hexagon:2611.00443v1

AUTOMORPHISMS OF THE MODULAR CURVES $X_\Delta(N)$

FILIP NAJMAN

Abstract. We show that every automorphism of a modular curve $X_\Delta(N)$ of genus at least 2, where $\Gamma_1(N) \subseteq \Gamma_\Delta(N) \subseteq \Gamma_0(N)$, is induced by the normalizer of $\Gamma_\Delta(N)$ in $\mathrm{PSL}_2(\mathbb{R})$, except for five curves, namely $X_0(37)$, $X_0(63)$, $X_0(108)$, a curve of level 37 found by Jeon, Kim and Schweizer, and a curve of level 63 whose non-modular automorphisms had, to our knowledge, not been noticed before. In particular every automorphism of $X_1(N)$ normalizes the group of diamond operators, as claimed for square-free N in an unpublished preprint of Momose. The proof combines a twisted Hecke relation, which comes from the Galois action on the Tate module of the Jacobian, with a uniform bound for the dimension of the CM part of the Jacobian and with computations for finitely many levels.

1. Introduction

Let N be a positive integer. The modular curve $X_0(N)$ has a group of automorphisms coming from the action on the upper half-plane $\mathcal{H}$ of the normalizer of $\Gamma_0(N)$ in $\mathrm{PSL}_2(\mathbb{R})$. We will call such automorphisms *modular*. Ogg [34] proved that for square-free N with $g(X_0(N)) \geq 2$ all the automorphisms of $X_0(N)$ are modular, except for $N = 37$. Kenku and Momose [25, Theorem 2.17] extended this to all N with $g(X_0(N)) \geq 2$, except for $N = 37$ and possibly $N = 63$. Elkies [16] showed that $N = 63$ is indeed an exception, as $\mathrm{Aut}(X_0(63)) \simeq S_4 \times \mathbb{Z}/2\mathbb{Z}$ contains the modular automorphisms as a subgroup of index 2. Harrison [18] found an error in the argument of [25] for $N = 108$ and showed that the modular automorphisms of $X_0(108)$ also form a subgroup of index 2 of $\mathrm{Aut}(X_0(108))$. Hence all the automorphisms of $X_0(N)$ are modular if $g(X_0(N)) \geq 2$ and $N \notin \{37, 63, 108\}$. The automorphism groups of the quotients of $X_0(N)$ by groups of Atkin-Lehner involutions have recently been studied by Bars and Dalal [4, 5].

Let Δ be a subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times$ containing -1, and let $X_\Delta(N)$ be the modular curve attached to the group $\Gamma_\Delta(N)$ of matrices in $\Gamma_0(N)$ whose lower right entry reduces to an element of Δ modulo N. These curves are intermediate between $X_1(N) = X_{\{\pm 1\}}(N)$ and $X_0(N) = X_{(\mathbb{Z}/N\mathbb{Z})^\times}(N)$, and their modular automorphisms, defined in the same way, include the diamond operators. Ishii and Momose [20] determined the hyperelliptic curves $X_\Delta(N)$, except for the curve $X_{\{\pm 1, \pm 8\}}(21)$, which Jeon and Kim [22, Theorem 2.3 and Remark 2.4] showed to be hyperelliptic (see also [23, Theorem 3.6] and [3, Remark 3.16]). Jeon [21, Theorem 3.1] showed that all the automorphisms of the hyperelliptic curves $X_1(13)$,

2020 *Mathematics Subject Classification.* 11G18, 11F11, 14H37.

Key words and phrases. modular curves, automorphism groups, intermediate modular curves.

The author was supported by the Croatian Science Foundation under the project no. IP-2022-10-5008, by the project "Implementation of cutting-edge research and its application as part of the Scientific Center of Excellence for Quantum and Complex Systems, and Representations of Lie Algebras", PK.1.1.10.0004, co-financed by the European Union through the European Regional Development Fund – Competitiveness and Cohesion Programme 2021–2027, and by the European Union – NextGenerationEU through the National Recovery and Resilience Plan 2021–2026, via an institutional grant of the University of Zagreb Faculty of Science, IK IA 1.1.3, Impact4Math.

$X_1(16)$ and $X_1(18)$ are modular (see also [20]). In an unpublished preprint [30], Momose claimed that for square-free N all the automorphisms of $X_\Delta(N)$ are modular. Kamienny [24, Theorem 1] showed that for primes $p > 311$ the automorphism group of every curve $X_\Delta(p)$ of genus at least 2 is generated by the diamond operators and the lifts of the Atkin-Lehner involution, so all the automorphisms of $X_\Delta(p)$ are modular (see also [15, proof of Theorem 3.13]). Kim and Koo [26] and Lang [28] determined the normalizer of $\Gamma_1(N)$ in $\mathrm{PSL}_2(\mathbb{R})$, and Zemel [42, Corollary 2.6] gave a criterion for an element of $\mathrm{PSL}_2(\mathbb{R})$ to normalize $\Gamma_\Delta(N)$ for all N and Δ (see also [19]). While determining the bielliptic curves $X_\Delta(N)$, Jeon, Kim and Schweizer [23, Lemma 4.2 and Theorem 4.4] found a curve $X_\Delta(37)$ with non-modular automorphisms, contradicting the claim of [30]. Bars [3, Theorem 3.13 and Remark 3.15] surveys these results and points out that Momose's work needs a revision.

