A CLASSIFICATION OF LOW GENUS MODULAR CURVES

ERAY KARABIYIK

ABSTRACT. Let G be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ satisfying $\det(G) = \widehat{\mathbb{Z}}^\times$ and $-I \in G$. Associated to G, there is a modular curve X_G defined over $\mathbb{Q}$, which weakly 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 for computing 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 $E[N]$ be the N-torsion of $E(\overline{\mathbb{Q}})$, it is a free $(\mathbb{Z}/N\mathbb{Z})-$module of rank 2. The group $\mathrm{Gal}_{\mathbb{Q}}$ acts naturally on $E[N]$ and respects the group structure. This gives rise to a Galois representation

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

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

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

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 $\rho_E(\mathrm{Gal}_{\mathbb{Q}})$ is a closed subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ with respect to the profinite topology. In [Ser72], Serre proved that $\rho_E(\mathrm{Gal}_{\mathbb{Q}})$ is an open subgroup $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

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 $\det \circ \rho_E$ agrees with χ_{cyc}, and hence the image of ρ_E has full determinant i.e, $\det(\rho_E(\mathrm{Gal}_{\mathbb{Q}})) = \widehat{\mathbb{Z}}^\times$. Let G be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ such that $\det(G) = \widehat{\mathbb{Z}}^\times$ and $-I \in G$. 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] to compute projective models for more than one million modular curves.

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

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 $\mathsf{G} \subseteq \mathsf{G}' \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$, induces a morphism of curves $X_\mathsf{G} \to X_{\mathsf{G}'}$. 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 $\mathsf{G}' = \mathrm{GL}_2(\widehat{\mathbb{Z}})$, we have the associated j-map

$$\pi_\mathsf{G} \colon X_\mathsf{G} \longrightarrow \mathbb{P}^1_\mathbb{Q}.$$

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 [Zyw22].

Proposition 1.1. *Let G be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ that satisfies $\det(\mathsf{G}) = \widehat{\mathbb{Z}}^\times$ and $-I \in \mathsf{G}$. Let E be any elliptic curve defined over $\mathbb{Q}$ with $j_E \notin \{0, 1728\}$. 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 $\pi_\mathsf{G}(X_\mathsf{G}(\mathbb{Q})) \subseteq \mathbb{Q} \cup \{\infty\}$.*

Throughout the paper, by the genus of an open subgroup $\mathsf{G} \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$, 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.

There are many different but 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 $M_{k,\mathsf{G}}$, 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 $[\mathsf{G}, \mathsf{G}] = [\mathcal{G}, \mathcal{G}]$. Since, there is a map $X_\mathsf{G} \to X_\mathcal{G}$, the genus of $\mathcal{G}$ is less than or equal to the genus of G.

The set of agreeable subgroups are closed under conjugation in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. We denote by $\mathscr{A}_g$ a set of representatives of all 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 $[\mathcal{G}, \mathcal{G}] \subseteq B \subseteq \mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$.

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

In §4, we will show that for a fixed G in $\mathscr{F}(\mathcal{G}, \mathsf{B})$, the family $\mathscr{F}(\mathcal{G}, \mathsf{B})$ consists of the groups

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

with $\gamma \colon \widehat{\mathbb{Z}}^\times \longrightarrow \mathcal{G}/\mathsf{G}$ 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 rest of the paper, by a *family of groups*, we mean a 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 map $\pi_\mathsf{G} : X_\mathsf{G} \to X_\mathcal{G}$. The group $\mathcal{G}$ acts on X_G where the restricted action of G is trivial. Hence, there is an action of $\mathcal{G}/\mathsf{G}$ on X_G. We have $\mathrm{Aut}(X_\mathsf{G}/X_\mathcal{G}) = \mathcal{G}/\mathsf{G}$ 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, 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 twisting the curve X_G with the cocycle ξ, we get a modular 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 of them 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 $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ with full determinant and $-I \in \mathsf{G}$ of genus g.*

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

(2) Let $\mathscr{F}(\mathcal{G}, \mathsf{B})$ be a family of genus g. Fix a group $\mathsf{G} \in \mathscr{F}(\mathcal{G}, \mathsf{B})$. Let $\gamma : \widehat{\mathbb{Z}}^\times \to \mathcal{G}/\mathsf{G}$ be a continuous homomorphism. There is an effective algorithm that takes as input a group $\mathsf{G}_\gamma \in \mathscr{F}(\mathcal{G}, \mathsf{B})$ and outputs a projective curve $C_{\mathsf{G}_\gamma} \subseteq \mathbb{P}^r_\mathbb{Q}$ for some $r > 0$ such that C_{G_γ} is isomorphic to X_{G_γ}. This algorithm computes the model C_{G_γ} by twisting a projective model C_G of X_G with respect to the cocycle $\gamma \circ \chi_{cyc}$, where χ_{cyc} is the cyclotomic character.

Remark 1.5. Fix a non-negative integer g. For the implementation of the algorithm of Theorem 1.4, we first compute the finitely many families of genus g. Afterwards, we choose a representative group $\mathsf{G} \in \mathscr{F}(\mathcal{G}, \mathsf{B})$ for each family, and precompute a projective model for X_G. This reduces the computation of C_{G_γ} to a twisting argument, which is computationally equivalent to a collection of linear algebra problems.

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

1.4. **Example.** 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

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

hand, for an arbitrary open subgroup $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ with $-I \in G$ and $\det(G) = \widehat{\mathbb{Z}}$, the only such algorithm is the one implemented in [Zyw22] which we describe in §2.

