cdot (2g-2) + k/2 \cdot r + \lfloor k/4 \rfloor \nu_2 + \lfloor k/3 \rfloor \cdot \nu_3$ where ν_2 and ν_3 are the number of elliptic points of $X_G(\mathbb{C})$ of order 2 and 3. The degree of $\mathcal{F}$ is given by

$$\deg \mathcal{F} = \deg \mathscr{L}_k - \sum_{i=1}^{r} e_i = k/2 \cdot (2g-2) + k/2 \cdot r + \lfloor k/4 \rfloor \cdot \nu_2 + \lfloor k/3 \rfloor \cdot \nu_3 - \sum_{i=1}^{r} e_i. \tag{2.3}$$

2.7.1. *Getting the model for* X_G. First, assume $g \geqslant 3$. Choosing the divisor $E = \sum_{i=1}^{r} P_i$, we can compute the canonical map $\varphi\colon X_G \to \mathbb{P}_{\mathbb{Q}}^{g-1}$ (for more details on the canonical map refer to [Zyw20]). If X_G is not geometrically hyperelliptic then this map is an embedding and $C = \varphi(X_G)$ is a curve isomorphic to X_G.

Consider the general case. Note that if $\deg \mathcal{F} \geqslant 2g+1$, the Riemann-Roch theorem implies that $\mathcal{F}$ is very ample, so the map φ is an embedding and C is isomorphic to X_G as the homomorphism

$$\eta\colon \mathbb{Q}[x_0, \dots, x_d]/I(C) \to \bigoplus_{n \geqslant 0} H^0(X_G, \mathcal{F}^{\otimes n})$$

defined by $x_i \to \psi_k(f_i)$ is an isomorphism of $\mathbb{Q}$-algebras [Mum70]. To ensure that $\deg \mathcal{F} \geqslant 2g+1$, we can choose the even integer $k \geqslant 2$ large enough and choose the divisor $E = \sum_{i=1}^{r} e_i P_i$ suitably. In this case, the map φ is an embedding and $C := \varphi(X_G)$ is isomorphic to the modular curve X_G.

2.7.2. *Actions on the embedding.* Let $\mathcal{G}$ be any subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ such that G is a normal subgroup of $\mathcal{G}$. The group $\mathcal{G}$ acts on $M_{k,G}$ and one can choose the divisor E accordingly so that $\mathcal{G}$ acts on V and $\deg \mathscr{L}_k(-E) \geqslant 2g+1$ at the same time. The action of $\mathcal{G}/G$ on V gives a homomorphism $\alpha : \mathcal{G} \to \mathrm{GL}_{d+1}(\mathbb{Q}^{\mathrm{ab}})$.

The action of $\mathcal{G}/G$ on V also induces automorphisms of X_G defined over $\mathbb{Q}^{\mathrm{ab}}$ and consequently automorphisms of $C \subseteq \mathbb{P}_{\mathbb{Q}}^{d+1}$. Using the homomorphism α, these automorphisms of X_G extend to automorphisms of $\mathbb{P}_{\mathbb{Q}}^{d+1}$, defined over $\mathbb{Q}^{\mathrm{ab}}$, that stabilize C.

3. Agreeable Subgroups

In this section we describe the agreeable subgroups of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. They were first introduced in [Zyw22] and were studied more generally in [Zyw24]. We will mostly follow their exposition.

Definition 3.1. We say that a subgroup $\mathcal{G}$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ is agreeable if it is open in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, satisfies $\det(\mathcal{G}) = \widehat{\mathbb{Z}}^\times$, contains the scalar matrices $\widehat{\mathbb{Z}}^\times \cdot I$, and the levels of $\mathcal{G}$ in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and $\mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ have the same odd prime divisors.

Fix an open subgroup G of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ such that $\det(G) = \widehat{\mathbb{Z}}^\times$ and $-I \in G$. In general, G will not be an agreeable subgroup. Associated to G, there is a unique minimal agreeable subgroup that contains G.

Proposition 3.2. Let G be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ with $\det(G) = \widehat{\mathbb{Z}}^\times$. Let N be the product of primes that divide the level of $[G, G]$ in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$. Define the subgroup

$$\mathcal{G} := (\mathbb{Z}_N^\times \cdot G_N) \times \prod_{\ell \nmid N} \mathrm{GL}_2(\mathbb{Z}_\ell) \tag{3.1}$$

of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. Then $\mathcal{G}$ is the unique minimal agreeable subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, with respect to inclusion, that satisfies $G \subseteq \mathcal{G}$. We have $[G, G] = [\mathcal{G}, \mathcal{G}]$ and hence G is a normal subgroup of $\mathcal{G}$ with $\mathcal{G}/G$ finite and abelian.

Proof. This is Proposition 8.1 in [Zyw22]. $\square$

Definition 3.3. With notation as in Proposition 3.2, we define the agreeable closure of G as the agreeable subgroup $\mathcal{G}$.

Remark 3.4. Note that the integer N in Proposition 3.2 is even, because the commutator subgroup G always has even level. The group $\mathcal{G}$ contains the group G and the scalar matrices $\widehat{\mathbb{Z}}^\times \cdot I$. The scalar matrices are contained in the center of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ so G_N and $\widehat{\mathbb{Z}}^\times \cdot \mathsf{G}_\mathsf{N}$ have the same commutator subgroups.

3.1. **Constructing the agreeable closure.** The statement of Proposition 3.2 suggests that the level of $[\mathsf{G},\mathsf{G}]$ needs to be known to compute the agreeable closure $\mathcal{G}$. Unfortunately, computing the commutator subgroup of G can be unfeasible, especially if the level of the group is large or contains large prime factors. However, we can relate the levels of $[\mathcal{G},\mathcal{G}]$ and $\mathcal{G}\cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$.

Lemma 3.5.

(i) For an odd prime ℓ, we have $\mathsf{G}_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$ if and only if $\mathcal{G}_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$.

(ii) The levels of $[\mathcal{G},\mathcal{G}]$ and $\mathcal{G}\cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ and the level of $\mathcal{G}$ in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ have the same odd prime divisors as N.

Proof. This is proven in [Zyw22, Lemma 8.3]. $\square$

Using the above lemma, one can find the prime divisors of $[\mathsf{G},\mathsf{G}]$ from the level of $\mathsf{G}\cap\mathrm{SL}_2(\widehat{\mathbb{Z}})$ in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$. The latter is significantly easier to compute.

Lemma 3.6. Let $\mathsf{G} \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ be an open subgroup with full determinant. Let $\mathsf{B} := \mathsf{G}\cap\mathrm{SL}_2(\widehat{\mathbb{Z}})$. Then the level of $[\mathsf{G},\mathsf{G}]$ and level of B in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ have the same odd prime divisors.

