CLASSIFICATION OF MODULAR CURVES WITH LOW GONALITY

DAVID ZYWINA

ABSTRACT. A congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ acts on the complex upper half-plane via linear fractional transformations and the quotient gives rise to a Riemann surface. After adding cusps, we obtain a smooth compact Riemann surface which corresponds to a smooth projective curve X_Γ defined over $\mathbb{C}$. We give a complete classification of the congruence subgroups Γ for which X_Γ has gonality 1, 2 or 3. We also give a complete classification of the congruence subgroups Γ for which the curve X_Γ is bielliptic. The key ingredients are explicit gonality bounds and algorithms for computing models of modular curves over number fields.

1. INTRODUCTION

Let C be an algebraic curve defined over a field k. Assume that C is nice, i.e., it is smooth, projective and geometrically integral. The gonality of C, which we denote by $\mathrm{gon}(C)$, is the minimal degree of a nonconstant morphism $C \to \mathbb{P}^1_k$. The geometric gonality of C is the gonality of the base extension C_L of C to L, where L is any algebraically closed field containing k. We say that C is bielliptic it has a degree 2 morphism to an elliptic curve. We say that C is geometrically bielliptic if C_L is bielliptic, where L is any algebraically closed field containing k. An elliptic curve has gonality 2 and hence a bielliptic curve has gonality at most 4.

1.1. **Modular curves over $\mathbb{C}$.** The group $\mathrm{SL}_2(\mathbb{Z})$ acts by linear fractional transformations on the complex upper half-plane $\mathcal{H}$ and the extended upper half-plane $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$.

Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. The quotient $\mathcal{X}_\Gamma := \Gamma\backslash\mathcal{H}^*$ is a smooth compact Riemann surface (away from the cusps and elliptic points use the analytic structure coming from $\mathcal{H}$ and extend to the full quotient). We define the modular curve X_Γ to be the nice curve over $\mathbb{C}$ with the same function field as $\mathcal{X}_\Gamma$. In particular, we can identify $\mathcal{X}_\Gamma$ with $X_\Gamma(\mathbb{C})$ endowed with the analytic topology. The curve X_Γ does not change if we replace Γ by $\pm\Gamma$, so we will often focus on the case where Γ contains $-I$.

Our main result gives a complete classification of the congruence subgroups for which the curve X_Γ has gonality at most 3 and for which the curve X_Γ is bielliptic.

Theorem 1.1.

(i) *There are exactly* 132, 524 *and* 489 *congruence subgroups* $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ *with* $-I \in \Gamma$, *up to conjugacy in* $\mathrm{SL}_2(\mathbb{Z})$, *for which* X_Γ *has gonality equal to* 1, 2 *and* 3, *respectively.*

(ii) *There are exactly* 1090 *congruence subgroups* $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ *with* $-I \in \Gamma$, *up to conjugacy in* $\mathrm{SL}_2(\mathbb{Z})$, *for which* X_Γ *is bielliptic.*

The actual congruences subgroups in the classification of Theorem 1.1 can be found in the repository [Zyw25]. The count of congruence subgroups in our classification broken up in terms of the genus of X_Γ can be found in Table 1.1 (we exclude the gonality 1 case since X_Γ has gonality 1 if and only if it has genus 0).

To prove Theorem 1.1 we make use of a gonality bound of Zograf that reduce the theorem to a finite, yet still very large, number of congruence subgroups. Using another gonality bound originating from the work of Ogg along with other constraints, like the Castelnuovo-Severi inequality, we are able to further reduce the number of congruence subgroups that need to be

2020 *Mathematics Subject Classification.* Primary 11G18; Secondary 14H45.

genus	0	1	2	3	4	5	6	7	8	9	10	11	12	13	≥ 14
gonality 2	0	187	177	99	12	34	2	6	1	3	0	3	0	0	0
gonality 3	0	0	0	185	249	1	24	5	16	0	8	0	1	0	0
bielliptic	0	187	132	267	173	179	21	79	5	23	18	4	0	2	0

TABLE 1. Number of congruence subgroups $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ containing $-I$ of a given genus, up to conjugacy in $\mathrm{SL}_2(\mathbb{Z})$, for which X_Γ has gonality 2, gonality 3 or is bielliptic.

dealt with. The congruences subgroups for which the corresponding modular curve has genus at most 24 has been computed by Cummins and Pauli and we will make use of this classification.

For many congruence subgroups Γ, we will need to compute an explicit model of X_Γ and directly check if it has low gonality or directly check if it is bielliptic. Since we have to perform exact computations, it will be preferable to compute a model over a number field instead of $\mathbb{C}$.

1.2. **Modular curves over number fields.** Fix a positive integer N and fix the N-th root of unity $\zeta_N := e^{2\pi i/N} \in \mathbb{C}$. There is a group isomorphism $(\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$, $d \mapsto \sigma_d$, where $\sigma_d(\zeta_N) = \zeta_N^d$. For concreteness, we will let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$.

Take any subgroup G of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ containing $-I$. Define the number field $K_G := \mathbb{Q}(\zeta_N)^{\det(G)}$, i.e., the subfield of $\mathbb{Q}(\zeta_N)$ fixed by σ_d for all $d \in \det(G)$. In particular, $K_G = \mathbb{Q}$ if and only if $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$. Associated to the group G is a modular curve X_G; it is a nice curve defined over K_G, cf. §3.4. When base extended from K_G to $\mathbb{C}$, we will have an isomorphism

$$(X_G)_{\mathbb{C}} \cong X_{\Gamma_G}$$

of curves over $\mathbb{C}$, where Γ_G is the congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ consisting of those matrices whose image modulo N lies in G. The geometric gonality of X_G thus agrees with the gonality of X_{Γ_G}. Also the curve X_G is geometrically bielliptic if and only if X_{Γ_G} is bielliptic.

Thus the classification of Theorem 1.1 describes when X_G has geometric gonality 1, 2 or 3 and describes when X_G is geometrically bielliptic. The following is an immediate application of our classification to quadratic points of a modular curve X_G of sufficiently large genus.

Theorem 1.2. *Let G be any subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ containing $-I$ for which the genus of X_G is at least 12 and not 13. Then the set*

$$\{P \in X_G(\overline{\mathbb{Q}}) : [K_G(P) : K_G] \leq 2\}$$

is finite.

Proof. Let g be the genus of X_G; equivalently, the genus of X_{Γ_G}. Suppose that there are infinitely many $P \in X_G(\overline{\mathbb{Q}})$ for which $[K_G(P) : K_G] \leq 2$. Then [HS91, Corollary 3] implies that $X_{\Gamma_G} \cong (X_G)_{\mathbb{C}}$ is hyperelliptic or bielliptic. Using the genera of the congruences subgroup in Table 1.1, we deduce that $g \leq 13$ and $g \neq 12$. The theorem follows since this contradicts the assumption on g. □

When $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$ and hence $K_G = \mathbb{Q}$, we described how to compute an explicit model for X_G in [Zyw22a]; this was used to make Serre's open image theorem effective for non-CM elliptic curves over $\mathbb{Q}$. We will extend the construction to general G. Code for computing models of X_G can be found in [Zyw25]; this `Magma` code is also being used in the LMFDB database of modular curves [LMFDB]. Note that we are viewing X_G as a geometrically irreducible curve over K_G (some might instead consider a modular curve corresponding to G to be defined over $\mathbb{Q}$ and not necessarily geometrically irreducible).

Let g be the genus of X_G and assume that $g \geq 2$. For our application to Theorem 1.1, we will need to compute the image C of the *canonical map*

$$\phi\colon X_G \to \mathbb{P}^{g-1}_{K_G}.$$

We will use that the curve X_G has geometric gonality 2 if and only if C has genus 0. If X_G does not have geometric gonality 2, we will show that X_G has geometric gonality 3 if and only if C is not cut out by homogeneous polynomials of degree 2 and C is not geometrically isomorphic to a smooth plane quintic. When X_G does not have geometric gonality 2 and $g \geq 4$, we will also give a geometric condition on C that checks whether X_G is geometrically bielliptic.

1.3. **Some earlier results.** There has been much earlier work on classifying modular curves with small gonality with most attention being on the modular curves $X_0(N)$ and $X_1(N)$ which are defined over $\mathbb{Q}$.

Remark 1.3. Theorem 1.1 focuses on geometric gonality and being geometrically bielliptic; we now observe that for genus large enough, this agrees for $X_0(N)$ and $X_1(N)$ with the analogous notion over $\mathbb{Q}$. Let X be one of the curves $X_0(N)$ or $X_1(N)$ for some positive integer N. The key observation is that the curve X is defined over $\mathbb{Q}$ and has a rational point at one of the cusps. Using this, we find that if X has genus at least 2, then X has gonality 2 if and only if it has geometric gonality 2, cf. [RX18, Theorems 1 and 2]. If X has genus at least 5, then X has gonality 3 if and only if it has geometric gonality 3, cf. [RX18, Theorems 1 and 2]. If X has genus at least 6, then one can show that X is bielliptic if and only if it is geometrically bielliptic, cf. Lemma 2.7.

Here is a partial list of prior results.

- Ogg [Ogg74] classified the curves $X_0(N)$ that are hyperelliptic. The curve $X_0(N)$ is hyperelliptic and has genus at least 2 for exactly 19 different N.
- Ishii and Momose [IM91] classified the hyperelliptic modular curves arising from a congruence subgroup $\Gamma_1(N) \subseteq \Gamma \subseteq \Gamma_0(N)$ though also see [JK07].
- Hasegawa and Shimura [HS99] classified the curves $X_0(N)$ which have gonality 3. Jeon and Kim [JK07] show that there are no congruence subgroups $\Gamma_1(N) \subseteq \Gamma \subseteq \Gamma_0(N)$ for which X_Γ has genus at least 5 and gonality 3.
- Bars classified the curves $X_0(N)$ that are bielliptic [Bar99] (Harris and Silverman [HS91] had left a finite number of N to consider). The curve $X_0(N)$ is bielliptic and has genus at least 2 for exactly 41 different N.
- Jeon and Kim [JK04] classified the curves $X_1(N)$ which are bielliptic.
- Jeon, Kim and Schweizer [JKS20] classified the bielliptic modular curves arising from a congruence subgroup $\Gamma_1(N) \subseteq \Gamma \subseteq \Gamma_0(N)$.

From our explicit classification in Theorem 1.1 and Remark 1.3, we can immediately recover all the above results excluding the small genus cases where the equivalences in Remark 1.3 fail.

Outside the scope of our theorem, Najman and Orlić [NO24] have classified the modular curves $X_0(N)$ that have gonality 4, 5 and 6.

1.4. **Overview.** In §2, we give some basic background on the geometry of curves. We recall some results on gonality in §2.1. We review the canonical map in §2.2 which will be important for our methods of computing low gonalities. We give basic properties of bielliptic curves in §2.3. Proposition 2.6 shows that for a canonical curve the bielliptic morphisms have a geometric description. Proposition 2.8 implies that if a nice curve of genus at least 2 is geometrically bielliptic, then its reduction is geometrically bielliptic at all good primes; this gives a useful way to show that a curve is not geometrically bielliptic by consider its reductions.

Consider a subgroup $G \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ containing $-I$. In §3, we define our modular curve X_G over the number field $K_G := \mathbb{Q}(\zeta_N)^{\det(G)}$. For each integer $k \geq 0$, we define a finite dimensional K_G-vector space $M_{k,G}$ that consists of certain modular forms of weight k. We define our curve

X_G to be $\operatorname{Proj} R_G$, where R_G is the graded K_G-algebra $\oplus_{k\geq 0} M_{k,G}$. We shall describe how to explicitly compute a basis for $M_{k,G}$ by using Eisenstein series of weight 1. Finding bases for some spaces $M_{k,G}$ allow us to compute explicit models of X_G. When X_G has genus at least 2, the space of cusp forms $S_{2,G}$ in $M_{2,G}$ will let us compute the image of the canonical map of X_G.

More background on modular curves is given in §4 where we discuss the moduli approach. In particular, this will extend X_G to a smooth proper curve over $\mathcal{O}_{K_G}[1/N]$.

In §5, we give explicit gonality bounds for the curves X_Γ. Consider a congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ that contains $-I$. Theorem 5.1 shows that the gonality of X_Γ is strictly larger than $\frac{325}{32768}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$. In particular, if we only consider Γ for which X_Γ has a fixed gonality, then the index $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$ is bounded and hence there are only finitely many such Γ. We also give an improved gonality bound when Γ has level at most 226 since we can make use of known cases of Selberg's eigenvalue conjecture. We also give another explicit gonality bounds using ideas of Ogg and Poonen.

In §6, we explain how one can computationally check if a modular curve X_G is geometrically bielliptic or not.

The main part of our classification is outlined in §7 where we prove the classification of Theorem 1.1 and Table 1.1 when restricted to congruence subgroups of genus at most 24. This constraint on the genus arises since we are using the classification of Cummins and Pauli of all congruence subgroups of genus at most 24. Finally in §8 we complete the proof of Theorem 1.1 by showing that there are no congruence subgroups Γ of genus at least 25 for which X_Γ has gonality at most 3 or X_Γ is bielliptic.

1.5. **Notation.** For a number field K, let $\mathcal{O}_K$ be its ring of integers. For a nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, let $\mathbb{F}_\mathfrak{p}$ be the residue field $\mathcal{O}_K/\mathfrak{p}$. Let $K_\mathfrak{p}$ be the $\mathfrak{p}$-adic completion of K and let $\mathcal{O}_\mathfrak{p}$ be its valuation ring. For an R-scheme X and a (commutative) R-algebra R', we denote $X \times_{\operatorname{Spec} R} \operatorname{Spec} R'$ by $X_{R'}$ or $X \times_R R'$.

1.6. **Acknowledgements.** Our algorithms are implemented in `Magma` [BCP97]; the code can be found in the public repository [Zyw25].

2. Background on curves

In this section, we collect background information on gonality and bielliptic curves.

Let C be a nice curve of genus g defined over a perfect field k. Fix an algebraic closure $\bar{k}$ of k. We say that C is hyperelliptic if there is a nonconstant morphism $C \to \mathbb{P}^1_k$ of degree 2. We say that C is geometrically hyperelliptic if $C_{\bar{k}}$ is hyperelliptic. We say that C is trigonal if there is a nonconstant morphism $C \to \mathbb{P}^1_k$ of degree 3.

2.1. **Gonality.** Recall that the gonality of C, which we denote by $\operatorname{gon}(C)$, is the minimal degree of a nonconstant morphism $C \to \mathbb{P}^1_k$. The geometric gonality of C is the gonality of $C_{\bar{k}}$. The curve C has gonality 1 if and only if C is isomorphic to $\mathbb{P}^1_k$. Therefore, C has geometric gonality 1 if and only if $g = 0$. When $g \geq 1$, C is hyperelliptic if and only if it has gonality 2.

We now recall various properties of gonality.

Proposition 2.1.

(i) *If L is a field extension of k, then* $\operatorname{gon}(C_L) \leq \operatorname{gon}(C)$.
(ii) *If k is algebraically closed and L is a field extension of k, then* $\operatorname{gon}(C_L) = \operatorname{gon}(C)$.
(iii) *If k is algebraically closed, then* $\operatorname{gon}(C) \leq \lfloor \frac{g+3}{2} \rfloor$.
(iv) *If $C \to C'$ is a nonconstant morphism of curves over k, then* $\operatorname{gon}(C') \leq \operatorname{gon}(C)$.

Proof. See [Poo07, Appendix A]. □

From Proposition 2.1(iii), C has geometric gonality 2 whenever the genus g is 1 or 2.

The following theorem will be useful for ruling out various kinds of maps. For example when $g \geq 2$, it implies that there is at most one morphism $C \to \mathbb{P}^1_k$ of degree 2 (up to composition with an automorphism of $\mathbb{P}^1_k$).

Theorem 2.2 (Castelnuovo–Severi inequality)**.** *Let $\pi_1 \colon C \to C_1$ and $\pi_2 \colon C \to C_2$ be nonconstant morphisms, respectively, where C_1 and C_2 are nice curves over k. Assume there is no morphism $\pi \colon C \to C'$ of degree > 1 through which both π_1 and π_2 factor. Then*

$$g \leq d_1 g_1 + d_2 g_2 + (d_1 - 1)(d_2 - 1),$$

where g_i is the genus of C_i and d_i is the degree of π_i.

Proof. See [Sti09, Theorem 3.11.3]. □

Proposition 2.3. *Let K be a nonarchimedean local field of characteristic 0 with local ring R and residue field $\mathbb{F}$. Suppose that C is a nice curve of genus $g \geq 2$ defined over K that has good reduction, i.e., there is a smooth proper model $\mathcal{C}$ over $\operatorname{Spec} R$ with $\mathcal{C}_K = C$. Then*

$$\operatorname{gon}(\mathcal{C}_{\mathbb{F}}) \leq \operatorname{gon}(C).$$

Proof. See [Der12, Theorem 2.5]. Such a result is also asserted by Frey in the proof of [Fre94, Proposition 3] and is attributed to Deuring [Deu42]. □

2.2. **Canonical map.** We now suppose that $g \geq 2$. The k-vector space $V := H^0(C, \Omega_{C/k})$ has dimension g and gives rise to a morphism

$$\phi \colon C \to \mathbb{P}(V)$$

called the canonical map. The morphism ϕ has degree 2 when C is geometrically hyperelliptic and is an embedding otherwise. The canonical ring of C is the graded k-algebra

$$R(C) := \bigoplus_{d=0}^{\infty} H^0(C, \Omega_{C/k}^{\otimes d}).$$

Define the symmetric algebra $\operatorname{Sym}(V) := \bigoplus_{d=0}^{\infty} \operatorname{Sym}^d(V)$ and let $\varphi \colon \operatorname{Sym}(V) \to R(C)$ be the homomorphism of graded k-algebras for which $\operatorname{Sym}^1(V) = V \to V = R(C)_1$ is the identity map. Let $I(C) \subseteq \operatorname{Sym}(V)$ be the kernel of φ. We have $I(C) = \bigoplus_{d=0}^{\infty} I(C)_d$ and $I(C)_1 = 0$.

When we choose a basis of V, we can identify $\mathbb{P}(V)$ with $\mathbb{P}^{g-1}_k$, $\operatorname{Sym}(V)$ with $k[x_1, \ldots, x_g]$, and $I(C)$ with the homogeneous ideal in $k[x_1, \ldots, x_g]$ corresponding to the curve $\phi(C) \subseteq \mathbb{P}^{g-1}_k$.

Proposition 2.4.

(i) *If C is not geometrically hyperelliptic, then*

$$\dim_k I(C)_n = \tbinom{n+g-1}{n} - (2n-1)(g-1)$$

for all $n \geq 2$.

(ii) *We have*

$$\dim_k I(C)_2 = \begin{cases} \binom{g-1}{2} & \text{if } C \text{ is geometrically hyperelliptic} \\ \binom{g-2}{2} & \text{otherwise.} \end{cases}$$

(iii) *Suppose C is not geometrically hyperelliptic. If $g > 3$, then the ideal $I(C)$ is generated by $I(C)_2$ and $I(C)_3$. If $g = 3$, then $I(C)$ is generated by $I(C)_4$ and $\dim_k I(C)_4 = 1$.*

(iv) *Suppose that C is not geometrically hyperelliptic and $g > 3$. Let $W \subseteq I(C)_3$ be the image of $V \otimes_k I(C)_2$ in $I(C)_3$. Then the following are equivalent:*

- *$C_{\bar{k}}$ is trigonal or isomorphic to a smooth plane quintic,*
- *$W \neq I(C)_3$,*

- $\dim_k I(C)_3/W = g-3$.

Proof. Set $R = R(C)$ and $I = I(C)$, and let $R_{\geq 1}$ be the irrelevant ideal of R. The *Poincaré polynomial* of I is $P(I;t) = \sum_{d=1}^{\infty} \dim_k (I/R_{\geq 1}I)_d \cdot t^d$. An explicit description of $P(I;t)$ can be found in [VZB22, Table (Ia)] and is broken up into several cases. The proposition can be easily read off this table. □

2.3. **Bielliptic curves.** We say that C is bielliptic if there is a degree 2 morphism $C \to E$, where E is an elliptic curve over k. We say that C is geometrically bielliptic if $C_{\bar{k}}$ is bielliptic.

Lemma 2.5. *Suppose that C is geometrically bielliptic.*

(i) *If $g \geq 4$, then C is not geometrically hyperelliptic.*
(ii) *If $g \geq 5$, then $C_{\bar{k}}$ is not trigonal.*
(iii) *If $C \to C'$ is a nonconstant morphism of nice curves, then C' has geometric gonality at most 2 or is geometrically bielliptic.*
(iv) *If k has characteristic 0, then $C_{\bar{k}}$ is not isomorphic to a smooth plane quintic.*

Proof. Parts (i) and (ii) are immediate consequences of Theorem 2.2. Part (iii) follows from [HS91, Proposition 1]. Part (iv) follows from [HKO08, Theorem 2.1]; we have the characteristic 0 assumption since [HKO08] works implicitly over the complex numbers. □

The following is presumably well-known but lacking a reference we give a proof.