However, even for the curves $X_1(N)$ it was unknown whether all the automorphisms are modular for non-square-free N other than 16 and 18, and for square-free $N \neq 13$ the only argument in the literature is the one of [30], which contains errors (see Remark 9.3). In this paper we determine all the curves $X_\Delta(N)$ of genus at least 2 that have non-modular automorphisms. Our main result is the following theorem.

Theorem 1.1. *Let N be a positive integer and let Δ be a subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times$ containing -1 such that $g(X_\Delta(N)) \geq 2$. Then every automorphism of $X_\Delta(N)$ (over $\overline{\mathbb{Q}}$) is modular, except for the following 5 curves:*

$$X_0(37), \quad X_0(63), \quad X_0(108), \quad X_{\Delta_{37}}(37), \quad X_{\Delta_{63}}(63).$$

Here $\Delta_{37} = \langle \pm 8 \rangle$ is the subgroup of index 3 of $(\mathbb{Z}/37\mathbb{Z})^\times$, and Δ_{63} is the kernel of the even quadratic character of $(\mathbb{Z}/63\mathbb{Z})^\times$ of conductor 21. The curve $X_{\Delta_{63}}(63)$ has genus 9 and 96 automorphisms, of which 48 are modular.

Combining Theorem 1.1 with the description of the normalizer of $\Gamma_1(N)$ from [26, 28], we obtain the following corollary. We denote by w_Q, for $Q \parallel N$, the Atkin-Lehner operators on $X_1(N)$ (which are well defined up to diamond operators), and by $\omega(N)$ the number of prime divisors of N.

Corollary 1.2. *Let $N = 13$ or $N \geq 16$ (these are the N with $g(X_1(N)) \geq 2$). Then*

$$\mathrm{Aut}(X_1(N)_{\overline{\mathbb{Q}}}) = \langle \langle d \rangle,\ w_Q : d \in (\mathbb{Z}/N\mathbb{Z})^\times,\ Q \parallel N \rangle,$$

a group of order $2^{\omega(N)}\varphi(N)/2$. In particular every automorphism of $X_1(N)$ normalizes the group of diamond operators, and hence induces an automorphism of $X_0(N)$.

For square-free N, Theorem 1.1 is the statement claimed in [30], corrected by the single exception found in [23].

Corollary 1.3. *Let N be square-free and suppose that $g(X_\Delta(N)) \geq 2$. Then every automorphism of $X_\Delta(N)$ is modular, unless $N = 37$ and $\Delta = (\mathbb{Z}/37\mathbb{Z})^\times$ or $\Delta = \Delta_{37}$.*

The curve $X_{\Delta_{63}}(63)$ is an étale double cover of $X_0(63)$ to which all the 48 automorphisms of $X_0(63)$, including the non-modular ones found by Elkies, lift (see Section 9), just as all the automorphisms of $X_0(37)$ lift to $X_{\Delta_{37}}(37)$. To the best of our knowledge this has not been noticed before. By Theorem 1.1, the non-modular automorphisms of $X_0(63)$ and $X_0(108)$ lift to no other curves $X_\Delta(63)$ and $X_\Delta(108)$ (see Remark 9.2).

In Section 10 we make Zemel's description of the normalizer of $\Gamma_\Delta(N)$ explicit and compute its index (Theorem 10.6), which together with Theorem 1.1 gives $\#\,\mathrm{Aut}(X_\Delta(N)_{\overline{\mathbb{Q}}})$ for every curve $X_\Delta(N)$ of genus at least 2 (Corollary 10.7). For example, if $4 \nmid N$, $9 \nmid N$

and, for every prime p with $p^2 \mid N$, some element of Δ is not ± 1 modulo p, then apart from the curves of Theorem 1.1, $\#\operatorname{Aut}(X_\Delta(N)_{\overline{\mathbb{Q}}})$ is $[(\mathbb{Z}/N\mathbb{Z})^\times : \Delta]$ times the number of $Q \parallel N$ such that the Atkin-Lehner operator w_Q normalizes $\Gamma_\Delta(N)$ (Corollary 10.5, see also [23, Lemma 1.3]). In general the normalizer of $\Gamma_\Delta(N)$ need not be contained in the normalizer of $\Gamma_0(N)$, and in Table 2 we list the 28 curves with $N \leq 200$ and $g(X_\Delta(N)) \geq 2$ for which it is not.

Our approach differs from the ones of [34, 25, 30], which rely on the reduction of the modular curve modulo primes p dividing N and on the geometry of its special fiber, as described by Deligne and Rapoport. This works well for primes p that divide N exactly once, but the special fibers become much more complicated when $p^2 \mid N$. We instead use only primes of good reduction and the arithmetic of the Jacobian $J_\Delta(N)$ of $X_\Delta(N)$, as Dose, Lido and Mercuri did for the modular curves attached to Cartan subgroups [14] and, more recently, for general modular curves [15].

