A CLASSIFICATION OF LOW GENUS MODULAR CURVES

ERAY KARABIYIK

ABSTRACT. Let G be an open subgroup of $GL_2(\widehat{\mathbb{Z}})$ satisfying $\det(G) = \widehat{\mathbb{Z}}$ and $-I \in G$. Associated to G, there is a modular curve X_G defined over $\mathbb{Q}$, which weakly parametrizes elliptic curves whose image of the Galois representation lies in G. Fixing a genus g, we give a classification of modular curves of genus g. In particular, we show that modular curves of genus g lie in finitely many families of $\mathbb{Q}^{ab}$-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 modular curves of genus g.

1. INTRODUCTION

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

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

Fixing compatible bases for $E[N]$ for all N and combining them via the inverse limit we get the adelic representation

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

where $\widehat{\mathbb{Z}}$ is the profinite completion of $\mathbb{Z}$. The image of ρ_E is uniquely determined up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and does not depend on the choice of bases. The image of ρ_E is a closed subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ with respect to the profinite topology. In [Ser72], Serre proved that essentially this image is as large as possible.

Theorem 1.1. *(Serre's open image theorem) Let E be a non-CM elliptic curve over the rational numbers. Then $\rho_E(\mathrm{Gal}(\overline{\mathbb{Q}}))$ is an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. Equivalently, $\rho_E(\mathrm{Gal}(\overline{\mathbb{Q}}))$ has finite index in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.*

Consider the cyclotomic character $\chi_{\mathrm{cyc}} : \mathrm{Gal}(\overline{\mathbb{Q}}) \to \widehat{\mathbb{Z}}^\times$. 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. Let G be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ such that $\det(G) = \widehat{\mathbb{Z}}^\times$ and $-I \in G$. Let $\rho_E^*\colon \mathrm{Gal}(\overline{\mathbb{Q}}) \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$ be the dual representation of ρ_E defined by $\rho_E^*(\sigma) = \rho_E(\sigma^{-1})^\intercal$. Associated to G there is a modular curve X_G (whose rational points) "parametrizes" elliptic curves for which the image of the dual representation ρ_E^* is conjugate to a subgroup of G.

In this article we give a complete classification for modular curves X_G whose genus is at most 24. Additionally, we describe an algorithm for finding a projective model for such modular curves, this algorithm has been implemented and can be found at [EK25]. Let g

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

be the genus of the modular curve X_G. Our algorithm computes a canonical model for the modular curve X_G when $g > 2$ and X_G is not geometrically hyperelliptic, and it computes an embedded model otherwise.

1.1. **Modular curves.** Let $G \subseteq GL_2(\widehat{\mathbb{Z}})$ be an open subgroup such that $\det(G) = \widehat{\mathbb{Z}}^\times$ and $-I \in G$. We will define the associated modular curve X_G in Section §3. It is a smooth, projective, geometrically irreducible curve defined over $\mathbb{Q}$. An inclusion $G \subseteq G' \subseteq GL_2(\widehat{\mathbb{Z}})$, induces a morphism of curves $\pi\colon X_G \to X_{G'}$. For the group $GL_2(\widehat{\mathbb{Z}})$, we have $X_{GL_2(\widehat{\mathbb{Z}})} = \mathbb{P}^1_{\mathbb{Q}} = \mathbb{A}^1_{\mathbb{Q}} \cup \{\infty\}$. Taking $G' = GL_2(\widehat{\mathbb{Z}})$, we have the associated j-map

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

The curve X_G has the following important moduli property. Let $E/\mathbb{Q}$ be an elliptic curve. Then $\rho_E^*(\mathrm{Gal}(\overline{\mathbb{Q}}))$ is conjugate to a subgroup of G in $GL_2(\widehat{\mathbb{Z}})$ if and only if $j_E \in \pi(X_G(\mathbb{Q}))$ where j_E is the j-invariant of E. Throughout the paper, by the genus of an open subgroup $G \subseteq GL_2(\widehat{\mathbb{Z}})$, we mean the genus of the associated modular curve X_G.

In §3, 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 §8, using a twisting argument, we explain a method to compute the model of any modular curve X_G, whose genus is at most a fixed genus g.

There are many different but equivalent definitions of the modular curve X_G. One can define X_G by explicitly giving its function field or as the general fiber of the coarse stack M_G defined over $\mathbb{Z}[1/N]$ that parametrizes elliptic curves with G-level structure, see [DR73] for details. One can also refer to [KM85] for the fine arithmetic of modular curves, where the level structure has a meaning over schemes where N is not invertible. We will opt to define X_G through a certain space of modular forms $M_{k,G}$, which is defined in §3.

1.2. **Families attached to a pair.** We give a classification of modular curves in terms of finitely many families of abelian twists. Let $\mathcal{G} \subseteq GL_2(\widehat{\mathbb{Z}})$ be an open subgroup such that $\det(\mathcal{G}) = \widehat{\mathbb{Z}}^\times$ and $-I \in \mathcal{G}$. Fix a subgroup B of $\mathcal{G}$ such that $[\mathcal{G}, \mathcal{G}] \subseteq B \subseteq \mathcal{G} \cap SL_2(\widehat{\mathbb{Z}})$.

Definition 1.2. *The family attached to pair $(\mathcal{G}, B)$ is the set of open subgroups of G of $\mathcal{G}$ such that $\det(G) = \widehat{\mathbb{Z}}^\times$ and $G \cap SL_2(\widehat{\mathbb{Z}}) = B$. We denote the family by $\mathscr{F}(\mathcal{G}, B)$.*

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

$$G_\gamma := \{g \in \mathcal{G}\colon g \cdot G = \gamma(\det(g))\}$$

where $\gamma\colon \widehat{\mathbb{Z}}^\times \longrightarrow \mathcal{G}/G$ is a continuous homomorphism.

The families $\mathscr{F}(\mathcal{G}, B)$ were first introduced by Zywina 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 section §4.

For the rest of the paper, by a *family of groups*, we mean a family attached to an arbitrary pair $(\mathcal{G}, B)$.

1.3. **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 $-I$. In order to show that all modular curves X_G of genus at most g, lie in finitely many families of twists, we will use a certain kind of special subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ that contains the group G.

Definition 1.3. *An open subgroup $H \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ is agreeable if $\det(H) = \widehat{\mathbb{Z}}^\times$, H contains scalar matrices, i.e. $\widehat{\mathbb{Z}}^\times I \subseteq H$ and the levels of H in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and $H \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ and $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ have the same odd prime divisors.*

Let $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ be an open subgroup. There exists a group $\mathcal{G}$, called the agreeable closure of G, which is minimal -with respect to inclusion- among all agreeable subgroups that contain G. The group G is normal in $\mathcal{G}$ and satisfies $[G, G] = [\mathcal{G}, \mathcal{G}]$. The genus of $\mathcal{G}$ is less than or equal to the genus of G.

In particular, the group G lies in the family $\mathscr{F}(\mathcal{G}, G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}))$. 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 conjugacy classes of all agreeable subgroups up to genus g.

We show in section §6 that $\mathscr{A}_g$ is a finite set. This leads to finitely many families, which we use in our classification:

Theorem 1.4. *Fix an integer g. There are finitely many pairs $((\mathcal{G}_i, B_i))_{i\in\{1,\dots,r\}}$, as in 1.2 satisfying the following:*

(1) For all $i \in \{1, \dots, r\}$, $\mathcal{G}_i$ is an agreeable subgroup of genus at most g.

(2) If G is an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ satisfying $\det(G) = \widehat{\mathbb{Z}}^*$ and $-I \in G$ then there is a $j \in \{1, ..., r\}$ such that after conjugating G in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, we have $G \in \mathscr{F}(\mathcal{G}_j, B_j)$.