Proof. The inclusion $[\mathsf{G},\mathsf{G}] \subseteq \mathsf{B}$ implies that the level of B divides the level of $[\mathsf{G},\mathsf{G}]$. Let $\mathcal{G}$ be the agreeable closure of G. Since $\mathsf{G} \subseteq \mathcal{G}$, the level of $\mathcal{G}\cap\mathrm{SL}_2(\widehat{\mathbb{Z}})$ divides the level of B. The Lemma 3.5 implies that the level of $[\mathcal{G},\mathcal{G}] = [\mathsf{G},\mathsf{G}]$ and $\mathcal{G}\cap\mathrm{SL}_2(\widehat{\mathbb{Z}})$ in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ have the same odd prime divisors. Therefore, any odd prime ℓ that divides the level of $[\mathsf{G},\mathsf{G}] = [\mathcal{G},\mathcal{G}]$ also divides the level of $\mathrm{SL}_2(\widehat{\mathbb{Z}})\cap\mathcal{G}$ and consequently the level of B. $\square$

Proposition 3.7. Let G be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. Let $\mathcal{G}$ be the agreeable closure of G. Then

$$\mathcal{G} = \mathcal{G}_\mathsf{N} \times \prod_{\ell\nmid \mathsf{N}} \mathrm{GL}_2(\mathbb{Z}_\ell) = (\mathbb{Z}_\mathsf{N}^\times \cdot \mathsf{G}_\mathsf{N}) \times \prod_{\ell\nmid \mathsf{N}} \mathrm{GL}_2(\mathbb{Z}_\ell)$$

where N is the least common multiple of 2 and the radical of the level of $\mathsf{B} = \mathsf{G}\cap\mathrm{SL}_2(\widehat{\mathbb{Z}})$ in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$. If G has odd level, then so has $\mathcal{G}$.

Proof. By Lemma 3.6, the levels of B and $[\mathsf{G},\mathsf{G}]$ have the same odd prime divisors in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$. From the construction of the agreeable subgroup $\mathcal{G}$ the assertion follows.

Since $\mathsf{G} \subset \mathcal{G}$, the level of $\mathcal{G}$ in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ divides the level of G in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. Therefore, if the level of G is an odd integer, so is the level of $\mathcal{G}$. $\square$

4. Families of Modular Curves

In this section, we define the families of groups that we use in our classification and collect some results about them. Later in §6, we will show that these families of groups correspond to families of modular curves in a natural way.

Let $\mathcal{G}$ be an agreeable subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. Fix a subgroup B of $\mathcal{G}$ satisfying $[\mathcal{G},\mathcal{G}] \subseteq \mathsf{B} \subseteq \mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$.

Definition 4.1. The family of groups associated to the pair $(\mathcal{G}, \mathsf{B})$ is the set $\mathscr{F}(\mathcal{G}, \mathsf{B})$ of subgroups H of $\mathcal{G}$ that satisfy $\det(\mathsf{H}) = \widehat{\mathbb{Z}}^\times$ and $\mathsf{H} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = \mathsf{B}$.

Assume that $\mathscr{F}(\mathcal{G}, \mathsf{B})$ is nonempty. Fix a group $\mathsf{G} \in \mathscr{F}(\mathcal{G}, \mathsf{B})$. We know that G is an open subgroup of $\mathcal{G}$. Since $[\mathcal{G},\mathcal{G}] \subset \mathsf{G}$, we have that G is a normal subgroup of $\mathcal{G}$, and the quotient $\mathcal{G}/\mathsf{G}$ is finite and abelian. Consider any continuous homomorphism $\gamma\colon \widehat{\mathbb{Z}}^\times \to \mathcal{G}/\mathsf{G}$. Define the group

$$\mathsf{G}_\gamma := \{g \in \mathcal{G} : g \cdot \mathsf{G} = \gamma(\det g)\}.$$

Lemma 4.2 ([Zyw22] Lemma 14.2)**.** With notation as above, the set $\mathscr{F}(\mathcal{G}, \mathsf{B})$ consists of the groups G_γ with $\gamma\colon \widehat{\mathbb{Z}}^\times \to \mathcal{G}/\mathsf{G}$ a continuous homomorphism.

Proof. First take any γ. We have $\mathsf{G}_\gamma \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = \mathsf{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = \mathsf{B}$. The natural map $(\mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}))/\mathsf{B} \to \mathcal{G}/\mathsf{G}$ is an isomorphism since $\mathsf{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = \mathsf{B}$ and $\det(\mathsf{G}) = \widehat{\mathbb{Z}}^\times$. Using this isomorphism, we find that $\det(\mathsf{G}_\gamma) = \widehat{\mathbb{Z}}^\times$. Therefore, $\mathsf{G}_\gamma \in \mathscr{F}(\mathcal{G}, \mathsf{B})$.

Conversely, take any $\mathsf{H} \in \mathscr{F}(\mathcal{G}, \mathsf{B})$. The quotient map $\mathsf{H} \to \mathcal{G}/\mathsf{G}$ induces a homomorphism $f\colon \mathsf{H}/(\mathsf{H} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})) \to \mathcal{G}/\mathsf{G}$ since $\mathsf{H} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = \mathsf{B} = \mathsf{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$. Let $\gamma\colon \widehat{\mathbb{Z}}^\times \to \mathcal{G}/\mathsf{G}$ be the homomorphism obtained by composing the inverse of the determinant map $\mathsf{H}/(\mathsf{H} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})) \xrightarrow{\sim} \widehat{\mathbb{Z}}^\times$ with f. For each $h \in \mathsf{H}$, we have $h \cdot \mathsf{G} = \gamma(\det h)$. Therefore, $\mathsf{H} \subseteq \mathsf{G}_\gamma$. Since H and G_γ both have full determinant and have the same intersection with $\mathrm{SL}_2(\widehat{\mathbb{Z}})$, we conclude that $\mathsf{H} = \mathsf{G}_\gamma$. $\square$

Let N be the least common multiple of levels of $\mathcal{G}$ in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and B in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$. We define $\mathsf{N}_1 := \mathsf{N}$ if N is odd and $\mathsf{N}_1 := \mathrm{lcm}(\mathsf{N}, 8)$ if N is even. Then

Theorem 4.3. Let S be the 2-power torsion in $\mathbb{Z}_\mathsf{N}^\times$. Then the following are equivalent:

(1) There is an open subgroup $\mathsf{G} \subseteq \mathcal{G}$ with $\mathsf{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = \mathsf{B}$ and $\det(\mathsf{G}) = \widehat{\mathbb{Z}}^\times$.

(2) There is a homomorphism $\beta\colon \mathsf{S} \to \mathcal{G}_\mathsf{N}/\mathsf{B}_\mathsf{N}$ such that $\det(\beta(a)) = a$ for all $a \in \mathsf{S}$.

(3) There is a homomorphism $\beta\colon \mathsf{S} \to \mathcal{G}(\mathsf{N}_1)/\mathsf{B}(\mathsf{N}_1)$ such that $\det(\beta(a)) \equiv a \pmod{\mathsf{N}_1}$ for all $a \in \mathsf{S}$.

Moreover, if a group G, as in (1) exists, then there is such a group whose level divides a power of 2 times N.

Proof. This is a special case of [Zyw24, Theorem 4.5] with $\mathsf{U} = \widehat{\mathbb{Z}}^\times$. $\square$

Theorem 4.4. Take $\mathsf{G}, \mathsf{H} \in \mathscr{F}(\mathcal{G}, \mathsf{B})$. Then

(1) X_G and X_H have the same genus.

(2) $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathsf{G}] = [\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathsf{H}]$.

Proof. (1) First note that $\Gamma_G = \Gamma_H$. Since $X_H(\mathbb{C})$ and $X_G(\mathbb{C})$ are both isomorphic to $\mathcal{X}_{\Gamma_G}$ as Riemann surfaces. The assertion follows.
(2) Let $N = \operatorname{lcm}(N_G, N_H)$ where N_G and N_H are the levels of G and H, respectively. Then we have $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G] = [\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : G]$ and $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : H] = [\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : H]$, so we can work in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. As subgroups of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, $|G| = |B| \cdot \phi(N)$ and $|H| = |B| \cdot \phi(N)$. □

For an open subgroup $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$, there is a natural choice of family for G.

Corollary 4.5. Let G be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and let $B = G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$. Let $\mathcal{G}$ be the agreeable closure of G. Then $G \in \mathscr{F}(\mathcal{G}, B)$.