Proposition 2.6. *Suppose that C is not geometrically hyperelliptic. We may assume $C \subseteq \mathbb{P}^{g-1}_k$ via the canonical map.*

(i) *Suppose that $g \geq 4$ and that there is a morphism $\pi\colon C \to C'$ of degree 2, where C' is a nice curve of genus 1 over k. Then there is a unique point $a \in \mathbb{P}^{g-1}(k)$ not in C such that the projection of $\mathbb{P}^{g-1}_k$ from the point a defines a morphism $C \to \mathbb{P}^{g-2}_k$ that agrees with π composed with an embedding $C' \hookrightarrow \mathbb{P}^{g-2}_k$.*
(ii) *Suppose that $g \geq 5$, k has characteristic 0, and that there is a point $a \in \mathbb{P}^{g-1}(k)$ not in C such that a projection $\phi\colon C \to \mathbb{P}^{g-2}_k$ from the point a defines a degree 2 morphism of C. Then $\phi(C)$ is a curve of genus 1 and hence C is geometrically bielliptic.*

Proof. We first assume we are in the setting of (i) with k algebraically closed. For each point $p \in C'(k)$, let l_p be the line in $\mathbb{P}^{g-1}_k$ passing through the two points of the divisor $\pi^*(p)$ where we take l_p to be a tangent line of C if the support of $\pi^*(p)$ consists only of one point.

We claim that there is a unique point $a \in \mathbb{P}^{g-1}(k)$ that is the intersection of l_p and l_q for all distinct $p, q \in C'(k)$. Take any distinct $p, q \in C'(k)$ and define $D := \pi^*(p+q)$; it is an effective divisor of degree 4 on C. Applying the Riemann–Roch theorem to the divisor $p+q$ of the genus 1 curve C', we have $\dim |p+q| = 1$ and hence $\dim |D| \geq 1$. Let $\iota\colon C \hookrightarrow \mathbb{P}^{g-1}_k$ be the inclusion obtained by identifying C with the image of its canonical map. Let $\overline{D}$ be the intersection of all hyperplanes $H \subseteq \mathbb{P}^{g-1}_k$ such that $\iota^*(H) \geq D$. By the geometric interpretation of the Riemann–Roch theorem, cf. [AGI, Chapter 2 §3.2], we have

$$\dim \overline{D} = \deg D - \dim |D| - 1 \leq 4 - 1 - 1 = 2.$$

Since $\dim \overline{D} \leq 2$ and $g \geq 4$, $\overline{D}$ is a proper subvariety of $\mathbb{P}^{g-1}_k$ and hence D is special. By Clifford's theorem [AGI, Chapter 2 §3.2], we have $\dim |D| < \frac{1}{2} \deg D = 2$. Therefore, $\dim |D| = 1$ and hence $\dim \overline{D} = 2$. We have shown that the two lines l_p and l_q span the plane $\overline{D}$ and hence they must intersect at a point. Since l_p and l_q intersect at a point for all distinct $p, q \in C'(k)$, we find that all the lines l_p intersect at a single point or all the lines l_p lie in a common plane. The canonical curve C does not lie a plane in $\mathbb{P}^{g-1}_k$ since $g \geq 4$. Therefore, there is a unique point $a \in \mathbb{P}^{g-1}(k)$ such that l_p and l_q intersect at exactly a for all distinct $p, q \in C'(k)$.

We claim that $a \notin C(k)$. Assume to the contrary that $a \in C(k)$. Fix a point $p \in C'(k)$ so that the divisor $D' := \pi^*(p) + a$ of C consists of three distinct points. We have $\overline{D'} = l_p$ and hence $\dim |D'| = 1$ by the geometric interpretation of the Riemann–Roch theorem. So there is a nonconstant rational f on C with $\operatorname{div}(f) + D' \geq 0$; it has degree 3 since C is not hyperelliptic. Let σ be the involution of C corresponding to π and let n be the number of points of C fixed by σ. We have $f \circ \sigma = \pm f$ since σ is an involution, the support of D is stable under σ, and $\dim |D'| = 1$. Since f has degree 3 and hence does not factor through π, we have $f \circ \sigma = -f$. Therefore, all the points of C fixed by σ are zeros of f or the pole a, and hence $n \leq 4$. However, the Riemann–Hurwitz formula applied to π and using $g \geq 4$ shows that $n > 4$. This contradiction proves the claim.

From the construction of a, it has the properties in (i). This completes the proof of (i) in the case where k is algebraically closed. The general case of (i) follows easily; we obtain a unique point $a \in \mathbb{P}^{g-1}(\bar{k})$ not in C that is fixed by $\mathrm{Gal}(\bar{k}/k)$ and hence is defined over k.

Suppose we are in the setting of (ii). Define the curve $C' := \phi(C)$. Since ϕ has degree 2, there is a corresponding involution σ of C; for any point p in C, the line through p and a intersects C at the two points p and $\sigma(p)$ counted with multiplicity. We can view C' as the quotient of C by σ. Since C is a canonical curve, it has degree $2g - 2$. Since ϕ has degree 2, we deduce that C' has degree $g - 1$ in $\mathbb{P}^{g-2}_k$. By Castelnuovo's bound [ACGH85, III §2], and using that $g \geq 5$ and k has characteristic 0, we find that C' can have genus at most 1. The curve C' has genus 1 since C is not geometrically hyperelliptic. □

Lemma 2.7. *Assume that $g \geq 6$ and that C is geometrically bielliptic. Then there exists a morphism $\pi\colon C \to C'$ of degree 2 with C' a nice curve over k of genus 1. Moreover, π is unique up to composition with an automorphism of C'. If C has a k-point, then C is bielliptic.*

Proof. By Lemma 2.5(i), we may assume $C \subseteq \mathbb{P}^{g-1}_k$ after replacing the curve with its image under the canonical map. Let A be the set of $a \in \mathbb{P}^{g-1}(\bar{k})$ so that the projection of $\mathbb{P}^{g-1}_{\bar{k}}$ from a defines a morphism of degree 2 from $C_{\bar{k}}$ to a genus 1 curve. The set A is nonempty by Proposition 2.6 and our assumption that C is geometrically bielliptic. The set A is finite since each element gives rise to a distinct bielliptic involution of $C_{\bar{k}}$ and the set of automorphisms of $C_{\bar{k}}$ is finite since $g \geq 2$. Theorem 2.2 and our assumption $g \geq 6$ implies that A has cardinality 1.

Since C is defined over k, the absolute Galois group Gal_k acts on A and hence A consists of a unique point $a \in \mathbb{P}^{g-1}(k)$. The existence of the morphism π of C is obtained by using the projecting from the point a. The uniqueness of π, up to composition with an automorphism of C', follows from Theorem 2.2 and $g \geq 6$.

Finally if C has a k-point, then so does C' by using π and hence C' can be made into an elliptic curve. This proves the last statement of the lemma. □

Proposition 2.8. *Let K be a nonarchimedean local field of characteristic 0 with valuation ring R and residue field $\mathbb{F}$. Let C be a nice curve of genus $g \geq 2$ defined over K and suppose there is a smooth proper model $\mathcal{C}$ over $\operatorname{Spec} R$ that extends C.*

(i) *If C is bielliptic, then $\mathcal{C}_{\mathbb{F}}$ is bielliptic.*
(ii) *If C is geometrically bielliptic, then $\mathcal{C}_{\mathbb{F}}$ is geometrically bielliptic.*

Proof. Assume that C is bielliptic. There is a morphism $f\colon C \to E$ of degree 2, where E is an elliptic curve over K. Associated to f is a nontrivial involution σ_0 of C. The involution σ_0 extends uniquely to an involution σ of the R-scheme $\mathcal{C}$ by [Liu02, §10.3 Corollary 3.37]. Let G be the subgroup of $\mathrm{Aut}(C)$ generated by σ. By [Liu02, Proposition 3.38 and its proof], the involution σ acts nontrivially on $\mathcal{C}_{\mathbb{F}}$ and the quotient $p\colon \mathcal{C} \to \mathcal{C}/G =: \mathcal{X}$ exists. Observe that $\mathcal{X}_K \cong E$. Since G has order 2 and only fixes a finite number of points in each fiber of $\mathcal{C}$ over R, we find that there is an open subscheme $U \subseteq \mathcal{X}$ that excludes a finite number of points in each fiber of $\mathcal{X}$ such

that $p^{-1}(U) \xrightarrow{p} U$ is étale with Galois group G. We find that $\mathcal{C}_{\mathbb{F}} \to \mathcal{X}_{\mathbb{F}}$ is a morphism of degree 2 and $\mathcal{X}_{\mathbb{F}}$ has genus 1. So there is a nice curve Y over $\mathbb{F}$ of genus 1 and a morphism $\mathcal{C}_{\mathbb{F}} \to Y$ of degree 2. By the Weil bounds and $\mathbb{F}$ being finite, we find that Y has an $\mathbb{F}$-point and hence we can view it as elliptic curve over $\mathbb{F}$. Therefore, $\mathcal{C}_{\mathbb{F}}$ is bielliptic. This completes the proof of (i). Part (ii) follows directly from (i) by replacing K by a finite extension for which the curve is bielliptic. □

3. Modular curves and forms

In this section, we give background on modular forms and modular curves. In particular, for a subgroup G of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ we will define a modular curve X_G. Our approach is motivated by the need to compute explicit models of X_G. Much of this material follows the exposition of [Zyw22a, §4] except we allow modular curves defined over number fields besides $\mathbb{Q}$.

3.1. **Modular curves and forms over $\mathbb{C}$.** For the basics on modular forms and curves see see [Shi94]. The group $\mathrm{SL}_2(\mathbb{Z})$ acts by linear fractional transformations on the complex upper half-plane $\mathcal{H}$ and the extended upper half-plane $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$.

Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. The quotient $\mathcal{X}_\Gamma := \Gamma\backslash\mathcal{H}^*$ is a smooth compact Riemann surface (away from the cusps and elliptic points use the analytic structure coming from $\mathcal{H}$ and extend to the full quotient). Let X_Γ be the nice curve over $\mathbb{C}$ corresponding to $\mathcal{X}_\Gamma$. The genus of X_Γ is

$$g = 1 + \tfrac{1}{12}[\mathrm{SL}_2(\mathbb{Z}) : \pm\Gamma] - \tfrac{1}{4}\nu_2 - \tfrac{1}{3}\nu_3 - \tfrac{1}{2}\nu_\infty, \tag{3.1}$$

where ν_∞ is the number of cusps of $\mathcal{X}_\Gamma$, and ν_2 and ν_3 are the number of elliptic points of $\mathcal{X}_\Gamma$ of order 2 and 3, respectively, cf. [Shi94, Proposition 1.40].

Consider an integer $k \geq 0$. The group $\mathrm{SL}_2(\mathbb{R})$ acts on the complex upper half-plane via linear fractional transformations. For a meromorphic function f on $\mathcal{H}$ and a matrix $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$, define the meromorphic function $f|_k\gamma$ on $\mathcal{H}$ by

$$(f|_k\gamma)(\tau) := (c\tau + d)^{-k} f(\gamma\tau);$$

we call this the slash operator of weight k. Recall that a modular form of weight k on Γ is a holomorphic function f on $\mathcal{H}$ such that the following hold:

- for any $\gamma \in \Gamma$, $f|_k\gamma = f$,
- for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, $(f|_k\gamma)(\tau)$ is bounded as $\mathrm{Im}(\tau) \to +\infty$.

A cusp form of weight k on Γ is a modular form f of weight k on Γ such that $(f|_k\gamma)(\tau) \to 0$ as $\mathrm{Im}(\tau) \to +\infty$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. We denote by $M_k(\Gamma)$ the set of modular forms of weight k on Γ; it is a finite dimensional complex vector space. We denote by $S_k(\Gamma) \subseteq M_k(\Gamma)$ the subspace of cusp forms.

Fix a positive integer N that is divisible by the level of Γ. For each modular form $f \in M_k(\Gamma)$, we have a Fourier expansion

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

with unique $a_n(f) \in \mathbb{C}$, where $q_N := e^{2\pi i\tau/N}$. We call this power series the q-expansion of f (at the cusp ∞). For a subring R of $\mathbb{C}$, we denote by $M_k(\Gamma, R)$ the R-submodule of $M_k(\Gamma)$ consisting of modular forms whose q-expansion has coefficients in R.

The ring

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

is a finitely generated $\mathbb{C}$-algebra. Each $M_k(\Gamma)$ can be identified with the global sections of a line bundle on X_Γ which is very ample for all sufficiently large even k. Using this, we obtain an isomorphism

$$X_\Gamma = \operatorname{Proj} R_\Gamma$$

This description of X_Γ gives a concrete approach to constructing a model of X_Γ over a number field $K \subseteq \mathbb{C}$, i.e., use $\operatorname{Proj} R$, where R is a graded K-algebra for which we have an isomorphism $R \otimes_K \mathbb{C} \cong R_\Gamma$ of graded $\mathbb{C}$-algebras.

3.2. **Modular forms of level N.** Fix a positive integer N. Since $\Gamma(N)$ is normal in $\mathrm{SL}_2(\mathbb{Z})$, the slash operator of a fixed weight $k \geq 0$ gives a right action of $\mathrm{SL}_2(\mathbb{Z})$ on $M_k(\Gamma(N))$. This produces a right action of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ on $M_k(\Gamma(N))$ since $\Gamma(N)$ acts trivially.

Take any modular form $f = \sum_{n=0}^{\infty} a_n(f) q_N^n$ in $M_k(\Gamma(N))$. For a field automorphism σ of $\mathbb{C}$ and a modular form $f \in M_k(\Gamma(N))$, there is a unique modular form $\sigma(f) \in M_k(\Gamma(N))$ whose q-expansion is $\sum_{n=0}^{\infty} \sigma(a_n(f))\, q_N^n$. This defines an action of $\mathrm{Aut}(\mathbb{C})$ on $M_k(\Gamma(N))$.

The next lemma shows that these actions induce a right action $*$ of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on the $\mathbb{Q}$-vector space $M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$, where $\zeta_N := e^{2\pi i/N}$. Recall that there is a group isomorphism

$$(\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}), \quad d \mapsto \sigma_d,$$

where $\sigma_d(\zeta_N) = \zeta_N^d$.

Proposition 3.1. *There is a unique right action $*$ of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on $M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$ such that the following hold for all modular forms $f \in M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$:*

- *$f * A = f|_k\gamma$ for $A \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ and $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ congruent to A modulo N,*
- *$f * A = \sigma_d(f)$ for $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$.*

Proof. See [BN19, §3]. □

3.3. **The spaces $M_{k,G}$.** Fix a positive integer N and let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. For each integer $k \geq 0$, we define

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

where we are considering the subgroup fixed by G under action $*$ from Proposition 3.1. Observe that $M_{k,G}$ is a vector space over K_G, where $K_G := \mathbb{Q}(\zeta_N)^{\det(G)}$ is the subfield of $\mathbb{Q}(\zeta_N)$ fixed by σ_d for all $d \in \det(G)$.

Let Γ_G be the congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ consisting of those matrices that are congruent modulo N to an element of G. We have an inclusion $M_{k,G} \subseteq M_k(\Gamma_G, \mathbb{Q}(\zeta_N))$.

Lemma 3.2. *The natural homomorphisms*

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

are isomorphisms for all integers $k \geq 0$ with $k \neq 1$.

Proof. Since $k \neq 1$, the natural map $M_k(\Gamma(N), \mathbb{Q}(\zeta_N)) \otimes_{\mathbb{Q}(\zeta_N)} \mathbb{C} \to M_k(\Gamma(N))$ is an isomorphism of complex vector spaces, cf. [Kat73, §1.7]. Taking Γ_G-invariants shows that the natural map

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

is an isomorphism. In particular, $M_k(\Gamma_G, \mathbb{Q}(\zeta_N))$ is a finite dimensional vector space over $\mathbb{Q}(\zeta_N)$.

Define $H := G \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Since H is normal in G, we have a right action of G/H on $M_k(\Gamma(N), \mathbb{Q}(\zeta_N))^H = M_k(\Gamma_G, \mathbb{Q}(\zeta_N))$. Let $\varphi\colon G/H \to \mathrm{Gal}(\mathbb{Q}(\zeta_N)/K_G)$ be the isomorphism $\varphi(A) = \sigma_{\det A}$. Since G/H is abelian, the isomorphism φ induces a (left) action $\bullet$ of $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/K_G)$ on $M_k(\Gamma_G, \mathbb{Q}(\zeta_N))$. We have $\sigma \bullet (cf) = \sigma(c)(\sigma \bullet f)$ for all $c \in \mathbb{Q}(\zeta_N)$, $f \in M_k(\Gamma_G, \mathbb{Q}(\zeta_N))$ and $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/K_G)$. By Galois descent for finite dimensional vector spaces (see the corollary to Proposition 6 in Chapter V §10 of [Bou03]), the natural homomorphism

$$M_{k,G} \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_N) = M_k(\Gamma_G, \mathbb{Q}(\zeta_N))^{\mathrm{Gal}(\mathbb{Q}(\zeta_N)/K_G)} \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_N) \to M_k(\Gamma_G, \mathbb{Q}(\zeta_N))$$

is an isomorphism of $\mathbb{Q}(\zeta_N)$-vector spaces. By tensoring to $\mathbb{C}$ and using the isomorphism (3.2), we obtain the other isomorphism of the lemma. □

3.4. **The modular curve X_G.** Fix a positive integer N and let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. We further assume that $-I \in G$. Define

$$R_G := \bigoplus_{k\geq 0} M_{k,G};$$

it is a graded K_G-algebra. We define the K_G-scheme

$$X_G := \operatorname{Proj} R_G.$$

Our assumption $-I \in G$ implies that $M_k(\Gamma_G) = 0$, and hence $M_{k,G} = 0$, for all odd k. By Lemma 3.2, we obtain a natural isomorphism $R_G \otimes_{K_G} \mathbb{C} \xrightarrow{\sim} R_{\Gamma_G}$ of graded $\mathbb{C}$-algebras and hence have an isomorphism

$$(X_G)_{\mathbb{C}} = X_{\Gamma_G}$$

of schemes over $\mathbb{C}$ which we will use an identification. In particular, X_G is a nice curve over K_G that has the same genus as X_{Γ_G}.

Consider an open subgroup $\mathcal{G}$ of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ that contains $-I$. Fix a positive integer N that is divisible by the level of $\mathcal{G}$ and let $\overline{\mathcal{G}} \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be the reduction of $\mathcal{G}$ modulo N. The field $K_{\mathcal{G}} := K_{\overline{\mathcal{G}}}$ and the ring $R_{\mathcal{G}} := R_{\overline{\mathcal{G}}}$ do not depend on the choice of N, so we can define the modular curve $X_{\mathcal{G}} := \operatorname{Proj} R_{\mathcal{G}} = X_{\overline{\mathcal{G}}}$.

Now consider any two open subgroups G and G' of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ that contains $-I$ and satisfy $G \subseteq G'$ and $\det(G) = \det(G')$. Then the inclusion of rings $R_{G'} \subseteq R_G$ induces a morphism $X_G \to X_{G'}$ of curves over $K_G = K_{G'}$. Base changing to $\mathbb{C}$, this corresponds to the natural morphism $X_{\Gamma_G} \to X_{\Gamma_{G'}}$ of degree $[\Gamma_{G'} : \Gamma_G] = [G' : G]$.

Remark 3.3. In [Zyw22a], we gave an alternate definition of X_G in terms of its function field which we now briefly explain. Let $\mathcal{F}_N$ be the field of meromorphic functions on $\mathcal{X}_{\Gamma(N)}$ whose q-expansion at ∞ is of the form $\sum_{n\in\mathbb{Z}} a_n(f) q_N^n$, where the $a_n(f)$ lie in $\mathbb{Q}(\zeta_N)$; we have $a_n(f) = 0$ for all but finitely many $n < 0$. There is an right action $*$ of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on $\mathcal{F}_N$ defined the same way as in Proposition 3.1. Let $\mathcal{F}_N^G$ be the subfield of $\mathcal{F}_N$ fixed by the action of G.

The function field L of X_G is the field of modular functions consisting of quotients f/f' with $f, f' \in M_{k,G}$, where $k \geq 0$ is even and $f' \neq 0$. We have $L \subseteq \mathcal{F}_N^G$. One can prove that $L = \mathcal{F}_N^G$ by showing that both are extensions of $K_G(j)$ of degree $|G/\{\pm I\}|$, where j is modular j-invariant. So an alternate definition of X_G is the nice curve over K_G with function field $\mathcal{F}_N^G$.