Theorem 1.4 will be proved (in the language of modular curves) in §7.

In the following, we list the number of families of low genus. Note that the number of infinite families is given by the number of families minus the number of agreeable groups.

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

1.4. **Models of modular curves.** Let $\mathscr{F}(\mathcal{G}, B)$ be a family of groups in the sense of 1.2. Fix a group $G \in \mathscr{F}(\mathcal{G}, B)$. The family consists of groups of the form G_γ, where $\gamma\colon \widehat{\mathbb{Z}}^\times \to \mathcal{G}/G$ is a continuous homomorphism. Consider the associated modular curves X_G. Precomposing the function γ with the cyclotomic character we get a 1-cocycle $\xi\colon \mathrm{Gal}(\mathbb{Q}^{ab}) \longrightarrow \mathcal{G}/G$ of the modular curve X_G. We will show in section §7 that twisting the curve X_G with the cocycle ξ gives a modular curve $(X_G)_\xi$ and that $(X_G)_\xi = X_{G_\gamma}$. Hence the family $\mathscr{F}(\mathcal{G}, B)$ can be viewed

as a family of twists of modular curves.

Let Γ_G be the congruence subgroup of $SL_2(\mathbb{Z})$ consisting of matrices that are congruent modulo N to an element of $H := G \cap SL_2(\mathbb{Z}/N\mathbb{Z})$. In [Zyw22], a finite dimensional $\mathbb{Q}$-vector space $M_{k,G}$ is defined which carries an isomorphism $M_{k,G} \otimes \mathbb{C} \xrightarrow{\sim} M_k(\Gamma_G)$. The spaces $M_{k,G}$ are isomorphic to the global sections of a line bundle on X_G, which is very ample when k is large enough. It is this property that is used to produce a model for the modular curve X_G.

We will expand on the algorithm described by Zywina to compute a model for a fixed modular curve $X_G \in \mathscr{F}(\mathcal{G}, B)$. Viewing X_G as a representative in the family $\mathscr{F}(\mathcal{G}, B)$, assume a projective model C for X_G is computed via Zywina's method. In §7, we will explain how to twist the projective model C to compute models for any curve in the family $\mathscr{F}(\mathcal{G}, B)$.

1.5. **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 hand, for an arbitrary open subgroup $G \subseteq GL_2(\widehat{\mathbb{Z}})$ with $-I \in G$ and $\det(G) = \widehat{\mathbb{Z}}$, the only such algorithm is the one implemented in [Zyw22] which we describe in §3.

Consider the example

$$G = \left\langle \begin{pmatrix} 119 & 0 \\ 0 & 119 \end{pmatrix}, \begin{pmatrix} 9 & 8 \\ 936 & 937 \end{pmatrix}, \begin{pmatrix} 69 & 244 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 8 & 1 \end{pmatrix}, \begin{pmatrix} 55 & 769 \\ 10 & 33 \end{pmatrix}, \begin{pmatrix} 41 & 813 \\ 0 & 15 \end{pmatrix}, \begin{pmatrix} 1 & 8 \\ 0 & 1 \end{pmatrix} \right\rangle \subset GL_2(\mathbb{Z}/944\mathbb{Z})$$

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

$$\mathcal{G} = \left\langle \begin{pmatrix} 9 & 8 \\ 8 & 9 \end{pmatrix}, \begin{pmatrix} 1 & 8 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 8 & 1 \end{pmatrix}, \begin{pmatrix} 15 & 0 \\ 0 & 15 \end{pmatrix}, \begin{pmatrix} 7 & 0 \\ 0 & 7 \end{pmatrix}, \begin{pmatrix} 13 & 4 \\ 4 & 5 \end{pmatrix}, \begin{pmatrix} 12 & 9 \\ 11 & 4 \end{pmatrix}, \begin{pmatrix} 3 & 14 \\ 14 & 5 \end{pmatrix}, \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix} \right\rangle \subset GL_2(\mathbb{Z}/16\mathbb{Z})$$

$$B = \left\langle \begin{pmatrix} 7 & 0 \\ 0 & 7 \end{pmatrix} \right\rangle \subset SL_2(\mathbb{Z}/8\mathbb{Z})$$

On the same machine, Zywina's method took ~ 40 seconds to compute a model for the modular curve X_G (without the j-map), while our algorithm took ~ 6 seconds to compute a model and the j-map for the modular curve X_G.

Our algorithm uses effective Hilbert 90 and linear algebra methods to compute the modular curve X_G along with the j-map $X_G \to \mathbb{P}^1_{\mathbb{Q}}$ (after an initial and finite precomputation). Since it does not need to deal with computational aspects of computing q-expansions, it continues to be efficient as the level of X_G increases. Despite not computing q-expansions to find the models, it should be noted that the current implementation of our algorithm also computes a certain subspace of the space $M_{k,G}$ (see §3 for definition) by twisting.

1.6. **Motivation.** In [Maz77a], Mazur classifies the $\mathbb{Q}$ torsion of a non-CM elliptic curve E and describes the following program (widely known as Mazur's Program B):

Mazur's Program B. *Given a number field* K *and a subgroup* H *of* $GL_2(\widehat{\mathbb{Z}}) = \prod_p GL_2(\mathbb{Z}_p)$ *classify all elliptic curves* E/K *whose associated Galois representation on torsion points maps* $\mathrm{Gal}(\overline{K}/K)$ *<u>into</u>* $H \subseteq GL_2(\widehat{\mathbb{Z}})$.

Mazur's Program B serves as a motivation for finding projective models of modular curves, along with the computation of the j-map $\pi_G : X_G \to \mathbb{P}^1_{\mathbb{Q}}$. In addition, classification of modular curves of bounded genus into finitely many well-behaving families is helpful for tracking various properties of such curves.

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 $GL_2(\widehat{\mathbb{Z}})$.

In [Zyw22], it is conjectured that if $G \subset \mathrm{GL}_2(\widehat{\mathbb{Z}})$ is an open subgroup with subjective 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}).

Hence, as a follow up of our result we suggest the following program:

Program 1.5. *One can consider the following steps to resolve Mazur's Program B:*

(1) Prove Serre's uniformity problem (or a stronger version of it: Conjecture 1.2 in [Zyw22]).

(2) Classify all the 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 $\ell > 37$, the mod ℓ representation $\rho_{E,\ell}$ is surjective or not. By investigating maximal subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, works of Mazur [Maz78],[Maz77b] and Bilu, Parent and Rebolledo [BPR13] handled all cases but normalizer of non-split Cartan subgroups and modular curves $X_{ns}^+(\ell)$. Using Chabauty methods, Balakrishnan et al. [BDM+19], [BDM+23] determined rational points on $X_{ns}^+(\ell)$ for some small primes ℓ.

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

In [Zyw22], David 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 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 that works for elliptic curves over number fields.

[Rak24] has given a classification of genus 0 modular curves X_G over $\mathbb{Q}$ such that $\det(G) = \widehat{\mathbb{Z}}^\times$, $-I \in G$ and $X_G \cong \mathbb{P}^1_{\mathbb{Q}}$, in terms of families of abelian twists.

Let G be as above. In [SZ17], Sutherland and Zywina determine all such groups G of prime power level for which $X_G(\mathbb{Q})$ is infinite. This work additionally provides a classification for possible images of ℓ-adic Galois representations arising from elliptic curves for almost all j-invariants.

In [RSZB15], Rouse, Sutherland and Zureick-Brown give a classification of possible 2-adic images of Galois representations associated to elliptic curves over $\mathbb{Q}$.

Most recently [BBH+25] completed the classification of 3-adic images of Galois representations arising from elliptic curves, extending the work in [RSZB15].