Let u be an automorphism of $X_\Delta(N)_{\overline{\mathbb{Q}}}$. In Section 3 we study the action of u on the Tate module of $J_\Delta(N)$ and show that on the part $J_\Delta(N)^{\mathrm{nCM}}$ of $J_\Delta(N)$ without complex multiplication (CM), u satisfies the relations

$$T_\ell \circ u = u^{\sigma_\ell} \circ T_\ell \quad \text{and} \quad \langle d \rangle \circ u \circ \langle d \rangle^{-1} = u^{\sigma_{d^2}},$$

where T_ℓ is the Hecke operator at a prime $\ell \nmid N$ and σ_a is (any lift to $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of) the automorphism $\zeta_N \mapsto \zeta_N^a$ of $\mathbb{Q}(\zeta_N)$. If the CM part of $J_\Delta(N)$ has dimension less than $(g(X_\Delta(N)) - 1)/2$, then u is defined over $\mathbb{Q}(\zeta_N)$, the second relation holds on all of $J_\Delta(N)$, and together with the Eichler-Shimura relation it gives the first one on all of $J_\Delta(N)$.

In Section 4 we show that, under suitable conditions, this equality of endomorphisms is an equality of correspondences on $X_\Delta(N)$. We do this either by computing an intersection number on $X_\Delta(N) \times X_\Delta(N)$ or by using Abramovich's lower bound for the gonality of modular curves [1]. In Section 5 we use the equality of correspondences to show that u maps cusps to cusps and elliptic points to elliptic points of the same order, by comparing the multiplicities of points in the divisors $T_\ell^n(P)$. It follows that u lifts to an automorphism of $\mathcal{H}$ normalizing $\Gamma_\Delta(N)$, i.e. that u is modular.

The main difficulty is the condition on the CM part of $J_\Delta(N)$. In Section 6 we count CM newforms using Hecke characters of imaginary quadratic fields, and obtain an upper bound for the dimension of the CM part of $S_2(N, \chi)$ that depends only on the local components of χ. From it we obtain a uniform bound, which proves the condition for all Δ and all $N \geq 2$ outside an explicit finite set of 2 370 285 integers. Evaluating the first bound at these integers leaves 58 levels $N > 200$, the largest being 6912, which we deal with using the bound for each Δ separately and, where this is not enough, modular symbols. The proof of Theorem 1.1 for $N > 200$ is completed in Section 7.

Unfortunately, none of our criteria apply to 87 of the 1449 curves $X_\Delta(N)$ of genus at least 2 with $N \leq 200$, as for small levels the CM part of the Jacobian can be too large and the gonality too small. For the 37 curves $X_0(N)$ among them we use the results of [34, 25, 16, 18], and the remaining 50 curves are treated in Sections 8 and 9, by computing the automorphism group of an explicit model, over $\mathbb{Q}$ or over a finite field, or by descent to a quotient curve whose automorphisms are known. For $N > 200$ our argument does not use [25, 18], so it gives an independent proof of their results for $N > 200$.

Our methods are perhaps most similar to those of Dose, Lido and Mercuri [14], who proved that for n large enough all the automorphisms of the modular curves attached to Cartan subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, and to certain subgroups of their normalizers, are

modular, by an argument with the same structure as ours. However, they assume that the group defining the modular curve contains the scalar matrices, which for $X_\Delta(N)$ is the case only if $\Delta = (\mathbb{Z}/N\mathbb{Z})^\times$. Otherwise the diamond operators need not commute with u, and u need not be defined over a compositum of quadratic fields (already the modular automorphisms of $X_1(N)$ are not). We deal with this using the twisted Hecke relation, which holds on $J_\Delta(N)^{\mathrm{nCM}}$ without any a priori control of the field of definition of u.

While finishing this paper, we became aware of the recent preprint [15], in which Dose, Lido and Mercuri extend the methods of [14] to the modular curves X_H attached to all the subgroups H of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ that contain -1 and have surjective determinant. They obtain independently an analogue of Proposition 3.2 b) [15, Theorem 2.15], and their criterion [15, Theorem 3.12] is the analogue of Theorem 5.6 with condition c) of Proposition 4.1. With it they prove that all the automorphisms of the curves X_H of prime level $p > 311$ are modular [15, Theorem 3.13]. For composite levels their results are computational: they compute the modular automorphisms of the curves X_H of level at most 39, and their criterion holds for 63.69% of the curves X_H of level at most 70 and genus at least 2, but for none of genus less than 10 [15, Section 5]. They conjecture that all the automorphisms of X_H are modular if its genus is large enough [15, Conjecture 1.1]. Theorem 1.1 proves this for the curves $X_\Delta(N)$, with the optimal bound $g(X_\Delta(N)) \geq 11$, as $g(X_0(108)) = 10$.