Consider the the following group.

$$G = \left\langle \left(\begin{smallmatrix} 119 & 0 \\ 0 & 119 \end{smallmatrix}\right), \left(\begin{smallmatrix} 9 & 8 \\ 936 & 937 \end{smallmatrix}\right), \left(\begin{smallmatrix} 69 & 244 \\ 0 & 5 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 8 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 55 & 769 \\ 10 & 33 \end{smallmatrix}\right), \left(\begin{smallmatrix} 41 & 813 \\ 0 & 15 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 8 \\ 0 & 1 \end{smallmatrix}\right) \right\rangle \subset \mathrm{GL}_2(\mathbb{Z}/944\mathbb{Z}).$$

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

$$\mathcal{G} = \left\langle \left(\begin{smallmatrix} 9 & 8 \\ 8 & 9 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 8 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 8 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 15 & 0 \\ 0 & 15 \end{smallmatrix}\right), \left(\begin{smallmatrix} 7 & 0 \\ 0 & 7 \end{smallmatrix}\right), \left(\begin{smallmatrix} 13 & 4 \\ 4 & 5 \end{smallmatrix}\right), \left(\begin{smallmatrix} 12 & 9 \\ 11 & 4 \end{smallmatrix}\right), \left(\begin{smallmatrix} 3 & 14 \\ 14 & 5 \end{smallmatrix}\right), \left(\begin{smallmatrix} 5 & 0 \\ 0 & 5 \end{smallmatrix}\right) \right\rangle \subset \mathrm{GL}_2(\mathbb{Z}/16\mathbb{Z}),$$

$$B = \left\langle \left(\begin{smallmatrix} 7 & 0 \\ 0 & 7 \end{smallmatrix}\right) \right\rangle \subset \mathrm{SL}_2(\mathbb{Z}/8\mathbb{Z}).$$

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

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

G and 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 $C_H \subseteq \mathbb{P}^4_{\mathbb{Q}}$

$$-x_1x_4 - x_2^2 + x_3^2 = 0$$
$$2x_1x_4 + 2x_2^2 + x_5^2 = 0$$
$$-2x_1^2 + 2x_3x_5 + x_4^2 = 0$$

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

$$-2x_2x_5 - x_3^2 + 2x_4^2 = 0$$
$$59x_1^2 + 4x_3x_4 - 2x_5^2 = 0$$
$$-59x_1^2 - 4x_2^2 + 4x_3x_4 = 0$$

is isomorphic to X_G. The curves X_H and X_G are isomorphic over the number field $K \subset \mathbb{Q}(\zeta_{944})$ with the defining polynomial $f(x) = x^2 + 228x + 12878$. The model of X_H given above comes from the cusp forms $S_{2,H}$ which is a $\mathbb{Q}$ vector space of dimension 5. The agreeable closure

$\mathcal{G}$ has index 96 in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and so $\mathcal{G}/G$ is isomorphic to the cyclic group of order 2. The nontrivial element of $\mathcal{G}/G$ acts on $S_{2,H}$ (with respect to our choice of basis) via the matrix

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

The cocycle (which is actually 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

$$A = \begin{pmatrix} 0 & 0 & 0 & (\alpha+144)/236 & 0 \\ 0 & 0 & 0 & 0 & 1/2 \\ 0 & 0 & (\alpha+144)/236 & 0 & 0 \\ 0 & (\alpha+144)/236 & 0 & 0 & 0 \\ (\alpha+144)/236 & 0 & 0 & 0 & 0 \end{pmatrix}$$

where α 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.

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), while our implementation took 0.41 seconds to compute a model and the j-map for the modular curve X_G. For modular curves of high level, the computation of j-maps are especially time consuming as it involves finding relations between the j invariant and the cusp forms whose coefficients lie in $\mathbb{Q}(\zeta_N)$ where N is the level. We avoid this computation via twisting in our algorithm, so we do not compute explicit modular forms. As a result our algorithm stays efficient as the level of the input curve X_G increases. Despite not computing q-expansions to find the models, it should be noted that the current implementation of our algorithm can be used to compute a certain subspace of the space $M_{k,G}$ ($S_{2,G}$ for the above example) by twisting.

1.5. **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 $\mathrm{Gal}(\overline{K}/K)$ $\underline{into}$ $H \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$.*

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.

1.6. **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.

1.7. **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.

1.8. **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.

1.9. **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, $\mathbb{Z}_N$ is the profinite group obtained by taking the inverse limit of $\mathbb{Z}/N^s\mathbb{Z}$ where s ranges over $\mathbb{N}$. There are natural isomorphisms

$$\mathbb{Z}_N \cong \prod_{l|N} \mathbb{Z}_l \quad \text{and} \quad \widehat{\mathbb{Z}} \cong \prod_{l} \mathbb{Z}_l$$

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 $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. 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 $\mathrm{GL}_2(\mathbb{Z}_N)$ is the smallest positive integer n that divides a power of N and such that G is equal to the inverse image of its image under the reduction modulo n map $\mathrm{GL}_2(\mathbb{Z}_N) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. The levels of an open subgroup of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ and $\mathrm{SL}_2(\mathbb{Z}_N)$ are defined similarly.

For $0 < n \in \mathbb{N}$, 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 $-I \in G$.

1.10. **Overview of the paper.** In §2, we review the background material on modular curves and modular forms. In §4, we define a family of groups associated to a pair $(\mathcal{G}, B)$, denoted by $\mathscr{F}(\mathcal{G}, B)$. In §3, we will discuss agreeable subgroups, define the agreeable closure of a subgroup G and discuss how to compute it. 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 up to a 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. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. For any N divisible by the level of G, the projection $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ gives a group whose inverse image is the open subgroup G. We will often abuse the 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 $\mathrm{SL}_2(\mathbb{Z})$ 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 upper half plane $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$ by linear fractional transformations. Fix a congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$. 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]. 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 $k \geqslant 0$ 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 $(f|_k\gamma)(\tau) := \det(\gamma)^{k/2}(c\tau+d)^{-k}f(\gamma\tau)$. (Eray: [choice here!]) 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 and let $q_w := e^{2\pi i\tau/w}$, where w is the width of Γ at ∞. 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

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

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 only possible when $f(\gamma\tau)d(\gamma\tau)^{k/2} = f(\tau)(d\tau)^{k/2}$. A quick computation shows that 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 refer to [DS05].