1.8. **Implementation.** The implementation of our algorithm can be found in the repository [EK25]. All computations are done in MAGMA [BCP97].

Until section §7, we describe the necessary notions that we use in our algorithm. Finally in §8, we describe the algorithm for computing the model of an arbitrary modular curve X_G. The algorithm consists of two parts; a one-time precomputation that produces all the data we need and the second part, that takes an arbitrary G as input and produces a projective model for X_G. Practically, the precomputation that is needed to make our code work is the most computationally intense part of this project. We needed to compute a model for one modular curve in each family used in the main theorem. This sums up to tens of thousands of modular curves. The precomputation needed to implement the algorithm for modular curves up to genus 1 took 17 days in our department computers. The same precomputation for classifying modular curves up to genus 6 took 4-5 months.

1.9. **Further Work.** We would like to mention some immediate questions arising from our result.

We are working on generalizing the algorithm of section §9 to $\overline{\mathbb{Q}}$–gonality 3 modular curves.

In joint work with Yongyuan Huang and Rakvi, we are working on creating an algorithm to compute models of universal elliptic curve for subgroups G of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ with $\det(G) = \widehat{\mathbb{Z}}^\times$ and $-I \notin G$.

In joint work with Zachary Couvillion (yeah?), we are working on describing the Jacobian decomposition of modular curves in a fixed family $\mathscr{F}$.

1.10. **Acknowledgments.** I would like thank David Zywina for his valueable 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, Barinder Banwait and Eran Assaf for fruitful mathematical discussions.

1.11. **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

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

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 $-I \in G$.

2. Overview of the Paper

In section §3 , we review the background material on modular curves and modular forms. In section §4, we define a family of groups associated to a pair $(\mathcal{G}, B)$. These will turn out to be a family of abelian twists of modular curves. In section §5 we will discuss agreeable subgroups. We will also define the agreeable closure of a subgroup G and discuss how to compute it. In section §6 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 section §7, we will describe how to twist the spaces $M_{k,G}$ and discuss how we can twist the models of modular curves produced by Zywina's algorithm. In section §8, we finally describe an algorithm for computing the model of any modular curve up to genus g. This algorithm has been implemented up to genus 12. In section §9, we describe an algorithm to determine whether a geometrically hyperelliptic modular curve has $\mathbb{Q}-$gonality 2 or 4.

3. 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 such that $\det(G) = \widehat{\mathbb{Z}}^\times$ and $-I \in G$, let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. The first step is to consider the spaces of modular forms with respect to Γ. The modular curve X_G will be defined in an alternative way, using certain subspaces, denoted $M_{k,G}$.

Going back to the group G, it has a well defined level, and 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 and its image. 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 $G \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

3.1. **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 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 $\mathbb{C}$.

Let Γ be any congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. The quotient $X_\Gamma := \Gamma\backslash\mathcal{H}^*$ is a smooth compact Riemann surface [DS05]. Let g be the genus of the Riemann surface X_Γ. Let w be the width of the cusp ∞, i.e. the smallest positive integer such that $\left[\begin{smallmatrix} 1 & w \\ 0 & 1 \end{smallmatrix}\right] \in \Gamma$.

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

3.2. **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 known growth condition. This means that $f[\gamma]_k$ is holomorphic at infinity for all $\gamma in \mathrm{SL}_2(\mathbb{Z})$. 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 $q_w := e^{2\pi i/w}$, 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 weight k form a graded algebra denoted by

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

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

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

We let $M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$ be the space of modular forms with respect to $\Gamma(N)$ with coefficients in the N-th cyclotomic field.

3.3. **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 $f(\tau) = (c\tau + d)^k f(\gamma\tau)$ 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

$$f(\tau)\,(d\tau)^{k/2} = \left(\frac{w}{(2\pi i)}\right)^{k/2} \left(\sum_{n=0}^{\infty} a_n(f)\, q_w^n\right) \left(\frac{dq_w}{q_w}\right)^{k/2} \tag{3.1}$$

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 log divisor of Γ-equivalence classes of cusps. For any modular form $f \in M_k(\Gamma)$, we have $\mathrm{div}(\omega_f) + \mathcal{D}_k \geqslant 0$. Hence f gives an effective divisor linearly equivalent to $\mathcal{D}_k$. This defines a map of complex vector spaces

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

Moreover any differential form $H^0(\mathcal{X}_\Gamma, \Omega^1(\mathcal{D}_k)^{\otimes k/2})$ pulls back to a differential form on $\mathcal{H}$ as in (3.1). f is holomorphic and satisfies the growth conditions on 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:

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

3.4. **Eisenstein Series.** For our applications -in order to find models of modular curves- 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 completely generate $R_{\Gamma(N)}$.

Theorem 3.1. *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). One can then use the Eisenstein series and the dimension formulas for $M_k(\Gamma(N))$ to find explicit bases for $M_k(\Gamma(N))$ for arbitrary $k > 1$.

3.5. **Actions.** We will now describe a set of actions on $M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$ that will lead us to the spaces $M_{k,G}$.

Fix positive integers k and N. $\Gamma(N)$ is normal in $SL_2(\mathbb{Z})$ and the weight-k operator gives a right action on $M_k(\Gamma(N))$. Let $f = \sum_{n=0}^{\infty} a_n(f) q_N^n$ be a modular form in $M_k(\Gamma(N))$, where $w = N$. Let σ be a field automorphism of $\mathbb{C}$. σ 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 $\sum_{n=0}^{\infty} \sigma(a_n(f)) q_N^n$. This way, we get an action of $\mathrm{Aut}(\mathbb{C})$ on $M_k(\Gamma(N))$.

Consider the isomorphism $(\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$, $d \mapsto \sigma_d$, where $\sigma_d(\zeta_N) = \zeta_N^d$. We now describe an action of $GL_2(\mathbb{Z}/N\mathbb{Z})$ on $M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$ viewed as a $\mathbb{Q}$-vector space.

Lemma 3.2. *There is a unique right action $*$ of $GL_2(\mathbb{Z}/N\mathbb{Z})$ on $M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$ such that the following hold:*

- *if $A \in SL_2(\mathbb{Z}/N\mathbb{Z})$, then $f * A = f|_k\gamma$, where γ is any matrix in $SL_2(\mathbb{Z})$ 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 3.2 for all k, we get a right action $*$ of $GL_2(\mathbb{Z}/N\mathbb{Z})$ on the graded ring $\bigoplus_{k\geqslant 0} M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$. Tensoring the spaces $M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$ with $\mathbb{C}$ gives a natural isomorphism

$$M_k(\Gamma(N), \mathbb{Q}(\zeta_N)) \otimes_{\mathbb{Q}(\zeta_N)} \mathbb{C} \to M_k(\Gamma(N))$$

cf. [Kat73]. For any congruence subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ whose level divides N, taking Γ-invariants gives a natural isomorphism of complex vector spaces

$$M_k(\Gamma, \mathbb{Q}(\zeta_N)) \otimes_{\mathbb{Q}(\zeta_N)} \mathbb{C} \to M_k(\Gamma) \tag{3.2}$$

In particular, the action $*$ is well understood on the Eisenstein series mentioned above:

Lemma 3.3. *Let* $(a_1, b_1), \ldots, (a_k, b_k)$ *and* $A \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. *We have*

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

3.6. **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 3.2. Note that $M_{k,G} \subseteq M_k(\Gamma(N), \mathbb{Q}(\zeta_N))^{G \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})} = M_k(\Gamma_G, \mathbb{Q}(\zeta_N))$.

Similar to 3.2, tensoring $M_{k,G}$ with $\mathbb{Q}(\zeta_N)$ and $\mathbb{C}$ give natural isomorphisms.