The main new ingredients compared to [14, 15] are the bound for the CM part of $S_2(N, \chi)$ for all χ, which proves (CM) outside an explicit finite set of levels, and conditions a) and b) of Proposition 4.1, which replace the gonality bound by an intersection number and hold for many curves of small level. Together with the computations for the remaining curves, this allows us to deal with all the curves $X_\Delta(N)$, and not only with those of large level. A disadvantage of our approach is its reliance on computations, both for the CM bound and for the curves of small level.

All the code used in the paper, together with its logs, can be found at

`https://github.com/F-Najman/automorphisms_XDelta`

This paper refers to its revision `67347db`, whose README lists the code and the logs of each computation. All of our computations were performed on the *Mordell* server at the Department of Mathematics, University of Zagreb with an AMD EPYC 9175F CPU (16 cores, 32 threads) and 384 GB of RAM, using Magma V2.29-4 [9], SageMath 10.7, Python 3.11 and gcc 15.2.

Proposition 10.3, Theorem 10.6, the statements of Corollary 10.5 about the normalizer of $\Gamma_\Delta(N)$ and its index, and the description of the normalizer of $\Gamma_1(N)$ from [26, 28] used in Corollary 1.2 have been formalized in Lean 4 with Mathlib, with all the definitions and statements fixed before the proofs were written. The formalization can be found at

`https://github.com/F-Najman/normalizer-lean`

This paper refers to its revision `1f4c27e` (see [33] and Section 10).

AI disclosure and comments. Anthropic's Claude Opus 5.5 produced almost all of the mathematical content of the first versions of the proofs, carried out the computations, wrote the draft of the present manuscript, organized the code repository and wrote the corresponding Lean formalizations.

2. Conventions and notation

Throughout the paper N is a positive integer and Δ is a subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times$ containing -1. Let

$$\Gamma_\Delta(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) : d \bmod N \in \Delta \right\}.$$

Then $\pm\Gamma_1(N) \subseteq \Gamma_\Delta(N) \subseteq \Gamma_0(N)$. Let $X_\Delta(N)$ be the modular curve $\Gamma_\Delta(N)\backslash\mathcal{H}^*$, where $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$. The curve $X_\Delta(N)$ has a model over $\mathbb{Q}$ whose non-cuspidal points correspond to isomorphism classes of pairs (E, s), where E is an elliptic curve and s is the Δ-orbit of a point of order N on E. We write g_Δ for the genus of $X_\Delta(N)$, $J_\Delta(N)$ for its Jacobian and

$$i_\Delta = [(\mathbb{Z}/N\mathbb{Z})^\times : \Delta]$$

for the degree of the natural map $X_\Delta(N) \to X_0(N)$. The group $(\mathbb{Z}/N\mathbb{Z})^\times/\Delta$ acts on $X_\Delta(N)$ by the diamond operators $\langle d\rangle$, and $X_0(N)$ is the quotient of $X_\Delta(N)$ by this action. We denote by $\Delta^\perp$ the group of Dirichlet characters modulo N which are trivial on Δ. As $-1 \in \Delta$, all these characters are even, and

$$S_2(\Gamma_\Delta(N)) = \bigoplus_{\chi\in\Delta^\perp} S_2(N,\chi), \qquad g_\Delta = \sum_{\chi\in\Delta^\perp} \dim S_2(N,\chi).$$

Let $\mathcal{N}(\Gamma_\Delta(N))$ be the normalizer in $\mathrm{PSL}_2(\mathbb{R})$ of the image $\overline{\Gamma}_\Delta(N)$ of $\Gamma_\Delta(N)$ in $\mathrm{PSL}_2(\mathbb{R})$. Every element of $\mathcal{N}(\Gamma_\Delta(N))$ induces an automorphism of $X_\Delta(N)_\mathbb{C}$, and we call the automorphisms obtained in this way *modular*. They form a group isomorphic to $\mathcal{N}(\Gamma_\Delta(N))/\overline{\Gamma}_\Delta(N)$, which contains the diamond operators and those Atkin-Lehner operators w_Q, $Q \parallel N$, that normalize $\Gamma_\Delta(N)$ (not all of them do, see [23, Lemma 1.3 and Example 1.5]). Note that $\mathcal{N}(\Gamma_\Delta(N))$ need not be contained in the normalizer of $\Gamma_0(N)$ (see Section 10). If $g_\Delta \geq 2$, all the automorphisms of $X_\Delta(N)_\mathbb{C}$ are defined over $\overline{\mathbb{Q}}$, and we will identify $\mathrm{Aut}(X_\Delta(N)_{\overline{\mathbb{Q}}})$ with $\mathrm{Aut}(X_\Delta(N)_\mathbb{C})$.

For a non-cuspidal point $P = (E, s)$ of $X_\Delta(N)$, let $\mathrm{Aut}(E, s)$ be the group of automorphisms α of E such that $\alpha(s) = s$, and let $e(P)$ be the order of $\mathrm{Aut}(E, s)/\{\pm1\}$. Then $e(P) \in \{1, 2, 3\}$ is the order of the stabilizer in $\overline{\Gamma}_\Delta(N)$ of any point of $\mathcal{H}$ above P, and P is an *elliptic point* if $e(P) > 1$.