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

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

supported on cusps and elliptic points [Zyw22]. For any modular form $f \in M_k(\Gamma)$, we have $\operatorname{div}(\omega_f) + \mathcal{D}_k \geqslant 0$. 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_G that we consider contain $-I$, which means that $M_k(\Gamma_G) = 0$ when k is odd. Combining the isomorphisms ψ_k for even $k \in \mathbb{N}$, we get an isomorphism of $\mathbb{C}$ algebras:

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

2.4. **Eisenstein series.** For our applications, we will need to work with explicit modular forms in the graded algebra R_{Γ_G}. One way of constructing such forms is via Eisenstein series. Let $(a, b) \in \mathbb{Z}/N\mathbb{Z}$ and let $\tilde{a}, \tilde{b} \in \mathbb{Z}$ be any two integers that represent a, b. Define the Eisenstein series

$$E^{(k)}_{(a,b)}(\tau) = \frac{(k-1)!}{(-2\pi i)^k} \sum_{\substack{\omega \in \mathbb{Z} + \mathbb{Z}\tau \\ \omega \neq -(\tilde{a}\tau + \tilde{b})/N}} \left(\frac{\tilde{a}\tau + \tilde{b}}{N} + \omega \right)^{-k} \cdot \left| \frac{\tilde{a}\tau + \tilde{b}}{N} + \omega \right|^{-2s} \Bigg|_{s=0}$$

where the last part denotes the analytic continuation to $s = 0$. For $k = 1$ or $k \geqslant 3$, $E^{(k)}_{(a,b)}$ is a modular form of weight k with respect to $\Gamma(N)$. In the case $k = 2$, $E^{(k)}_{(a,b)} - E^{(k)}_{(0,0)}$ is a modular form for $\Gamma(N)$.

Consider the graded algebra $R_{\Gamma(N)} = \bigoplus_{k \geqslant 0} M_k(\Gamma(N))$. Khuri-Makdisi shows [KM12] that the Eisenstein series almost generate $R_{\Gamma(N)}$.

Theorem 2.1. *Let $N \geqslant 3$ and let $\mathcal{R}_N$ be the subalgebra of $R_{\Gamma(N)}$ generated by the Eisenstein series $E^{(1)}_{(a,b)}$ with $a, b \in \mathbb{Z}/N\mathbb{Z}$. Then $\mathcal{R}_N$ contains all modular forms on $\Gamma(N)$ of weight 2 and above.*

Proof. This is Theorem 3.1 in [BN19]. □

Computing modular forms explicitly involves computing the coefficients of the q-expansion up to a certain bound. The coefficients for $E^{(1)}_{(a,b)}$ have explicit formulas c.f. [Zyw22, Lemma 4.7].

2.5. **Actions.** Fix positive integers k and N. $\Gamma(N)$ 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 $\sigma_d(\zeta_N) = \zeta_N^d$. There is 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 2.2. *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 2.2 for all k, we get a right action $*$ of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on the graded $\mathbb{Q}$-algebra $\bigoplus_{k \geqslant 0} M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$. In particular, the action $*$ is well understood on the Eisenstein series mentioned above:

Lemma 2.3. *Let $(a_1, b_1), \dots, (a_k, b_k)$ and $A \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. We have*

$$(E^{(1)}_{(a_1,b_1)} \cdots E^{(1)}_{(a_k,b_k)}) * A = E^{(1)}_{(a_1,b_1)A} \cdots E^{(1)}_{(a_k,b_k)A}.$$

2.6. **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 2.2. 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 2.4. *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. Lemma 4.5 in [Zyw22]. □

2.7. **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 2.5. *The* modular curve *X_G associated to group G is the $\mathbb{Q}$-scheme $\mathrm{Proj}(\bigoplus_{k=0}^{\infty} M_{k,G})$.*

Remark 2.6. X_G is a nice curve over $\mathbb{Q}$. For open subgroups $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$, 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. This definition is independent of the integer N.

When $G := \mathrm{GL}_2(\widehat{\mathbb{Z}})$, we have $X_G = \mathrm{Proj}(\bigoplus_{k=0}^{\infty} M_{k,G}) = \mathrm{Proj}(\mathbb{Q}[E_4, E_6])$. We can identify this curve 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 of the space of modular forms $M_{k,G'} \subseteq M_{k,G}$, hence 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 $\pi\colon X_G \to \mathbb{P}^1_{\mathbb{Q}}$.

2.7.1. *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 $R_{\Gamma_G} := \bigoplus_{k\geqslant 0} M_k(\Gamma_G)$. 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 $\mathrm{Proj}(R_{\Gamma_G}) \cong \mathcal{X}_{\Gamma_G}$ as schemes [VZB22].

Similarly, the graded ring $R := \mathrm{Proj}(\bigoplus_{k=0}^{\infty} M_{k,G})$ is finitely generated over $\mathbb{Q}$. Lemma 2.4 shows that tensoring R with $\mathbb{C}$ gives the ring R_{Γ_G}. Using this equality we identify $X_G(\mathbb{C})$ with $\mathcal{X}_{\Gamma_G}$. Tensoring the map $\pi\colon X_G \to \mathbb{P}^1_{\mathbb{Q}}$ with $\mathbb{C}$, we get the complex projection map $\mathcal{X}_{\Gamma_G} \to \mathbb{P}^1_{\mathbb{C}}$. [Zyw22] defines the modular curve X_G by explicitly giving its function field.

Let X_G be as in [Zyw22], which is defined by explicitly giving its function field. Let $\mathcal{L}_k := \Omega^1(\mathcal{D}_k)$, the invertible sheaf on the Riemann surface $\mathcal{X}_{\Gamma_G}$ where 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 $H^0(\mathcal{X}_G, \mathscr{L}_k) \subseteq H^0(X_{\Gamma_G}, \mathcal{L}_k)$. In particular, it is shown that the map ψ_k induces an isomorphism between $M_{k,G}$ and $H^0(X_G, \mathscr{L}_k)$. 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.

2.8. **Models of modular curves.** In this section, we briefly describe how to compute projective models of modular curves, as explained in [Zyw22]. 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:

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

Let $\dim_{\mathbb{Q}} V = d + 1$ with $d \geqslant 1$, and let $f_0, \cdots, f_d$ be a basis of V. One can compute such a basis by computing Eisenstein series and multiplying them. Note that the quotients f_j/f_i are rational functions of X_G. 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. The image of X_G is a curve in $\mathbb{P}^d_{\mathbb{Q}}$ denoted by C. Let $I(C) \subseteq \mathbb{Q}[x_0, \ldots, x_d]$ be its homogeneous ideal. There is an algorithm to compute a basis for each graded part $I(C)_n$ [Zyw22].