Lemma 3.4. *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] □

3.7. **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 spaces $M_{k,G}$ given by

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

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 3.5. *The modular curve* X_G *associated to group* G *is the smooth, geometrically irreducible curve over* $\mathbb{Q}$ *given by* $\mathrm{Proj}(\bigoplus_{k=0}^{\infty} M_{k,G})$.

Remark 3.6. 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.

When $G := \mathrm{GL}_2(\widehat{\mathbb{Z}})$, we have that $X_G = \mathrm{Proj}(\bigoplus_{k=0}^{\infty} M_{k,G}) = \mathrm{Proj}(\mathbb{Q}[E_4, E_6])$. We can identify this curve with $\mathbb{P}^1_{\mathbb{Q}}$. It is commonly called as the j-line.

Let's consider the inclusions $G \subseteq G' \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ where G and G' are open subgroups of full determinant. It induces 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 j-map $\pi\colon X_G \to \mathbb{P}^1_{\mathbb{Q}}$

3.7.1. *Compatibility with other definitions.* Consider the space of modular forms $M_k(\Gamma_G)$ as in section §3.2. It is a finite dimensional complex vector space. The map ψ_k shows us that $M_k(\Gamma_G)$ is isomorphic to $H^0(\mathcal{X}_\Gamma, \Omega^1(\mathcal{D}_k)^{\otimes k/2})$, the global sections of the line bundle $\Omega^1(\mathcal{D}_k)^{\otimes k/2}$ on the Riemann surface $\mathcal{X}_\Gamma$. Let's consider the graded ring $R_\Gamma := \bigoplus_{k\geqslant 0} M_k(\Gamma)$. R_Γ 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 $\mathrm{Proj}(R_\Gamma) \cong \mathcal{X}_\Gamma$ as schemes.

Similarly, the graded ring $R := \mathrm{Proj}(\bigoplus_{k=0}^{\infty} M_{k,G})$ is finitely generated over $\mathbb{Q}$. Lemma 3.4 shows that tensoring R with $\mathbb{C}$ gives the ring R_Γ. 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 $\mathcal{X}_{\Gamma_G} \to \mathbb{P}^1_{\mathbb{C}}$.

We will now compare our definition of the modular curve X_G with other definitions in the literature. The well known modular curve $X(N)$ of level N can be defined in different ways. In particular, there are the big modular curve $X(N)^{\mathrm{big}}$, the classical modular curve $X(N)$ and the arithmetic modular curve $X(N)^{\mathrm{arith}}$. The Deligne-Rapaport definition of X_G as the generic fiber of the smooth proper $\mathbb{Z}[1/N]$-scheme which is the coarse moduli space for the algebraic stack M_G is commonly used, however we do not prefer it in view of our computational approach. [Zyw22] (and many previous papers) defines the modular curve X_G by explicitly giving its function field. Let's show that our definition is equivalent to Zywina's definition.

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 log divisor defined in equation (4.3) in loc. cit. The divisor D_k is defined over $\mathbb{Q}$ so we can consider it as a divisor on X_G where we view X_G as defined in loc. cit. 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 in [Zyw22] that the map ψ_k induces an isomorphism between $M_{k,G}$ and $H^0(X_{\gamma_G}, \mathscr{L}_k)$. 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.

3.8. **Models of Modular Curves.** In our applications, we need to compute models for a finite set of modular curves X_G. Our definition of X_G uses the space of modular forms $M_{k,G}$ and so the method described in [Zyw22], which uses $M_{k,G}$ to get an explicit projective model suits our purposes. In this section, we will briefly describe this method.

Let G be as above and let N be a positive integer divisible by the level of G. Consider $\mathcal{X}_{\Gamma_G}$ which we identify with $X_G(\mathbb{C})$. Let $P_1, \cdots, P_r$ be the cusps of $X_G(\mathbb{C})$. They 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 using computing Eisenstein series and multiplying them. Note that $f_j/f_i \in \mathbb{Q}(X_G)$, a rational function of X_G. The modular forms $f_0, \cdots, f_d$ define a morphism

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

via $\varphi(P) = [f_0(P), \ldots, f_d(P)]$ for all but finitely many P. Up to an automorphism of $\mathbb{P}^d_{\mathbb{Q}}$, the map φ does not depend on the choice of basis. The image of X_G is a curve in $\mathbb{P}^d_{\mathbb{Q}}$, we denote it 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 $I(C)_n$.

To get a model of X_G, we want an invertible sheaf $\mathcal{F}$ such that the image $\psi_k(V)$ gives the global sections of $\mathcal{F}$. One observes that $\mathcal{F} := \mathscr{L}_k(-E)$ on X_G satisfies this when E is chosen carefully, i.e. 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. Then the degree of $\mathcal{F}$ is given by

(3.3)
$$\deg \mathcal{F} = \deg \mathscr{L}_k - \sum_{i=1}^{r} e_i = k/2 \cdot (2g-2) + k/2 \cdot r + \lfloor k/4 \rfloor \cdot \nu_2 + \lfloor k/3 \rfloor \cdot \nu_3 - \sum_{i=1}^{r} e_i.$$

3.8.1. *Getting the model for* X_G. First, assume that $g \geqslant 3$. Choosing the divisor $E = \sum_{i=1}^{r} P_i$, we can compute the canonical map $\varphi \colon X_G \to \mathbb{P}^{g-1}_{\mathbb{Q}}$ (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. Define a homomorphism

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

by $x_i \to \psi_k(f_i)$. In this case, η is an isomorphism of $\mathbb{Q}$-algebras.

In any other case, 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, using the above argument, we see that φ is an embedding and $C := \varphi(X_G)$ is isomorphic to X_G.

4. Families of Modular Curves

In the previous section, we have defined the modular curve X_G associated to $G \subseteq \mathrm{GL}_2 \widehat{\mathbb{Z}}$ with $\det(G) = \widehat{\mathbb{Z}}$ and $-I \in G$. In this section, we give a definition of the families of groups (more precisely open subgroups of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$) that we use in our classification and collect some results about them. Later in §7, we will show that these families of groups correspond to families of modular curves in a natural way.

Let $\mathcal{G}$ be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ satisfying $\det(\mathcal{G}) = \widehat{\mathbb{Z}}^\times$ and $-I \in \mathcal{G}$. Fix a closed subgroup B of $\mathcal{G}$ satisfying $[\mathcal{G}, \mathcal{G}] \subseteq B \subseteq \mathrm{SL}_2(\widehat{\mathbb{Z}})$.

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

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

$$G_\gamma := \{g \in \mathcal{G} : g \cdot G = \gamma(\det g)\}$$

We claim that our family $\mathscr{F}(\mathcal{G}, B)$ consists of groups of the form G_γ:

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

There is a result in [Zyw24] which gives a criterion for deciding the existence of an element in families. 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. Let U be an open subgroup of $\det(\mathcal{G})$ (in our case this is the whole group $\widehat{\mathbb{Z}}^\times$). We define $N_1 := N$ if N is odd and $N_1 := \mathrm{lcm}(N, 8)$ if N is even. Then

Theorem 4.3. *([Zyw24] Theorem 4.5) Let U be an open subgroup of $\det(\mathcal{G})$ 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 $G \cap SL_2(\widehat{\mathbb{Z}}) = B$ 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 the least common multiple of N and level of $U \subseteq \widehat{\mathbb{Z}}^\times$.

In particular, it is mentioned in Remark 4.6 in [Zyw24] that in the case such a group G exists, it can be found by a direct search at levels $2^i N$ for $i \in \mathbb{N}$. An algorithm for this kind of search has been implemented for use in loc. cit.