3.5. **Computing a basis of $M_{k,G}$.** Fix a positive integer N. Our approach to computing modular forms is using Eisenstein series of weight 1. Take any $(a, b) \in \mathbb{Z}^2$ and let $\alpha \in (\mathbb{Z}/N\mathbb{Z})^2$ be its image modulo N. There is a modular form E_α in $M_1(\Gamma(N), \mathbb{Q}(\zeta_N))$ with q-expansion

$$c_0 + \sum_{\substack{m,n\geq 1\\ m\equiv a \bmod N}} \zeta_N^{bn} q_N^{mn} - \sum_{\substack{m,n\geq 1\\ m\equiv -a \bmod N}} \zeta_N^{-bn} q_N^{mn},$$

where

$$c_0 = \begin{cases} 0 & \text{if } a \equiv b \equiv 0 \pmod N,\\ \frac{1}{2}\frac{1+\zeta_N^b}{1-\zeta_N^b} & \text{if } a \equiv 0 \pmod N \text{ and } b \not\equiv 0 \pmod N,\\ \frac{1}{2} - \frac{a_0}{N} & \text{if } a \not\equiv 0 \pmod N \end{cases}$$

and $0 \leq a_0 < N$ is the integer congruent to a modulo N. For details on the Eisenstein series E_α see §2 of [BN19] (where it is denoted $E_\alpha^{(1)}$).

Lemma 3.4. *Fix an integer $k \geq 1$ and pairs $\alpha_1, \dots, \alpha_k \in (\mathbb{Z}/N\mathbb{Z})^2$. Then the modular form $f := E_{\alpha_1} \cdots E_{\alpha_k}$ lies in $M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$ and satisfies $f * A = E_{\alpha_1 A} \cdots E_{\alpha_k A}$ for all $A \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.*

Proof. The lemma follows directly from the $k = 1$ case, so we may assume that $k = 1$ and we fix a pair $\alpha \in (\mathbb{Z}/N\mathbb{Z})^2$. The modular form E_α has weight 1 and its q-expansion has coefficients in $\mathbb{Q}(\zeta_N)$. As noted in [BN19, §3], we have $E_\alpha * A = E_{\alpha A}$ for all $A \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. □

Proposition 3.5. *Suppose that $N \geq 3$. Take any subgroup G of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and integer $k \geq 2$. Then the K_G-vector space $M_{k,G}$ is spanned by the modular forms*

$$f = \sum_{g \in G} \zeta_N^{j \det(g)} E_{\alpha_1 g} \cdots E_{\alpha_k g} \tag{3.3}$$

with pairs $\alpha_1, \ldots, \alpha_k \in (\mathbb{Z}/N\mathbb{Z})^2$ and integers $0 \leq j < |\det(G)|$. With $f \in M_{k,G} \subseteq M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$ as above, we have

$$f * A = \sum_{g \in G} \zeta_N^{j \det(g) \det(A)} E_{\alpha_1 gA} \cdots E_{\alpha_k gA}$$

for $A \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

Proof. Let S_0 be the set of modular forms $E_{\alpha_1} \cdots E_{\alpha_k}$ with $\alpha_1, \ldots, \alpha_k \in (\mathbb{Z}/N\mathbb{Z})^2$. Let S_1 be the set of modular forms $\zeta_N^j f$ with $f \in S_0$ and $0 \leq j < |\det(G)|$. Since $N \geq 3$, the set S_0 spans $M_k(\Gamma(N))$ as vector space over $\mathbb{C}$ by a theorem of Khuri-Makdisi [KM12]; Theorem 3.1 of [BN19] gives a reformulation of this result similar to ours. Since $S_0 \subseteq M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$, Lemma 3.2 with trivial group implies that S_0 spans $M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$ over $\mathbb{Q}(\zeta_N)$. Therefore, S_1 spans $M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$ over K_G; note that the ζ_N^j, with $0 \leq j < |\det(G)| = [\mathbb{Q}(\zeta_N) : K_G]$, is a basis of $\mathbb{Q}(\zeta_N)$ over K_G. Therefore, $M_{k,G}$ is spanned as a vector space over K_G by the $\sum_{g \in G} f' * g$ with $f' \in S_1$. With $f' = \zeta_N^j E_{\alpha_1} \cdots E_{\alpha_k}$, $\sum_{g \in G} f' * g$ agrees with (3.3) by Lemma 3.4. The last statement of the proposition now follows from Lemma 3.4. □

Fix a subgroup G of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that contains $-I$ and fix an even integer $k \geq 2$. We now explain how to find an explicit basis of the K_G-vector space $M_{k,G}$. When $N < 3$, we have $M_{k,G} = M_{k,G'}$, where G' is the subgroup of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ consisting of matrices whose image modulo N lies in G. So we may assume that $N \geq 3$.

The dimension $d := M_k(\Gamma_G)$ is straightforward to compute, cf. [Shi94, §2.6], and is equal to the dimension of $M_{k,G}$ over K_G by Lemma 3.2. By varying over the finite number of pairs $\alpha_1, \ldots, \alpha_k \in (\mathbb{Z}/N\mathbb{Z})^2$ and integers $0 \leq j < \det(G)$, we construct modular forms of the form (3.3) that span $M_{k,G}$. By computing enough terms of the q-expansions, we will eventually find d modular forms $f_1, \ldots, f_d$ whose q-expansions are linearly independent over K_G. This will be the desired basis of $M_{k,G}$. This has been fully implemented in `Magma` in [Zyw25].

3.6. **The canonical map and low gonality.** Fix a subgroup G of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that contains $-I$. Denote the genus of X_G by g and assume that $g \geq 2$.

We will want to understand the image of the canonical map of X_G. As a starting point, recall that the complex vector space of holomorphic differential forms on $\mathcal{X}_{\Gamma_G} = \Gamma_G \backslash \mathcal{H}^*$ arises from the forms $f(z)\,dz$ on $\mathcal{H}$ with $f \in S_2(\Gamma_G)$, cf. [Shi94, Corollary 2.17].

We define $S_{2,G}$ to be the K_G-subspace consisting of those modular forms in $M_{2,G}$ whose q-expansion at each cusp has 0 constant term. Using that the subscheme of cusps of X_G is defined over K_G, we find that the isomorphism from Lemma 3.2 gives rise to an isomorphism

$$S_{2,G} \otimes_{K_G} \mathbb{C} \xrightarrow{\sim} S_2(\Gamma_G).$$

As explained in §3.5, one can find an explicit basis of $M_{2,G}$ over K_G. Recall that each element of this basis can be expressed in terms of Eisenstein series of weight 1 and we can thus compute arbitrarily many terms of its q-expansion at each cusp of X_G. We can then find an explicit basis

$$f_1, \ldots, f_g$$

of $S_{2,G}$ over K_G. Moreover, we can compute arbitrarily many terms of the q-expansion of each f_i at each cusp of X_G. With respect to the basis $f_1, \dots, f_g$, we have the canonical map

$$\phi\colon X_G \to \mathbb{P}^{g-1}_{K_G}.$$

Let C be the curve $\phi(X_G)$; it is unique up to composition with an automorphism of $\mathbb{P}^{g-1}_{K_G}$. Let $I(C)$ be the homogeneous ideal in $K_G[x_1, \dots, x_g]$ corresponding to C. For each integer $n \geq 0$, $I(C)_n$ is the K_G-vector space consisting of homogeneous polynomials $F \in K_G[x_1, \dots, x_g]$ of degree d such that $F(f_1, \dots, f_g) = 0$.

For a fixed $n \geq 0$, we now explain how to compute a basis of $I(C)_n$ over K_G. Let $m_1, \dots, m_r$ be the monomials in $K_G[x_1, \dots, x_g]$ of total degree n; they are are basis of $K_G[x_1, \dots, x_g]_n$. After expanding out the expression

$$\sum_{j=1}^{r} c_j \cdot m_j(f_1, \dots, f_g)$$

by using all the computed terms of the q-expansions of the f_i, the coefficients of this q-expansion gives a set $\mathcal{P}$ of degree 1 homogeneous polynomials in $K_G[c_1, \dots, c_r]$. Let V be the K_G-vector space consisting of the solutions in K_G^r to all the linear polynomials $\mathcal{P}$ (note that the polynomials in $\mathcal{P}$ will have coefficients in $\mathbb{Q}(\zeta_N)$). We then have $I(C)_n \subseteq I'_n$, where

$$I'_n := \{\textstyle\sum_{i=1}^{r} a_i m_i : a \in V\}.$$

Unfortunately, $I(C)_n$ and I'_n need not agree if we do not use enough terms of the q-expansions of the f_i. Using the Sturm bound from [Zyw22a, Lemma 4.1], we can compute sufficiently many terms of the q-expansions of the f_i so that we are guaranteed to have $I(C)_n = I'_n$.

Remark 3.6. There are many cases where we can determine $\dim_{K_G} I(C)_n$ ahead of time and hence do not need to use the Sturm bound. Note that $I(C)_n = I'_n$ if and only if $\dim_{K_G} I(C)_n = \dim_{K_G} I'_n$. For example if $n = 2$ and $\dim_{K_G} I'_2 < \binom{g-1}{2}$, then we have $\dim_{K_G} I(C)_2 = \binom{g-2}{2}$ by Proposition 2.4(ii). If X_G is known to not be geometrically hyperelliptic, then $\dim_{K_G} I(C)_n$ is given for $n \geq 2$ by Proposition 2.4(i).

We shall now explain how to computationally determine if X_G has geometric gonality 2 or 3.

3.6.1. *Checking for geometric gonality* 2. We may assume that $g \geq 3$ since otherwise X_G is hyperelliptic. By Proposition 2.4(ii), the integer $d = \dim_K I(C)_2$ is $\binom{g-1}{2}$ if X_G is geometrically hyperelliptic and $\binom{g-2}{2}$ otherwise. We have $\binom{g-2}{2} < \binom{g-1}{2}$ since $g \geq 3$. Therefore, X_G has geometric gonality 2 if and only if $d = \binom{g-1}{2}$. Thus our computation of a K_G-basis of $I(C)_2$ will determine if X_G has geometric gonality 2.

Remark 3.7. Instead of solving for a basis of $I(C)_2$, we can sometimes just set up the linear equations (using modular forms of a fixed precision) to find an upper bound on d. If we find that $d < \binom{g-1}{2}$, then X_G is not geometrically hyperelliptic. Taking our linear equations to have coefficients in $\mathcal{O}_K$ then reducing them modulo maximal ideals, we can sometimes deduce that $d < \binom{g-1}{2}$; this is preferable since linear algebra is significantly faster over finite fields.

3.6.2. *Checking for geometric gonality* 3. By applying the method from §3.6.1, we may assume that X_G is known to have geometric gonality at least 3. We may also assume that we have computed a basis $F_1, \dots, F_d$ of $I(C)_2$ over K_G. We may further assume that $g \geq 5$ since Proposition 2.1(iii) implies that X_G has geometric gonality 3 when g is 3 or 4.

Let W be the K_G-subspace of $K_G[x_1, \dots, x_g]_3$ spanned by $x_i F_j(x_1, \dots, x_g)$ with $1 \leq i \leq g$ and $1 \leq j \leq d$. One can compute the dimension of W. By Proposition 2.4(i) and (iv), we have

$$\dim_{K_G} W \leq \tbinom{g+2}{3} - 5(g-1)$$

with a strict inequality holding if and only if $(X_G)_{\overline{K}_G}$ is trigonal or isomorphic to a smooth plane quintic.

We can now assume that $\dim_{K_G} W < \binom{g+2}{3} - 5(g-1)$ since otherwise X_G has geometric gonality at least 4. A smooth plane quintic has genus 6 so we may assume that $g = 6$ since otherwise X_G will have geometric gonality 3. By Proposition 2.4(iv), the quotient I_3/W has dimension $g - 3 = 3$ over K.

By computing a basis for $I(C)_3$ over K_G, we can then find $H_1, H_2, H_3 \in I(C)_3$ that form a basis of $I(C)_3/W$ over K_G. By Proposition 2.4(iii), the polynomials $F_1, \dots, F_d, H_1, H_2, H_3$ define the curve C in $\mathbb{P}^5_K$ which is isomorphic to X_G. The geometric gonality of the genus 6 curve $C \cong X_G$ can be computed using the algorithms of [Har13]; this has been implemented in the `Magma` function `Genus6GonalMap`.

4. Modular curves revisited

We will need more information about modular curves than what is given in §3. In particular, there are a few place where we need an integral model so that we can talk about reduction modulo a prime ideal in a careful manner. Throughout we fix an integer $N \geq 3$.

Our main reference is the book of Deligne and Rapoport [DR73]; in particular, the introduction gives a readable overview of the relevant moduli problems. Note that we will consider schemes over $\mathbb{Z}[1/N]$ and $\mathbb{Z}[\zeta_N, 1/N]$ which will simplify some of the material in [DR73] which often works over $\mathbb{Z}$ and $\mathbb{Z}[\zeta_N]$ instead.

4.1. The modular curve M_N°.

4.1.1. *Over* $\mathbb{Z}[1/N]$. For a fixed $\mathbb{Z}[1/N]$-scheme S, we consider pairs (E, α), where E is an elliptic curve over S and $\alpha\colon (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E[N]$ is an isomorphism of group schemes. Two such pairs (E, α) and (E', α') are *isomorphic* if there is an isomorphism $f\colon E \to E'$ of elliptic curves over S such that $f \circ \alpha\colon (\mathbb{Z}/N\mathbb{Z})^2 \to E[N] \to E'[N]$ agrees with α'.

Let $M_N^\circ(S)$ be the set of isomorphism classes of such pairs (E, α). This gives a functor M_N° from the category of $\mathbb{Z}[1/N]$-schemes to the category of sets where the functoriality comes from base change. Since $N \geq 3$, this functor is representable by a $\mathbb{Z}[1/N]$-scheme that we also denote by M_N°. The scheme M_N° is a smooth curve over $\mathbb{Z}[1/N]$.

There is an a left action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on M_N° given by $A \cdot (E, \alpha) = (E, \beta)$, where $\beta(v) = \alpha(vA)$ for $v \in (\mathbb{Z}/N\mathbb{Z})^2$.

Remark 4.1. In [DR73], they instead consider α as an isomorphism $E[N] \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^2$. This does not affect the definition of M_N° but does lead to a different convention concerning the $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$-action; our choice is made so that the action better agrees with the classical setting of §3.

4.1.2. *Over* $\mathbb{Z}[\zeta_N, 1/N]$. For a pair (E, α) defined over S, the Weil pairing of $\alpha((1,0))$ and $\alpha((0,1))$ gives a primitive N-th root of unity $\zeta(\alpha)$ over S. Since M_N° is representable, there is a universal pair (E', α') over M_N° with which the Weil pairings allow us to identify any $\zeta(\alpha)$ with a particular primitive N-th root of unity ζ_N (over M_N°). The map $(E, \alpha) \mapsto \zeta(\alpha) = \zeta_N$ gives rise to a morphism of schemes

$$M_N^\circ \to \operatorname{Spec} \mathbb{Z}[\zeta_N, 1/N].$$

Using this morphism, we shall view M_N° as a scheme over $\mathbb{Z}[\zeta_N, 1/N]$. As a $\mathbb{Z}[\zeta_N, 1/N]$-scheme, M_N° classifies the isomorphism classes of $(E, \alpha)/S$, with S a $\mathbb{Z}[\zeta_N, 1/N]$-scheme, such that $\zeta(\alpha) = \zeta_N$. The left action of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ on M_N° as a scheme over $\mathbb{Z}[1/N]$ is also an action as a scheme over $\mathbb{Z}[\zeta_N, 1/N]$.

4.1.3. *Analytic setting.* We now consider the analytic story. We view $\mathbb{C}$ as a $\mathbb{Z}[\zeta_N, 1/N]$-algebra, by identifying ζ_N with $e^{2\pi i/N}$. For each τ in the upper half-plane $\mathcal{H}$, let E_τ be the elliptic curve over $\mathbb{C}$ arising from the quotient $\mathbb{C}/\Lambda_\tau$, where $\Lambda_\tau := \mathbb{Z} + \mathbb{Z}\tau$. Let $\alpha_\tau \colon (\mathbb{Z}/n\mathbb{Z})^2 \xrightarrow{\sim} E_\tau[N]$ be the group isomorphism for which $\alpha_\tau((1,0)) = \tau/N + \Lambda_\tau$ and $\alpha_\tau((0,1)) = 1/N + \Lambda_\tau$. The Weil pairing of $\alpha_\tau((1,0))$ and $\alpha_\tau((0,1))$ is ζ_N. Therefore, the pair (E_τ, α_τ) gives a complex point on $M_N^\circ \times_{\mathbb{Z}[\zeta_N,1/N]} \mathbb{C}$. Moreover, the map $\tau \mapsto (E_\tau, \alpha_\tau)$ induces an isomorphism

$$\Gamma(N)\backslash\mathcal{H} \xrightarrow{\sim} (M_N^\circ \times_{\mathbb{Z}[\zeta_N,1/N]} \mathbb{C})^{\mathrm{an}} \tag{4.1}$$

of complex analytic spaces. One can check that the actions of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ on both sides of (4.1) agree.

Remark 4.2. Note that $(M_N^\circ \times_{\mathbb{Z}[1/N]} \mathbb{C})^{\mathrm{an}}$ is isomorphic to $\varphi(N)$ copies of $\Gamma(N)\backslash\mathcal{H}$.

Fix $\tau \in \mathcal{H}$ and define $q := e^{2\pi i\tau}$ and $q^{1/N} := e^{2\pi i\tau/N}$. For later comparison with the Tate curve, note that applying the function $e^{2\pi iz}$ gives an isomorphism between (E_τ, α_τ) and the pair $(\mathbb{C}^\times/q^{\mathbb{Z}}, \alpha')$ where $\alpha'((1,0))$ and $\alpha'((0,1))$ are represented by $q^{1/N}$ and ζ_N, respectively.

4.2. **The modular curve M_N.** Deligne and Rapoport compactify M_N° by giving a moduli interpretation of the cusps in terms of *generalized elliptic curves*. For the definition of generalized elliptic curves see [DR73, I Definition 1.12].

There is a functor M_N from the category of $\mathbb{Z}[1/N]$-schemes to the category of sets defined so that $M_N(S)$ corresponds to pairs (E, α), where E is a generalized elliptic curve over S and $\alpha \colon (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E[N]$ is an isomorphism of group schemes; see [DR73, IV §2] for the construction (they define an algebraic stack and then show it is a scheme M_N assuming $N \geq 3$). The scheme M_N over $\mathbb{Z}[1/N]$ is smooth and projective. We can naturally identify M_N° with an open subscheme of M_N. The complement of M_N° in M_N is a finite étale scheme M_N^∞ over $\mathbb{Z}[1/N]$. The action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on M_N° extends to M_N by using the same definition.

Arguing as in §4.1.2, we can give M_N the structure of a $\mathbb{Z}[\zeta_N, 1/N]$-scheme. Using our $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$-action, we find that $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ acts on M_N when viewed as a $\mathbb{Z}[\zeta_N, 1/N]$-scheme. The isomorphism (4.1) extends to an isomorphism

$$\mathcal{X}_{\Gamma(N)} \xrightarrow{\sim} (M_N \times_{\mathbb{Z}[\zeta_N,1/N]} \mathbb{C})^{\mathrm{an}}$$

of smooth compact Riemman surfaces, where $\mathcal{X}_{\Gamma(N)}$ was defined in §3.1. In particular, we have an isomorphism between $X_{\Gamma(N)}$ and $M_N \times_{\mathbb{Z}[\zeta_N,1/N]} \mathbb{C}$.

4.3. **Modular forms of level N.** There is a universal generalized elliptic curve $\mathscr{E} \to M_N$ and we let ω be the invertible sheaf on M_N that is the pushforward of the relative dualizing sheaf. We have a natural isomorphism

$$\Omega^1_{M_N}(M_N^\infty) \cong \omega^{\otimes 2}, \tag{4.2}$$

cf. [DR73, VI 4.5.2].

Fix an integer $k \geq 2$. Following the definition [DR73, VII 3.6], we say that a modular form of level N and weight k over $\mathbb{Z}[\zeta_N, 1/N]$ an element of $H^0(M_N, \omega^{\otimes k})$. We can view $H^0(M_N, \omega^{\otimes k})$ as a $\mathbb{Z}[\zeta_N, 1/N]$-module by using that M_N is a $\mathbb{Z}[\zeta_N, 1/N]$-scheme. Our action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on M_N gives a right action on $H^0(M_N, \omega^{\otimes k})$ as a $\mathbb{Z}[1/N]$-module (and a right action of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ as a $\mathbb{Z}[\zeta_N, 1/N]$-module).

Fix a modular form $f \in H^0(M_N, \omega^{\otimes k})$. To better explain the connection with the classical definition of modular forms in §3, we will now describe the q-expansion of f algebraically; for details see [DR73, Chapter VII]. The *Tate curve* gives an elliptic curve E_q defined over the Laurent series ring $\mathbb{Z}((q))$ which can be expressed as $\mathbb{G}_m/q^{\mathbb{Z}}$. The curve comes with a canonical invariant differential dx/x, where x is a parameter of $\mathbb{G}_m$. After base extending E_q to $\mathbb{Z}[\zeta_N, 1/N]((q^{1/N}))$,

where $q^{1/N}$ is a fixed N-th root of q, we obtain an isomorphism $\alpha\colon (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E_q[N]$ of group schemes, where $\alpha((1,0))$ and $\alpha((0,1))$ are represented by $q^{1/N}$ and ζ_N, respectively. The pair (E_q,α) gives a $\mathbb{Z}[\zeta_N,1/N](\!(q^{1/N})\!)$-point on M_N which is a morphism $h\colon \operatorname{Spec}\mathbb{Z}[\zeta_N,1/N](\!(q^{1/N})\!) \to M_N$ of $\mathbb{Z}[\zeta_N,1/N]$-schemes. We have

$$h^*(f) = F_f \cdot (\tfrac{dx}{x})^{\otimes k}$$

for a unique $F_f \in \mathbb{Z}[\zeta_N,1/N](\!(q^{1/N})\!)$. Moreover, we have $F_f \in \mathbb{Z}[\zeta_N,1/N][\![q^{1/N}]\!]$; this is shown in [DR73, VII §3] by instead starting with the Tate curve as a generalized elliptic curve over $\mathbb{Z}[\![q]\!]$. We call F_f the q-expansion of f.