Let $\ell \nmid N$ be a prime. For $m \geq 1$ we denote by $T_{\ell^m}^{\mathrm{cyc}}$ the correspondence on $X_\Delta(N)$ that sends a non-cuspidal point (E, s) to the divisor

$$T_{\ell^m}^{\mathrm{cyc}}(E, s) = \sum_C (E/C, s_C),$$

where C runs over the cyclic subgroups of E of order ℓ^m and s_C is the image of s in E/C. We write $T_\ell = T_\ell^{\mathrm{cyc}}$ and $T_1^{\mathrm{cyc}} = \mathrm{id}$. The correspondence T_ℓ induces the Hecke operator T_ℓ on $S_2(\Gamma_\Delta(N))$ and on $J_\Delta(N)$, which we denote by the same letter.

Let $K = \mathbb{Q}(\zeta_N)$. For $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ let $\sigma_a \in \mathrm{Gal}(K/\mathbb{Q})$ be the automorphism satisfying $\sigma_a(\zeta_N) = \zeta_N^a$, and by a *lift* of σ_a we mean an element of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ whose restriction to K is σ_a. For $u \in \mathrm{Aut}(X_\Delta(N)_{\overline{\mathbb{Q}}})$ and $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ we write $u^\sigma = \sigma \circ u \circ \sigma^{-1}$.

For a newform f of weight 2 we denote by N_f its level, by χ_f its character and by $a_n(f)$ its coefficients. For a Dirichlet character ψ we denote by $f \otimes \psi$ the newform whose ℓ-th coefficient is $\psi(\ell)a_\ell(f)$ for all but finitely many primes ℓ. We fix a prime r and an isomorphism $\mathbb{C} \simeq \overline{\mathbb{Q}}_r$, and denote by $\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{Q}}_r)$ the r-adic Galois representation attached to f, normalized such that Frob_ℓ has characteristic polynomial

$X^2 - a_\ell(f)X + \chi_f(\ell)\ell$ for the primes $\ell \nmid N_f r$. Then $\rho_{f\otimes\psi} \simeq \rho_f \otimes \psi$, where we view ψ also as a character of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

For an imaginary quadratic field F of discriminant $-D$ we denote by $\mathcal{O}_F$ its ring of integers, by $h(-D)$ its class number and by ε_F its quadratic character, and for a prime p we write $\mathcal{O}_{F,p} = \mathcal{O}_F \otimes \mathbb{Z}_p$. A newform f *has CM* if $f \otimes \varepsilon_F = f$ for some imaginary quadratic field F. We denote by $J_\Delta(N)^{\mathrm{CM}}$ the abelian subvariety of $J_\Delta(N)$ corresponding to the CM newforms (and their old forms) in $S_2(\Gamma_\Delta(N))$, and by $J_\Delta(N)^{\mathrm{nCM}}$ the one corresponding to the remaining newforms. Then $J_\Delta(N)$ is isogenous to $J_\Delta(N)^{\mathrm{CM}} \times J_\Delta(N)^{\mathrm{nCM}}$, and there are no non-zero homomorphisms between the two factors. Let $g_{\mathrm{CM}}(\Delta) = \dim J_\Delta(N)^{\mathrm{CM}}$. We will often use the condition

$$2g_{\mathrm{CM}}(\Delta) < g_\Delta - 1. \tag{CM}$$

For computations we use Magma [9]. Throughout the paper, in places where we used Magma or one of our other programs to compute something, we use the phrase "we compute" or something very similar.

3. The Galois action on the Tate module

We first describe when two newforms give isomorphic Galois representations over a number field.

Lemma 3.1. *Let f be a newform of weight 2 without CM and let h be a newform of weight 2.*

a) *Let L be a number field which is Galois over $\mathbb{Q}$. Then $\rho_f|_{\mathrm{Gal}(\overline{\mathbb{Q}}/L)} \simeq \rho_h|_{\mathrm{Gal}(\overline{\mathbb{Q}}/L)}$ if and only if $h = f \otimes \psi$ for a Dirichlet character ψ which is trivial on $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$.*

b) *Suppose that $h = f \otimes \psi$ for a Dirichlet character ψ, and that N_f and N_h divide N. Then the conductor of ψ divides N. In particular ψ is trivial on $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_N))$.*

Proof. a) By the results of Ribet [37] and Momose [31] on the image of ρ_f, the restriction of ρ_f to $\mathrm{Gal}(\overline{\mathbb{Q}}/L')$ is absolutely irreducible for every number field L'. If $h = f \otimes \psi$ with ψ trivial on $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$, then $\rho_h \simeq \rho_f \otimes \psi$ has the same restriction to $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$ as ρ_f. Conversely, suppose that the restrictions are isomorphic. By Schur's lemma the space $\mathrm{Hom}_{\mathrm{Gal}(\overline{\mathbb{Q}}/L)}(\rho_f, \rho_h)$ is one-dimensional, and as $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$ is a normal subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, the group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on it, by a character ψ which is trivial on $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$. Then $\rho_h \simeq \rho_f \otimes \psi$, and comparing the traces of Frobenius elements shows that $h = f \otimes \psi$, where we view ψ as a Dirichlet character.