Theorem 4.4. *Let $G, H \in \mathscr{F}(\mathcal{G}, B)$ and assume that $I \in B$. 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 $\Gamma_G = \Gamma_H$. Hence as Riemann surfaces $X_H(\mathbb{C})$ and $X_G(\mathbb{C})$ are both isomorphic to $\mathcal{X}_{\Gamma_G}$. 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 $|H| = |B| \cdot \phi(N)$.

□

4.1. **Canonical Representatives.** Let $\mathscr{F}(\mathcal{G}, B)$ be a non-empty family. Following the work of Andrew Sutherland, there is a canonical choice of representative for $\mathscr{F}$.

4.1.1. *Similarity Invariants and Canonical Generators.* Consider $M_2(\mathbb{Z}/p^e\mathbb{Z})$ of 2×2 matrices. We call that A and B are similar if $EA = BE$ for some $E \in \mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$.

Lemma 4.5. *Each $M \in M_2(\mathbb{Z}/p^e\mathbb{Z})$ is similar to a matrix of the form*

$$\alpha := dI + p^j \begin{bmatrix} 0 & 1 \\ \det(p^{-j}(M - dI)) & \mathrm{tr}(p^{-j}(M - dI)) \end{bmatrix}$$

where $j \in 0, \dots, e$ *maximal such that* M *is congruent to a scalar matrix* mod p^j, $dI = M \bmod p^j$.

Proof. Lemma 2.2 in [AOPV09]. □

This assignment $M \to \mathrm{inv}(M) := \alpha$ is a similarity invariant. Sutherland extends this invariant to general moduli $N = p_1^{e_1} \cdots p_n^{e_n}$ with $p_1 < \cdots < p_n$ via

$$\mathrm{inv}(M) := (\mathrm{inv}(M) \bmod p_1^{e_1}, \cdots, \mathrm{inv}(M) \bmod p_n^{e_n}).$$

Lemma 4.6. *Two matrices* $A, B \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ *are conjugate if and only if* $\mathrm{inv}(A) = \mathrm{inv}(B)$.

Given an open $H \leqslant \mathrm{GL}_2(\widehat{\mathbb{Z}})$, we wants to choose a representative of the conjugacy class of H, $[H]$ and generators for this representative. This is done in LMFDB as follows:

First, we fix an ordering of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ of conjugacy classes of elements $[g]$, sorting by decresing $|g|$, $\#[g]$ and by decreasing similarity invariants. Then the canonical generators for H of level N are the lexicographically minimal sequence $h_1, \dots, h_n \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ such that

- $h_1, \dots, h_n$ generate $H(N)$ and $H(N) \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) = \langle h_1, \dots, h_m \rangle$ for some $m \leqslant n$.
- $\langle h_1, \dots, h_j \rangle < \langle h_1, \dots, h_{j+1} \rangle$.
- $[h_1], \dots, [h_m]$ and $[h_{m+1}], \dots, [h_n]$ are nondecreasing.

This leads us to the following definition.

Definition 4.7. Let $\mathscr{F}(G, B)$ be a family of groups where $-I \in B$. Let S be the set of groups (up to conjugacy) in $\mathscr{F}$ with minimal level in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. *The canonical representative* for $\mathscr{F}$ is the group $H \in S$ such that the canonical generators of H is lexicographically minimal among the canonical generators of all groups in S.

In our definition for families of groups, we do not have strict conditions on G. Since there are infinitely many such open subgroups of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, there are infinitely many such families. In the next section we will describe a special family of subgroups of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ which will be used to construct the finitely many families we need.

5. Agreeable Subgroups

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

We say that a subgroup G of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ is agreeable if it is open in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, satisfies $\det(G) = \widehat{\mathbb{Z}}^\times$, contains all the scalar matrices, each prime dividing the level of $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ and $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) \subseteq \mathrm{SL}_2(\widehat{\mathbb{Z}})$ 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 we will be interested in:

Proposition 5.1. *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*

$$G := (\mathbb{Z}_N^\times \cdot G_N) \times \prod_{\ell \nmid N} \mathrm{GL}_2(\mathbb{Z}_\ell) \tag{5.1}$$

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* $\mathsf{G} \subseteq \mathcal{G}$. *We call* $\mathcal{G}$ *the agreeable closure of* G. *We have* $[\mathsf{G},\mathsf{G}] = [\mathcal{G},\mathcal{G}]$ *and hence* G *is a normal subgroup of* $\mathcal{G}$ *with* $\mathcal{G}/\mathsf{G}$ *finite and abelian.*

Proof. This is Proposition 8.1 in [Zyw22]. □

Remark 5.2. Note that the integer N is even since the commutator subgroup G always has even level. The group $\mathcal{G}$ contains the group G and the scalar matrices $\widehat{\mathbb{Z}}^\times \cdot \mathrm{I}$. The scalar matrices are contained in the center of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ so G_N and $\widehat{\mathbb{Z}}^\times \cdot \mathsf{G}_\mathsf{N}$ have the same commutator subgroups.

5.1. **Constructing the agreeable closure.** The statement of 5.1 implies that the level of $[\mathsf{G},\mathsf{G}]$ 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 high or contains large prime factors. However, we can relate the levels of $[\mathsf{G},\mathsf{G}]$ and $\mathsf{G} \cap \mathrm{SL}_2\,\widehat{\mathbb{Z}}$.

Lemma 5.3.

(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 $[\mathsf{G},\mathsf{G}]$ only by looking at the level of $\mathsf{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$. The latter is easier to compute on most computer algebra systems.

Lemma 5.4. *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 5.5. *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.
Assume now that the level of G is an odd integer and N be as above. Then G_N and $\mathsf{G}_{\mathsf{N}/2}$ have the same inverse image in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and hence $\mathcal{G}$ has odd level. □

Fix an open subgroup $\mathsf{G} \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ that satisfies $\det(\mathsf{G}) = \widehat{\mathbb{Z}}^\times$ and $-\mathrm{I} \in \mathsf{G}$. The agreeable closure of G gives us a natural choice of family of groups which contains G.

Corollary 5.6. *Let* G *be as above. Let* $\mathsf{T} = \mathsf{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$. *Let* $\mathcal{G}$ *be the agreeable closure of* G. *Then* $\mathsf{G} \in \mathscr{F}(\mathcal{G},\mathsf{T})$.

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 $G \in \mathscr{F}(\mathcal{G}, T)$. □

Remark 5.7. Note that the genus of $\mathcal{G}$ is less than or equal to the genus of G.

Our goal is to compute a finite number of families $\mathscr{F}(\mathcal{G}, B)$ that can be used in the classification. The above corollary implies that in place of $\mathcal{G}$'s, it is sufficient to use agreeable subgroups of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

6. Finiteness of Agreeable Subgroups

Fix a positive 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] in a more general setting. We first start by some observations.

Let G be an agreeable subgroup of genus at most g. Let $H := G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ be the 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 its level. 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 is given in the [CP03] database.

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

Theorem 6.1. *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 $N_1 := 2 \cdot \mathrm{lcm}(N, 12)$. The following lemma is central to the proof. It is also proven in [Zyw24].

Lemma 6.2. *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 $N' = \mathrm{lcm}(N, 12)$. 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 that $[H, H] \subset [G, G]$ and 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 $\mathbb{Z}_{N_1}^\times \cdot H$ is contained in G_{N_1} and it follows from [Zyw22] Lemma 7.6 that $\mathbb{Z}_{N_1}^\times \cdot H$ is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_{N_1})$ whose level divides N_1 (note that this is where we need the additional factor of 2). We conclude that the level of G_{N_1} divides N_1.