From [DR73, VII Construction 4.6], and the remarks following it, we find that there is an isomorphism

$$\beta\colon H^0(M_N,\omega^{\otimes k}) \otimes_{\mathbb{Z}[\zeta_N,1/N]} \mathbb{C} \xrightarrow{\sim} M_k(\Gamma(N)) \tag{4.3}$$

that preserves q-expansions. When k is even, the isomorphism (4.2) also lets us view (4.3) as the usual isomorphism between $M_k(\Gamma(N))$ and certain differential $k/2$-forms on $\mathcal{Y}_{\Gamma(N)}$. The actions of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ are compatible with β (the construction in [DR73] makes use of the isomorphism (4.1) and we have chosen actions so that they do agree).

Proposition 4.3.

(i) *The $\mathbb{Z}[\zeta_N,1/N]$-submodule $M_k(\Gamma(N),\mathbb{Z}[\zeta_N,1/N])$ of $M_k(\Gamma(N),\mathbb{Q}(\zeta_N))$ is stable under the right $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$-action from §3.2.*

(ii) *There are unique isomorphisms*

$$H^0(M_N,\omega^{\otimes k}) \xrightarrow{\sim} M_k(\Gamma(N),\mathbb{Z}[\zeta_N,1/N]) \quad \text{and} \quad H^0((M_N)_{\mathbb{Q}},\omega^{\otimes k}) \xrightarrow{\sim} M_k(\Gamma(N),\mathbb{Q}(\zeta_N))$$

of modules over $\mathbb{Z}[\zeta_N,1/N]$ and $\mathbb{Q}(\zeta_N)$, respectively, that preserves q-expansions. The actions of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ are compatible with these isomorphisms.

Proof. The isomorphism β restricts to an injective homomorphism

$$H^0(M_N,\omega^{\otimes k}) \hookrightarrow M_k(\Gamma(N),\mathbb{Z}[\zeta_N,1/N]). \tag{4.4}$$

Let $F \in \mathbb{Z}[\zeta_N,1/N][\![q_N]\!]$ be the q-expansion of any modular form in $M_k(\Gamma(N),\mathbb{Z}[\zeta_N,1/N])$. Since β is an isomorphism, there is a unique $f \in H^0(M,\omega^{\otimes k}) \otimes_{\mathbb{Z}[\zeta_N,1/N]} \mathbb{Q}(\zeta_N)$ such that f has q-expansion F. By [DR73, VII Théorème 3.10(i) and Corollaire 3.13], the q-expansion of f at each cusp has coefficients in $\mathbb{Z}[\zeta_N,1/N]$ and hence $f \in H^0(M_N,\omega^{\otimes k})$ by [DR73, VII Théorème 3.9]. This proves that (4.4) is surjective and hence is an isomorphism of $\mathbb{Z}[\zeta_N,1/N]$-modules. Since $H^0(M_N,\omega^{\otimes k})$ is stable under its $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$-action and β is an isomorphism that respects the $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$-action, we deduce that $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ acts on $M_k(\Gamma(N),\mathbb{Z}[\zeta_N,1/N])$ and the isomorphism (4.4) respects the $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$-action. Part (i) now follows since $\mathbb{Z}[\zeta_N,1/N]$ is stable under the action of $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$.

Take any $d \in (\mathbb{Z}/N\mathbb{Z})^\times$. We claim that the action of the matrix $A := \left(\begin{smallmatrix}1&0\\0&d\end{smallmatrix}\right)$ is compatible with the isomorphism (4.4). We have $(E_q,\alpha') = A\cdot(E_q,\alpha)$, where $\alpha'\colon (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E_q[N]$ is the isomorphism of group schemes for which $\alpha'((1,0))$ and $\alpha'(0,1))$ are represented by $q^{1/N}$ and ζ_N^d, respectively. Take any $f \in H^0(M_N,\omega^{\otimes k})$ and define $f' := f\cdot A$. We have $h^*(f') = h'^*(f)$, where $h'\colon \operatorname{Spec}\mathbb{Z}[\zeta_N,1/N](\!(q^{1/N})\!) \to M_N$ is the morphism of $\mathbb{Z}[\zeta_N,1/N]$-schemes given by the point (E_q,α'). Using that E_q is defined over $\mathbb{Z}(\!(q^{1/N})\!)$, we find that $h'^*(f) = \sigma_d(F_f)\cdot(\frac{dx}{x})^{\otimes k}$ and hence $\sigma_d(F_f) = F_{f'}$. We have now proved the part of (ii) concerning the isomorphism (4.4). Part (ii) follows by base changing to $\mathbb{Q}(\zeta_N)$; note that we a natural isomorphism $H^0(M_N,\omega^{\otimes k}) \otimes_{\mathbb{Z}[\zeta_N,1/N]} \mathbb{Q}(\zeta_N) \xrightarrow{\sim} H^0((M_N)_{\mathbb{Q}},\omega^{\otimes k})$ by [DR73, VII Théorème 3.10(i)]. □

The following will be useful for proving the integrality of the coefficients of a q-expansion at a prime ideal $\mathfrak{p}$ given only finitely many coefficients.

Proposition 4.4. *Take any subgroup G of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Define $H := G \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ and let R be a set of representatives of the cosets $H\backslash \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Take any nonzero prime ideal $\mathfrak{p} \nmid N$ of $\mathbb{Z}[\zeta_N]$ and consider a modular form $f \in M_{k,G} = M_k(\Gamma(N), \mathbb{Q}(\zeta_N))^G$. For each $A \in R$, let $m_A \geq 1$ be an integer for which $a_n(f*A)$ is integral at $\mathfrak{p}$ for all $n \leq m_A$, where $f*A = \sum_{n=0}^{\infty} a_n(f*A)q_N^n$. If $\sum_{A\in R} m_A > k/12$, then $a_n(f*A)$ is integral at $\mathfrak{p}$ for all $n \geq 0$ and all $A \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.*

Proof. Take any nonzero $f \in M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$. We define $v_{\mathfrak{p}}(f) := \min\{v_{\mathfrak{p}}(a_n) : n \geq 0\}$, where $\sum_{n=0}^{\infty} a_n(f)q_N^n$ is the q-expansion of f and $v_{\mathfrak{p}}$ is the $\mathfrak{p}$-adic valuation of K. By [DR73, VII Corollaire 3.12] and $\mathfrak{p} \nmid N$, we have $v_{\mathfrak{p}}(f) = v_{\mathfrak{p}}(f*A)$ for all $A \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

Suppose that f is a counterexample to the proposition. By multiplying f by an appropriate element of $\mathbb{Q}(\zeta_N)^\times$, we obtain a nonzero modular form $f' \in M_k(\Gamma(N), \mathbb{Z}[\zeta_N])^H$ for which $v_{\mathfrak{p}}(f') = 0$ and $a_n(f'*A) \equiv 0 \pmod{\mathfrak{p}}$ for all $A \in R$ and $n \leq m_A$. For any $A \in R$ and any B in the coset $H\cdot A \in H\backslash \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, define $m_B := m_A$; we have $a_n(f'*B) \equiv 0 \pmod{\mathfrak{p}}$ for all $n \leq m_B$ since f' is fixed by H. We have

$$\frac{1}{|R|}\sum_{A\in R} m_A = \frac{1}{|\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})|}\sum_{B\in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})} m_B \leq k/12,$$

where the inequality follows from [DR73, VII Corollaire 3.14] and our assumption $\mathfrak{p} \nmid N$. Therefore, no counterexamples will occur if $\frac{1}{|R|}\sum_{A\in R} m_A > k/12$. □

4.4. **The modular curve X_G revisited.** Fix a subgroup $G \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ containing $-I$. Let M_G be the $\mathbb{Z}[1/N]$-scheme that is the quotient of M_N by the action of G. By [DR73, IV Proposition 3.10], M_G is proper and flat over $\mathbb{Z}[1/N]$ and agrees with the coarse moduli space of generalized elliptic curves with G-level structure. The scheme M_G is also smooth over $\mathbb{Z}[1/N]$, cf. [DR73, VI Proposition 6.7].

With notation as in §4.1.2, for a pair (E,α) and a matrix $A \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, we have $\zeta(A\cdot(E,\alpha)) = \zeta(E,\alpha)^{\det(A)}$. We obtain a morphism

$$M_G \to \mathrm{Spec}(\mathbb{Z}[\zeta_N, 1/N]^{\det G}),$$

where $\mathbb{Z}[\zeta_N, 1/N]^{\det G}$ is the subring of $\mathbb{Z}[\zeta_N, 1/N]$ fixed by σ_d for all $d \in \det(G)$. In particular, M_G can be viewed as a scheme over $\mathcal{O}_{K_G}[1/N] = \mathbb{Z}[\zeta_N, 1/N]^{\det G}$. Moreover, M_G is a smooth proper curve over $\mathcal{O}_{K_G}[1/N]$.

Define the graded K_G-module

$$R'_G := \bigoplus_{k\geq 0 \text{ even}} H^0((M_N)_{\mathbb{Q}}, \omega^{\otimes k})^G.$$

The isomorphisms from Proposition 4.3(ii) induce an isomorphism $R'_G \xrightarrow{\sim} R_G$ of graded K_G-modules, where R_G is defined in §3.4. From §3.4, we find that tensoring up to $\mathbb{C}$ gives an isomorphism $R'_G \otimes_{K_G} \mathbb{C} \xrightarrow{\sim} R_{\Gamma_G}$ of graded $\mathbb{C}$-algebras. One can show that $M_G \times_{\mathcal{O}_{K_G}[1/N]} \mathbb{C} \cong X_{\Gamma_G}$. Since $X_{\Gamma_G} \cong \mathrm{Proj}\, R_{\Gamma_G}$, we find that the curve $M_G \times_{\mathcal{O}_{K_G}[1/N]} K_G$ is isomorphic to $\mathrm{Proj}\, R'_G$. Since $R'_G \cong R_G$, we deduce that $M_G \times_{\mathcal{O}_{K_G}[1/N]} K_G$ is isomorphic to $\mathrm{Proj}\, R_G = X_G$.

In summary, M_G is a smooth proper curve over $\mathcal{O}_{K_G}[1/N]$ whose generic fiber is a nice curve over K_G isomorphic to X_G.

5. Explicit gonality bounds

Throughout this section we fix a congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ containing $-I$. Let g be the genus of X_Γ, let N be the level of Γ and let D be the index $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$.

The natural morphism $X_\Gamma \to X_{\mathrm{SL}_2(\mathbb{Z})} \cong \mathbb{P}^1_{\mathbb{C}}$ has degree D since $-I \in \Gamma$ and hence $\mathrm{gon}(X_\Gamma) \leq D$. The following shows that $\mathrm{gon}(X_\Gamma)$ can also be uniformly bounded below by D times a positive constant.

Theorem 5.1. *We have* $\mathrm{gon}(X_\Gamma) > \frac{325}{32768}D$. *If* $N \leq 226$, *then* $\mathrm{gon}(X_\Gamma) > \frac{1}{96}D$.

Proof. The theorem will follow from inequalities of Zograf in [Zog87]. Set $\gamma := \mathrm{gon}(X_\Gamma)$. In [Zog87], our Riemann surface X_Γ is denoted $\overline{\Gamma\backslash\mathcal{H}}$ and the quantity $\mu(\overline{\Gamma\backslash\mathcal{H}})$ that arises there is equal to $D\pi/3$ (this uses the footnote on [Zog87, p.109] and (3.1)).

We may assume that $\gamma \leq D/96$ since otherwise the theorem holds immediately. The hypothesis of [Zog87, Theorem 3] holds since $\gamma \leq D/96$ and we obtain an inequality

$$\lambda_1 < \tfrac{8\pi\gamma}{D\pi/3} = 24\gamma/D,$$

where $\lambda_1 := \lambda_1(\Gamma)$ is the minimal nonzero eigenvalue of the automorphic Laplacian operator on $L^2(\Gamma\backslash\mathcal{H})$ induced from the Laplace operator $\Delta = -y^2(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2})$. Equivalently, we have the bound

$$\gamma > \tfrac{\lambda_1}{24}D. \tag{5.1}$$

In [Sel65], Selberg conjectured that $\lambda_1 \geq 1/4$ and proved the inequality $\lambda_1 \geq 1/4 - (1/4)^2 = 3/16$. Using (5.1) with $\lambda_1 \geq 3/16$ gives $\gamma > D/128$ which is precisely [Zog87, Theorem 5]. The inequality $\lambda_1 \geq 1/4 - (7/64)^2 = 975/4096$ was proved by Kim and Sarnak in [Kim03, Appendix 2]. Using (5.1) with the bound of Kim and Sarnak gives $\gamma > \frac{325}{32768}D$ which proves the first inequality of the theorem.

We may now assume that $N \leq 226$. Since N is the level of Γ, we have $\Gamma \supseteq \Gamma(N)$ and hence $\lambda_1 := \lambda_1(\Gamma) \geq \lambda_1(\Gamma(N))$. Booker, Lee and Strömbergsson [BLS20] have shown that Selberg's conjecture holds for all congruence subgroups $\Gamma(N)$ with $N \leq 226$. Therefore, we have $\lambda_1 \geq \lambda_1(\Gamma(N)) \geq 1/4$. Using the bound (5.1), we deduce that $\gamma > \frac{1/4}{24}D = D/96$. □

Corollary 5.2.

(i) *Suppose that* $\mathrm{gon}(X_\Gamma) = 2$. *Then* $D \leq 201$. *If* $N \leq 226$, *then* $D \leq 191$.
(ii) *Suppose that* $\mathrm{gon}(X_\Gamma) = 3$. *Then* $D \leq 302$. *If* $N \leq 226$, *then* $D \leq 287$.
(iii) *Suppose that* $\mathrm{gon}(X_\Gamma) = 4$. *Then* $D \leq 403$. *If* $N \leq 226$, *then* $D \leq 383$.

Proof. This follows directly from Theorem 5.1, which gives upper bounds on D in terms of $\mathrm{gon}(X_\Gamma)$, and using that D is an integer. □

Remark 5.3. There are similar bounds of Abramovich which are perhaps better known than Zagorof's. Using the bounds of [Abr96], we obtain $\gamma \geq \frac{\lambda_1}{24}D$ instead of (5.1) in the proof of Theorem 5.1; Zagorof obtains a strict inequality by considering the cusps. When $\mathrm{gon}(X_\Gamma) = 2$, this weaker bound would give Corollary 5.2(i) except we would only have $D \leq 192$ when $N \leq 226$. This slight difference is relevant since there are 470 congruence subgroups Γ of $\mathrm{SL}_2(\mathbb{Z})$, up to conjugacy in $\mathrm{GL}_2(\mathbb{Z})$, that contain $-I$ and satisfy $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma] = 192$.

When the level N of Γ is not divisible by a small prime, we can sometimes improve on these bounds for D.

Theorem 5.4. *Let* p *be a prime not dividing* N.

(i) *If* $\mathrm{gon}(X_\Gamma) = 2$ *and* $g \geq 2$, *then* $D \leq 24(p^2+1)/(p-1)$.
(ii) *If* $\mathrm{gon}(X_\Gamma) = 3$ *and* $g \geq 5$, *then* $D \leq 36(p^2+1)/(p-1)$.
(iii) *If* X_Γ *is bielliptic and* $g \geq 6$, *then* $D \leq 24(p^2+2p+1)/(p-1)$.

Proof. We may assume that $g \geq 2$. We have $N \geq 3$ since otherwise X_Γ would have genus 0. Since $p \nmid N$, we can choose a prime ideal $\mathfrak{p}$ of $\mathbb{Z}[\zeta_N, 1/N]$ containing p. Let $\mathbb{F}_{p^2}$ be the subfield of $\overline{\mathbb{F}}_\mathfrak{p}$ of cardinality p^2.

Let $G \subseteq \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ be the image of Γ modulo N. Define the field $K_G := \mathbb{Q}(\zeta_N)^{\det(G)} = \mathbb{Q}(\zeta_N)$. In §4.4, we defined a smooth proper curve M_G over $\mathcal{O}_{K_G}[1/N] = \mathbb{Z}[\zeta_N, 1/N]$ whose generic fiber is isomorphic to X_G. We have isomorphisms

$$(M_G)_\mathbb{C} \cong (X_G)_\mathbb{C} \cong X_\Gamma.$$

Note that $(M_G)_{\mathbb{F}_\mathfrak{p}}$ is a nice curve of genus g since $\mathfrak{p} \nmid N$. Below we will make use of the schemes M_N° and M_N from §4 and they will be viewed as schemes over $\mathbb{Z}[\zeta_N, 1/N]$.

We claim that there is a curve C over $\mathbb{F}_{p^2}$ such that $(M_G)_{\overline{\mathbb{F}}_\mathfrak{p}} \simeq C_{\overline{\mathbb{F}}_\mathfrak{p}}$ and

$$|C(\mathbb{F}_{p^2})| \geq (p-1)D/12. \tag{5.2}$$

We define C following the construction of Poonen in §3 of [Poo07] which builds off of the ideas of Ogg [Ogg74]. Define $L := (\mathbb{Z}/N\mathbb{Z})^2$ which we turn into a $\mathrm{Gal}(\overline{\mathbb{F}}_\mathfrak{p}/\mathbb{F}_{p^2})$-module by letting the p^2-th power Frobenius automorphism act as multiplication by $-p$. We fix a group isomorphism $\iota\colon \wedge^2 L \to \mu_N$, with $\mu_N \subseteq \overline{\mathbb{F}}_\mathfrak{p}$ the group of N-th roots of unity, so that the $\mathrm{Gal}(\overline{\mathbb{F}}_\mathfrak{p}/\mathbb{F}_{p^2})$-actions are compatible. Let Y be the smooth affine curve over $\mathbb{F}_{p^2}$ that parametrizes pairs (E, α) where $\alpha\colon L \xrightarrow{\sim} E[N]$ is an isomorphism under which the Weil pairing corresponds to ι. Observe that we have a canonical isomorphism $Y_{\overline{\mathbb{F}}_\mathfrak{p}} = (M_N^\circ)_{\overline{\mathbb{F}}_\mathfrak{p}}$ since they describe the same moduli space. We can extend Y to a smooth projective curve X defined over $\mathbb{F}_{p^2}$ and we have $X_{\overline{\mathbb{F}}_\mathfrak{p}} = (M_N)_{\overline{\mathbb{F}}_\mathfrak{p}}$. The action of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ on L gives rise to an action on Y and X that respects the isomorphism $X_{\overline{\mathbb{F}}_\mathfrak{p}} = (M_N)_{\overline{\mathbb{F}}_\mathfrak{p}}$. Therefore, $(M_G)_{\overline{\mathbb{F}}_\mathfrak{p}} = G\backslash(M_N)_{\overline{\mathbb{F}}_\mathfrak{p}}$ is isomorphic to $C_{\overline{\mathbb{F}}_\mathfrak{p}}$, where C is the nice curve over $\mathbb{F}_{p^2}$ that is the quotient of X by G. In §3 of [Poo07], it is observed that

$$|C(\mathbb{F}_{p^2})| \geq (p-1)[\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) : G]/12 = (p-1)D/12 \tag{5.3}$$

by considering supersingular elliptic curves defined over $\mathbb{F}_{p^2}$. This completes the proof of the claim.

We now prove (i) and (ii), so assume that $\gamma := \mathrm{gon}(X_\Gamma)$ is 2 or 3 with $g \geq 5$ if $\gamma = 3$. The geometric gonality of $(M_G)_{K_G}$ is γ since $(M_G)_{\mathbb{C}}$ is isomorphic to X_Γ. Define $d := \mathrm{gon}((M_G)_{\overline{\mathbb{F}}_\mathfrak{p}})$. We have $d \leq \gamma$ by applying Proposition 2.3. We have $2 \leq d \leq \gamma$ since $(M_G)_{\overline{\mathbb{F}}_\mathfrak{p}}$ has genus $g \geq 2$. The curve C has geometric gonality d since it is isomorphic over $\overline{\mathbb{F}}_\mathfrak{p}$ to $(M_G)_{\overline{\mathbb{F}}_\mathfrak{p}}$. By Theorems 1 and 2 of [RX18], which uses that $g \geq 2$ when $d = 2$ and $g \geq 5$ when $d = 3$, there is a morphism $\pi\colon C \to Z$ of degree d, where Z is a nice curve over $\mathbb{F}_{p^2}$ of genus 0. We have $Z \simeq \mathbb{P}^1_{\mathbb{F}_{p^2}}$ since we are working over a finite field. Using that π has degree d, we obtain the easy upper bound

$$|C(\mathbb{F}_{p^2})| \leq d|Z(\mathbb{F}_{p^2})| = d(p^2+1) \leq \gamma(p^2+1).$$

Combining with (5.3) gives $D \leq 12\gamma(p^2+1)/(p-1)$ which completes the proof of (i) and (ii).