b) Let p be a prime and put $e = v_p(N)$. By strong multiplicity one, the local components at p of the automorphic representations attached to f and h are π and $\pi \otimes \psi_p$, where ψ_p is the local component at p of the character of $\mathbb{A}_{\mathbb{Q}}^\times/\mathbb{Q}^\times$ attached to ψ, and their conductor exponents $a(\pi)$ and $a(\pi \otimes \psi_p)$ are at most e. It is enough to show that $a(\psi_p) \leq e$. Suppose that $a(\psi_p) > e$. The central character χ_p of π is the local component at p of the character attached to χ_f, so $a(\chi_p) \leq v_p(N_f) \leq e$. Hence $a(\chi_p\psi_p) = a(\psi_p)$, and as $a(\psi_p) + a(\chi_p\psi_p) = 2a(\psi_p) > a(\pi)$, it follows from [8, Lemma 1.4] that $a(\pi \otimes \psi_p) = \max\{a(\pi), 2a(\psi_p)\} = 2a(\psi_p) > e$, which is a contradiction. □

Proposition 3.2. *Let u be an automorphism of $X_\Delta(N)_{\overline{\mathbb{Q}}}$, which we view also as an automorphism of $J_\Delta(N)_{\overline{\mathbb{Q}}}$. Then on $J_\Delta(N)^{\mathrm{nCM}}$ the following relations hold:*

a) *$u^\sigma = u$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$,*

b) $\langle d\rangle \circ u \circ \langle d\rangle^{-1} = u^\sigma$ *for all* $d \in (\mathbb{Z}/N\mathbb{Z})^\times$ *and every lift* σ *of* σ_{d^2},
c) $T_\ell \circ u = u^\sigma \circ T_\ell$ *for every prime* $\ell \nmid N$ *and every lift* σ *of* σ_ℓ.

Proof. Let $V = V_r(J_\Delta(N)) \otimes_{\mathbb{Q}_r} \overline{\mathbb{Q}}_r$. As a module over $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and the Hecke algebra, we have

$$V \simeq \bigoplus_f \rho_f \otimes M_f,$$

where f runs over the newforms of level dividing N with character in $\Delta^\perp$, and M_f is a vector space of dimension equal to the number of divisors of N/N_f, on which T_ℓ acts by $a_\ell(f)$ for $\ell \nmid N$ and $\langle d\rangle$ acts by $\chi_f(d)$ (see [12, Theorem 6.6.6 and Section 9.5]).

For a non-CM newform f let Ψ_f be the set of Dirichlet characters ψ such that $f \otimes \psi$ occurs in V, and put

$$V_{[f]} = \bigoplus_{\psi \in \Psi_f} \rho_{f\otimes\psi} \otimes M_{f\otimes\psi} \simeq \rho_f \otimes M_{[f]}, \qquad M_{[f]} = \bigoplus_{\psi\in\Psi_f} M_{f\otimes\psi}.$$

Since $\rho_{f\otimes\psi} \simeq \rho_f \otimes \psi$, an element $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $V_{[f]}$ as $\rho_f(\sigma) \otimes A(\sigma)$, where $A(\sigma)$ acts on $M_{f\otimes\psi}$ as multiplication by $\psi(\sigma)$. By Lemma 3.1 b), every $\psi \in \Psi_f$ is trivial on $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$, so $A(\sigma)$ depends only on the restriction of σ to K. As the nebentypus of $f \otimes \psi$ is $\chi_f\psi^2$, we have

$$T_\ell = a_\ell(f)A(\sigma) \text{ for any lift } \sigma \text{ of } \sigma_\ell,$$
$$\langle d\rangle = \chi_f(d)A(\sigma)^2 \text{ for any lift } \sigma \text{ of } \sigma_d$$

on $V_{[f]}$. The subspace of V corresponding to $J_\Delta(N)^{\mathrm{nCM}}$ is the direct sum of the spaces $V_{[f]}$, and for every number field $L \supseteq K$ which is Galois over $\mathbb{Q}$ these are the isotypic components of its restriction to $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$ by Lemma 3.1.

Let $L \supseteq K$ be a number field which is Galois over $\mathbb{Q}$ and such that u is defined over L. Then u commutes with $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$, so u preserves each $V_{[f]}$ and acts on it as $1 \otimes U$ for some $U \in \mathrm{End}(M_{[f]})$. It follows that

$$u^\sigma = 1 \otimes A(\sigma)UA(\sigma)^{-1}$$

on $V_{[f]}$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Since $A(\sigma)$ is the identity for $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$, this proves a). Relations b) and c) follow directly from the displayed formulas for $\langle d\rangle$ and T_ℓ. □

Lemma 3.3. *Let* X *be a curve of genus* $g \geq 2$ *and let* $v \neq 1$ *be an automorphism of* X. *If* v *acts trivially on an abelian subvariety* A *of* $\mathrm{Pic}^0(X)$, *then* $\dim A \leq (g+1)/2$.