Proof. We have $G \subseteq \mathcal{G}$. Since the commutator subgroups of G and $\mathcal{G}$ agree (Proposition 3.2), we have $[\mathcal{G}, \mathcal{G}] = [G, G] \subseteq B$, implying that $G \in \mathscr{F}(\mathcal{G}, B)$. □

Remark 4.6. An open subgroup G may lie in more than one family. However, Corollary 4.5 suggests a canonical choice of family that contains G, i.e the family $\mathscr{F}(\mathcal{G}, B)$ where $\mathcal{G}$ is the agreeable closure of G and $B = G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$. We have a description of $\mathcal{G}$ that depends on G and B. In particular, one can easily compute the group $\mathcal{G}$ and subsequently identify the family $\mathscr{F}(\mathcal{G}, B)$ which contains G.

5. Finiteness of Agreeable Subgroups

Fix a non-negative integer g. In this section, we recall a result from [Zyw24] that there are finitely many agreeable subgroups up to conjugacy, of genus less than or equal to g. We will also describe a method for computing all such agreeable subgroups. We first start by making some observations.

Let $\mathbf{G}$ be an agreeable subgroup of genus at most g. Let $H := \mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$; it is an open subgroup in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$. We have $-I \in H$. Let N be the level of H in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$. The associated congruence subgroup $\Gamma_G := H \cap \mathrm{SL}_2(\mathbb{Z})$ is the congruence subgroup of level N consisting of elements in $\mathrm{SL}_2(\mathbb{Z})$ whose image modulo N lies in H modulo N. Similarly we have that $-I \in \Gamma_G$, and Γ_G has genus at most g. In particular, [CP03] asserts that there are only finitely many congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ of genus less than g and contain $-I$. All such congruence subgroups of genus at most 24, up to conjugacy in $\mathrm{SL}_2(\mathbb{Z})$, are given in the [CP03] database.

In the proof, we will reverse this process and explain how to obtain the finitely many agreeable subgroups up to genus g arising from a congruence subgroup Γ of genus at most g.

Theorem 5.1. There are finitely many agreeable subgroups of $\mathrm{GL}_2 \widehat{\mathbb{Z}}$ with genus at most g.

Proof. Fix a genus g and fix a congruence subgroup Γ that has genus at most g and contains $-I$. There are finitely many such congruence subgroups. Consider the corresponding subgroup of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ which we call H. The level of H is equal to the level of Γ, which we call N. In particular H is the subgroup of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ whose image modulo N is equal to Γ modulo N.

We explain how the level of an agreeable subgroup $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ such that $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = H$ relates to the level of H. Let $N_1 := 2 \cdot \operatorname{lcm}(N, 12)$.

Lemma 5.2. Any agreeable subgroup $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ with $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = H$ has level dividing N_1.

Proof. See [Zyw24, Lemma 5.1].

□

Let Γ and H be as above. Assume $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ is an agreeable subgroup with $G \cap \mathrm{SL}(\widehat{\mathbb{Z}}) = H$. We have seen that G has level dividing N_1, so G corresponds to a subgroup $\bar{G}$ of $\mathrm{GL}_2(\mathbb{Z}/N_1\mathbb{Z})$ such that $\bar{G} \cap \mathrm{SL}_2(\mathbb{Z}/N_1\mathbb{Z}) = \bar{H}$ where $\bar{H}$ denotes the reduction to modulo N_1. There are only finitely many such subgroups of $\mathrm{GL}(\mathbb{Z}/N_1\mathbb{Z})$, so only finitely many agreeable subgroups of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ arise from a fixed congruence subgroup Γ. Since there are finitely many congruence subgroups Γ of genus less than g and contain $-I$, we conclude that there are finitely many agreeable subgroups with genus less than g. □

5.1. **Computing agreeable subgroups.** We explain how to explicitly compute all agreeable subgroups of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ of genus at most g. Let Γ and N_1 be as in the proof of 5.1. We first directly search in $\mathrm{GL}_2(\mathbb{Z}/N_1\mathbb{Z})$ for subgroups $\bar{G}$ with $(\mathbb{Z}/N_1\mathbb{Z})^\times \subseteq \bar{G}$, $\det(\bar{G}) = \mathbb{Z}/N_1\mathbb{Z}$, $-I \in \bar{G}$ and $\bar{G} \cap \mathrm{SL}(\mathbb{Z}/N_1\mathbb{Z}) = \bar{H}$. These groups give rise to finitely many, potentially agreeable, subgroups $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ such that $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = H$. For each such G, we then check if it is an agreeable subgroup, i.e. if its level in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ has the same odd prime divisors as the level of $\mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$.

We are ready to state the first part of Theorem 1.4 in terms of families of groups.

Theorem 5.3. Fix a non-negative integer g. There are only finitely many families of groups of genus g.

Proof. By Theorem 5.1, there are only finitely many agreeable subgroups of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ up to a fixed genus g. We denote this set by $\mathscr{A}_g$, which is stable under conjugation in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. For each agreeable subgroup $\mathcal{G} \in \mathscr{A}_g$, the groups $[\mathcal{G}, \mathcal{G}]$ and $\mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ are open subgroups of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$, hence there are only finitely many subgroups B of $\mathcal{G}$ such that $[\mathcal{G}, \mathcal{G}] \subseteq B \subseteq \mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$. Combining the finiteness of agreeable subgroups $\mathcal{G}$ of genus at most g and the finitely many subgroups B arising from $\mathcal{G}$, we get a finite set of pairs $(\mathcal{G}_i, B_i)$ and associated families $\mathscr{F}(\mathcal{G}_i, B_i)$.

Let G be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ of genus g with full determinant and $-I \in G$. By Corollary 4.5, G lies in the family $\mathscr{F}(\mathcal{G}, B)$ where $B = G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ and $\mathcal{G}$ is the agreeable closure of G. The agreeable closure $\mathcal{G}$ has genus at most g and so it is in the finite set $\mathscr{A}_g$. Hence, $\mathscr{F}(\mathcal{G}, B)$ is among the finite set of families $\mathscr{F}(\mathcal{G}_i, B_i)$ and these families cover the set of all open subgroups $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ of genus g with full determinant and $-I \in G$. □

6. Twisting Modular Curves

We have stated in §1.3 that a family of groups $\mathscr{F}(\mathcal{G}, B)$ corresponds to a family of twists of modular curves. In this section, we will describe the spaces of modular curves $M_{k,G}$ as we vary G in a family $\mathscr{F}(\mathcal{G}, B)$ and, consequently, describe how to twist the modular curves X_G.

Fix a nonempty family $\mathscr{F}(\mathcal{G}, B)$ and a group $G \in \mathscr{F}(\mathcal{G}, B)$ such that $\mathcal{G}$ is the agreeable closure of G. Let X_G be the modular curve associated to G, and let $\pi_G : X_G \to X_{\mathcal{G}}$ be the morphism coming from the inclusion $G \subseteq \mathcal{G}$. We start with a definition:

Definition 6.1. A $\mathcal{G}$–twist of (X_G, π_G) is a pair (Y, π) where Y is a curve over $\mathbb{Q}$, with a morphism $\pi : Y \to X_{\mathcal{G}}$ defined over $\mathbb{Q}$, such that there is an isomorphism $f : (X_G)_{\mathbb{Q}^{ab}} \to (Y)_{\mathbb{Q}^{ab}}$

that satisfies $\pi \circ f = \pi_G$. We call the pairs (X_G, π_G) and (Y, π) isomorphic if f is defined over $\mathbb{Q}$.