Let $\mathcal{F} := \mathscr{L}_k(-E)$ be the invertible sheaf on X_G. The map ψ_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

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

2.8.1. *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]. 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 so that $\deg \mathcal{F} \geqslant 2g+1$. Hence, φ is an embedding and $C := \varphi(X_G)$ is isomorphic to X_G.

3. Agreeable Subgroups

In this section we will describe 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 all the scalar matrices, and the levels of $\mathcal{G} \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ and $\mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) \subseteq \mathrm{SL}_2(\widehat{\mathbb{Z}})$ 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 agreeable subgroup that contains G, called the agreeable closure of 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* $[G, G] \subseteq \mathrm{SL}_2(\widehat{\mathbb{Z}})$. *Consider 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 call* $\mathcal{G}$ *the agreeable closure of* 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]. □

Remark 3.3. Note that the integer N 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 $\widehat{\mathbb{Z}}^\times \cdot G_N$ have the same commutator subgroups.

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

Lemma 3.4.

(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]. □

Using the above lemma, we 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 3.5. *Let $\mathsf{G} \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ be an open subgroup with full determinant. Let $\mathsf{T} := \mathrm{SL}_2(\widehat{\mathbb{Z}}) \cap \mathsf{G}$. Then the level of $[\mathsf{G}, \mathsf{G}]$ and level of T have the same odd prime divisors.*

Proof. $[\mathsf{G}, \mathsf{G}] \subseteq \mathsf{T}$ implies that the level of T 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 T. The above lemma 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 T. □

Thus, we can find all the prime divisors of the level of $\mathcal{G}$.

Proposition 3.6. *Let G be as above. 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 $\mathsf{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$. If G has odd level, then so has $\mathcal{G}$.*

Proof. T and $[\mathsf{G}, \mathsf{G}]$ have the same odd prime divisors. From the construction of the agreeable subgroup $\mathcal{G}$ the assertion follows.

When the level of G is an odd integer and N is as above, G_N and $\mathsf{G}_{\mathsf{N}/2}$ have the same inverse image in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and so the level of $\mathcal{G}$ is odd. □

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 closed subgroup B of $\mathcal{G}$ satisfying $[\mathcal{G}, \mathcal{G}] \subseteq \mathsf{B} \subseteq \mathrm{SL}_2(\widehat{\mathbb{Z}})$.

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 open 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. Pick a group $\mathsf{G} \in \mathscr{F}(\mathcal{G}, \mathsf{B})$. We know that G is an open subgroup of $\mathcal{G}$ and 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 $\gamma \colon \widehat{\mathbb{Z}}^\times \to \mathcal{G}/\mathsf{G}$. γ gives rise to 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 $G_\gamma \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = B$. The natural map $(\mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}))/B \to \mathcal{G}/G$ is an isomorphism since $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = B$ and $\det(G) = \widehat{\mathbb{Z}}^\times$. Using this isomorphism, we find that $\det(G_\gamma) = \widehat{\mathbb{Z}}^\times$. Therefore, $G_\gamma \in \mathscr{F}(\mathcal{G}, B)$.

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

Let $\mathscr{F}(\mathcal{G}, B)$ be a family as above. Let N be the least common multiple of levels of $\mathcal{G}$ and B. We define $N_1 := N$ if N is odd and $N_1 := \mathrm{lcm}(N, 8)$ if N is even. Then

Theorem 4.3. *Let $U = \widehat{\mathbb{Z}}^\times$ and let $S := U_N[2^\infty]$ be the 2-power torsion subgroup of U_N. Then the following are equivalent:*

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

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

(3) There is a homomorphism $\beta\colon S \to \mathcal{G}(N_1)/B(N_1)$ such that $\det(\beta(a)) \equiv a \pmod{N_1}$ for all $a \in S$.

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]. □

An algorithm for this kind of search has been implemented for use by the author.

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

(1) X_G and X_H have the same genus.

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

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 $N = \mathrm{lcm}(N_G, N_H)$ 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 $|H| = |B| \cdot \phi(N)$. □

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

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

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

5. Finiteness of Agreeable Subgroups

Fix a non-negative integer g. In this section, we prove that there are finitely many agreeable subgroups up to conjugacy, of genus less than or equal to g. Our proof will also give us a method for computing all of them. This is also proven in [Zyw24]. We first start by making some observations.

Let G be an agreeable subgroup of genus at most g. Let $H := G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ be its intersection with $\mathrm{SL}_2(\widehat{\mathbb{Z}})$. It is an open subgroup in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$. We have $-I \in H$, let N be the level of H. 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 (up to conjugacy) congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ of genus less than g and contain $-I$. All such groups up to genus 24 are given in the [CP03] database.

In our 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, up to conjugacy, 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 up to conjugacy. 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 will now explain how to find all agreeable subgroups $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ such that $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = H$. Let $N_1 := 2 \cdot \operatorname{lcm}(N, 12)$. The following lemma is central to the proof. It is also proven in [Zyw24].