□

Let Γ and H be as above. Assume $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ is an agreeable subgroup with $G \cap \mathrm{SL}(\widehat{\mathbb{Z}}) = H$. We have seen that G has level dividing N_1, so G corresponds to a subgroup $\bar{G}$ of $\mathrm{GL}_2(\mathbb{Z}/N_1\mathbb{Z})$ such that $\bar{G} \cap \mathrm{SL}_2(\mathbb{Z}/N_1\mathbb{Z}) = \bar{H}$. There are only finitely many such subgroups of $\mathrm{GL}(\mathbb{Z}/N_1\mathbb{Z})$, so only finitely many agreeable subgroups of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ arise from a the 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 $\mathrm{GL}_2(\mathbb{Z}/N_1\mathbb{Z})$ for subgroups $\bar{G}$ with $(\mathbb{Z}/N_1\mathbb{Z})^\times \subseteq \bar{G}$, $\det(\bar{G}) = \mathbb{Z}/N_1\mathbb{Z}$, $-I \in \bar{G}$ and $\bar{G} \cap \mathrm{SL}(\mathbb{Z}/N_1\mathbb{Z}) = \bar{H}$. These groups give rise to finitely many, potentially agreeable, subgroups $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ such that $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = H$. For each such G, we then check if it is an agreeable subgroup, i.e. if its $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ 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 $\mathscr{A}_g$ a set of representatives of conjugacy classes of all agreeable subgroups up to genus g.

Remark 6.3. An open subgroup G may lie in more than one family. However, Corollary 5.6 suggests a canonical choice of family that contains G, i.e the family $\mathscr{F}(\mathcal{G}, B)$ where $\mathcal{G}$ is the agreeable closure of G and $B = G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$. We have a description of $\mathcal{G}$ that depends on G and B. In particular, we can easily compute the group $\mathcal{G}$ and subsequently identify the family $\mathscr{F}(\mathcal{G}, B)$ which contains G.

We are ready to state our main result in terms of families of groups.

Theorem 6.4. *Fix a positive integer g. Let G be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ such that $\det(G) = \widehat{\mathbb{Z}}^*$ and $-I \in G$. There are finitely many pairs $((\mathcal{G}_i, B_i))_{i \in \{1,\dots,r\}}$, as in §4, such that if G has genus at most g, then, up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, $G \in \mathscr{F}(\mathcal{G}_j, B_j)$ for some $j \in \{1, \dots, r\}$.*

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 $\mathcal{A}_g$. For each agreeable subgroup $\mathcal{G} \in \mathcal{A}_g$, the groups $[\mathcal{G}, \mathcal{G}]$ and $\mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ are open subgroups of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$, hence there are finitely many subgroups B of $\mathcal{G}$ such that $[\mathcal{G}, \mathcal{G}] \subseteq B \subseteq \mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$. Combining $\mathcal{G}$'s and B's, we get a finite set of pairs $(\mathcal{G}_i, B_i)$ and associated families $\mathscr{F}(\mathcal{G}_i, B_i)$.

Let G be as above, whose genus is at most g. Then G lies in the family $\mathscr{F}(\mathcal{G}, B)$ where $B = G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ and $\mathcal{G}$ is the agreeable closure of G. $\mathcal{G}$ has genus at most g and so it is conjugate to an agreeable subgroup $\mathcal{G}'$ in the finite set $\mathcal{A}_g$ and G is conjugate to a subgroup $G' \subseteq \mathcal{G}'$. We conclude that G is conjugate to a group lying in the family $\mathscr{F}(\mathcal{G}', B')$ where $B' = G' \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$, proving the assertion. □

7. Twisting Modular Curves

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

Fix a family $\mathscr{F}(\mathcal{G}, B)$ and fix a group $G \in \mathscr{F}(\mathcal{G}, B)$. Consider the modular curve X_G. There is the projection map $\pi_G \colon X_G \to X_{\mathcal{G}}$. We start with a definition:

Definition 7.1. Let H be a group in $\mathscr{F}(\mathcal{G}, B)$, X_H be the associated modular curve, and let $\pi_H : X_H \to X_{\mathcal{G}}$ be the morphism coming from the inclusion $H \subseteq \mathcal{G}$. A $\mathcal{G}$–twist of (X_H, π_H) is a pair (X_K, π) where X_K is a modular curve over $\mathbb{Q}$ with a morphism $\pi : X_K \to X_{\mathcal{G}}$ coming from the inclusion $K \subseteq \mathcal{G}$, such that there is an isomorphism $f : (X_H)_{\mathbb{Q}^{ab}} \to (X_K)_{\mathbb{Q}^{ab}}$ that satisfies $\pi \circ f = \pi_H$.

Remark 7.2. The curves X_H and Y above can be isomorphic over a subfield $K \subseteq \mathbb{Q}^{ab}$. We call them isomorphic if there is an isomorphism $(X_H)_{\mathbb{Q}} \to Y_{\mathbb{Q}}$.

Consider the family $\mathscr{F}(\mathcal{G}, B)$ and the group G above. Let $\pi \colon X_G \to X_{\mathcal{G}}$ be the morphism of modular curves induced by the inclusion $G \subseteq \mathcal{G}$. G is a normal subgroup of $\mathcal{G}$. $\mathcal{G}$ acts on $M_{k,G}$ for all k and consequently on X_G . The subgroup G acts trivialy on X_G so there is an action of $\mathcal{G}/G$ on X_G. We have $\mathrm{Aut}(X_G/X_{\mathcal{G}}) \cong \mathcal{G}/G$ where $\mathrm{Aut}(X_G/X_{\mathcal{G}})$ is the group of automorphisms f of the curve X_G that satisfy $\pi \circ f = \pi$. Note that these are modular automorphisms and since there is a natural isomorphism $\mathcal{G}/G \simeq (\mathcal{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}))/B$ and the automorphisms in $\mathrm{Aut}(X_G/X_{\mathcal{G}})$ are defined over $\mathbb{Q}$.

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

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

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

Lemma 7.3. *There is a bijection between $\mathcal{G}$–twists of X_G and $\mathrm{H}^1(\mathrm{Gal}(\mathbb{Q}^{ab}), \mathrm{Aut}(X_G/X_{\mathcal{G}}))$.*

Proof. □

Let G be as above and X_G be the associated modular curve. Let $H := G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$. Let $\gamma : \widehat{\mathbb{Z}}^\times \to \mathcal{G}/G$ be a 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 will now prove that $(X_G)_\xi = X_{G_\gamma}$, where G_γ is the group defined in §4.

We will start with X_{G_γ} and prove that it's equal to the curve $(X_G)_\xi$. Before that, let's write down the various actions we have on modular forms. We first 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 §3, one can see that

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

Firstly, there is an action of $\mathcal{G}$ on $M_{k,G}$ where G acts trivially. Hence there is an induced action of $\mathcal{G}/G$. Note that this is an action on only $M_{k,G}$.

The group $\mathcal{G}$ also acts on $M_{k,G} \otimes \mathbb{Q}^{ab}$ separately . Let $g \in \mathcal{G}$ and $\sigma \in \mathrm{Gal}(\mathbb{Q}^{ab})$ such that $\chi_{cyc}(\sigma) = \det(g)$. Then 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. We restrict the action of $\mathcal{G}$ to G and G_γ and get the induced actions of G/H and G_γ/H on $M_{k,G} \otimes \mathbb{Q}^{ab}$. Composing these with the isomorphisms

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

and

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

we get two different Galois actions on $M_{k,G} \otimes \mathbb{Q}^{ab}$.