The group G is a normal subgroup of $\mathcal{G}$. The latter acts on $M_{k,G}$ for all $k > 0$ via the $*$ action of Lemma 2.1. By definition, G acts trivially on $M_{k,G}$ so there is an action of $\mathcal{G}/G$ on $M_{k,G}$. Consequently, $\mathcal{G}/G$ acts on X_G by Definition 2.3. The degree of π_G is $|\mathcal{G}/G|$, therefore we have $\mathrm{Aut}(X_G/X_{\mathcal{G}}) = \mathcal{G}/G$ where $\mathrm{Aut}(X_G/X_{\mathcal{G}})$ is the group of automorphisms f of the curve X_G that satisfy $\pi_G \circ f = \pi_G$. Note that these are modular automorphisms, and since there is a natural isomorphism $\mathcal{G}/G \simeq (\mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}))/B$, the automorphisms in $\mathrm{Aut}(X_G/X_{\mathcal{G}})$ are defined over $\mathbb{Q}$.

Let $\gamma : \widehat{\mathbb{Z}}^\times \to \mathcal{G}/G$ be a continuous homomorphism. By precomposing with the cyclotomic character χ_{cyc} we obtain a homomorphism

$$\xi := \gamma \circ \chi_{\mathsf{cyc}} : \mathrm{Gal}_{\mathbb{Q}^{\mathrm{ab}}} \to \mathcal{G}/G \cong \mathrm{Aut}(X_G/X_{\mathcal{G}}).$$

In particular, ξ is a 1-cocycle of X_G.

Lemma 6.2. There is a bijection between isomorphism classes of $\mathcal{G}-$twists of X_G and $H^1(\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}), \mathrm{Aut}(X_G/X_{\mathcal{G}}))$.

Proof. Let $(X, \pi_X) := (X_G, \pi_G)$, and let (Y, π_Y) be a $\mathcal{G}-$twist of (X, π_X). So there is an isomorphism $f : X_{\mathbb{Q}^{\mathrm{ab}}} \to Y_{\mathbb{Q}^{\mathrm{ab}}}$ such that $\pi_Y \circ f = \pi_X$. Let $\xi : \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}) \to \mathsf{Aut}(X, \pi_X)$ be defined as $\xi_\sigma = f^{-1} \circ \sigma(f)$. One can check that ξ is a 1-cocycle. We have $\pi_X \circ \xi_\sigma = \pi_X \circ f^{-1} \circ \sigma(f) = \pi_Y \circ \sigma(f) = \sigma(\pi_Y \circ f) = \sigma(\pi_X) = \pi_X$, because π_X and π_Y are defined over $\mathbb{Q}$. We define the map λ such that $\lambda((Y, \pi_Y)) = [\xi]$.

Let's first show that λ is well defined and does not depend on the choice of the isomorphism. Let $g : X_{\mathbb{Q}^{\mathrm{ab}}} \to Y_{\mathbb{Q}^{\mathrm{ab}}}$ be another such isomorphism. Then $f^{-1} \circ \sigma(f)$ and $g^{-1} \circ \sigma(g)$ are cohomologous, so the class of the cocycle is well defined.

Let Y and Z be two curves that are isomorphic over $\mathbb{Q}$ with a map $h : Y \to Z$ such that $\pi_Z \circ h = \pi_Y$. Then we have an isomorphism $h \circ f : X_{\mathbb{Q}^{\mathrm{ab}}} \to Z_{\mathbb{Q}^{\mathrm{ab}}}$ satisfying $\pi_Z \circ h \circ f = \pi_X$. Looking at associated cocycles, we have $(h \circ f)^{-1} \circ \sigma(h \circ f) = f^{-1} \circ h^{-1} \circ \sigma(h) \circ \sigma(f) = f^{-1} \circ \sigma(f)$ because h is defined over $\mathbb{Q}$. So, the $[\xi]$ is independent of the $\mathbb{Q}$ isomorphism class of Y.

Let ξ_1 and ξ_2 be two cocycles that are cohomologous corresponding to Y_1 and Y_2. This means that there is $T \in \mathrm{Aut}(X_G/X_{\mathcal{G}})$ such that $\xi_1(\sigma) = T^{-1} \circ \xi_2(\sigma) \circ \sigma(T)$. Then $f_2 \circ T \circ f_1^{-1} : Y_1 \to Y_2$ is an isomorphism defined over $\mathbb{Q}$, proving the injectivity of λ.

To show surjectivity, let $[\xi]$ be a class in $H^1(\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}), \mathrm{Aut}(X_G, X_{\mathcal{G}}))$. By Galois descent we get a nice curve Y over $\mathbb{Q}$ with an isomorphism $f : X_{\mathbb{Q}^{\mathrm{ab}}} \to Y_{\mathbb{Q}^{\mathrm{ab}}}$ where $\sigma \to f^{-1} \circ \sigma(f)$ is cohomologous to ξ [Ser02, Chapter III, Proposition 5]. Precisely this means that there is $T \in \mathrm{Aut}(X_G/X_{\mathcal{G}})$ such that $f^{-1} \circ \sigma(f) = T^{-1} \circ \xi_\sigma \circ \sigma(T)$. Set $g = f \circ T^{-1}$. We have $g^{-1} \circ \sigma(g) = \xi_\sigma$. Define $\pi_Y := \pi_X \circ g^{-1}$. Note that we have $\pi_X \circ \xi_\sigma = \pi_X$. Let $P \in Y_{\mathbb{Q}^{\mathrm{ab}}}$ let $Q = g^{-1}(\sigma^{-1}(P))$ and $P' := \sigma^{-1}(P)$. We have

$$\sigma(\pi_Y)(P) = \sigma(\pi_X(g^{-1}(P')))$$

π_X is defined over $\mathbb{Q}$ so

$$\sigma(\pi_X)(g^{-1}(P')) = \pi_X(\sigma(g^{-1}(P'))) = \pi_X(\sigma(g^{-1})(P))$$

which is equal to

$$\pi_X(\xi_\sigma^{-1} \circ g^{-1}(P)) = \pi_X(g^{-1}(P)) = \pi_Y(P).$$

Hence $\pi_Y = \sigma(\pi_Y)$ and (Y, π_Y) is the associated $\mathcal{G}$-twist of X.

$\square$

Let $\gamma : \widehat{\mathbb{Z}}^\times \to \mathcal{G}/\mathsf{G}$ be a continuous homomorphism and let $\xi : \mathrm{Gal}_{\mathbb{Q}^{ab}} \to \mathcal{G}/\mathsf{G} \cong \mathrm{Aut}(X_\mathsf{G}/X_\mathcal{G})$ be the associated cocycle by precomposing with the cyclotomic character. Twisting via this cocycle, we get a $\mathcal{G}$-twist $((X_\mathsf{G})_\xi, (\pi_\mathsf{G})_\xi)$. We prove that $((X_\mathsf{G})_\xi, (\pi_\mathsf{G})_\xi)$ is isomorphic to $(X_{\mathsf{G}_\gamma}, \pi_{\mathsf{G}_\gamma})$, where G_γ is the group defined in §4.

Observe that $\mathsf{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = \mathsf{G}_\gamma \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = \mathsf{B}$. Hence, from the definition of $M_{k,\mathsf{G}}$ in §2, we get the following equalities

$$M_{k,\mathsf{B}} = M_{k,\mathsf{G}} \otimes_\mathbb{Q} \mathbb{Q}^{ab} = M_{k,\mathsf{G}_\gamma} \otimes_\mathbb{Q} \mathbb{Q}^{ab}.$$

Let $g \in \mathcal{G}$ be an element and let $\sigma \in \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$ be such that $\chi_{cyc}(\sigma) = \det(g)$. The group $\mathcal{G}$ acts on $M_{k,\mathsf{G}} \otimes_\mathbb{Q} \mathbb{Q}^{ab}$ where g sends $f \otimes c$ to $(f * g) \otimes \sigma(c)$.