Lemma 5.2. *Any agreeable subgroup* $G \subseteq GL_2(\widehat{\mathbb{Z}})$ *with* $G \cap SL_2(\widehat{\mathbb{Z}}) = H$ *has level dividing* N_1*.*

Proof. Let $N' = \operatorname{lcm}(N, 12)$. The level of H is N, so we have

$$H := H_{N'} \times \prod_{l \nmid N'} \mathrm{SL}_2(\mathbb{Z}_l)$$

It is know that the commutator subgroup of $\mathrm{SL}_2(\mathbb{Z}_l)$ is equal to $\mathrm{SL}_2(\mathbb{Z}_l)$ for all primes $l > 3$, hence we have

$$[H, H] := [H_{N'}, H_{N'}] \times \prod_{l \nmid N'} \mathrm{SL}_2(\mathbb{Z}_l)$$

which implies the primes dividing the level of $[H, H]$ are contained in the set of primes dividing N_1. Consider the agreeable subgroup G. Since $H \subset G$, we have $[H, H] \subset [G, G]$, so the primes dividing the level of $[G, G]$ are similarly contained in the set of primes dividing N_1. G is agreeable, and in particular the levels of H and $[G, G]$ in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ and the level of G in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ have the same odd prime divisors. Hence

$$[G, G] := [G_{N_1}, G_{N_1}] \times \prod_{l \nmid N_1} \mathrm{GL}_2(\mathbb{Z}_l)$$

and the level of G is divides a power of N_1. Since G is agreeable $\mathbb{Z}_{\mathsf{N}_1}^{\times} \cdot \mathsf{H}$ is contained in $\mathsf{G}_{\mathsf{N}_1}$ and it follows from [Zyw22] Lemma 7.6 that $\mathbb{Z}_{\mathsf{N}_1}^{\times} \cdot \mathsf{H}$ is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_{\mathsf{N}_1})$ whose level divides N_1 (note that this is where we need the additional factor of 2). We conclude that the level of $\mathsf{G}_{\mathsf{N}_1}$ divides N_1.

□

Let Γ and H be as above. Assume $\mathsf{G} \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ is an agreeable subgroup with $\mathsf{G} \cap \mathrm{SL}(\widehat{\mathbb{Z}}) = \mathsf{H}$. We have seen that G has level dividing N_1, so G corresponds to a subgroup $\bar{\mathsf{G}}$ of $\mathrm{GL}_2(\mathbb{Z}/\mathsf{N}_1\mathbb{Z})$ such that $\bar{\mathsf{G}} \cap \mathrm{SL}_2(\mathbb{Z}/\mathsf{N}_1\mathbb{Z}) = \bar{\mathsf{H}}$ where $\bar{\mathsf{H}}$ denotes the reduction to modulo N_1. There are only finitely many such subgroups of $\mathrm{GL}(\mathbb{Z}/\mathsf{N}_1\mathbb{Z})$, 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.

We now explain how to explicitly compute all such agreeable subgroups. Let Γ and N_1 be as above. We first directly search in $\mathrm{GL}_2(\mathbb{Z}/\mathsf{N}_1\mathbb{Z})$ for subgroups $\bar{\mathsf{G}}$ with $(\mathbb{Z}/\mathsf{N}_1\mathbb{Z})^{\times} \subseteq \bar{\mathsf{G}}$, $\det(\bar{\mathsf{G}}) = \mathbb{Z}/\mathsf{N}_1\mathbb{Z}$, $-I \in \bar{\mathsf{G}}$ and $\bar{\mathsf{G}} \cap \mathrm{SL}(\mathbb{Z}/\mathsf{N}_1\mathbb{Z}) = \bar{\mathsf{H}}$. These groups give rise to finitely many, potentially agreeable, subgroups $\mathsf{G} \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ such that $\mathsf{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = \mathsf{H}$. For each such G, we then check if it is an agreeable subgroup, i.e. if its $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ level has the same odd prime divisors as its $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ level. □

The set of agreeable subgroups up to genus g is stable under conjugation in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. We denote by $\mathscr{A}_{\mathsf{g}}$ a set of representatives of conjugacy classes of all agreeable subgroups up to genus g.

Remark 5.3. 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 $\mathscr{F}(\mathcal{G}, \mathsf{B})$ where $\mathcal{G}$ is the agreeable closure of G and $\mathsf{B} = \mathsf{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$. We have a description of $\mathcal{G}$ that depends on G and B. In particular, we can easily compute the group $\mathcal{G}$ and subsequently identify the family $\mathscr{F}(\mathcal{G}, \mathsf{B})$ which contains G.

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

Theorem 5.4. *Fix a non-negative integer* g. *There are only finitely many families of groups of genus* g, *up to conjugacy in* $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

Proof. Previously we have shown that there are finitely many agreeable subgroups (up to conjugacy) of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ up to a fixed genus g. We have denoted this set by $\mathscr{A}_{\mathsf{g}}$. For each agreeable subgroup $\mathcal{G} \in \mathscr{A}_{\mathsf{g}}$, 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 finitely many subgroups B of $\mathcal{G}$ such that $[\mathcal{G}, \mathcal{G}] \subseteq \mathsf{B} \subseteq \mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$. Combining $\mathcal{G}$'s and B's, we get a finite set of pairs $(\mathcal{G}_i, \mathsf{B}_i)$ and associated families $\mathscr{F}(\mathcal{G}_i, \mathsf{B}_i)$.

Let G be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ of genus g. Then G lies in the family $\mathscr{F}(\mathcal{G}, \mathsf{B})$ where $\mathsf{B} = \mathsf{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ and $\mathcal{G}$ is the agreeable closure of G. The agreeable closure $\mathcal{G}$ has genus at most g and so it is conjugate to an agreeable subgroup $\mathcal{G}'$ in the finite set $\mathscr{A}_{\mathsf{g}}$ and G is conjugate to a subgroup $\mathsf{G}' \subseteq \mathcal{G}'$. We conclude that G is conjugate to a group lying in the family $\mathscr{F}(\mathcal{G}', \mathsf{B}')$ where $\mathsf{B}' = \mathsf{G}' \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$. Hence, the families $\mathscr{F}(\mathcal{G}_i, \mathsf{B}_i)$ cover the set of all open subgroups of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ of genus g up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. □

6. Twisting Modular Curves

We have stated in §4 that a family of groups $\mathscr{F}(\mathcal{G},\mathsf{B})$ corresponds to a family of twists of modular curves. In this section, we will describe the spaces of modular curves $\mathsf{M}_{\mathsf{k},\mathsf{G}}$ as we vary G in a family $\mathscr{F}(\mathcal{G},\mathsf{B})$ and, consequently, how to twist the modular curves X_G.