Proof. The abelian variety A is contained in the image of $\mathrm{Pic}^0(X/\langle v\rangle)$, so $\dim A \leq g(X/\langle v\rangle)$. If $g(X/\langle v\rangle) \geq 1$, the Riemann-Hurwitz formula gives $2g-2 \geq 2(2g(X/\langle v\rangle)-2)$, from which it follows that $g(X/\langle v\rangle) \leq (g+1)/2$. □

Corollary 3.4. *Suppose that* $X_\Delta(N)$ *satisfies* (CM). *Then every automorphism* u *of* $X_\Delta(N)_{\overline{\mathbb{Q}}}$ *is defined over* K, *and*

$$\langle d\rangle \circ u \circ \langle d\rangle^{-1} = u^{\sigma_{d^2}} \quad \text{for all } d \in (\mathbb{Z}/N\mathbb{Z})^\times.$$

Proof. Condition (CM) is equivalent to $\dim J_\Delta(N)^{\mathrm{nCM}} > (g_\Delta+1)/2$. For $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$, the automorphism $u^\sigma u^{-1}$ acts trivially on $J_\Delta(N)^{\mathrm{nCM}}$ by Proposition 3.2 a), so it is trivial by Lemma 3.3. Hence u is defined over K, and u^σ depends only on the restriction of σ to K. The second claim follows in the same way from Proposition 3.2 b). □

Proposition 3.5. *Suppose that $X_\Delta(N)$ satisfies* (CM)*. Then for every automorphism u of $X_\Delta(N)_{\overline{\mathbb{Q}}}$ and every prime $\ell \nmid N$ we have*

$$T_\ell \circ u = u^{\sigma_\ell} \circ T_\ell \quad \textit{in } \operatorname{End}(J_\Delta(N)_{\overline{\mathbb{Q}}}).$$

Proof. Let $r' \neq \ell$ be a prime and let $V = V_{r'}(J_\Delta(N))$. Let $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be a Frobenius element at a prime above ℓ. Then σ restricts to σ_ℓ on K, and as u is defined over K by Corollary 3.4, we have $u^\sigma = u^{\sigma_\ell}$. Pullback along $X_1(N) \to X_\Delta(N)$ embeds V into $V_{r'}(J_1(N))$, compatibly with the actions of $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, T_ℓ and $\langle\ell\rangle$. By the Eichler-Shimura relation, in the form of [12, Theorem 9.5.1 and its proof], we have $\sigma^2 - T_\ell\sigma + \ell\langle\ell\rangle = 0$ on $V_{r'}(J_1(N))$, so

$$T_\ell = \sigma + \ell\langle\ell\rangle\sigma^{-1} \quad \text{on } V.$$

By Corollary 3.4, applied to $u^{\sigma^{-1}}$ with $d = \ell$, we have $\langle\ell\rangle u^{\sigma^{-1}} = u^\sigma\langle\ell\rangle$. As $\sigma u = u^\sigma\sigma$ and $\sigma^{-1}u = u^{\sigma^{-1}}\sigma^{-1}$ on V, it follows that

$$T_\ell u = u^\sigma\sigma + \ell\langle\ell\rangle u^{\sigma^{-1}}\sigma^{-1} = u^\sigma\sigma + \ell u^\sigma\langle\ell\rangle\sigma^{-1} = u^\sigma T_\ell$$

on V. As $\operatorname{End}(J_\Delta(N)_{\overline{\mathbb{Q}}})$ acts faithfully on V, the claim follows. □

For $X_0(N)$, Corollary 3.4 and Proposition 3.5 are [25, Lemmas 1.4 and 2.6] (see also [14, Lemma 4.1 and Proposition 2.2]). For all the curves X_H, analogues of Proposition 3.2 b) and Proposition 3.5 were obtained independently in [15, Theorem 2.15 and Lemma 3.9]. For $\Delta = (\mathbb{Z}/N\mathbb{Z})^\times$ the diamond operators are trivial, so u is defined over the compositum of the quadratic fields whose discriminant divides N, and the second relation of Corollary 3.4 is not needed.

4. From endomorphisms to correspondences

Let $\ell \nmid N$ be a prime. We view T_ℓ as a divisor on $X_\Delta(N) \times X_\Delta(N)$, namely the image of the modular curve attached to $\Gamma_\Delta(N) \cap \Gamma_0(\ell)$ under the product of the two degeneracy maps. It is a positive multiple of an irreducible curve, and both its projections have degree $\ell + 1$. We will say that an automorphism u of $X_\Delta(N)_{\overline{\mathbb{Q}}}$ satisfies the *correspondence identity at* ℓ if

$$T_\ell(uP) = u^\sigma(T_\ell(P)) \quad \text{for all } P \in X_\Delta(N)(\overline{\mathbb{Q}}) \tag{4.1}$$

and every lift σ of σ_ℓ.