Denote by cf, the element $f \otimes c \in M_{k,\mathsf{G}} \otimes_\mathbb{Q} \mathbb{Q}^{ab}$. We define twisted action of $\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$ on $M_{k,\mathsf{G}} \otimes_\mathbb{Q} \mathbb{Q}^{ab}$ by $\sigma \bullet (cf) := \sigma(c)(\xi_\sigma(f))$ where $\xi_\sigma(f)$ denotes the action of $\mathcal{G}/\mathsf{G}$ on $M_{k,\mathsf{G}}$ via the cocycle. For each $k \geqslant 0$, we define the twisted space $(M_{k,\mathsf{G}})_\xi$ by

$$(M_{k,\mathsf{G}})_\xi = \{f \in M_{k,\mathsf{G}} \otimes_\mathbb{Q} \mathbb{Q}^{ab} \mid \sigma \bullet f = f \text{ for all } \sigma \in \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})\}.$$

Restricting the action of $\mathcal{G}$ to G and G_γ, we obtain the induced actions of G/B and $\mathsf{G}_\gamma/\mathsf{B}$ on $M_{k,\mathsf{G}} \otimes_\mathbb{Q} \mathbb{Q}^{ab}$. Composing these with the isomorphisms

$$\varphi_1 \colon \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \to \widehat{\mathbb{Z}}^\times \xrightarrow{\det^{-1}} \mathsf{G}/\mathsf{B}$$

and

$$\varphi_2 \colon \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \to \widehat{\mathbb{Z}}^\times \xrightarrow{\det^{-1}} \mathsf{G}_\gamma/\mathsf{B}$$

we get two different Galois actions of $\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$ on $M_{k,\mathsf{G}} \otimes_\mathbb{Q} \mathbb{Q}^{ab}$ and hence on $M_{k,\mathsf{B}}$.

It is important that the action $\bullet$ of $\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$ and the action of $\mathsf{G}_\gamma/\mathsf{B}$ on $M_{k,\mathsf{G}} \otimes_\mathbb{Q} \mathbb{Q}^{ab}$ are compatible in the following sense.

Lemma 6.3. If $\sigma \in \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$ and $g \in \mathsf{G}_\gamma$ with $\det(g) = \chi_{cyc}(\sigma)$ then $\sigma \bullet f = f * g$ for all $f \in M_{k,\mathsf{G}} \otimes_\mathbb{Q} \mathbb{Q}^{ab}$.

Proof. Let $cf := f \otimes c \in M_{k,\mathsf{G}} \otimes_\mathbb{Q} \mathbb{Q}^{ab}$. We have $\sigma \bullet (cf) = \sigma(c)(\xi_\sigma(f)) = (\xi_\sigma(f)) \otimes \sigma(c)$. Let g be as in the statement of the lemma. Then we have that

$$\xi_\sigma = \gamma(\det(g)) = g\mathsf{G}$$

in $\mathcal{G}/\mathsf{G}$.

Hence $(cf) * g = \sigma(c)(f * g) = f * g \otimes \sigma(c) = \xi_\sigma(f) \otimes \sigma(c) = \sigma \bullet (cf)$. ☐

Theorem 6.4. Let $\gamma : \widehat{\mathbb{Z}}^\times \to \mathcal{G}/\mathsf{G}$ be a continuous homomorphism. Let $\xi = \gamma \circ \chi_{cyc} : \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \to \mathcal{G}/\mathsf{G}$ be the associated cocycle. Then $(M_{k,\mathsf{G}})_\xi = M_{k,\mathsf{G}_\gamma}$.

Proof. Let $f \in M_{k,\mathsf{G}_\gamma}$. Then for all $\sigma \in \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$ and $g \in \mathsf{G}_\gamma$ such that $\det(g) = \chi_{cyc}(\sigma)$, we have $\sigma \bullet f = f * g = f$, which implies that $f \in (M_{k,\mathsf{G}})_\xi$.

For the converse, let $f \in (M_{k,\mathsf{G}})_\xi$. Then for all $g \in \mathsf{G}_\gamma$ and $\sigma \in \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$ such that $\det(g) = \chi_{cyc}(\sigma)$, we have $f * g = \sigma \bullet f = f$. Hence $f \in M_{k,\mathsf{G}_\gamma}$. ☐

The action $\bullet$ on $M_{k,\mathsf{G}} \otimes_\mathbb{Q} \mathbb{Q}^{ab}$ induces an action of $\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$ on the $\mathbb{Q}^{ab}$-algebra $\bigoplus_{k=0}^\infty M_{k,\mathsf{G}} \otimes_\mathbb{Q} \mathbb{Q}^{ab}$. We define

$$(R_\mathsf{G})_\xi := \bigoplus_{k=0}^\infty (M_{k,\mathsf{G}})_\xi.$$

We immediately get the following:

Corollary 6.5. With notation as above, the pair $(X_{G_\gamma}, \pi_{G_\gamma})$ is isomorphic to $((X_G)_\xi, (\pi_G)_\xi)$.

Proof. By definition, we have $X_{G_\gamma} = \mathrm{Proj}(\bigoplus_{k=0}^{\infty} M_{k,G_\gamma})$, where the nonconstant map π_{G_γ} is induced by the inclusion $M_{k,G_\gamma} \subseteq M_{k,\mathcal{G}}$. The $\mathcal{G}$-twist $((X_G)_\xi, (\pi_G)_\xi)$ is isomorphic to $(\mathrm{Proj}((R_G)_\xi), \pi)$, where π is induced by the inclusion $(M_{k,G})_\xi \subseteq M_{k,\mathcal{G}}$. Theorem 6.4 implies that these two pairs are isomorphic. □

We conclude from Corollary 6.5 our family of groups $\mathscr{F}(\mathcal{G}, B)$ in fact corresponds to a family of abelian twists of modular curves, i.e. it consists of curves of the form $X_{G_\gamma} \simeq (X_G)_\xi$.

We denote by $\mathscr{F}_g$ finitely many families of modular curves of genus at most g, arising from the set of agreeable subgroups $\mathscr{A}_g$. The set $\mathscr{F}_g$ has been computed for $g = 24$ [Kar25].

6.0.1. *Getting a basis for* M_{k,G_γ}. Assume that, using the methods described in §2.7, we have an explicit basis $\mathcal{B} := \{f_0, \cdots, f_d\}$ for $M_{k,G}$. In particular, one can use Eisenstein series of weight 1 to compute such a basis, cf. [KM12] and [Zyw22, Algorithm 4.14]. The group $\mathcal{G}/G$ is finite and abelian. It also acts on $M_{k,G}$ via $\mathbb{Q}$-linear automorphisms. We can compute the action of any $gG \in \mathcal{G}/G$ on the basis $\mathcal{B}$ and get a matrix in $\mathrm{GL}_{d+1}(\mathbb{Q})$. Hence, for any 1-cocycle $\xi : \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \to \mathcal{G}/G$, we get a cocycle

$$\bar{\xi} : \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \to \mathrm{GL}_{d+1}(\mathbb{Q}).$$

By Hilbert 90, $\mathrm{H}^1(\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}), \mathrm{GL}_{d+1}(\mathbb{Q}^{\mathrm{ab}}))$ is the trivial group, so there exists a matrix $A \in \mathrm{GL}_{d+1}(\mathbb{Q}^{\mathrm{ab}})$ such that $\bar{\xi}(\sigma) = A^{-1}\sigma(A)$ for every $\sigma \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$.