Fix a family $\mathscr{F}(\mathcal{G},\mathsf{B})$ and fix a group $\mathsf{G}\in\mathscr{F}(\mathcal{G},\mathsf{B})$ where $\mathcal{G}$ is the agreeable closure of G. Let X_G be the modular curve asociated to G, and let $\pi_\mathsf{G}:\mathsf{X}_\mathsf{G}\to\mathsf{X}_\mathcal{G}$ be the morphism coming from the inclusion $\mathsf{G}\subseteq\mathcal{G}$. We start with a definition:

Definition 6.1. A $\mathcal{G}$—twist of $(\mathsf{X}_\mathsf{G},\pi_\mathsf{G})$ is a pair (Y,π) where Y is a curve over $\mathbb{Q}$, with a morphism $\pi:\mathsf{Y}\to\mathsf{X}_\mathcal{G}$ defined over $\mathbb{Q}$, such that there is an isomorphism $\mathsf{f}:(\mathsf{X}_\mathsf{H})_{\mathbb{Q}^{\mathrm{ab}}}\to(\mathsf{Y})_{\mathbb{Q}^{\mathrm{ab}}}$ that satisfies $\pi\circ\mathsf{f}=\pi_\mathsf{G}$.

Remark 6.2. The curves X_H and Y above can be isomorphic over a subfield $\mathsf{L}\subseteq\mathbb{Q}^{\mathrm{ab}}$. We call them isomorphic if there is an isomorphism $(\mathsf{X}_\mathsf{H})_\mathbb{Q}\to\mathsf{Y}_\mathbb{Q}$.

The group G is a normal subgroup of $\mathcal{G}$, and the latter acts on $\mathsf{M}_{\mathsf{k},\mathsf{G}}$ for all k and consequently on X_G . The subgroup G acts trivially on X_G so there is an action of $\mathcal{G}/\mathsf{G}$ on X_G. We have $\mathrm{Aut}(\mathsf{X}_\mathsf{G}/\mathsf{X}_\mathcal{G})=\mathcal{G}/\mathsf{G}$ where $\mathrm{Aut}(\mathsf{X}_\mathsf{G}/\mathsf{X}_\mathcal{G})$ is the group of automorphisms f of the curve X_G that satisfy $\pi_\mathsf{G}\circ\mathsf{f}=\pi_\mathsf{G}$. Note that these are modular automorphisms and since there is a natural isomorphism $\mathcal{G}/\mathsf{G}\simeq(\mathcal{G}\cap\mathrm{SL}_2(\widehat{\mathbb{Z}}))/\mathsf{B}$, the automorphisms in $\mathrm{Aut}(\mathsf{X}_\mathsf{G}/\mathsf{X}_\mathcal{G})$ are defined over $\mathbb{Q}$.

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

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

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

Lemma 6.3. *There is a bijection between $\mathcal{G}$—twists of X_G and $\mathrm{H}^1(\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}),\mathrm{Aut}(\mathsf{X}_\mathsf{G}/\mathsf{X}_\mathcal{G}))$.*

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

Let's first show that λ is well defined and does not depend on the choice of the isomorphism. Let $\mathsf{g}:\mathsf{X}_{\mathbb{Q}^{\mathrm{ab}}}\to\mathsf{Y}_{\mathbb{Q}^{\mathrm{ab}}}$ be another such isomorphism. Then $\mathsf{f}^{-1}\circ\sigma(\mathsf{f})$ and $\mathsf{g}^{-1}\circ\sigma(\mathsf{g})$ 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 $\mathsf{h}:\mathsf{Y}\to\mathsf{Z}$ such that $\pi_\mathsf{Z}\circ\mathsf{h}=\pi_\mathsf{Y}$. Then we have an isomorphism $\mathsf{h}\circ\mathsf{f}:\mathsf{X}_{\mathbb{Q}^{\mathrm{ab}}}\to\mathsf{Z}_{\mathbb{Q}^{\mathrm{ab}}}$ satisfying $\pi_\mathsf{Z}\circ\mathsf{h}\circ\mathsf{f}=\pi_\mathsf{X}$. Looking at associated cocycles, we have $(\mathsf{h}\circ\mathsf{f})^{-1}\circ\sigma(\mathsf{h}\circ\mathsf{f})=\mathsf{f}^{-1}\circ\mathsf{h}^{-1}\circ\sigma(\mathsf{h})\circ\sigma(\mathsf{f})=\mathsf{f}^{-1}\circ\sigma(\mathsf{f})$ 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 $\mathsf{T}\in\mathrm{Aut}(\mathsf{X}_\mathsf{G}/\mathsf{X}_\mathcal{G})$ such that $\xi_1(\sigma)=\mathsf{T}^{-1}\circ\xi_2(\sigma)\circ\sigma(\mathsf{T})$. Then $\mathsf{f}_2\circ\mathsf{T}\circ\mathsf{f}_1^{-1}:\mathsf{Y}_1\to\mathsf{Y}_2$ is an isomorphism defined over $\mathbb{Q}$, proving the injectivity of λ.

To show surjectivity, let $[\xi]$ be a class in $\mathsf{H}^1(\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}),\mathrm{Aut}(\mathsf{X}_\mathsf{G},\mathsf{X}_\mathcal{G}))$. By Galois descent we get a nice curve Y over $\mathbb{Q}$ with an isomorphism $\mathsf{f}:\mathsf{X}_{\mathbb{Q}^{\mathrm{ab}}}\to\mathsf{Y}_{\mathbb{Q}^{\mathrm{ab}}}$ where $\sigma\to\mathsf{f}^{-1}\circ\sigma(\mathsf{f})$ is cohomologous to ξ [Ser02, Chapter III, Proposition 5]. Precisely this means that there is $\mathsf{T}\in\mathrm{Aut}(\mathsf{X}_\mathsf{G}/\mathsf{X}_\mathcal{G})$ such that $\mathsf{f}^{-1}\circ\sigma(\mathsf{f})=\mathsf{T}^{-1}\circ\xi(\sigma)\circ\sigma(\mathsf{T})$. Set $\mathsf{g}=\mathsf{f}\circ\mathsf{T}^{-1}$. 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 $P \in Y_{\mathbb{Q}^{ab}}$ 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.