We now prove (iii), so assume X_Γ is bielliptic and $g \geq 6$. Therefore, $(M_G)_{K_G}$ is geometrically bielliptic since it is isomorphic over $\mathbb{C}$ to X_Γ. Proposition 2.8 implies that $(M_G)_{\overline{\mathbb{F}}_\mathfrak{p}}$ is geometrically bielliptic. By the claim, C is also geometrically bielliptic. Since C has genus $g \geq 6$, Lemma 2.7 implies that there is a degree 2 morphism $C \to Z$, where Z is a nice curve of genus 1 defined over $\mathbb{F}_{p^2}$. Using the Weil bounds, we have

$$|C(\mathbb{F}_{p^2})| \leq 2|Z(\mathbb{F}_{p^2})| \leq 2(p^2+2p+1).$$

Combining with (5.3) gives $D \leq 24(p^2+2p+1)/(p-1)$ which completes the proof of (iii). □

6. Checking if a modular curve is geometrically bielliptic

Fix a positive integer N and subgroup G of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that contains $-I$. In this section, we explain how to computationally verify if the modular curve X_G is geometrically bielliptic. Let g be the genus of X_G. We may assume that $g \geq 2$ since X_G is not geometrically bielliptic when $g = 0$ and is geometrically bielliptic when $g = 1$. We have $N \geq 3$ since $g \geq 2$. To ease notation, we set $K := K_G$ for the rest of the section.

As outlined in §3.6, one can compute a basis $f_1, \dots, f_g$ of the K-vector space $S_{2,G}$. Moreover for each f_i, we can compute arbitrary many terms of its q-expansion at each cusp. With respect

to the basis $f_1, \dots, f_g$, we have the canonical map

$$\phi\colon X_G \to \mathbb{P}^{g-1}_K$$

Let C be the image of ϕ and let $I(C)$ be the corresponding homogeneous ideal of $K[x_1, \dots, x_g]$. As described in §3.6, we can compute a basis $F_1, \dots, F_d$ of the K-vector space $I(C)_2$. As noted in §3.6.1, the integer d allows us to determine whether or not X_G is geometrically hyperelliptic.

6.1. **Geometrically hyperelliptic case.** Suppose that X_G is geometrically hyperelliptic. If X_G is also geometrically bielliptic, then $g \leq 3$ by Theorem 2.2. So we may assume that $g = 2$ or $g = 3$.

We have a basis $f_1, \dots, f_g$ of $S_{2,G}$ over K. Using this, we can construct a basis $w_1, \dots, w_g$ of $S_{2,G} \otimes_K \mathbb{Q}(\zeta_N) \subseteq S_2(\Gamma_G)$ over $\mathbb{Q}(\zeta_N)$ so that the order of vanishing of w_i at the cusp at infinity is strictly increasing as a function of i. As usual we have $q = e^{2\pi i \tau}$. The function field of $(X_G)_{\mathbb{Q}(\zeta_N)}$ is generated by $x := w_{g-1}/w_g$ and $y := dx/(w_g dq)$, and there is a unique polynomial $h(x) \in \mathbb{Q}(\zeta_N)[x]$ of degree at most $2g+2$ such that $y^2 = h(x)$, see Lemma 2.5 of [BGJGP05] and the computations that follow the lemma. By using enough terms of the q-expansions of our modular forms, we can set up linear equations and solve for the coefficients of h. By changing variables, we will obtain a model

$$y^2 = h(x)$$

of $(X_G)_{\mathbb{Q}(\zeta_N)}$ where $h(x)$ is separable of degree $2g+2$ with coefficients in $\mathbb{Z}[\zeta_N]$. Let R be the ring of S-integers in $\mathbb{Z}[\zeta_N]$, where S consists of the nonzero prime ideals $\mathfrak{p}$ that divide the leading coefficients of h or divide $2\operatorname{disc}(h)$. Let $\mathcal{X}$ be the smooth projective curve over $\operatorname{Spec} R$ defined by the affine equation $y^2 = h(x)$.

Define $H(x,z) := z^{2g+2}h(x/z) \in \mathbb{Z}[\zeta_N][x,z]$; it is a homogeneous polynomial of degree $2g+2$. Let $\mathcal{Z}$ be the closed reduced subscheme of $\mathbb{A}^4_R$ such that for any algebraically closed field k that is an R-algebra and any point $(a,b,c,d) \in k^4$, (a,b,c,d) lies in $\mathcal{Z}(k)$ if and only if $A := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ satisfies $A^2 = I$, $\operatorname{tr}(A) = 0$ and $H(ax+b, cx+d) = h(x)$.

Lemma 6.1. *Let k be an algebraically closed field that is an R-algebra. Then $\mathcal{X}_k$ is bielliptic if and only if $\mathcal{Z}(k) \neq \emptyset$.*

Proof. First suppose there is a point $(a,b,c,d) \in \mathcal{Z}(k)$ and define $A := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. We have $(cx+d)^{2g+2}h(\frac{ax+b}{cx+d}) = h(x)$. From this and a fixed $\varepsilon \in \{\pm 1\}$, we obtain an automorphism $\sigma(x,y) = (\frac{ax+b}{cx+d}, \frac{\varepsilon y}{(cx+d)^{g+1}})$ of $\mathcal{X}_k$. Using $A^2 = I$, we find that $\sigma^2 = 1$. The matrix A is nonscalar since $\operatorname{tr}(A) = 0$ and k does not have characteristic 2, and hence σ is not the identity map or the hyperelliptic involution. Also by choosing an appropriate $\varepsilon \in \{\pm 1\}$, we may assume that $\mathcal{X}_k$ has a point fixed by σ. Consider the degree 2 morphism $\pi\colon \mathcal{X}_k \to \mathcal{X}_k/\langle\sigma\rangle =: C'$. The curve C' has genus $g' > 0$ since σ is not the hyperelliptic involution (which is unique by Theorem 2.2). We have $0 < g' < g$. We cannot have $(g,g') = (3,2)$ since otherwise the Riemann–Hurwitz formula implies that π is unramified and hence σ has no fixed points. Since $g \in \{2,3\}$, we deduce that $g' = 1$ and hence $\mathcal{X}_k$ is bielliptic.

Now suppose that $\mathcal{X}_k$ is bielliptic and let σ be a bielliptic involution. By [BGJGP05, Proposition 6.11], there is a matrix $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\overline{K})$ satisfying $A^2 = I$ and a number $\varepsilon \in \{\pm 1\}$ such that $\sigma(x,y) = ((ax+b)/(cx+d), \varepsilon y/(cx+d)^{g+1})$. Note that the section containing [BGJGP05, Proposition 6.11] has a characteristic 0 assumption but the proof of this proposition works fine in odd characteristic. Since σ is an automorphism of $\mathcal{X}_k$, we have $(cx+d)^{2g+2}h((ax+b)/(cx+d)) = y^2 = h(x)$ for points $(x,y) \in \mathcal{X}(k)$ not at infinity and hence we have an equality $H(ax+b, cx+d) = h(x)$ of polynomials. To complete the proof of the lemma, we need to show that $\operatorname{tr}(A) = 0$. Suppose to the contrary that $\operatorname{tr}(A) \neq 0$. Since $A^2 = I$, $\operatorname{tr}(A) \neq 0$ and the characteristic of k is not 2, we have $A = \pm I$. However, $A = \pm I$ implies that σ is the identity or hyperelliptic automorphism of $\mathcal{X}_k$ which is a contradiction. Therefore, $\operatorname{tr}(A) = 0$. □

We now explain how to check if X_G is geometrically bielliptic. Consider any nonzero prime ideal $\mathfrak{p} \notin S$ of $\mathcal{O}_K$; we use the same notation to denote the prime ideal $\mathfrak{p}R$ of R. We then check if the subvariety $\mathcal{I}_{\mathbb{F}_\mathfrak{p}}$ of $\mathbb{A}^4_{\mathbb{F}_\mathfrak{p}}$ is empty or not.

Suppose that $\mathcal{I}_{\mathbb{F}_\mathfrak{p}}$ is empty. Since $\mathcal{I}(\overline{\mathbb{F}}_\mathfrak{p}) = \emptyset$, Lemma 6.1 implies that $\mathcal{X}_{\mathbb{F}_\mathfrak{p}}$ is not geometrically bielliptic. Since $\mathcal{X}$ is a smooth projective curve over R, Proposition 2.8(ii) implies that $\mathcal{X}_{\mathbb{Q}(\zeta_N)} \cong (X_G)_{\mathbb{Q}(\zeta_N)}$ is not geometrically bielliptic. In particular, X_G is not geometrically bielliptic.

Now suppose that $\mathcal{I}_{\mathbb{F}_\mathfrak{p}}$ is nonempty. Then there is a point $\bar{z} \in \mathcal{I}(\mathbb{F})$ for some finite extension $\mathbb{F}$ of $\mathbb{F}_\mathfrak{p}$. We can then try to use Hensel's lemma to lift $\bar{z}$ to a point $z \in \mathcal{I}(L)$ for some local field L containing $\mathbb{Q}(\zeta_N)$. If such a lift exists, then $\mathcal{X}_L \cong (X_G)_L$ is geometrically bielliptic by Lemma 6.1; in particular, X_G is geometrically bielliptic.

By looking at sufficiently many nonzero prime ideals $\mathfrak{p} \notin S$ of $\mathcal{O}_K$, the above arguments will eventually determine whether or not X_G is geometrically bielliptic (taking S large enough, we get a smooth scheme $\mathcal{I}$ over R and Hensel's lemma will always apply to give lifts).

6.2. **Genus 3 case.** Assume that $g = 3$. We may assume that X_G is not geometrically hyperelliptic since we have already dealt with this case.

By Proposition 2.4(iii), the curve C is defined by a homogenous polynomial $F(x_1, x_2, x_3) \in K[x_1, x_2, x_3]$ of degree 4 that is unique up to a nonzero scalar. In this case we are going to directly check if $C_{\overline{K}}$ has a bielliptic involution.

Lemma 6.2. *The curve C is geometrically bielliptic if and only if there is a matrix $A \in M_3(\overline{K})$ satisfying $A^2 = I$, $\mathrm{tr}(A) = -1$ and $F(xA^t) = F(x)$.*

Proof. First suppose that $C_{\overline{K}}$ has a bielliptic involution σ. The involution σ induces an automorphism A of the $\overline{K}$-vector space $H^0(C_{\overline{K}}, \Omega_{C/\overline{K}})$ that satisfies $A^2 = I$. Moreover, A has a 1-dimensional $+1$-eigenspace and a 2-dimensional -1-eigenspace since $C/\langle\sigma\rangle$ has genus 1. Thus $A^2 = I$ and $\mathrm{tr}(A) = -1$. Since $C \subseteq \mathbb{P}^2_K$ is the canonical embedding, we can make a choice of isomorphism $H^0(C_{\overline{K}}, \Omega_{C/\overline{K}}) \cong \overline{K}^3$ so that A can be identified with a matrix in $M_3(\overline{K})$ that induces an action on the curve $C_{\overline{K}}$. We thus have $F(xA^t) = cF(x)$ for some nonzero $c \in \overline{K}$ since $I(C_{\overline{K}})_4$ is spanned by F. We have $c = \pm 1$ since $A^2 = I$. If $c = -1$ and $vA^t = -v$ with $v \in \overline{K}^3$, then $F(v) = F(-v) = F(vA^t) = -1 \cdot F(v)$ and hence $F(v) = 0$. So if $c = -1$, then $C_{\overline{K}}$ contains a genus 0 curve by considering the -1-eigenspace of A. Since C has genus 3, we conclude that $F(xA^t) = F(x)$.

Now suppose that there is a matrix $A \in M_3(\overline{K})$ satisfying $A^2 = I$, $\mathrm{tr}(A) = -1$ and $F(xA^t) = F(x)$. The matrix A defines an automorphism σ of $C_{\overline{K}}$ since it is invertible and satisfies $F(xA^t) = F(x)$. We have $\sigma^2 = 1$ since $A^2 = I$. Since $C_{\overline{K}} \subseteq \mathbb{P}^2_{\overline{K}}$ is the canonical embedding, σ acts on the $\overline{K}$-vector space $H^0(C_{\overline{K}}, \Omega_{C/\overline{K}})$ and with an appropriate choice of basis it will act as cA for some nonzero $c \in \overline{K}$. The matrix A is not scalar by the $A^2 = I$ and $\mathrm{tr}(A) = -1$ conditions, so σ induces a nonscalar automorphism of $H^0(C_{\overline{K}}, \Omega_{C/\overline{K}})$ and hence $\sigma \neq 1$.

We have a degree 2 morphism $\phi\colon C_{\overline{K}} \to C_{\overline{K}}/\langle\sigma\rangle =: C'$. Since C has genus 3 and is not geometrically hyperelliptic, C' has genus 1 or 2. Suppose that C' has genus 2. From the Riemann–Hurwitz formula, ϕ is a covering, i.e., there is no ramification. By [Acc94, Lemma 5.10] this implies that $C_{\overline{K}}$ is geometrically hyperelliptic (the first step of the proof is to use ϕ to lift the hyperelliptic involution of C' to a new involution of $C_{\overline{K}}$). Since C is not geometrically hyperelliptic, we deduce that C' has genus 1 and hence C is geometrically bielliptic. □

We can identify a matrix in $M_3(\overline{K})$ with a $\overline{K}$-point of $\mathbb{A}^9_K$. Let Z be the subvariety of $\mathbb{A}^9_K$ whose $\overline{K}$-points correspond to matrices in $M_3(\overline{K})$ that satisfy $A^2 = I$, $\mathrm{tr}(A) = -1$ and $F(xA^t) = F(x)$.

By Lemma 6.2, $X_G \cong C$ is geometrically bielliptic if and only if Z is nonempty. Checking that Z is nonempty or not is something that is straightforward to check (at least in this case, directly

checking for bielliptic involutions becomes infeasible for higher genus). Also Z is finite (one can check that every $\overline{K}$-point of Z corresponds to a different bielliptic involution of $C_{\overline{K}}$).

6.3. **Aside: smooth models.** Assume that $g \geq 4$ and that X_G is not geometrically hyperelliptic; this holds in the cases that remain.

We have $d = \binom{g-2}{2}$ by Proposition 2.4(ii). Let W be the K-subspace of $K[x_1, \dots, x_g]_3$ spanned by $x_i F_j(x_1, \dots, x_g)$ with $1 \leq i \leq g$ and $1 \leq j \leq d$. By computing a basis for $I(C)_3$ over K as in §3.6, we can find polynomials $H_1, \dots, H_r \in K[x_1, \dots, x_g]_3$ that give rise to a basis of $I(C)_3/W$. By Proposition 2.4(iv), we have $r = 0$ or $r = g - 3$. By Proposition 2.4(iii), the ideal $I(C)$ of $K[x_1, \dots, x_g]$ is generated by the polynomials:

$$F_1, \dots, F_d, H_1, \dots, H_r.$$

By scaling the F_i and H_j appropriately, we may assume that these polynomials all have coefficients in $\mathcal{O}_K$.

We define $\mathcal{C}$ to be the closed subscheme of $\mathbb{P}^{g-1}_{\mathcal{O}_K}$ defined by the polynomials $F_1, \dots, F_d, H_1, \dots, H_r$. We have $\mathcal{C}_K = C$ which is isomorphic to X_G since X_G is not geometrically hyperelliptic. For all but finitely many prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$, $\mathcal{C}_{\mathcal{O}_\mathfrak{p}}$ will be a smooth proper curve over $\mathcal{O}_\mathfrak{p}$. Whether this holds for a particular prime ideal $\mathfrak{p}$ can be checked using the Jacobian criterion for smoothness; unfortunately this turns out to be much too slow for our application (which involves canonical models of relatively large genus and hence many equations). The goal of this section is to explain an alternate way to show that $\mathcal{C}_{\mathcal{O}_\mathfrak{p}}$ is a smooth curve over $\mathcal{O}_\mathfrak{p}$.

Lemma 6.3. *Let $\mathfrak{p} \nmid N$ be a nonzero prime ideal of $\mathcal{O}_K$ and let $\mathfrak{P}$ be a nonzero prime ideal of $\mathbb{Z}[\zeta_N] = \mathcal{O}_{\mathbb{Q}(\zeta_N)}$ that divides $\mathfrak{p}$. Assume that for each $1 \leq i \leq g$, all the coefficients of the q-expansion of f_i are integral at $\mathfrak{P}$ and let $\bar{f}_i \in \mathbb{F}_\mathfrak{P}[\![q_N]\!]$ be the power series obtained by reducing the coefficients of the q-expansion modulo $\mathfrak{P}$. For a polynomial $F \in \mathcal{O}_K[x_1, \dots, x_g]$, let $\overline{F} \in \mathbb{F}_\mathfrak{P}[x_1, \dots, x_g]$ be the polynomial obtained by reducing the coefficients modulo $\mathfrak{P}$.*

Assume that the following hold:

(a) *$\bar{f}_1, \dots, \bar{f}_g$ are linearly independent over $\mathbb{F}_\mathfrak{P}$,*
(b) *$\overline{F}_1, \dots, \overline{F}_d$ is a basis for the $\mathbb{F}_\mathfrak{P}$-vector space consisting of homogeneous polynomials $F \in \mathbb{F}_\mathfrak{P}[x_1, \dots, x_g]$ of degree 2 for which $F(\bar{f}_1, \dots, \bar{f}_g) = 0$.*
(c) *the $\mathbb{F}_\mathfrak{P}$-subspace $\mathcal{W}$ of $\mathbb{F}_\mathfrak{P}[x_1, \dots, x_g]$ spanned by $x_i \overline{F}_j(x_1, \dots, x_g)$, with $1 \leq i \leq g$ and $1 \leq j \leq d$, has dimension $\dim_K W$.*
(d) *$\overline{H}_1, \dots, \overline{H}_r$ are linearly independent over $\mathbb{F}_\mathfrak{P}$ and $\mathcal{W} \cap (\mathbb{F}_\mathfrak{P}\overline{H}_1 + \cdots + \mathbb{F}_\mathfrak{P}\overline{H}_r) = 0$.*

Then $\mathcal{C}_{\mathcal{O}_\mathfrak{p}}$ is a smooth curve over $\mathcal{O}_\mathfrak{p}$.

Proof. We claim that $\mathcal{C}_{\mathbb{F}_\mathfrak{P}} \subseteq \mathbb{P}^{g-1}_{\mathbb{F}_\mathfrak{P}}$ is the image of the canonical map of some nice curve over $\mathbb{F}_\mathfrak{P}$ of genus g that is not geometrically hyperelliptic. To prove the claim we may base extend so that we are in the case where $G \subseteq \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ and hence $K = \mathbb{Q}(\zeta_N)$ and $\mathfrak{p} = \mathfrak{P}$.

After scaling the f_i by suitable elements of $\mathcal{O}_K - \mathfrak{p}$, we may assume without loss of generality that that the q-expansion of each f_i has coefficients in $\mathbb{Z}[\zeta_N]$. By Lemma 4.3(ii) we can view each f_i as an element of $H^0(M_N, \omega^{\otimes 2})$ that is stable under the G-action. By using the isomorphism of Lemma 4.3(ii), we can view each $\bar{f}_i$ as an element of $H^0(M_N, \omega^{\otimes 2}) \otimes_{\mathbb{Z}[\zeta_N, 1/N]} \mathbb{F}_\mathfrak{P} = H^0((M_N)_{\mathbb{F}_\mathfrak{P}}, \omega^{\otimes 2})$ that is stable under the G-action, where $(M_N)_{\mathbb{F}_\mathfrak{P}} = M_N \times_{\mathbb{Z}[\zeta_N, 1/N]} \mathbb{F}_\mathfrak{P}$. Since $f_i \in S_{2,G}$ and M_N^∞ is étale, using (4.2) we can view f_i as an element of $H^0(M_N, \Omega^1_{M_N})$ and $\bar{f}_i$ as an element of $H^0((M_N)_{\mathbb{F}_\mathfrak{P}}, \Omega^1_{(M_N)_{\mathbb{F}_\mathfrak{P}}})$. We have a natural homomorphism

$$\bigoplus_{d=0}^{\infty} H^0(M_N, \Omega_{M_N}^{\otimes d}) \to \bigoplus_{d=0}^{\infty} H^0((M_N)_{\mathbb{F}_\mathfrak{P}}, \Omega_{(M_N)_{\mathbb{F}_\mathfrak{P}}}^{\otimes d})$$

of graded $\mathbb{Z}[\zeta_N, 1/N]$-algebras. Let I be the ideal of $\mathbb{F}_{\mathfrak{P}}[x_1,\dots,x_g]$ generated by homogeneous polynomials F for which $F(\bar{f}_1,\dots,\bar{f}_g)=0$. We have have $\overline{F}_1,\dots,\overline{F}_d \in I_2$ and $\overline{H}_1,\dots,\overline{H}_r \in I_3$.