Let $f \in M_{k,G}$ be a modular form. Let ν be its corresponding coordinate vector with respect to the basis $\mathcal{B}$. Consider the modular form $g \in M_{k,G} \otimes_{\mathbb{Q}} \mathbb{Q}^{\mathrm{ab}}$ with the coordinate vector $\nu \cdot A^{-1} \in (\mathbb{Q}^{\mathrm{ab}})^{\dim_{\mathbb{Q}}(M_{k,G})}$. The $\bullet$ action on $M_{k,G} \otimes_{\mathbb{Q}} \mathbb{Q}^{\mathrm{ab}}$ gives an action on the vector space $(\mathbb{Q}^{\mathrm{ab}})^{\dim_{\mathbb{Q}}(M_{k,G})}$ with respect to the basis $\mathcal{B}$. For all $\sigma \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$, we have that

$$\sigma \bullet (\nu \cdot A^{-1}) = (\sigma \bullet \nu) \cdot \sigma(A^{-1}) = \nu \cdot \bar{\xi}_\sigma \cdot \sigma(A^{-1}) = \nu \cdot A^{-1}\sigma(A)\sigma(A^{-1}) = \nu \cdot A^{-1}.$$

Hence, f is a modular form in M_{k,G_γ}. Applying the matrix A^{-1} on the basis $\mathcal{B}$, we get a set of modular forms $\mathcal{B}'$ which forms a basis of M_{k,G_γ}.

6.1. **Twisting the models of modular curves.** Assume that we have an explicit smooth projective model $C \subseteq \mathbb{P}^r_{\mathbb{Q}}$ for X_G, obtained from a very ample sheaf as in §2.7, where $G \in \mathscr{F}(\mathcal{G}, B)$. The model C arises from linearly independent modular forms $f_0, \ldots, f_r \in V \subseteq M_{k,G}$ as explained in §2.7. The $\mathbb{Q}$-vector space V is chosen so that there is an action of $\mathcal{G}/G$ on V. In particular C is defined by $F_1, \ldots, F_s \in \mathbb{Q}[x_0, \ldots, x_r]$ where $F_i(f_0, \ldots, f_r) = 0$. Let γ and ξ be as above. Let $(F_i)_\xi := F_i((x_0, \ldots, x_r)A^T)$.

Theorem 6.6. The curve C' defined by $(F_1)_\xi, \ldots, (F_s)_\xi$ is defined over $\mathbb{Q}$ and is isomorphic to the twist of C by ξ. In particular C' is a model of X_{G_γ}.

Proof. First, observe that ξ_σ is an automorphism of X_G defined over $\mathbb{Q}$ and so that each $\overline{\xi}(\sigma)$ is an automorphism of the model C of the modular curve X_G. The map $\overline{\xi}$ is a group homomorphism and $\overline{\xi}(\sigma)$ fixes the polynomials F_i for $i = 1, \ldots, s$.

Let $\mathcal{B}$:=$\{f_0, \ldots, f_r\}$ be the basis of V as above. Applying A^{-1} to the basis $\mathcal{B}$ as in 6.0.1, we get a basis $\mathcal{B}'$ for a vector space V_γ which is acted on by $\mathcal{G}$. The space V_γ is associated to a sheaf $\mathcal{F}_\gamma$ on X_{G_γ} which is very ample. The polynomials $(F_i)_\xi$ satisfy the basis $\mathcal{B}'$, so C' is isomorphic to X_{G_γ} over $\mathbb{Q}$. Hence, the ideal $\langle (F_i)_\xi \rangle \subseteq \mathbb{Q}[x_0, \ldots, x_r]$ is defined over $\mathbb{Q}$. □

6.1.1. *Computing the matrix* A. In practice, we work over the field $\mathbb{Q}(\zeta_N)$ to obtain a basis for M_{k,G_γ} where N is the least common multiple of the levels of G and $\ker(\gamma)$. The Hilbert 90 Theorem states that $H^1(\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}), \mathrm{GL}_n(\mathbb{Q}(\zeta_N))$ is the trivial group so given a cocycle η, there exists a matrix $A \in \mathrm{GL}_n(\mathbb{Q}(\zeta_N))$ such that $\eta(\sigma) = A^{-1}\sigma(A)$.

This matrix can be explicitly computed. In practice, we are using the algorithm and implementation given in [Rak24, §5.3].

7. The Algorithm

In this section, we put together the work done in previous sections and describe an algorithm to compute a projective model of a modular curve X_G where $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ is an open subgroup with genus at most g for a fixed natural number g.

Our algorithm has two parts. The families mentioned in Theorem 7.5 must be computed along with a chosen representative for each family. Using these precomputed data, we then provide an algorithm that, given a modular curve X_G, finds the family of groups it lies in, computes the cocycle with respect to the representative, and twists the representative curve to get a projective model of X_G.

Algorithm 7.1 (Precomputation).

(i) Compute $\mathscr{A}_g$, the set of all the agreeable subgroups of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ whose genus is at most g. In subsection 5.1, we have described an algorithm for computing them. In practice, we only compute $\mathscr{A}_g$ up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

(ii) For each $\mathcal{G} \in \mathscr{A}_g$, compute the subgroups B such that $[\mathcal{G}, \mathcal{G}] \subseteq B \subseteq \mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$. Note that $[\mathcal{G}, \mathcal{G}]$ and $\mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ are open subgroups of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$, so for each agreeable subgroup there are only finitely many such subgroups B.

(iii) Form all the possible families (up to conjugacy) $\mathscr{F}(\mathcal{G}, B)$. We call this set $\mathcal{F}_g$.

(iv) For each family in $\mathscr{F}_g$, determine if the family is empty or not. If it is not empty find a representative $W \in \mathscr{F}(\mathcal{G}, B)$. Empty families can be discarded.

(v) Take a family $\mathscr{F}(\mathcal{G}, B)$ and the representative W. Compute a model $C \subseteq \mathbb{P}^{d+1}_{\mathbb{Q}}$ of X_W and the associated relative j-map $\pi_W : X_W \to X_{\mathcal{G}}$ via the methods described in §2. Since W is a normal subgroup of $\mathcal{G}$, we are in the situation of §2.7.2, where $\mathcal{G}/W$ maps into $\mathrm{GL}_{d+1}(\mathbb{Q})$ and its action on $\mathbb{P}^{d+1}_{\mathbb{Q}}$ stabilizes C. In particular, we have modular forms $f_0, ..., f_d \in M_{k,G}$ for suitable k, and C is defined by homogeneous polynomials $F_1, \cdots, F_s \in \mathbb{Q}[x_0, \cdots, x_d]$ such that $F_i(f_0, \cdots, f_d) = 0$ for $i = 1, \cdots, s$. To do this computation, we are using the algorithm given by Zywina in [Zyw22].

Remark 7.2. Here are some remarks about the precomputation:

- If two open subgroups $G, G' \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ are conjugate to each other in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, then X_G and $X_{G'}$ are isomorphic over $\mathbb{Q}$. Therefore, it is enough to consider the agreeable subgroups and families of modular curves up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.
- For the first step, we start from the data of congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ which is given in [CP03] for $g \leqslant 24$. Hence we obtain the set $\mathscr{A}_g$ for $g = 24$.
- Theorem 4.3 gives a criterion for checking whether a family is empty or not. Based on this theorem, an implementation is given in [Zyw24] to find a representative in $\mathscr{F}(\mathcal{G}, B)$.