□

Let $H := G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$. Let $\gamma : \widehat{\mathbb{Z}}^\times \to \mathcal{G}/G$ be a continuous homomorphism and let $\xi : \mathrm{Gal}_{\mathbb{Q}^{ab}} \to \mathcal{G}/G \cong \mathrm{Aut}(X_G/X_{\mathcal{G}})$ be the associated cocycle by precomposing with the cyclotomic character. Twisting via this cocycle, we get a curve $(X_G)_\xi$. We prove that $(X_G)_\xi = X_{G_\gamma}$, where G_γ is the group defined in §4.

Observe that $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = G_\gamma \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = H$. Hence, from the definition of $M_{k,G}$ in §2, one can see that

$$M_{k,H} = M_{k,G} \otimes \mathbb{Q}^{ab} = M_{k,G_\gamma} \otimes \mathbb{Q}^{ab}.$$

Note that G is normal in $\mathcal{G}$, so there is an action of $\mathcal{G}$ on $M_{k,G}$, as in Lemma 2.2, where G acts trivially. This leads to an induced action of $\mathcal{G}/G$ on $M_{k,G}$.

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

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

$$(M_{k,G})_\xi = \{f \in M_{k,G} \otimes \mathbb{Q}^{ab} \mid \quad \sigma \bullet f = f \quad \forall \sigma \in \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})\}.$$

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

$$\varphi_1 \colon \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \to \widehat{\mathbb{Z}}^\times \to G/H$$

and

$$\varphi_2 \colon \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \to \widehat{\mathbb{Z}}^\times \to G_\gamma/H$$

we get two different Galois actions of $\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$ on $M_{k,G} \otimes \mathbb{Q}^{ab}$ which correspond to the different Galois actions on $M_{k,G}$ and M_{k,G_γ}.

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

Lemma 6.4. *If* $\sigma \in \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$ *and* $g \in G_\gamma$ *with* $\det(g) = \chi_{\mathrm{cyc}}(\sigma)$ *then* $\sigma \bullet f = f * g$ *for all* $f \in M_{k,G} \otimes \mathbb{Q}^{ab}$.

Proof. Let $cf := f \otimes c \in M_{k,G} \otimes \mathbb{Q}^{ab}$. 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

$$\xi(\sigma) = \gamma(\det(g)) = gG$$

in $\mathcal{G}/G$.

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

Theorem 6.5. $(M_{k,G})_\xi = M_{k,G_\gamma}$.

Proof. Let $f \in M_{k,G_\gamma}$. Then for all σ and compatible $g \in G_\gamma$, we have $\sigma \bullet f = f * g = f$, which implies that $f \in (M_{k,G})_\xi$.

For the converse, let $f \in (M_{k,G})_\xi$. Then for all $g \in G_\gamma$ and compatible σ we have $f * g = \sigma \bullet f = f$. Hence $f \in M_{k,G_\gamma}$. □

We immediately get the following:

Corollary 6.6.

$$(X_G)_\xi = X_{G_\gamma}.$$

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

$$(R_G)_\xi := \{a \in \bigoplus_{k=0}^{\infty} M_{k,G} \otimes \mathbb{Q}^{ab} | \quad \sigma \bullet a = a \quad \forall \sigma \in \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})\}.$$

Corollary 6.6 shows that $X_{G_\gamma} = \mathrm{Proj}((R_G)_\xi)$. Hence, 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 $(X_G)_\xi$. Combining the results of this section with the previous ones, we restate Theorem 1.4 in terms of modular curves:

Theorem 6.7. *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.

Theorem 6.8. *Fix a non-negative integer g. There are only finitely many families of modular curves of genus g.*

Proof. The family of groups mentioned in Theorem 5.4 corresponds to a family of twists of modular curves. The algorithm is explained in detail in the next section. □

We denote by $\mathscr{F}_g$ finitely many families of genus at most g up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, arising from the set of agreeable subgroups $\mathscr{A}_g$. The set $\mathscr{F}_g$ has been computed for $g = 24$.

6.0.1. *Getting a basis for M_{k,G_γ}.* Assume that, using the methods described in §2.8, we have an explicit basis $\mathcal{B} := \{f_0, \cdots, f_d\}$ for $M_{k,G}$ (or a set of modular forms in $M_{k,G}$ whose span is acted on by $\mathcal{G}$). $\mathcal{G}/G$ is a finite abelian group, and we can compute the action of any $gG \in \mathcal{G}/G$ on the basis $\mathcal{B}$ and get a matrix in $\mathrm{GL}_{d+1}(\mathbb{Q})$ [Zyw22]. Hence, for any 1-cocycle $\xi : \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \to \mathcal{G}/G$, we get a cocycle $\bar{\xi} : \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \to \mathrm{GL}_{d+1}(\mathbb{Q})$. By Hilbert 90, $\mathrm{H}^1(\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}), \mathrm{GL}_{d+1}(\mathbb{Q}^{ab}))$ is the trivial group, so there exists a matrix $A \in \mathrm{GL}_{d+1}(\mathbb{Q}^{ab})$ such that $\bar{\xi}(\sigma) = A^{-1}\sigma(A)$ for every $\sigma \in \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$.

Let $f \in M_{k,G}$ be a modular form. Consider the modular form $A^{-1} \cdot f \in M_{k,G_\gamma} \otimes \mathbb{Q}^{ab}$. For all $\sigma \in$, we have that

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

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 form 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 where $G \in \mathscr{F}(\mathcal{G}, B)$. The model C arises from linearly independent modular forms $f_0, \dots, f_r \in V \subseteq M_{k,G}$ as explained in §2. 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 $F_1, \dots, F_s \in \mathbb{Q}[x_0, \dots, x_r]$ where $F_i(f_0, \dots, f_r) = 0$. Let γ and ξ be as above. Let $(F_i)_\xi := F_i((x_0, ..., x_r)A^T)$.

Theorem 6.9. *The curve C' defined by $(F_i)_\xi$ 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, notice $\xi(\sigma)$ 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. $\overline{\xi}$ is a group homomorphism and $\overline{\xi}(\sigma)$ fixes the polynomials F_i for $i = 1, \dots, s$.