From §4.4, we have a smooth proper curve $M_G = G\backslash M_N$ over $\mathcal{O}_K[1/N]$ with $(M_G)_K \cong X_G$. Since each $\bar{f}_i$ is an element of $H^0((M_N)_{\mathbb{F}_{\mathfrak{P}}}, \Omega^1_{(M_N)_{\mathbb{F}_{\mathfrak{P}}}})$ stable under the G-action, we can view $\bar{f}_1,\dots,\bar{f}_g$ as elements of $H^0((M_G)_{\mathbb{F}_{\mathfrak{P}}}, \Omega^1_{(M_G)_{\mathbb{F}_{\mathfrak{P}}}})$. Therefore, $\bar{f}_1,\dots,\bar{f}_g$ is a basis of $H^0((M_G)_{\mathbb{F}_{\mathfrak{P}}}, \Omega^1_{(M_G)_{\mathbb{F}_{\mathfrak{P}}}})$ over $\mathbb{F}_{\mathfrak{P}}$ since they are linearly independent by assumption (a) and since X_G, and hence also $(M_G)_{\mathbb{F}_{\mathfrak{P}}}$, has genus g. Let C' be the image of the canonical map

$$\bar{\phi}\colon (M_G)_{\mathbb{F}_{\mathfrak{P}}} \to \mathbb{P}^{g-1}_{\mathbb{F}_{\mathfrak{P}}}$$

arising from the basis $\bar{f}_1,\dots,\bar{f}_d$. The ideal $I(C') \subseteq \mathbb{F}_{\mathfrak{P}}[x_1,\dots,x_g]$ corresponding to $C' \subseteq \mathbb{P}^{g-1}_{\mathbb{F}_{\mathfrak{P}}}$ equals I. By assumption (b), $\overline{F}_1,\dots,\overline{F}_d$ is a basis of $I(C')_2$ over $\mathbb{F}_{\mathfrak{P}}$. Since $d = \binom{g-2}{2}$, Proposition 2.4(ii) implies that $(M_G)_{\mathbb{F}_{\mathfrak{P}}}$ is not geometrically hyperelliptic and is thus isomorphic to C'. By assumption (c), $\dim_{\mathbb{F}_{\mathfrak{P}}} \mathcal{W} = \dim_K W$. We have $\dim_K I(C)_3 = \dim_{\mathbb{F}_{\mathfrak{P}}} I(C')_3$ by Proposition 2.4(i). Therefore, $\dim_{\mathbb{F}_{\mathfrak{P}}} I(C')_3/\mathcal{W} = \dim_K I(C)_3/W = r$. Thus by assumption (d) and $g \geq 4$, $I(C')_3/\mathcal{W}$ has basis $\overline{H}_1,\dots,\overline{H}_r$. By Proposition 2.4(iii), the ideal $I(C')$ is generated by the polynomials $\overline{F}_1,\dots,\overline{F}_d,\overline{H}_1,\dots,\overline{H}_r$. This proves that $\mathcal{C}_{\mathbb{F}_{\mathfrak{P}}} = C'$ and the claim follows; $\mathcal{C}_{\mathbb{F}_{\mathfrak{P}}}$ is the image of the canonical map for the nice curve $(M_G)_{\mathbb{F}_{\mathfrak{P}}}$ of genus g.

We now prove the lemma. The $\mathcal{O}_{\mathfrak{p}}$-scheme $\mathcal{C}_{\mathcal{O}_{\mathfrak{p}}} \subseteq \mathbb{P}^{g-1}_{\mathcal{O}_{\mathfrak{p}}}$ is projective and its generic fiber $C_{K_{\mathfrak{p}}} = \mathcal{C}_{K_{\mathfrak{p}}} \subseteq \mathbb{P}^{g-1}_{K_{\mathfrak{p}}}$ is a nice curve of genus g over $K_{\mathfrak{p}}$ since $C_K \cong X_G$ is not geometrically hyperelliptic. From Proposition 2.4(i), one can show that the Hilbert polynomial of $\mathcal{C}_{K_{\mathfrak{p}}} \subseteq \mathbb{P}^{g-1}_{K_{\mathfrak{p}}}$ is $(2g-2)x-g+1$. From the claim and Proposition 2.4(i), $\mathcal{C}_{\mathbb{F}_{\mathfrak{p}}} \subseteq \mathbb{P}^{g-1}_{\mathbb{F}_{\mathfrak{p}}}$ is a nice curve over $\mathbb{F}_{\mathfrak{p}}$ of genus g whose Hilbert polynomial is $(2g-2)x-g+1$; this can be proved by base changing to $\mathbb{F}_{\mathfrak{P}}$ first. The scheme $\mathcal{C}_{\mathcal{O}_{\mathfrak{p}}}$ is flat over $\mathcal{O}_{\mathfrak{p}}$ by using that the Hilbert polynomials of the fibers agree [GW23, 23.155]. Therefore, $\mathcal{C}_{\mathcal{O}_{\mathfrak{p}}}$ is smooth over $\mathcal{O}_{\mathfrak{p}}$ since the fibers are nice curves [GW23, Corollary 18.57]. We conclude that $\mathcal{C}_{\mathcal{O}_{\mathfrak{p}}}$ is a smooth proper curve over $\mathcal{O}_{\mathfrak{p}}$. □

To apply Lemma 6.3, we will use Proposition 4.4 to ensure that the coefficients of the q-expansions of each f_i is integral at a prime ideal $\mathfrak{P} \nmid N$ of $\mathbb{Z}[\zeta_N]$. The conditions in Lemma 6.3 are straightforward to check assuming enough terms of the q-expansions have been computed. Note that Lemma 6.3 will apply to all but finitely many prime ideals $\mathfrak{p} \nmid N$ of $\mathcal{O}_K$.

6.4. **Genus at least 5 case.** Assume that $g \geq 5$. We may assume that X_G is not geometrically hyperelliptic since we have already dealt with this case.

Suppose that the ideal $I(C)$ is not generated by $I(C)_2$; whether this holds can be checked by §3.6.2 and Proposition 2.4. By Proposition 2.4, $(X_G)_{\overline{K}}$ is trigonal or is isomorphic to a smooth plane quintic. Therefore, X_G is not geometrically bielliptic by Lemma 2.5.

So we may now assume that $I(C)$ is generated by $I(C)_2$. We already have a basis $F_1,\dots,F_d$ of $I(C)_2$ over K. By scaling the F_i, we may further assume that each F_i is an element of $\mathcal{O}_K[x_1,\dots,x_g]$.

We define $\mathcal{C}$ to be the closed subscheme of $\mathbb{P}^{g-1}_{\mathcal{O}_K}$ defined by the polynomials $F_1,\dots,F_d$. We have $\mathcal{C}_K = C$ which is isomorphic to X_G since X_G is not geometrically hyperelliptic. For each $1 \leq i \leq d$, define the polynomial

$$P_i(x_1,\dots,x_g,y_1,\dots,y_g) := F_i(x_1+y_1,\dots,x_g+y_g) - F_i(x_1,\dots,x_g) - F_i(y_1,\dots,y_g)$$

in $\mathcal{O}_K[x_1,\dots,x_g,y_1,\dots,y_g]$. Since F_i is homogeneous of degree 2, we find that the polynomial $P_i(x_1,\dots,x_g,y_1,\dots,y_g)$ is homogeneous of degree 2 in all the variables and also homogeneous of degree 1 in just the variables $(x_1,\dots,x_g)$ (or $(y_1,\dots,y_g)$).

Let $\mathcal{Z}$ be the closed subscheme of $\mathbb{P}^{g-1}_{\mathcal{O}_K} = \operatorname{Proj} \mathcal{O}_K[y_1, \dots, y_g]$ defined by the coefficients of

$$F_i(y_1, \dots, y_g)P_j(x_1, \dots, x_g, y_1, \dots, y_g) - F_j(y_1, \dots, y_g)P_i(x_1, \dots, x_g, y_1, \dots, y_g)$$

when viewed as polynomials over $x_1, \dots, x_g$ as we vary over all $1 \le i < j \le d$; note that the polynomials in $\mathcal{O}_K[y_1, \dots, y_g]$ obtained are all homogeneous. We may view $\mathcal{C}$ and $\mathcal{Z}$ as subschemes of the same $\mathbb{P}^{g-1}_{\mathcal{O}_K}$.

Lemma 6.4.

(i) *There is a bijection between the bielliptic involutions of $\mathcal{C}_{\overline{K}}$ and the set $\mathcal{Z}(\overline{K}) - \mathcal{C}(\overline{K})$. In particular, the curve $\mathcal{C}_K$ is geometrically bielliptic if and only if $\mathcal{Z}(\overline{K}) - \mathcal{C}(\overline{K})$ is nonempty.*

(ii) *Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$ for which $\mathcal{C}_{\mathcal{O}_\mathfrak{p}}$ is a smooth proper curve over $\mathcal{O}_\mathfrak{p}$. If $\mathcal{Z}(\overline{\mathbb{F}}_\mathfrak{p}) - \mathcal{C}(\overline{\mathbb{F}}_\mathfrak{p})$ is empty, then $\mathcal{C}_K$ is not geometrically bielliptic.*

Proof. First consider any bielliptic involution σ of $\mathcal{C}_{\overline{K}}$. By Proposition 2.6(i), there is a unique $a \in \mathbb{P}^{g-1}(\overline{K}) - \mathcal{C}(\overline{K})$ such that the projection

$$\pi \colon \mathbb{P}^{g-1}_{\overline{K}} \dashrightarrow \mathbb{P}^{g-2}_{\overline{K}}$$

centered at a defines a degree 2 morphism from $\mathcal{C}_{\overline{K}}$ to a genus 1 curve that agrees with the quotient map $\mathcal{C}_{\overline{K}} \to \mathcal{C}_{\overline{K}}/\langle\sigma\rangle$ composed with an embedding. Take any $b \in \mathcal{C}(\overline{K})$ except for the finite number of points for which the line ℓ_b between a and b is tangent to $\mathcal{C}_{\overline{K}}$ (equivalently, the points where the degree 2 morphism is ramified). We choose lifts of a and b to $\overline{K}^g - \{0\}$ which we also denote by a and b, respectively. The line ℓ_b intersects $\mathcal{C}_{\overline{K}}$ at exactly two distinct points, so there is a unique $t \in \overline{K} - \{0\}$ for which we have $F_i(ta + b) = 0$ for all $1 \le i \le d$. We have

$$0 = F_i(ta + b) = P_i(ta, b) + F_i(ta) + F_i(b) = tP_i(a, b) + t^2F_i(a) + 0$$

and hence $tF_i(a) + P_i(b, a) = 0$. Since t is nonzero, we have

$$F_i(a)P_j(b, a) - F_j(a)P_i(b, a) = 0 \tag{6.1}$$

for all $1 \le i < j \le d$ and all but finitely many $b \in \mathcal{C}(\overline{K})$. Therefore,

$$F_i(a)P_j(x, a) - F_j(a)P_i(x, a) \tag{6.2}$$

is a polynomial in $\overline{K}[x_1, \dots, x_g]$ that lies in $I(C)_1 \otimes_K \overline{K}$. Since $I(C)_1 = 0$, the coefficients of (6.2) are all 0. This proves that a lies in $\mathcal{Z}(\overline{K})$ and we already have $a \notin \mathcal{C}(\overline{K})$.

We have just described an injective map f from the set of bielliptic involutions of $\mathcal{C}_{\overline{K}}$ to the set $\mathcal{Z}(\overline{K}) - \mathcal{C}(\overline{K})$. Now take any $a \in \mathcal{Z}(\overline{K}) - \mathcal{C}(\overline{K})$. Since $a \notin \mathcal{C}(\overline{K})$, there is a $1 \le j \le d$ such that $F_j(a) \ne 0$. Take any $b \in \mathcal{C}(\overline{K})$. We choose lifts of a and b to $\overline{K}^g - \{0\}$ which we also denote by a and b, respectively. By excluding finitely many b, we shall further assume that $P_j(b, a) \ne 0$. Define $t = -P_j(b, a)/F_j(a) \in \overline{K} - \{0\}$. The equation (6.1) holds for all $1 \le i \le d$ since a lies in $\mathcal{Z}(\overline{K})$. Therefore, t is the unique value for which $tF_i(a) + P_i(b, a) = 0$ holds for all i. Like above, we have $F_i(ta + b) = tP_i(a, b) + t^2F_i(a)$ and hence $F_i(ta + b) = 0$ for all i. We deduce that the line ℓ_b in $\mathbb{P}^{g-1}_{\overline{K}}$ through a and b intersects $\mathcal{C}_{\overline{K}}$ at precisely two points. So projection from a defines a morphism $\mathcal{C}_{\overline{K}} \to \mathbb{P}^{g-2}_{\overline{K}}$ which gives a degree 2 morphism $\pi \colon \mathcal{C}_{\overline{K}} \to C'$ for a curve C' over $\overline{K}$. By Proposition 2.6(ii), C' has genus 1. We have $f(\sigma) = a$, where σ is the involution of $\mathcal{C}_{\overline{K}}$ arising from π. This proves that f is a bijection which proves (i).

We will now prove (ii). Assume that $\mathcal{C}_{\mathcal{O}_\mathfrak{p}}$ is a smooth proper curve over $\mathcal{O}_\mathfrak{p}$. The curve $\mathcal{C}_{\mathbb{F}_\mathfrak{p}} \subseteq \mathbb{P}^{g-1}_{\mathbb{F}_\mathfrak{p}}$ is smooth, has genus g and degree $2g-2$, and is hence a canonical curve. Suppose that $\mathcal{C}_K$ is geometrically bielliptic. Using Proposition 2.8, one can show that $\mathcal{C}_{\mathbb{F}_\mathfrak{p}}$ is geometrically bielliptic. By Proposition 2.6(i), there is an $a \in \mathbb{P}^{g-1}(\overline{\mathbb{F}}_\mathfrak{p}) - \mathcal{C}(\overline{\mathbb{F}}_\mathfrak{p})$ such that the projection $\mathbb{P}^{g-1}_{\overline{\mathbb{F}}_\mathfrak{p}} \dashrightarrow \mathbb{P}^{g-2}_{\overline{\mathbb{F}}_\mathfrak{p}}$ centered at a defines a degree 2 morphism from $\mathcal{C}_{\overline{\mathbb{F}}_\mathfrak{p}}$ to a genus 1 curve. An identical argument

as above shows that a lies in $\mathcal{Z}(\overline{\mathbb{F}}_\mathfrak{p}) - \mathcal{C}(\overline{\mathbb{F}}_\mathfrak{p})$. So if $\mathcal{Z}(\overline{\mathbb{F}}_\mathfrak{p}) - \mathcal{C}(\overline{\mathbb{F}}_\mathfrak{p})$ is empty, then $\mathcal{C}_K$ cannot be geometrically bielliptic. □

The set $\mathcal{Z}(\overline{K}) - \mathcal{C}(\overline{K})$ is finite by Lemma 6.4(i) since a curve of genus at least 2 has only finitely many automorphisms. Moreover, Lemma 6.4(i) implies that $C = \mathcal{C}_K$ is geometrically bielliptic if and only if $\mathcal{Z}(\overline{K}) - \mathcal{C}(\overline{K})$ is nonempty. Since the set $\mathcal{Z}(\overline{K}) - \mathcal{C}(\overline{K})$ is finite, the quasiprojective variety $W := \mathcal{Z}_K - \mathcal{C}_K$ is closed and is either empty or has dimension 0.

We proceed by considering several nonzero prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ for which $\mathcal{C}_{\mathcal{O}_\mathfrak{p}}$ is a smooth proper curve over $\mathcal{O}_\mathfrak{p}$. Such primes can be found by making use of the approach from §6.3. Define the quasiprojective variety

$$W_\mathfrak{p} := \mathcal{Z}_{\mathbb{F}_\mathfrak{p}} - \mathcal{C}_{\mathbb{F}_\mathfrak{p}} \subseteq \mathbb{P}^{g-1}_{\mathbb{F}_\mathfrak{p}}.$$

If $W_\mathfrak{p}$ is empty, then Lemma 6.4(ii) implies that C is not geometrically bielliptic.

Suppose that $W_\mathfrak{p}$ is nonempty. Since $\mathcal{Z}(\overline{K}) - \mathcal{C}(\overline{K})$ is finite, we may assume that $W_\mathfrak{p}$ is a closed subvariety of dimension 0 by excluding a finite number of $\mathfrak{p}$. Consider one of the finitely many closed points of $W_\mathfrak{p}$; it gives a point $a \in W_\mathfrak{p}(\mathbb{F})$ for some finite extension $\mathbb{F}$ of $\mathbb{F}_\mathfrak{p}$. We have $a \in \mathcal{Z}(\mathbb{F})$ and $a \notin \mathcal{C}(\mathbb{F})$. There is a finite extension of $K_\mathfrak{p}$ whose ring of integers R has residue field $\mathbb{F}$; the ring R is Henselian. Using the defining equations for $\mathcal{Z}$, we can then check if a lifts uniquely to a point a' in $\mathcal{Z}(R)$; note that we do not need to compute a'. Now suppose we have proved the existence of a point $a' \in \mathcal{Z}(R)$ as above; we have $a' \notin \mathcal{C}(R)$ since $a \notin \mathcal{C}(\mathbb{F})$. We thus have a point a' in W and hence a' can be defined over $\overline{K}$ since W has dimension at most 0. Therefore, $\mathcal{Z}(\overline{K}) - \mathcal{C}(\overline{K})$ is nonempty and $C = \mathcal{C}_K$ is geometrically bielliptic.

By considering more and more nonzero prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$, this process will eventually determined if C is geometrically bielliptic or not. We could also try to check if $\mathcal{Z}(\overline{K}) - \mathcal{C}(\overline{K})$ is nonempty directly but the computations are significantly faster over finite fields. When $g \geq 6$, Theorem 2.2 implies that $C_{\overline{K}}$ has at most 1 bielliptic involution and hence W is empty or consists of a single point.

6.5. **Genus 4 case.** Assume that $g = 4$. We may assume that X_G is not geometrically hyperelliptic since we have already dealt with this case. By Proposition 2.1(iii), we deduce that X_G has geometric gonality 3.

We can compute a basis of $I(C)_2$ over K which by Proposition 2.4(ii) consists of a single polynomial $F \in K[x_1, \dots, x_4]_2$. By Proposition 2.4(iii) and (iv), there is a single polynomial $H \in K[x_1, \dots, x_4]_3$ such that the ideal $I(C)$ is generated by F and H. By scaling F and H, we may assume that they have coefficients in $\mathcal{O}_K$. We define $\mathcal{C}$ to be the closed subscheme of $\mathbb{P}^{g-1}_{\mathcal{O}_K}$ defined by the polynomials F and H. We have $\mathcal{C}_K = C$ which is isomorphic to X_G since X_G is not geometrically hyperelliptic.

With $x = (x_1, \dots, x_4)$ and $y = (y_1, \dots, y_4)$, we have polynomials $P, Q, R \in \mathcal{O}_K[x_1, \dots, x_4, y_1, \dots, y_4]$ such that

$$F(x+y) = F(x) + P(x,y) + F(y) \quad \text{and} \quad H(x+y) = H(x) + Q(x,y) + R(x,y) + H(y),$$

where $Q(x,y)$ and $R(x,y)$ are homogeneous polynomials of degree 3 that are homogeneous of degree 2 and 1, respectively, in just the variables $x_1, \dots, x_4$. The polynomial $P(x,y)$ is homogeneous of degree 2 and homogeneous of degree 1 in just the variables $x_1, \dots, x_4$.

Lemma 6.5. *Let L be the field K or a field $\mathbb{F}_\mathfrak{p}$ where $\mathfrak{p}$ is a nonzero prime ideal $\mathfrak{p}$ for which $\mathcal{C}_{\mathcal{O}_\mathfrak{p}}$ is a smooth proper curve over $\mathcal{O}_\mathfrak{p}$. Take any point $\overline{a} \in \mathbb{P}^{g-1}(\overline{L}) - \mathcal{C}(\overline{L})$ and choose a representative $a \in \overline{L}^g - \{0\}$. Let*

$$\phi\colon \mathcal{C}_{\overline{L}} \to \mathbb{P}^{g-2}_{\overline{L}}$$

be the projection from the point $\overline{a}$.

(i) *Suppose that* $F(a) \neq 0$. *Then* ϕ *has degree* 2 *if and only if* $P(x,a) \neq 0$ *and*

$$P(x,a)^2H(a) - P(x,a)F(a)R(x,a) + F(a)^2Q(x,a)$$

is a scalar multiple of F *in* $\bar{L}[x_1,\dots,x_4]$. *If* ϕ *has degree* 2, *then* ϕ *is ramified exactly at the points in* $\mathcal{C}_{\bar{L}}$ *for which* $P(x,a)$ *vanishes.*

(ii) *Suppose that* $F(a) = 0$, *that* $H(a) \neq 0$ *and that* $Q(x,a)$ *is not a scalar multiple of* F *in* $\bar{L}[x_1,\dots,x_4]$. *Then* ϕ *has degree* 2 *if and only if* $P(x,a) = 0$ *and*

$$R(x,a)^2 - 4H(a)Q(x,a)$$

is a scalar multiple of F.