- Algorithm 7.1 (v) is, computationally, the most expensive part of the precomputation as it includes the computation of Eisenstein series (and their q-expansions for possibly high precision) that span $M_{k,W}$ for a certain $k \in \mathbb{N}$.

Computing the models: After the precomputation, one can use the following algorithm to compute a projective model of X_G. It takes an open subgroup $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ with full determinant and $-I \in G$ as input.

Algorithm 7.3. Let $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ be an open subgroup where X_G genus at most g. This algorithm computes a model $C \subseteq \mathbb{P}^d_{\mathbb{Q}}$ of the modular curve X_G.

(i) Compute $B := G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ and the agreeable closure of G, which we call $\mathcal{G}$.

(ii) By Theorem 5.3, $\mathcal{G}$ is in $\mathscr{A}_g$, possibly up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. If necessary, conjugate G, $\mathcal{G}$ and B, and replace them with their suitable conjugates so $\mathcal{G} \in \mathscr{A}_g$. Find the family $\mathscr{F}(\mathcal{G}, B) \in \mathscr{F}_g$.

(iii) Since $\mathscr{F}(\mathcal{G}, B)$ is not empty, we have precomputed a representative $W \in \mathscr{F}(\mathcal{G}, B)$. Compute the homomorphism $\gamma : \widehat{\mathbb{Z}}^\times \cong G/B \to \mathcal{G}/W$. Then G is equal to W_γ by Theorem 4.2.

(iv) Compute the associated cocycle ξ by precomposing with the cyclotomic character χ_{cyc} and the related cocycle $\bar{\xi}$ as in §6.0.1.

(v) Compute the Hilbert 90 matrix A, as described in §6.1.1.

(vi) Apply the matrix A^T to the polynomials defining X_W to get polynomials $(F_1)_\xi, \cdots, (F_s)_\xi$. These have coefficients in $\mathbb{Q}^{\mathrm{ab}}$ but are defined over $\mathbb{Q}$.

(vii) By Theorem 6.6, the curve $C_\xi \subseteq \mathbb{P}^{d+1}_{\mathbb{Q}}$ defined by $(F_i)_\xi$ is a projective model of X_G defined over $\mathbb{Q}$. By [Zyw22, §5.3.2], $I(C_\xi)$ is generated by $I(C_\xi)_2 \cup I(C_\xi)_3 \cup I(C_\xi)_4$. Find a $\mathbb{Q}$-basis for $I(C_\xi)_m$ for $m \in \{2, 3, 4\}$ by Galois descent.

Remark 7.4. Let G be the input of our algorithm, and let N be its level. Let N_1, N_2 be the levels of $\mathcal{G}$ and W, respectively. The level of G is not bounded in terms of N_1 and N_2, it can be arbitrarily big. We do most of our computations modulo $\mathrm{lcm}(N_1, N_2)$. The level N is only used for computing the cocycle $(\mathbb{Z}/N\mathbb{Z})^\times \to \mathcal{G}/W$.

This algorithm has been implemented for $g = 12$ in [Kar25]. Combining our algorithm with previous results, we restate Theorem 1.4 in terms of modular curves.

Theorem 7.5. Fix a non-negative integer g.

(1) There are only finitely many families of modular curves of genus g. These families are effectively computable.

(2) There is an effective algorithm that takes as input a modular curve X_G of genus g and outputs a projective curve $C \subseteq \mathbb{P}^r_{\mathbb{Q}}$ for some $r > 0$ such that C is isomorphic to X_G.

Proof. By Corollary 6.5, the family of groups mentioned in Theorem 5.3 corresponds to a family of twists of modular curves. The algorithm is explained in Algorithm 7.3. □

8. $\mathbb{Q}$-gonality 2 Modular Curves

We refer to [Poo07] and [Zyw25] for general facts about gonality of curves.

Let $\mathscr{F}(\mathcal{G}, B)$ be a family of modular curves. Note that for all modular curves $X \in \mathscr{F}(\mathcal{G}, B)$, the corresponding congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ are the same. In [Zyw25], it is shown that there are only finitely many congruence subgroups Γ of $\mathrm{SL}_2(\mathbb{Z})$ such that X_Γ has geometric gonality 2. In particular, all such for all such congruence subgroups X_Γ has genus at most 11. A complete list of such congruence subgroups can be found in terms of Cummins-Pauli labels in the classification of [CP03] in [Zyw25].

The finitely many congruence subgroups give rise to finitely many families of geometrically hyperelliptic modular curves in the sense of §4 and §5. Note that we call these families geometrically hyperelliptic because all the modular curves in the family are hyperelliptic considered as curves over $\mathbb{C}$.

Assume that $X_G \in \mathscr{F}$ is a modular curve that has geometric gonality 2. The curve X_G corresponds to one of the congruence subgroups in Zywina's classification. The canonical model of X_G gives a degree 2 morphism $\varphi\colon X_G \to C \subseteq \mathbb{P}^{g-1}_{\mathbb{Q}}$ where C is a genus 0 curve. If the curve C has a rational point then it is isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$ and X_G has $\mathbb{Q}-$gonality 2. Let $X_H = X_{G_\gamma} \in \mathscr{F}$ be a modular curve distinct from X_G.

8.0.1. *Computing gonality:* The canonical model of X_G can be computed as described in §2.7. In particular, it is computed using the space of modular forms $S_{2,G}$ which is acted on by $\mathcal{G}$, the agreeable closure of G. The twisting process of §6 can be used to compute the space $S_{2,H}$. As a result the map $\varphi_\xi : X_{G_\gamma} \to C_\xi$ gives the canonical map φ_H and the genus 0 curve $C_H := C_\xi$ for X_H. Before continuing, we state the following useful result.

Proposition 8.1 (Castelnuovo-Severi Inequality)**.** Let k be a perfect field. Let F, F_1, F_2 be function fields of curves over k of genera g, g_1, g_2 respectively. Suppose $F_i \subseteq F$ for $i = 1, 2$ and the compositum of F_1 and F_2 in F is F. Let $d_i = [F : F_i]$ for $i = 1, 2$. Then

$$g \leqslant g_1 d_1 + g_2 d_2 + (d_1 - 1)(d_2 - 2)$$

Proof. See [Sti93, III.10.3]. □

Many useful facts follow from the Castelnuovo-Severi inequality. In particular, it implies that if C is a nice curve with $g \geqslant 2$, then there is at most one morphism $C \to Y$ of degree 2, where Y is a genus 0 curve.

Proposition 8.2. Assume $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ such that $-I \in G$ and $\det(G) = \widehat{\mathbb{Z}}^\times$ with genus g. Assume also that X_G has $\overline{\mathbb{Q}}-$gonality 2 and $g > 2$. There is an efficient and implemented algorithm to determine the $\mathbb{Q}-$gonality of the modular curve X_G.

Proof. We first explain how to compute the $\mathbb{Q}$-gonality from the canonical map. Let C be the image of the canonical map of X_G. Since X_G is geometrically hyperelliptic, C is a curve of genus 0. If it contains a rational point then X_G has $\mathbb{Q}$-gonality 2. One can check whether this is the case by using the Hasse principle.

Assume now that C has no rational points. Then the map $\varphi : X_G \to C$ is unique up to an automorphism of C, i.e. there is no other genus 0 curve C' with $\pi' : X_G \to C'$ of degree 2. To prove this, assume there is such a curve. Applying the Castelnuovo-Severi inequality to the maps π, π' we get $g \leqslant 1$, which is a contradiction.

Since C has no rational points, it must not have $\mathbb{Q}$-gonality 2. Castelnuovo-Severi inequality applied to X_G, C and $\mathbb{P}^1_{\mathbb{Q}}$ shows that X_G cannot have gonality 3. We conclude that X_G has $\mathbb{Q}-$gonality 4.