Let $\mathcal{B} :=\{f_0, \dots, f_r\}$ 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 $\langle (F_i)_\xi \rangle \subseteq \mathbb{Q}[x_0, \dots, x_r]$ 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 $\mathcal{G}, G$ and B. 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 Proposition 6.8 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 all the agreeable subgroups of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ whose genus is at most g, up to conjugacy. We have described an algorithm in the proof of 5.1 for computing them.

(ii) Consider the set $\mathscr{A}_g$ as in §5. 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, 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. Theorem 4.3 gives a method for finding a representative.

(v) Take a family $\mathscr{F}(\mathcal{G}, B)$ and the representative W. Compute a model C of X_W via the methods described in §2. In particular we are using the algorithm given by Zywina in [Zyw22]. Note that this means we have modular forms $f_0, ..., f_d \in M_{k,G}$ for suitable k and C is defined by 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 $i = 1, \cdots, s$.

Remark 7.2. Here are some remarks about the precomputation:

- For the first step, we start from the data of congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ which is given in [CP03]. Since these groups are given up to conjugacy, we get the set $\mathscr{A}_g$ mentioned in §5.
- Note that both $[\mathcal{G}, \mathcal{G}]$ and $\mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ are open subgroups of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ and hence they have finite index in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$.
- 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 $\mathscr{F}(\mathcal{G}, B)$.
- (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 Model: After the precomputation, one can use the following algorithm to compute a projective model of X_G. It takes an open subgroup $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ 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 $T := G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ and the agreeable closure of G, which we call $\mathcal{G}$.

(ii) By our main theorem, $\mathcal{G}$ is conjugate to a group in $\mathscr{A}_g$. Conjugate G, $\mathcal{G}$ and T, and replace them with their suitable conjugations so $\mathcal{G} \in \mathscr{A}_g$. Find the family $\mathscr{F}(\mathcal{G}, B) = \mathscr{F}(\mathcal{G}, T) \in \mathscr{F}_g$.

(iii) Since $\mathscr{G}(\mathcal{G}, B)$ is not empty, we have precomputed a representative $W \in \mathscr{G}(\mathcal{G}, B)$. Compute the homomorphism $\gamma : \widehat{\mathbb{Z}}^\times \cong G/T \to \mathcal{G}/W$. 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 6.0.1.

(vi) Apply the matrix A 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) Apply Galois descent to get polynomials $G_1, \cdots, G_s \in \mathbb{Q}[x_0, \ldots, x_d]$ defining X_G. By Theorem 6.9, the curve defined by G_i is a projective model of X_G.

Remark 7.4. Let G be the input of our algorithm and let N be its level. Let $\mathscr{F}(\mathcal{G}, B)$ be the family it is contained in. Let $W \in \mathscr{F}(\mathcal{G}, B)$ be the representative in the family and 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 $\mathbb{Z}/N\mathbb{Z} \to \mathcal{G}/W$.

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

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

Let $\mathscr{F} := \mathscr{F}(\mathcal{G}, B)$ be a family of modular curves. Note that for all modular curves $X \in \mathscr{F}$, the corresponding congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ are the same. In [Zyw25], the author shows that only finitely many congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ up to conjugacy have $\overline{\mathbb{Q}}-$gonality 2. A complete list of such congruence subgroups can be found in terms of Cummins-Pauli labels in the classification of [CP03].

The finitely many congruence subgroups (up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$) give rise to finitely many families of geometrically hyperelliptic modular curves in the sense of sections §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. 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 §2.8. 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. [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 $H \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ such that $-I \in H$ and $\det(H) = \widehat{\mathbb{Z}}^\times$ with genus g. Assume also that X_H has $\overline{\mathbb{Q}}-$gonality 2 and $g > 2$. There is an algorithm to determine the $\mathbb{Q}-$gonality of the modular curve X_H.*

Proof. X_H lies in a family $\mathscr{F}(\mathcal{G}, B)$ for which a representative along with the canonical map $\varphi : X_G \to C$ has been computed. Twisting the map φ with the cocycle ξ mentioned in §6, we get the canonical map $\varphi_\xi : X_H \to C_\xi$. C_ξ is a genus 0 curve, and if it contains a rational point then X_H has $\mathbb{Q}-$gonality 2. One can check whether this is the case by using the Hasse principle.

Assume now that C_ξ has no rational points. Then the map $\varphi_\xi : X_H \to C_\xi$ is unique up to an automorphism of C_ξ, i.e. there is no other genus 0 curve C' with $\pi' : X_H \to C'$ of degree 2. To prove this, sssume 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_ξ has no rational points, it must have $\mathbb{Q}-$gonality 2. Castelnuovo-Severi inequality applied to X_H, C_ξ and $\mathbb{P}^1_{\mathbb{Q}}$ shows that X_H cannot have gonality 3. We conclude that X_H has $\mathbb{Q}-$gonality 4. □

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]. ↑6

[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, 6

[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 ↑6

[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 ↑6

[BN19] François Brunault and Michael Neururer, *Fourier expansions at cusps*, The Ramanujan Journal (2019). ↑9, 10

[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 ↑6

[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. ↑6, 15, 21, 22

[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 ↑8

[Kar25] Eray Karabiyik, *Repository for classification*, 2025. https://github.com/eekarabiyik/twist. ↑1, 6, 23

[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 ↑9

[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. ↑6

[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 ↑5

[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 ↑6

[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 ↑6

[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 ↑12

[Poo07] Bjorn Poonen, *Gonality of modular curves in characteristic* 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 ↑6, 20

[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 ↑6

[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 ↑6

[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 ↑17

[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 ↑22

[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 ↑6

[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 ↑11

[Zyw20] David Zywina, *Computing actions on cusp forms* (2020). arXiv:2001.07270 [math.NT]. ↑12

[Zyw22] ———, *Explicit Open Images For Elliptic Curves Over* $\mathbb{Q}$ (2022). arXiv:2206.14959 [math.NT]. ↑2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 13, 16, 19, 21

[Zyw24] ———, *Open image computations for elliptic curves over number fields* (2024). arXiv:2403.16147 [math.NT]. ↑6, 12, 14, 15, 21

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

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