(iii) *Suppose that* $F(a) = 0$, *that* $H(a) \neq 0$ *and that* $Q(x,a)$ *is a scalar multiple of* F *in* $\bar{L}[x_1,\dots,x_4]$. *Then* ϕ *has degree* 2 *if and only if* $P(x,a) = 0$ *and* $R(x,a) \neq 0$.

Proof. When $L = \mathbb{F}_\mathfrak{p}$, $\mathcal{C}_{\mathbb{F}_\mathfrak{p}} \subseteq \mathbb{P}^{g-1}_{\mathbb{F}_\mathfrak{p}}$ is a nice curve of genus g and degree $2g-2$, and is hence a canonical curve. Thus for the ideal I of $\mathcal{C}_{\bar{L}}$, $I_1 = 0$ and I_2 is generated by the image of F. Since $\mathcal{C}_{\bar{L}}$ is a canonical curve, the morphism ϕ is nonconstant.

Take any $\bar{b} \in \mathcal{C}(\bar{L})$ except for the finite number of points for which the line $\ell_{\bar{b}}$ between $\bar{a}$ and $\bar{b}$ is tangent to $\bar{b}$ in $\mathcal{C}_{\bar{L}}$. Choose a lift of $b \in \bar{L}^{g-1} - \{0\}$ of $\bar{b}$. For $t \in \bar{L}$, we have $F(b+ta) = F(b) + tP(b,a) + t^2F(a) = tP(b,a) + t^2F(a)$ and $H(b+ta) = H(b) + tQ(b,a) + t^2R(b,a) + t^3H(a) = tQ(b,a) + t^2R(b,a) + t^3H(a)$. The line $\ell_{\bar{b}}$ intersects $\mathcal{C}_{\bar{L}}$ at a point that is not $\bar{b}$ if and only if there a $t \in \bar{L} - \{0\}$ with $F(b+ta) = 0$ and $H(b+ta) = 0$; equivalently, we have a $t \in \bar{L} - \{0\}$ such that

$$tF(a) + P(b,a) = 0 \tag{6.3}$$

and

$$t^2H(a) + tR(b,a) + Q(b,a) = 0. \tag{6.4}$$

Suppose that $F(a) \neq 0$. Then $\ell_{\bar{b}}$ intersects $\mathcal{C}_{\bar{L}}$ at a point that is not $\bar{b}$ if and only if $P(b,a) \neq 0$ and $P(b,a)^2H(a) - F(a)P(b,a)R(b,a) + F(a)^2Q(b,a) = 0$ (solve for t in (6.3) and then substitute into (6.4)). In particular, this implies that $\phi^{-1}(\bar{b})$ has cardinality at most 2 for all but finitely many $\bar{b} \in \mathcal{C}(\bar{L})$ and hence has degree at most 2. The morphism ϕ has degree 2 if and only if $P(x,a) \notin I_1$ and $P(x,a)^2H(a) - F(a)P(x,a)R(x,a) + F(a)^2Q(x,a) \in I_2$. When ϕ has degree 2, from the above computations we find that the points in $\mathcal{C}_{\bar{L}}$ for which ϕ is ramified are precisely those for which the linear equation $P(x,a)$ vanishes.

We shall now assume that $F(a) = 0$. We must have $H(a) \neq 0$ since a is not in $\mathcal{C}_{\bar{L}}$. For ϕ to have degree greater than 1, we need $P(x,a) \in I_1$ by (6.3). So we may assume that $P(x,a) = 0$ since $I_1 = 0$.

Suppose that $Q(x,a) \notin I_2$. So for all but finitely many $\bar{b} \in \mathcal{C}(\bar{L})$, we have $Q(b,a) \neq 0$ and hence $t = 0$ is not a root of (6.4). Therefore, ϕ is a morphism of degree 2 if and only if $R(x,a)^2 - H(a)Q(x,a)$ is in I_2 (this is needed so that (6.4) has one repeated root as a polynomial in t).

Suppose that $Q(x,a) \in I_2$. Then (6.4) has two roots $t = 0$ and $t = -R(b,a)/H(a)$. Therefore, ϕ is a morphism of degree 2 if and only if $R(x,a) \notin I_1$.

The lemma is now immediate since $I_1 = 0$ and I_2 is spanned by F. □

Consider a fixed prime ideal $\mathfrak{p} \nmid N$ of $\mathcal{O}_K$ for which $\mathcal{C}_{\mathcal{O}_\mathfrak{p}}$ is a smooth proper curve over $\mathcal{O}_\mathfrak{p}$. Such primes can be found by making use of the approach from §6.3.

With $L = \mathbb{F}_\mathfrak{p}$, we can then determine whether there is an $a \in \overline{\mathbb{F}}^g_\mathfrak{p} - \{0\}$ for which projection by its image $\bar{a} \in \mathbb{P}^{g-1}(\overline{\mathbb{F}}_\mathfrak{p})$ defines a degree 2 morphism

$$\phi\colon \mathcal{C}_{\overline{\mathbb{F}}_\mathfrak{p}} \to \mathbb{P}^{g-2}_{\mathbb{F}_\mathfrak{p}}$$

and $\overline{a} \notin \mathcal{C}(\overline{\mathbb{F}}_{\mathfrak{p}})$. Indeed, we need only check the three cases of Lemma 6.5. For the three cases of Lemma 6.5, the condition for ϕ to have degree 2 is equivalent to $\overline{a}$ being the $\overline{\mathbb{F}}_{\mathfrak{p}}$-point of a certain $\mathcal{O}_K$-scheme $\mathcal{Z}_1$, $\mathcal{Z}_2$ and $\mathcal{Z}_3$, respectively, that do not depend on $\mathfrak{p}$.

First suppose that we find that $(\mathcal{Z}_i)_{\mathbb{F}_{\mathfrak{p}}}$ is empty for all $1 \le i \le 3$. Then there is no projection from a point $\overline{a} \in \mathbb{P}^{g-1}(\overline{\mathbb{F}}_{\mathfrak{p}}) - \mathcal{C}(\overline{\mathbb{F}}_{\mathfrak{p}})$ that defines a degree 2 morphism of $\mathcal{C}_{\overline{\mathbb{F}}_{\mathfrak{p}}}$. Since $\mathcal{C}_{\overline{\mathbb{F}}_{\mathfrak{p}}} \subseteq \mathbb{P}^{g-1}_{\overline{\mathbb{F}}_{\mathfrak{p}}}$ is a canonical curve, Proposition 2.6(i) implies that $\mathcal{C}_{\overline{\mathbb{F}}_{\mathfrak{p}}}$ is not bielliptic. So $\mathcal{C}_{\mathbb{F}_{\mathfrak{p}}}$ is not geometrically bielliptic and hence $C = \mathcal{C}_K$ is not geometrically bielliptic by Proposition 2.8(ii). We deduce that $X_G \widetilde{=} C$ is not geometrically bielliptic.

Suppose that $(\mathcal{Z}_1)_{\mathbb{F}_{\mathfrak{p}}}$ is nonempty. There is a point $\overline{a} \in \mathcal{Z}_1(\mathbb{F})$ for some finite extension $\mathbb{F} \subseteq \overline{\mathbb{F}}_{\mathfrak{p}}$ of $\mathbb{F}_{\mathfrak{p}}$. Choose a lift $a \in \mathbb{F}^{g-1} - \{0\}$. There is a finite extension L of $K_{\mathfrak{p}}$ whose ring of integers R has residue field $\mathbb{F}$; the ring R is Henselian. Using the defining equations for $\mathcal{Z}_1$, we can then check if $\overline{a}$ lifts uniquely to a point a' in $\mathcal{Z}(R)$; note that we do not need to compute a'. Now suppose further that the hyperplane $P(x, a) = 0$ intersects $\mathcal{C}_{\mathbb{F}_{\mathfrak{p}}}$ at 6 distinct points (this is the generic behavior since $\mathcal{C}_{\mathbb{F}_{\mathfrak{p}}}$ has degree $2g-2 = 6$). Suppose that the Hensel lift a' exists and that moreover the 6 points above lift unique to points in $\mathcal{C}(R)$ that lie in the hyperplane $P(x, a') = 0$. Using Proposition 6.5(i), we find that the projection $\phi\colon \mathcal{C}_{\bar{L}} \to \mathbb{P}^{g-1}_{\bar{L}}$ from a' defines a morphism of degree 2 for which at least 6 points ramify. Since $\mathcal{C}_{\bar{L}} \widetilde{=} (X_G)_{\bar{L}}$ is not hyperelliptic, the Riemann–Hurwitz formula implies that $\phi(\mathcal{C}_{\bar{L}})$ has genus 1 and hence $\mathcal{C}_{\bar{L}}$ is bielliptic. Therefore, X_G is geometrically bielliptic.

If $(\mathcal{Z}_2)_{\mathbb{F}_{\mathfrak{p}}}$ or $(\mathcal{Z}_3)_{\mathbb{F}_{\mathfrak{p}}}$ are nonempty, then there are similar arguments to lift their points and see if it proves that X_G is geometrically bielliptic. We do not the give the details since they are similar and since these cases never arose in our actual computations!

By considering enough primes $\mathfrak{p} \nmid N$, the above arguments will sufficient to determine whether X_G is geometrically bielliptic (this can be deduced from Proposition 2.6(i) and Lemma 6.5).

7. Classieication for congruence subgroups of genus at most 24

In the section, we proof the classification of Theorem 1.1 when restricted to congruence subgroups of genus at most 24. In particular, we verify all of Table 1.1 except for the last column. `Magma` code for this process can be found in [Zyw25].

Cummins and Pauli [CP03] have given a complete classification of all congruence subgroups Γ of $\mathrm{SL}_2(\mathbb{Z})$ with $-I \in \Gamma$, up to conjugacy in $\mathrm{GL}_2(\mathbb{Z})$, for which X_Γ has genus at most 24. Note that the isomorphism class of the curve X_Γ does not change if we replace Γ by a conjugate in $\mathrm{GL}_2(\mathbb{Z})$.

There is a slight difference between conjugacy in $\mathrm{GL}_2(\mathbb{Z})$ and $\mathrm{SL}_2(\mathbb{Z})$ that needs to be taken into account for the values in Theorem 1.1 and Table 1.1. Define $A = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$; it is a representative of the nonidentity coset $\mathrm{GL}_2(\mathbb{Z})/\mathrm{SL}_2(\mathbb{Z})$. If Γ and $A\Gamma A^{-1}$ are conjugate in $\mathrm{SL}_2(\mathbb{Z})$, then the congruence subgroups conjugate to Γ in $\mathrm{SL}_2(\mathbb{Z})$ and $\mathrm{GL}_2(\mathbb{Z})$ agree. If Γ and $A\Gamma A^{-1}$ are not conjugate in $\mathrm{SL}_2(\mathbb{Z})$, then a congruence subgroup conjugate to Γ in $\mathrm{GL}_2(\mathbb{Z})$ is conjugate to either Γ or $A\Gamma A^{-1}$ in $\mathrm{SL}_2(\mathbb{Z})$.

We now fix one of the finitely many congruence subgroups Γ of $\mathrm{SL}_2(\mathbb{Z})$ containing $-I$ that are in the Cummins–Pauli classification. Let $\mathscr{C}_\Gamma$ be the finite set of congruence subgroups Γ' for which $\Gamma \subsetneq \Gamma' \subseteq \mathrm{SL}_2(\mathbb{Z})$. Let g be the genus of X_Γ, D the index of Γ in $\mathrm{SL}_2(\mathbb{Z})$, and N the level of Γ.

We can deal with the congruence subgroups ordered by increasing index in $\mathrm{SL}_2(\mathbb{Z})$. In particular, for a group $\Gamma' \in \mathscr{C}_\Gamma$ we will know if the gonality of $X_{\Gamma'}$ is 1, 2, 3 or at least 4; we will also know whether or not $X_{\Gamma'}$ is bielliptic.

The curve X_Γ has gonality 1 if and only if $g = 0$. If $g = 0$, then X_Γ is not bielliptic. If $g = 1$, then X_Γ has gonality 2 and it is bielliptic. So we need only consider the cases where $g \ge 2$.

7.1. **Choice of models.** For some Γ, we will need to choose a model of X_Γ defined over a number field. We can choose a subgroup $G \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ with $[\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : G]$ minimal for which $G \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ agrees with Γ modulo N. The modular curve X_G is defined over the number field $K_G = \mathbb{Q}(\zeta_N)^{\det(G)}$. Recall that $(X_G)_{\mathbb{C}}$ and X_Γ are isomorphic curves over $\mathbb{C}$. The reason for taking $[\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : G]$ minimal is so that K_G has relative small degree. For the groups G we will need to consider throughout §7, $[K_G : \mathbb{Q}]$ turns out to be a power of 2 that is at most 16.

7.2. **Gonality 2 classification.** We now determine whether X_Γ has gonality 2. The curve X_Γ has gonality 2 when $g = 2$ so we may assume that $g \geq 3$. If X_Γ has gonality 2, then Corollary 5.2(i), implies that $D \leq 201$ and that $D \leq 191$ when $N \leq 226$.

So we need only consider the cases where $D \leq 201$ or $D \leq 191$ when $N \leq 226$. By Theorem 5.4(i), we may assume further that $D \leq 24(p^2+1)/(p-1)$ for all primes $p \nmid N$ since otherwise X_Γ does not have gonality 2. We may assume that $X_{\Gamma'}$ has gonality at most 2 for all $\Gamma' \in \mathcal{C}_\Gamma$ since otherwise X_Γ does not have gonality 2 by Proposition 2.1(iv).

If there is a $\Gamma' \in \mathcal{C}_\Gamma$ for which $[\Gamma' : \Gamma] = 2$ and $X_{\Gamma'}$ has genus 0, then the morphism $X_\Gamma \to X_{\Gamma'}$ implies that X_Γ has gonality 2; we may thus assume that no such Γ' exists. Take any $\Gamma' \in \mathcal{C}_\Gamma$. If X_Γ has gonality 2, then the Castelnuovo–Severi inequality (Theorem 2.2), with the hyperelliptic map of X_Γ and the morphism $X_\Gamma \to X_{\Gamma'}$, gives

$$g \leq [\Gamma' : \Gamma]g' + ([\Gamma' : \Gamma] - 1), \tag{7.1}$$

where g' is the genus of $X_{\Gamma'}$. So we may assume that (7.1) holds for all $\Gamma' \in \mathcal{C}_\Gamma$ since otherwise X_Γ does not have gonality 2.

Finally if the above methods are inconclusive, we can determine if X_Γ has gonality 2 by applying the methods of §3.6.1 to X_G with a group G as in §7.1. In our computation, we needed to use this direct approach 455 times.

7.3. **Gonality 3 classification.** We now determine whether X_Γ has gonality 3. Using §7.2, we may assume that X_Γ has gonality at least 3. If X_Γ has gonality 3, then Corollary 5.2(ii), implies that $D \leq 302$ and that $D \leq 287$ when $N \leq 226$.

So we need only consider the case where $D \leq 302$ or $D \leq 287$ when $N \leq 226$. By Theorem 5.4(ii), if $g \geq 5$, then we may assume further that $D \leq 36(p^2+1)/(p-1)$ for all primes $p \nmid N$ since otherwise X_Γ does not have gonality 3. We may assume that $X_{\Gamma'}$ has gonality at most 3 for all $\Gamma' \in \mathcal{C}_\Gamma$ since otherwise X_Γ does not have gonality 3 by Proposition 2.1(iv).

If there is a $\Gamma' \in \mathcal{C}_\Gamma$ for which $[\Gamma' : \Gamma] = 3$ and $X_{\Gamma'}$ has genus 0, then the morphism $X_\Gamma \to X_{\Gamma'}$ implies that X_Γ has gonality 3; we may thus assume that no such Γ' exists. Take any $\Gamma' \in \mathcal{C}_\Gamma$. If X_Γ has gonality 3, then the Castelnuovo–Severi inequality (Theorem 2.2), with the hyperelliptic map of X_Γ and the morphism $X_\Gamma \to X_{\Gamma'}$, gives

$$g \leq [\Gamma' : \Gamma]g' + 2([\Gamma' : \Gamma] - 1), \tag{7.2}$$

where g' is the genus of $X_{\Gamma'}$. So we may assume that (7.2) holds for all $\Gamma' \in \mathcal{C}_\Gamma$ since otherwise X_Γ does not have gonality 3.

Finally if the above methods are inconclusive, we can determine if X_Γ has gonality 3 by applying the methods of §3.6.2 to X_G with a group G as in §7.1. In our computation, we needed to use this direct approach 988 times.

7.4. **Bielliptic classification.** We now determine whether X_Γ is bielliptic.

If X_Γ is bielliptic, then X_Γ has gonality at most 4. By Corollary 5.2 we may assume that $D \leq 403$ and that $D \leq 383$ when $N \leq 226$ since otherwise X_Γ has gonality at least 5. By Theorem 5.4(iii), if $g \geq 6$, then we may assume further that $D \leq 24(p^2+2p+1)/(p-1)$ for all primes $p \nmid N$ since otherwise X_Γ is not bielliptic.

For any $\Gamma' \in \mathscr{C}_\Gamma$, we have a morphism $X_\Gamma \to X_{\Gamma'}$. So if X_Γ is bielliptic, then $X_{\Gamma'}$ has gonality at most 2 or is bielliptic for all $\Gamma' \in \mathscr{C}_\Gamma$ by Lemma 2.5(iii). We can thus assume that $X_{\Gamma'}$ has gonality at most 2 or is bielliptic for all $\Gamma' \in \mathscr{C}_\Gamma$.

If there is a $\Gamma' \in \mathscr{C}_\Gamma$ for which $[\Gamma' : \Gamma] = 2$ and $X_{\Gamma'}$ has genus 1, then the morphism $X_\Gamma \to X_{\Gamma'}$ implies that X_Γ is bielliptic; we may thus assume that no such Γ' exists. Take any $\Gamma' \in \mathscr{C}_\Gamma$. If X_Γ is bielliptic, then the Castelnuovo–Severi inequality (Theorem 2.2), with a bielliptic map of X_Γ and the morphism $X_\Gamma \to X_{\Gamma'}$, gives

$$g \le [\Gamma' : \Gamma]g' + 2 + ([\Gamma' : \Gamma] - 1), \tag{7.3}$$

where g' is the genus of $X_{\Gamma'}$. So we may assume that (7.3) holds for all $\Gamma' \in \mathscr{C}_\Gamma$ since otherwise X_Γ is not bielliptic.

Finally if the above methods are inconclusive, we can determine if X_Γ is bielliptic by applying the methods of §6 to X_G with a group G as in §7.1. In our computation, we needed to use this direct approach 1324 times.

8. Proof of Theorem 1.1

In §7, we proved the part of the classification in Theorem 1.1 that concerns congruences subgroups Γ for which X_Γ has genus at most 24. This constraint on the genus arises from our use of the classification of low genus congruence subgroups due to Cummins and Pauli [CP03].

Suppose that there is a congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ containing $-I$ for which X_Γ has genus $g \ge 25$ and X_Γ has gonality at most 3 or is bielliptic. To complete the classification, we need to obtain a contradiction. We may assume that our Γ was chosen with $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$ minimal. Let N be the level of Γ and let D be the index of Γ in $\mathrm{SL}_2(\mathbb{Z})$.

Let N_1 be the largest power of 2 that divides N and define $N_2 := N/N_1$. For each $i \in \{1, 2\}$, let $H_i \subseteq \mathrm{SL}_2(\mathbb{Z}/N_i\mathbb{Z})$ be the image of Γ modulo N_i. Let Γ_i be the congruence subgroup consisting of matrices in $\mathrm{SL}_2(\mathbb{Z})$ whose image modulo N_i lies in H_i. Let M_i be the level of Γ_i; it divides N_i.