To compute the canonical map, one computes the space of cusp forms $S_{2,G}$. In practice, this can be computationally expensive as the level of G increases. We avoid this computation as follows. By [Zyw25, Table 1.1], X_G has genus at most 11. Hence, the curve X_G lies in a family $\mathscr{F}(\mathcal{G}, B)$ which has been computed along with a representative X_H, a model for X_H and the canonical map $\varphi : X_H \to C$[Kar25]. Twisting the map φ with the cocycle ξ as explained in §6, we get the canonical map $\varphi_\xi : X_G \to C_\xi$. Afterwards, we check the existence of rational points on C_ξ to compute the $\mathbb{Q}$-gonality of X_G as explained above. Therefore, our implementation does not explicitly compute cusp forms for G. Instead, we twist the precomputed canonical map $\varphi : X_H \to C$ to obtain the canonical map of X_G, which significantly improves the efficiency of computing $\mathbb{Q}$-gonality of X_G. $\square$

This algorithm has been implemented in [Kar25].

References

[BBH+25] Jennifer S. Balakrishnan, L. Alexander Betts, Daniel Rayor Hast, Aashraya Jha, and J. Steffen Muller, *Rational points on the non-split Cartan modular curve of level 27 and quadratic Chabauty over number fields* (2025). arXiv:2501.07833 [math.NT]. ↑8

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. Computational algebra and number theory (London, 1993). ↑1, 8

[BDM+19] Jennifer Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk, *Explicit Chabauty-Kim for the split Cartan modular curve of level 13*, Ann. of Math. (2) **189** (2019), no. 3, 885–944, DOI 10.4007/annals.2019.189.3.6. MR3961086 ↑7

[BDM+23] Jennifer S. Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk, *Quadratic Chabauty for modular curves: algorithms and examples*, Compos. Math. **159** (2023), no. 6, 1111–1152, DOI 10.1112/s0010437x23007170. MR4589060 ↑7

[BN19] François Brunault and Michael Neururer, *Fourier expansions at cusps*, The Ramanujan Journal (2019). ↑11

[BPR13] Yuri Bilu, Pierre Parent, and Marusia Rebolledo, *Rational points on* $X_0^+(p^r)$, Ann. Inst. Fourier (Grenoble) **63** (2013), no. 3, 957–984, DOI 10.5802/aif.2781 (English, with English and French summaries). MR3137477 ↑7

[CP03] C. J. Cummins and S. Pauli, *Congruence subgroups of* $\mathrm{PSL}(2, \mathbb{Z})$ *of genus less than or equal to 24*, Experiment. Math. **12** (2003), no. 2, 243–255. ↑7, 16, 21, 23

[DR73] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Lecture Notes in Math., vol. Vol. 349, Springer, Berlin-New York, 1973, pp. 143–316 (French). MR0337993 ↑2

[DS05] Fred Diamond and Jerry Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005. MR2112196 ↑9, 10

[Kar25] Eray Karabiyik, *Repository for classification*, 2025. `https://github.com/eekarabiyik/twist`. ↑1, 8, 20, 22, 24

[Kat73] Nicholas M. Katz, *p-adic properties of modular schemes and modular forms*, Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1973, pp. 69–190. Lecture Notes in Mathematics, Vol. 350. ↑

[KM85] Nicholas M. Katz and Barry Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, vol. 108, Princeton University Press, Princeton, NJ, 1985. MR0772569 ↑2

[KM12] Kamal Khuri-Makdisi, *Moduli interpretation of Eisenstein series*, Int. J. Number Theory **8** (2012), no. 3, 715–748, DOI 10.1142/S1793042112500418. MR2904927 ↑20

[LMF] LMFDB, *The L-functions and modular forms database*. `https://www.lmfdb.org`. ↑1

[MR25] Jacob Mayle and Jeremy Rouse, *Rational maps from Modular Curves To Elliptic Curves*, 2025. `https://github.com/rouseja/ModCrvToEC`. ↑8

[Maz77a] B. Mazur, *Rational points on modular curves*, Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), Lecture Notes in Math., vol. Vol. 601, Springer, Berlin-New York, 1977, pp. 107–148. MR0450283 ↑6

[Maz77b] ———, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186 (1978). With an appendix by Mazur and M. Rapoport. MR0488287 ↑7

[Maz78] ———, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162, DOI 10.1007/BF01390348. MR0482230 ↑7

[Mum70] David Mumford, *Varieties defined by quadratic equations*, Questions on Algebraic Varieties (C.I.M.E., III Ciclo, Varenna, 1969), Centro Internazionale Matematico Estivo (C.I.M.E.), Ed. Cremonese, Rome, 1970, pp. 29–100. MR0282975 ↑13

[Poo07] Bjorn Poonen, *Gonality of modular curves in characteristic* $\mathfrak{p}$, Math. Res. Lett. **14** (2007), no. 4, 691–701, DOI 10.4310/MRL.2007.v14.n4.a14. MR2335995 ↑22

[Rak24] Rakvi, *A classification of genus 0 modular curves with rational points*, Math. Comp. **93** (2024), no. 348, 1859–1902, DOI 10.1090/mcom/3907. MR4730250 ↑8, 21

[RZB15] Jeremy Rouse and David Zureick-Brown, *Elliptic curves over* $\mathbb{Q}$ *and 2-adic images of Galois*, Res. Number Theory **1** (2015), Paper No. 12, 34, DOI 10.1007/s40993-015-0013-7. MR3500996 ↑8

[RSZB22] Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown, *ℓ-adic images of Galois for elliptic curves over* $\mathbb{Q}$ *(and an appendix with John Voight)*, Forum Math. Sigma **10** (2022), Paper No. e62, 63, DOI 10.1017/fms.2022.38. With an appendix with John Voight. MR4468989 ↑8

[Ser72] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331. ↑1

[Ser02] Jean-Pierre Serre, *Galois cohomology*, English edition, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002. Translated from the French by Patrick Ion and revised by the author. MR1867431 ↑18

[Shi94] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original; Kanô Memorial Lectures, 1. MR1291394 ↑

[Sti93] Henning Stichtenoth, *Algebraic function fields and codes*, Universitext, Springer-Verlag, Berlin, 1993. MR1251961 ↑23

[SZ17] Andrew V. Sutherland and David Zywina, *Modular curves of prime-power level with infinitely many rational points*, Algebra Number Theory **11** (2017), no. 5, 1199–1229, DOI 10.2140/ant.2017.11.1199. MR3671434 ↑8

[VZB22] John Voight and David Zureick-Brown, *The canonical ring of a stacky curve*, Mem. Amer. Math. Soc. **277** (2022), no. 1362, v+144, DOI 10.1090/memo/1362. MR4403928 ↑12

[Zyw20] David Zywina, *Computing actions on cusp forms* (2020). arXiv:2001.07270 [math.NT]. ↑13

[Zyw22] ———, *Explicit Open Images For Elliptic Curves Over* $\mathbb{Q}$ (2022). arXiv:2206.14959 [math.NT]. ↑2, 3, 4, 7, 9, 10, 11, 12, 13, 14, 15, 20, 21, 22

[Zyw24] ———, *Open image computations for elliptic curves over number fields* (2024). arXiv:2403.16147 [math.NT]. ↑7, 13, 15, 16, 17, 21

[Zyw25] ———, *Classification of Modular Curves With Low Gonality* (2025). https://pi.math.cornell.edu/ zywina. ↑22, 23, 24

Department of Mathematics, Cornell University, Ithaca, NY 14853, USA
Email address: ek693@cornell.edu