Denote by cf, the element $f \otimes c \in M_{k,G} \otimes \mathbb{Q}^{ab}$. We define another action of $\mathrm{Gal}(\mathbb{Q}^{ab})$ on $M_{k,G} \otimes \mathbb{Q}^{ab}$ via $\sigma \bullet (cf) := \sigma(c)(\xi_\sigma(f))$ where $\xi_\sigma(f)$ denotes the action of $\mathcal{G}/G$ on $M_{k,G}$ via the cocycle. Remember that we have defined X_G as the scheme $\mathrm{Proj}(\bigoplus_{k=0}^{\infty} M_{k,G})$. The action $\bullet$ on $M_{k,G}$ induces an action of $\mathrm{Gal}(\mathbb{Q}^{ab})$ on the $\mathbb{Q}^{ab}$ algebra $\bigoplus_{k=0}^{\infty} M_{k,G} \otimes \mathbb{Q}^{ab}$. Let

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

For each graded piece of $\bigoplus_{k=0}^{\infty} M_{k,G} \otimes \mathbb{Q}^{ab}$, we define the twisted space $(M_{k,G})_\xi$ by

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

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

Lemma 7.4. *If* $\sigma \in \mathrm{Gal}(\mathbb{Q}^{ab})$ *and* $g \in G_\gamma$ *with* $\det(g) = \chi_{cyc}(\sigma)$ *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 $\sigma \cdot (cf) = \sigma(c)(\xi_\sigma(f)) = (\xi_\sigma(f)) \otimes \sigma(c)$. 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 $(cf) * g = \sigma(c)f * g = f * g \otimes \sigma(c) = \xi_\sigma(f) \otimes \sigma(c) = \sigma \cdot (cf)$. □

Thus, we see that the spaces M_{k,G_γ} and $(M_{k,G})_\xi$ are the same:

Theorem 7.5. $(M_{k,G})_\xi = M_{k,G_\gamma}$.

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 result:

Corollary 7.6.

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

In other words, $X_{G_\gamma} := \mathrm{Proj}((R_G)_\xi)$. 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 $(X_G)_\xi$. We can now restate our main theorem 6.4 in terms of modular curves:

Theorem 7.7. *Fix an integer* g. *Let* G *be an open subgroup of* $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ *such that* $\det(G) = \widehat{\mathbb{Z}}^*$ *and* $-I \in G$. *Let* X_G *be the associated modular curve. There are finitely many pairs* $((\mathcal{G}_i, B_i))_{i\in\{1,\dots,r\}}$, *as in 6.4, such that if* X_G *has genus at most* g, *then* $X_G \in \mathscr{F}(\mathcal{G}_j, B_j)$ *for some* $j \in \{1, \dots, r\}$.

Proof. The family of groups mentioned in 6.4 corresponds to a family of twists of modular curves. □

We denote by $\mathscr{F}_g$ the finite set of families arising from the set of agreeable subgroups $\mathscr{A}_g$. $\mathscr{F}_g$ has been computed for $g = 24$.

7.0.1. *Getting a basis for* M_{k,G_γ}. Assume that, using the methods described in section 3.8, 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 so we can compute the action of any $gG \in \mathcal{G}/G$ on the basis $\mathcal{B}$ and get a matrix in $\mathrm{GL}_{d+1}(\mathbb{Q}^{ab})$. Hence, for any 1-cocycle $\xi : \mathrm{Gal}(\mathbb{Q}^{ab}) \to \mathcal{G}/G$, we get a cocycle $\bar{\xi} : \mathrm{Gal}(\mathbb{Q}^{ab}) \to \mathrm{GL}_{d+1}(\mathbb{Q}^{ab})$. By Hilbert 90 theorem, $H^1(\mathrm{Gal}(\mathbb{Q}^{ab}), \mathrm{GL}_{d+1}(\mathbb{Q}^{ab}))$ 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 $\sigma \in \mathrm{Gal}(\mathbb{Q}^{ab})$. Applying the matrix A^{-1} on the basis $\mathcal{B}$, we get a set of modular forms $\mathcal{B}'$ which forms a basis of $M_{k,G_\gamma} \otimes \mathbb{Q}^{ab}$. M_{k,G_γ} is defined over $\mathbb{Q}$ so by applying Galois descent, we can get a basis $\mathcal{C}$ of $M_{k,G_\gamma} \otimes \mathbb{Q}^{ab}$ defined over $\mathbb{Q}$ and hence get a basis of M_{k,G_γ}.

7.1. **Twisting The Models of Modular Curves.** Assume that we have an explicit smooth projective model $C \subseteq \mathbb{P}^d_{\mathbb{Q}}$ for X_G where $G \in \mathscr{F}(\mathcal{G}, B)$. The model C arises from linearly independent modular forms $f_0, \dots, f_d \in M_{k,G}$ as explained in §3. In particular C is defined by $F_1, \dots, F_s \in \mathbb{Q}[x_0, \dots, x_d]$ where $F_i(f_0, \dots, f_d) = 0$. Let γ and ξ be as above. To get an explicit model for the modular curve X_{G_γ}, let $(F_i)_\xi := F_i((x_0, ..., x_d)A^T)$.

Theorem 7.8. *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 projective model of* X_{G_γ}.

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

Applying A^{-1} to the basis $\mathcal{B}$ in 7.0.1, we get a basis $\mathcal{B}'$ for M_{k,G_γ}. Even though the modular forms we get do not have coefficients in $\mathbb{Q}$, they are defined over $\mathbb{Q}$. The polynomials $(F_i)_\xi$ satisfy the basis $\mathcal{B}'$, so they give a curve that is isomorphic to X_{G_γ} over $\mathbb{Q}^{ab}$. Combining this with the previous paragraph one checks that $(F_i)_\xi$ have rational coefficients, i.e. the ideal $\langle (F_i)_\xi \rangle$ is defined over $\mathbb{Q}$. □

7.1.1. *Computing the matrix* A. The description for getting a basis of M_{k,G_γ} involved working over the field $\mathbb{Q}^{ab}$. In practice, we work over the field $\mathbb{Q}(\zeta_N)$ where N is the least common multiple of the levels of $\mathcal{G}, G$ and B. Let $\mathrm{Gal}(\mathbb{Q}(\zeta_N))$. The Hilbert 90 Theorem states that $H^1(G, \mathrm{GL}_n(\mathbb{Q}(\zeta_N)))$ is the trivial group so given a cocycle $\eta \in H^1(G, \mathrm{GL}_n(\mathbb{Q}(\zeta_N)))$ 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 (cite Serre, which serre?). In practice, we are using the algorithm and implementation given in [Rak24] in section §5.3.

8. 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 $G \subseteq GL_2(\widehat{\mathbb{Z}})$ is an open subgroup with full determinant, contains $-I$ and with genus at most g for a fixed genus g.

Our algorithm has two parts. Firstly, the families mentioned in Proposition 7.7 must be computed along with a chosen representative for each family. Using this precomputed data, we then provide an algorithm that given a modular curve finds the family it lies in, computes the cocycle with respect to the representative, and twists the representative curve to get the projective model.

8.1. **Precomputation.** Fix a genus g. In this section, we describe the necessary one time precomputation for our algorithm to work.

(i) Compute all the agreeable subgroups of $GL_2(\widehat{\mathbb{Z}})$ whose genus is at most g, up to conjugacy. We have described an algorithm in the proof of 6.1 for computing them.

(ii) Consider the set $\mathcal{A}_g$ as in section §6. For each $\mathcal{G} \in \mathcal{A}_g$, compute the subgroups B such that $[\mathcal{G}, \mathcal{G}] \subseteq B \subseteq \mathcal{G} \cap SL_2(\widehat{\mathbb{Z}})$. Note that$[\mathcal{G}, \mathcal{G}]$ and $\mathcal{G} \cap SL_2(\widehat{\mathbb{Z}})$ are open subgroups of $SL_2(\widehat{\mathbb{Z}})$, 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 as no modular curves we care about lies in them. Theorem 4.3 gives a method for this computation.

(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 section §3. 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 $i = 1, \cdots, s$.