Lemma 8.1. *Assume that N is even.*

(i) *We have $D = m[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_2]$ for some integer m of the form 2^e or 2^e3 with $e \ge 0$.*
(ii) *Every prime $p > 3$ that divides N also divides M_2.*
(iii) *Suppose $3 \nmid M_2$. The integer D is divisible by $6 \cdot [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_2]$. The index of the image of Γ modulo 6 in $\mathrm{SL}_2(\mathbb{Z}/6\mathbb{Z})$ is divisible by 6 and the image of Γ modulo 2 is not $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$.*
(iv) *If $D = 3[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_2]$, then Γ_1 has level 2 and $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_1] = 3$.*

Proof. Let $H \subseteq \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ be the image of Γ modulo N. We have a natural injective homomorphism $H \hookrightarrow H_1 \times H_2$, that we can view as an inclusion, such that the projection maps $p_i \colon H \to H_i$ are surjective. Let B_1 and B_2 be the normal subgroups of H_1 and H_2, respectively, for which $\ker(p_2) = B_1 \times \{1\}$ and $\ker(p_1) = \{1\} \times B_2$. In particular, we may view $B_1 \times B_2$ as a subgroup of H. By Goursat's lemma [Rib76, Lemma 5.2.1], the image of H in $(H_1 \times H_2)/(B_1 \times B_2) = H_1/B_1 \times H_2/B_2$ is the graph of an isomorphism $H_1/B_1 \xrightarrow{\sim} H_2/B_2$. We can view $H/(B_1 \times B_2)$ as an index $|H_1/B_1|$ subgroup of $(H_1 \times H_2)/(B_1 \times B_2)$ and hence $|H| = |H_1||H_2|/|H_1/B_1| = |B_1||H_2|$. Therefore, $D = [\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) : H] = [\mathrm{SL}_2(\mathbb{Z}/N_1\mathbb{Z}) : B_1][\mathrm{SL}_2(\mathbb{Z}/N_2\mathbb{Z}) : H_2]$ and hence

$$D = [\mathrm{SL}_2(\mathbb{Z}/N_1\mathbb{Z}) : B_1] \cdot [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_2]. \tag{8.1}$$

This proves (i) since $|\mathrm{SL}_2(\mathbb{Z}/N_1\mathbb{Z})| = 2^e3$ for some $e \ge 1$. The group H_1 is solvable since $\mathrm{SL}_2(\mathbb{Z}/2^m\mathbb{Z})$ is solvable for all $m \ge 1$. Therefore, $H_2/B_2 \cong H_1/B_1$ is solvable.

Consider any odd prime p that divides N but does not M_2. Let $p^e > 1$ the largest power of p that divides N_2 and define $N_2' := N_2/p^e$. Since $p \nmid M_2$, we have $H_2 = H_2' \times \mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})$ with a subgroup $H_2' \subseteq \mathrm{SL}_2(\mathbb{Z}/N_2'\mathbb{Z})$. From our description of H from Goursat's lemma and from Γ having level N, we obtain a nontrivial homomorphism

$$\varphi \colon \mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z}) \xrightarrow{\sim} \{I\} \times \mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z}) \subseteq H_2 \to H_2/B_2 \xrightarrow{\sim} H_1/B_1.$$

Suppose that $p > 3$ and hence the group $\mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})$ is equal to its own commutator subgroup, cf. [Zyw10, Lemma A.1]. So $\varphi(\mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z}))$ is a nontrivial subgroup of H_1/B_1 that is equal to its own commutator subgroup which contradicts that H_1/B_1 is solvable. This proves (ii). We now have $p = 3$ and $3 \nmid M_3$. The maximal abelian quotient of $\mathrm{SL}_2(\mathbb{Z}/3^e\mathbb{Z})$ is cyclic of order 3, cf. [Zyw10, Lemma A.1]. Since φ is nontrivial and H_1/B_1 is solvable, we deduce that H_1/B_1 has a normal subgroup of index 3. Let W_1 be the image of H_1 modulo 2. The kernel of the reduction modulo 2 homomorphism $H_1 \to W_1$ is a 2-group and hence W_1 contains a normal subgroup of index 3. Since $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3$, this implies that W_1 is the unique subgroup of $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ of order 3. Since H_1/B_1 has order divisible by 3, this implies that B_1 has trivial image modulo 2. We thus have a surjective homomorphism

$$\tilde{\varphi}\colon \mathrm{SL}_2(\mathbb{Z}/3^e\mathbb{Z}) \xrightarrow{\varphi} H_1/B_1 \to W_1$$

obtained by composing φ with reduction modulo 2. The maximal abelian quotient of $\mathrm{SL}_2(\mathbb{Z}/3^e\mathbb{Z})$ is cyclic of order 3 and factors through $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$, cf. [Zyw10, Lemma A.1], and hence $\tilde{\varphi}$ factors through a surjective homomorphism $\tilde{\varphi}'\colon \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z}) \to W_1$. From our description of H in terms of Goursat's lemma, we find that the image of H modulo 6 lies in the group

$$\{(A_1, A_2) \in \mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z}) : \tilde{\varphi}'(A_2) = A_1\},$$

where we have made an identification $\mathrm{SL}_2(\mathbb{Z}/6\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$. This proves that the image of H modulo 6 lies in an index 6 subgroup of $\mathrm{SL}_2(\mathbb{Z}/6\mathbb{Z})$ and that the image of H modulo 2 is not $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$. Since B_1 is the trivial group modulo 2, (8.1) implies that $|\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})|[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_2] = 6[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_2]$ divides D. This completes the proof of (iii).

We will now prove (iv). Suppose that $D = 3[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_2]$. By (8.1), we have $[\mathrm{SL}_2(\mathbb{Z}/N_1\mathbb{Z}) : B_1] = 3$. This implies that the image of B_1 in $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ has order 2 and that B_1 contains all $A \in \mathrm{SL}_2(\mathbb{Z}/N_1\mathbb{Z})$ with $A \equiv I \pmod 2$. Since B_1 is a normal subgroup of H_1, we find that H_1 modulo 2 equals B_1 modulo 2 (since $\mathrm{SL}_2(\mathbb{Z}/N_1\mathbb{Z})$ does not have a normal subgroup of index 3 by [Zyw10, Lemma A.1]). From these properties, we deduce that Γ_1 has level 2 and that its image modulo 2 has cardinality 2. This proves (iv). □

8.1. **Gonality 1 and 2 cases.** We know that X_Γ does not have gonality 1 since $g \geq 25 > 0$.

Suppose that X_Γ has gonality 2. Corollary 5.2(i) implies that $D \leq 201$. Equation (3.1) implies that $g \leq 1 + D/12 \leq 1 + 201/12 < 18$. Since $g \geq 25$, we deduce that X_Γ does not have gonality 2.

8.2. **Gonality 3 case.** Suppose that X_Γ has gonality 3.

Lemma 8.2. *We have* $294 \leq D \leq 302$, $N \equiv 0 \pmod{30}$, *and* $g = 25$.

Proof. We have $D \leq 302$ by Corollary 5.2(ii). Since X_Γ has a cusp, (3.1) implies that $g \leq 1 + D/12 - 1/2 \leq 1 + 302/12 - 1/2 < 26$. We have $g = 25$ since $g \geq 25$ by assumption. We have $D \geq 294$ since otherwise (3.1) implies that $g \leq 1 + 293/12 - 1/2 < 25$. The integer N is divisible by every prime $p \leq 5$ since otherwise $D \leq 36(p^2+1)/(p-1) < 294$ by Theorem 5.4(ii). Therefore, N is divisible by 30. □

By Lemma 8.1(ii) and Lemma 8.2, the level M_2 of Γ_2 is an odd integer that is divisible by 5. We have $\Gamma \subsetneq \Gamma_2$, where equality does not hold since the level N of Γ is even. Since $g = 25$, the genus of the modular curve X_{Γ_2} is at most 24. Proposition 2.1(iv) with the morphism $X_\Gamma \to X_{\Gamma_2}$ implies that X_{Γ_2} has gonality at most 3. By Lemmas 8.1(i) and 8.2, we have $D = m[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_2]$ and $294 \leq D \leq 302$, where m is not divisible by any prime $p > 3$ and can only be divisible by 3 once. Also when $3 \nmid M_2$, the level D will be divisible by $6[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_2]$ by Lemma 8.1(iii).

We now check which groups Γ_2 in our explicit classification of all congruence subgroups containing $-I$ with gonality at most 3 and genus at most 24 have all the above properties. There turns out to be a unique possibility for Γ_2 up to conjugacy in $\mathrm{GL}_2(\mathbb{Z})$; it has label $\mathtt{25E}^2$ in the classification of Cummins–Pauli. We can characterize Γ_2, up to conjugacy in $\mathrm{GL}_2(\mathbb{Z})$, as the

unique congruence subgroup containing $-I$ with level 25 and index 50 in $\mathrm{SL}_2(\mathbb{Z})$ such that X_{Γ_2} has genus 2.

Let Γ_3 be the congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ consisting of matrices whose image modulo 6 lies in the image of Γ modulo 6. Since Γ_2 and Γ_3 have relatively prime levels, the intersection $\Gamma_2 \cap \Gamma_3$ is uniquely determined up to conjugacy in $\mathrm{GL}_2(\mathbb{Z})$, and

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_2 \cap \Gamma_3] = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_2][\mathrm{SL}_2(\mathbb{Z}) : \Gamma_3] = 50[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_3].$$

Lemma 8.1(iii) implies that $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_2 \cap \Gamma_3]$ is divisible by $50 \cdot 6 = 300$. From the inclusion $\Gamma \subseteq \Gamma_2 \cap \Gamma_3$, we find that 300 also divides D. We thus have $D = 300$ since $294 \le D \le 302$ and this implies that $\Gamma = \Gamma_2 \cap \Gamma_3$. The integer N divides $6 \cdot 25 = 150$ since $\Gamma = \Gamma_2 \cap \Gamma_3$. Since X_Γ has gonality 3 and $N \le 150$, Corollary 5.2(ii) implies that $D \le 287$ which contradicts $D = 300$.

8.3. **Bielliptic case.** Finally suppose X_Γ is bielliptic.

Lemma 8.3. *We have* $294 \le D \le 403$ *and* $N \equiv 0 \pmod{210}$.

Proof. From the previous cases, we know that X_Γ has gonality at least 4. Since X_Γ is bielliptic, it has gonality at most 4. Thus X_Γ has gonality 4 and hence $D \le 403$ by Corollary 5.2(iii). We have $D \ge 294$ since otherwise (3.1) implies that $g \le 1 + 293/12 - 1/2 < 25$.

The integer N is divisible by every prime $p \le 7$ since otherwise $D \le 24(p^2+2p+1)/(p-1) < 294$ by Theorem 5.4(iii). Therefore, N is divisible by 210. □

We have $\Gamma \subsetneq \Gamma_2$, where equality does not hold since the level N of Γ is even by Lemma 8.3. By the minimality of our choice of Γ and Lemma 2.5(iii), X_{Γ_2} has gonality at most 2 or is bielliptic, and X_{Γ_2} has genus at most 24.

By Lemmas 8.1(ii) and 8.3, the level M_2 of Γ_2 is divisible by 35. By Lemmas 8.1(i) and 8.3, we have $D = m[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_2]$ and $294 \le D \le 403$, where m is not divisible by any prime $p > 3$ and can only be divisible by 3 once. Also when $3 \nmid M_2$, the level D will be divisible by $6[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_2]$ by Lemma 8.1(iii).

We now check for all groups Γ_2 as above in our explicit classification of congruence subgroups containing $-I$ for which X_Γ has genus at most 24 and X_Γ has gonality at most 2 or is bielliptic. There turns out to be a unique possibility for Γ_2 up to conjugacy in $\mathrm{GL}_2(\mathbb{Z})$; it has label $\texttt{105A}^{10}$ in the classification of Cummins–Pauli. We can characterize Γ_2, up to conjugacy in $\mathrm{GL}_2(\mathbb{Z})$, as the unique congruence subgroup containing $-I$ with level 105 and index 120 in $\mathrm{SL}_2(\mathbb{Z})$ such that X_{Γ_2} has genus 10.

Since $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_2] = 120$ divides D and $294 \le D \le 403$, we have $D = 360 = 3[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_2]$. Lemma 8.1(iv) implies that Γ_1 has level 2 and $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_1] = 3$. Since Γ_1 and Γ_2 have relatively prime levels, $\Gamma_1 \cap \Gamma_2$ has level $2 \cdot 105 = 210$ and $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_1 \cap \Gamma_2] = 3 \cdot 120 = 360$. We have $\Gamma = \Gamma_1 \cap \Gamma_2$ since we have an inclusion $\Gamma \subseteq \Gamma_1 \cap \Gamma_2$ and both groups have index 360 in $\mathrm{SL}_2(\mathbb{Z})$. In particular, $N = 210$ and $D = 360$. Since X_Γ is bielliptic, Theorem 5.4(iii) with $p = 11$ implies that $D < 346$ which contradicts $D = 360$.

References

[Abr96] Dan Abramovich, *A linear lower bound on the gonality of modular curves*, Internat. Math. Res. Notices **20** (1996), 1005–1011, DOI 10.1155/S1073792896000621. MR1422373 ↑5.3

[Acc94] Robert D. M. Accola, *Topics in the theory of Riemann surfaces*, Lecture Notes in Mathematics, vol. 1595, Springer-Verlag, Berlin, 1994. MR1329541 ↑6.2

[AGI] *Algebraic geometry. I*, Encyclopaedia of Mathematical Sciences, vol. 23, Springer-Verlag, Berlin, 1994. Algebraic curves. Algebraic manifolds and schemes; A translation of *Current problems in mathematics. Fundamental directions, Vol. 23 (Russian)*, Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow, 1988; Translation by D. Coray and V. N. Shokurov; Translation edited by I. R. Shafarevich. MR1287418 ↑2.3

[ACGH85] E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris, *Geometry of algebraic curves. Vol. I*, Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 267, Springer-Verlag, New York, 1985. MR770932 ↑2.3

[BGJGP05] Matthew H. Baker, Enrique González-Jiménez, Josep González, and Bjorn Poonen, *Finiteness results for modular curves of genus at least 2*, Amer. J. Math. **127** (2005), no. 6, 1325–1387. MR2183527 ↑6.1, 6.1

[Bar99] Francesc Bars, *Bielliptic modular curves*, J. Number Theory **76** (1999), no. 1, 154–165, DOI 10.1006/jnth.1998.2343. MR1688168 ↑1.3

[BLS20] Andrew R. Booker, Min Lee, and Andreas Strömbergsson, *Twist-minimal trace formulas and the Selberg eigenvalue conjecture*, J. Lond. Math. Soc. (2) **102** (2020), no. 3, 1067–1134, DOI 10.1112/jlms.12349. MR4186122 ↑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). ↑1.6

[Bou03] Nicolas Bourbaki, *Algebra II. Chapters 4–7*, Elements of Mathematics (Berlin), Springer-Verlag, Berlin, 2003. Translated from the 1981 French edition by P. M. Cohn and J. Howie; Reprint of the 1990 English edition [Springer, Berlin; MR1080964 (91h:00003)]. ↑3.3

[BN19] François Brunault and Michael Neururer, *Fourier expansions at cusps*, The Ramanujan Journal (2019). ↑3.2, 3.5, 3.5, 3.5

[CP03] C. J. Cummins and S. Pauli, *Congruence subgroups of* $\mathrm{PSL}(2,\mathbb{Z})$ *of genus less than or equal to 24*, Experiment. Math. **12** (2003), no. 2, 243–255. ↑7, 8

[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. 349, Springer, Berlin-New York, 1973, pp. 143–316 (French). MR337993 ↑4, 4.1, 4.2, 4.3, 4.3, 4.3, 4.3, 4.4

[Der12] Maarten Derickx, *Torsion points on elliptic curves and gonalities of modular curves* (2012). Master's thesis, Universiteit Leiden. ↑2.1

[Deu42] Max Deuring, *Reduktion algebraischer Funktionenkörper nach Primdivisoren des Konstantenkörpers*, Math. Z. **47** (1942), 643–654, DOI 10.1007/BF01180977 (German). MR15055 ↑2.1

[Fre94] Gerhard Frey, *Curves with infinitely many points of fixed degree*, Israel J. Math. **85** (1994), no. 1-3, 79–83, DOI 10.1007/BF02758637. MR1264340 ↑2.1

[GW23] Ulrich Görtz and Torsten Wedhorn, *Algebraic geometry II: Cohomology of schemes—with examples and exercises*, Springer Studium Mathematik—Master, Springer Spektrum, Wiesbaden, 2023. MR4704076 ↑6.3

[HS91] Joe Harris and Joe Silverman, *Bielliptic curves and symmetric products*, Proc. Amer. Math. Soc. **112** (1991), no. 2, 347–356, DOI 10.2307/2048726. MR1055774 ↑1.2, 1.3, 2.3

[Har13] Michael Harrison, *Explicit solution by radicals, gonal maps and plane models of algebraic curves of genus 5 or 6*, J. Symbolic Comput. **51** (2013), 3–21, DOI 10.1016/j.jsc.2012.03.004. MR3005778 ↑3.6.2

[HKO08] Takeshi Harui, Jiryo Komeda, and Akira Ohbuchi, *Double coverings between smooth plane curves*, Kodai Math. J. **31** (2008), no. 2, 257–262, DOI 10.2996/kmj/1214442797. MR2435894 ↑2.3

[HS99] Yuji Hasegawa and Mahoro Shimura, *Trigonal modular curves*, Acta Arith. **88** (1999), no. 2, 129–140, DOI 10.4064/aa-88-2-129-140. MR1700245 ↑1.3

[IM91] N. Ishii and F. Momose, *Hyperelliptic modular curves*, Tsukuba J. Math. **15** (1991), no. 2, 413–423, DOI 10.21099/tkbjm/1496161667. MR1138196 ↑1.3

[JK04] Daeyeol Jeon and Chang Heon Kim, *Bielliptic modular curves* $X_1(N)$, Acta Arith. **112** (2004), no. 1, 75–86, DOI 10.4064/aa112-1-5. MR2040593 ↑1.3

[JK07] ———, *On the arithmetic of certain modular curves*, Acta Arith. **130** (2007), no. 2, 181–193, DOI 10.4064/aa130-2-7. MR2357655 ↑1.3

[JKS20] Daeyeol Jeon, Chang Heon Kim, and Andreas Schweizer, *Bielliptic intermediate modular curves*, J. Pure Appl. Algebra **224** (2020), no. 1, 272–299, DOI 10.1016/j.jpaa.2019.05.007. MR3986422 ↑1.3

[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. ↑3.3

[Kim03] Henry H. Kim, *Functoriality for the exterior square of* GL_4 *and the symmetric fourth of* GL_2, J. Amer. Math. Soc. **16** (2003), no. 1, 139–183, DOI 10.1090/S0894-0347-02-00410-1. With appendix 1 by Dinakar Ramakrishnan and appendix 2 by Kim and Peter Sarnak. MR1937203 ↑5

[KM12] Kamal Khuri-Makdisi, *Moduli interpretation of Eisenstein series*, Int. J. Number Theory **8** (2012), no. 3, 715–748, DOI 10.1142/S1793042112500418. MR2904927 ↑3.5

[Liu02] Qing Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné; Oxford Science Publications. MR1917232 ↑2.3

[LMFDB] The LMFDB Collaboration, *The L-functions and modular forms database (beta)*. Online database, accessed June 2025. ↑1.2

[NO24] Filip Najman and Petar Orlić, *Gonality of the modular curve $X_0(N)$*, Math. Comp. **93** (2024), no. 346, 863–886, DOI 10.1090/mcom/3873. MR4678587 ↑1.3

[Ogg74] Andrew P. Ogg, *Hyperelliptic modular curves*, Bull. Soc. Math. France **102** (1974), 449–462. MR364259 ↑1.3, 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 ↑2.1, 5

[Rib76] Kenneth A. Ribet, *Galois action on division points of abelian varieties with real multiplications*, Amer. J. Math. **98** (1976), no. 3, 751–804. ↑8

[RX18] Joaquim Roé and Xavier Xarles, *Galois descent for the gonality of curves*, Math. Res. Lett. **25** (2018), no. 5, 1567–1589, DOI 10.4310/MRL.2018.v25.n5.a10. MR3917740 ↑1.3, 5

[Sel65] Atle Selberg, *On the estimation of Fourier coefficients of modular forms*, Proc. Sympos. Pure Math., Vol. VIII, Amer. Math. Soc., Providence, RI, 1965, pp. 1–15. MR182610 ↑5

[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. ↑3.1, 3.1, 3.5, 3.6

[Sti09] Henning Stichtenoth, *Algebraic function fields and codes*, 2nd ed., Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009. MR2464941 ↑2.1

[VZB22] John Voight and David Zureick-Brown, *The canonical ring of a stacky curve*, Mem. Amer. Math. Soc. **277** (2022), no. 1362, v+144, DOI 10.1090/memo/1362. MR4403928 ↑2.2

[Zog87] P. G. Zograf, *Small eigenvalues of automorphic Laplacians in spaces of parabolic forms*, Journal of Soviet Mathematics **36** (1987), no. 1, 106–114, DOI 10.1007/BF01104976. ↑5, 5

[Zyw10] David Zywina, *Elliptic curves with maximal Galois action on their torsion points*, Bull. Lond. Math. Soc. **42** (2010), no. 5, 811–826. ↑8

[Zyw22a] ———, *Explicit open images for elliptic curves over $\mathbb{Q}$* (2022). arXiv:2206.14959 [math.NT]. ↑1.2, 3, 3.3, 3.6

[Zyw22b] ———, GitHub repository related to *Explicit open images for elliptic curves over $\mathbb{Q}$*, 2022. `https://github.com/davidzywina/OpenImage`. ↑

[Zyw25] ———, GitHub repository related to *Classification of modular curves with low gonality*, 2025. `https://github.com/davidzywina/Modular`. ↑1.1, 1.2, 1.6, 3.5, 7

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