(vi) For $W \in \mathscr{F}(\mathcal{G}, B)$, compute the matrices in $GL_{d+1}(\mathbb{Q}^{ab})$ that describe the action of $gW \in \mathcal{G}/W$ on the span of $\{f_0, \cdots, f_d\}$ for all elements in $\mathcal{G}/W$. (This step makes it easier to compute the cocycle $\bar{\xi}$ below.)

Remark 8.1. Here are some remarks about the precomputation:

- For the first step, we start from the data of congruence subgroups of $SL_2(\mathbb{Z})$ which is given in [CP03]. Since these groups are given up to conjugacy, we get the set $\mathscr{A}_g$ mentioned in section 6.
- Note that both $[\mathcal{G}, \mathcal{G}]$ and $\mathcal{G} \cap SL_2(\widehat{\mathbb{Z}})$ are open subgroups of $SL_2(\widehat{\mathbb{Z}})$ and hence they have finite index in $SL_2(\widehat{\mathbb{Z}})$.
- Theorem 4.3 gives a criterion for checking whether a family is empty or not. Based on this theorem, an implementation is given by David Zywina 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 $k \in \mathbb{N}$.

8.2. **Computing The Model.** Once the precomputation is done, we can use that data to use the algorithm below. It takes an open subgroup $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ as input.

Algorithm 8.2. Let $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ be an open subgroup with full determinant, contains $-I$ and X_G has 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}. Then compute the related cocycle $\overline{\xi}$.

(v) Compute the Hilbert 90 matrix A, as described above.

(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 $G_1, \cdots, G_s$ defining X_G that are defined over $\mathbb{Q}$. By Theorem 7.8, the curve defined by G_i is a projective model of X_G.

Remark 8.3. It is important that a modular curve X_G lies in a unique family in our algorithm, which depends on the agreeable closure of G, denoted by $\mathcal{G}$.

- 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 familiy and let N_1, N_2 be the levels of $\mathcal{G}$ and W, respectively. The level of G does not depend on 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 computating the cocycle $\mathbb{Z}/N\mathbb{Z} \to \mathcal{G}/W$.
- We use the precomputation in part (iv) to compute the associated cocycle $\overline{\xi} : \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}) \to \mathrm{GL}_{d+1}(\mathbb{Q}^{\mathrm{ab}})$. This makes the computation of $\overline{\xi}$ significantly faster.

This algorithm has been implemented for genus up to 12. You can find it in the repository [EK25].

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

We refer to [Poo07] and [Zyw25] for general facts about the gonality of modular 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. David Zywina [Zyw25] showed 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 Zywina's paper in terms of their labels in the classification of [CP03]. This recent classification of

geometrically hyperelliptic curves allows us to have an algorithm that computes whether a geometrically hyperelliptic curve has $\mathbb{Q}-$gonality 2 or 4.

Assume that X_G is a modular curve that has geometric gonality 2. This means that X_G corresponds to one of the congruence subgroups Zywina's classification. The finitely many congruence subgroups (up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$) give rise to finitely many families of geometrically hyperellipttic modular curves in the sense of sections §4 and §6. Note that we call these families geometrically hyperelliptic because all the modular curves in the family are isomorphic to a hyperelliptic modular curve over $\mathbb{X}$. Going back to X_G, 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 [Zyw20]. If the curve C has a rational point then C is isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$ and X_G has $\mathbb{Q}-$gonality 2. We can use this setting and the twisting algorithm mentioned in the previous sections to compute the $\mathbb{Q}$-gonality of any geometrically hyperelliptic modular curve.

9.0.1. *Computing Gonality:* Assume X_G is geometrically hyperelliptic i.e. it has $\overline{\mathbb{Q}}-$gonality 2. The canonical model of X_G can be computed as described in Section §3.8. In particular, it is computed using the space of modular forms $M_{k,G}$ (or a subspace $V \subseteq M_{k,G}$).

Let $\mathscr{F} := \mathscr{F}(\mathcal{G}, B)$ be a family of modular curves such that $-I \in B$ and $G, H \in \mathscr{F}(\mathcal{G}, B)$ subgroups, of genus g, of $\mathcal{G}$ contained in the family $\mathscr{F}$. Assume we have computed the canonical map and model associated to X_G. i.e. we have a map φ and a curve C such that $\varphi\colon X_G \to C \subseteq \mathbb{P}^{g-1}_{\mathbb{Q}}$ has degree 2. When the family $\mathscr{F}$ has geometric gonality two, the canonical model is computed by considering the cusp forms on X_G, the curve C along with the map φ are uniquely determined.

The space of cusps forms $S_{2,G}$ are acted on by $\mathcal{G}$, the agreeable closure of G. The twisting process of §7 can be used to compute the space $S_{2,H}$ and by twisting the map φ and C, we get the canonical map φ_H and model $C_H := C_\xi$ for the modular curve X_H. Before we combine all these statements, we state the following useful inequality.

Proposition 9.1 (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 9.2. *Assume $H \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ such that $-I \in H$ and $\det(H) = \widehat{\mathbb{Z}}^*$ with genus g. Assume also that X_H has $\overline{\mathbb{Q}}-$gonality 2 and $g > 2$. There is a "fast" algorithm to determine the $\mathbb{Q}-$gonality of the modular curve X_H.*

Proof. X_H lies in a family $\mathscr{F} = \mathscr{F}(\mathcal{G}, B)$. We have computed a canonical representative X_G in $\mathscr{F}$. Twisting the canonical map $X_G \to C$ with respect to the cocycle ξ mentioned in §7, we get the canonical map $X_H \to C_\xi$. 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. We first claim that the map $\pi : X_H \to C_\xi$ 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. Assume there is such a curve. Applying the Castelnuovo-Severi inequality to the maps π, π' we get $g \leqslant 1$, which is a contradiction. Since C_ξ has no rational points it must $\mathbb{Q}-$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. Hence we conclude that X_H has $\mathbb{Q}-$gonality 4.

Note that to compute this canonical morphism $\pi : X_H \to C_\xi$, we do not need to compute cusp forms of $M_{k,H}$, we only need to twist a precomputed canonical morphism $X_G \to C$.

This algorithm is implemented in [EK25]. □

References

[AOPV09] Nir Avni, Uri Onn, Amritanshu Prasad, and Leonid Vaserstein, *Similarity classes of* 3×3 *matrices over a local principal ideal ring*, Comm. Algebra **37** (2009), no. 8, 2601–2615, DOI 10.1080/00927870902747266. MR2543507 ↑14

[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 ↑5

[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 ↑5

[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]. ↑5

[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 ↑5

[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). ↑6

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

[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. ↑5, 16, 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 ↑7, 8

[EK25] Eray Karabiyik, *Repository for classification*, 2025. https://github.com/eekarabiyik/twist. ↑1, 6, 22, 24

[Kat73] Nicholas M. Katz, p*-adic properties of modular schemes and modular forms*, Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1973, pp. 69–190. Lecture Notes in Mathematics, Vol. 350. ↑10

[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

[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 ↑4

[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 ↑5

[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 ↑5

[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 ↑5, 21

[RSZB15] Jeremy Rouse, Andrew Sutherland, 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 ↑5

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

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

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

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

[Zyw20] David Zywina, *Computing actions on cusp forms* (2020). arXiv:2001.07270 [math.NT]. ↑12, 23

[Zyw22] ———, *Explicit Open Images For Elliptic Curves Over* $\mathbb{Q}$ (2022). arXiv:2206.14959 [math.NT]. ↑2, 4, 5, 7, 9, 10, 11, 12, 14, 15, 17, 21

[Zyw24] ———, *Open image computations for elliptic curves over number fields* (2024). arXiv:2403.16147 [math.NT]. ↑5, 13, 14, 16

[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