For a prime $\ell \nmid N$ let $S_\ell = \sum_f |a_\ell(f)|^2$, where f runs over a basis of $S_2(\Gamma_\Delta(N))$ consisting of eigenforms for all the Hecke operators T_n with $(n, N) = 1$ (so old forms are counted with multiplicity), and let S_ℓ^{CM} and S_ℓ^{nCM} be the analogous sums over the eigenforms with and without CM. Since $\overline{a_\ell(f)} = \chi_f(\ell)^{-1}a_\ell(f)$, we have $S_\ell = \operatorname{tr}(\langle\ell\rangle^{-1}T_\ell^2 \mid S_2(\Gamma_\Delta(N)))$.

Proposition 4.1. *Let $\ell \nmid N$ be a prime and suppose that one of the following holds:*

a) *$X_\Delta(N)$ satisfies* (CM) *and $S_\ell > (\ell+1)^2$,*
b) *$S_\ell^{\mathrm{nCM}} - S_\ell^{\mathrm{CM}} > (\ell+1)^2$,*
c) *$X_\Delta(N)$ satisfies* (CM) *and $\operatorname{gon}_{\mathbb{C}} X_\Delta(N) > 2(\ell+1)$.*

Then every automorphism of $X_\Delta(N)_{\overline{\mathbb{Q}}}$ satisfies the correspondence identity at ℓ.

Proof. Let $X = X_\Delta(N)$, let u be an automorphism of $X_{\overline{\mathbb{Q}}}$ and let σ be a lift of σ_ℓ. Put

$$C_1 = (u^{-1} \times 1)(T_\ell), \qquad C_2 = (1 \times u^\sigma)(T_\ell).$$

Then $C_1(P) = T_\ell(uP)$ and $C_2(P) = u^\sigma(T_\ell(P))$ for all points P of X, so we need to show that $C_1 = C_2$. For correspondences C and C' on X we have

$$C \cdot C' = d_1(C)d_2(C') + d_2(C)d_1(C') - \operatorname{tr}\left(\gamma_C\, \gamma_{C'}^\dagger \mid H^1(X)\right),$$

where d_i is the degree of the i-th projection, γ_C is the endomorphism of $H^1(X)$ induced by C and $\dagger$ is the Rosati involution, which corresponds to transposing correspondences (this follows from [7, Propositions 11.5.2 and 11.5.3 and Exercise 11.12 (14)], as $C \cdot C'$ is the intersection number of the diagonal with the composition of C and the transpose of C'). The correspondences C_1 and C_2 induce the endomorphisms $T_\ell u$ and $u^\sigma T_\ell$ of $J_\Delta(N)$. Note that $u^\dagger = u^{-1}$ and $T_\ell^\dagger = \langle\ell\rangle^{-1} T_\ell$, so $\operatorname{tr}(T_\ell u (T_\ell u)^\dagger \mid H^1(X)) = \operatorname{tr}(T_\ell T_\ell^\dagger \mid H^1(X)) = 2S_\ell$.

Suppose first that a) holds. By Proposition 3.5, $T_\ell u = u^\sigma T_\ell$, so

$$C_1 \cdot C_2 = 2(\ell+1)^2 - 2S_\ell < 0.$$

As C_1 and C_2 are positive multiples of irreducible curves, they have a common component, and as their projections have the same degrees, it follows that $C_1 = C_2$.

Suppose now that b) holds. By Proposition 3.2 c), the endomorphisms $T_\ell u$ and $u^\sigma T_\ell$ agree on $J_\Delta(N)^{\mathrm{nCM}}$, where the trace above contributes $2S_\ell^{\mathrm{nCM}}$. On $J_\Delta(N)^{\mathrm{CM}}$ the Rosati involution is positive [32, Section 21, Theorem 1], so by the Cauchy-Schwarz inequality the contribution of $J_\Delta(N)^{\mathrm{CM}}$ to the trace has absolute value at most $2S_\ell^{\mathrm{CM}}$. Hence

$$C_1 \cdot C_2 \le 2(\ell+1)^2 - 2S_\ell^{\mathrm{nCM}} + 2S_\ell^{\mathrm{CM}} < 0,$$

and we conclude as in a).

Suppose finally that c) holds. Then $T_\ell u = u^\sigma T_\ell$ by Proposition 3.5, so the map $P \mapsto [C_1(P) - C_2(P)]$ from X to $J_\Delta(N)$ is constant, and the effective divisors $C_1(P) + C_2(Q)$ and $C_2(P) + C_1(Q)$ of degree $2(\ell+1)$ are linearly equivalent for all $P, Q \in X$. Since $2(\ell+1) < \operatorname{gon}_{\mathbb{C}} X$, they are equal. For a given P we may choose Q such that $C_1(P)$ and $C_1(Q)$ have disjoint supports, as only finitely many Q fail this. Then $C_1(P) \le C_2(P)$, and as both divisors have degree $\ell+1$, it follows that $C_1(P) = C_2(P)$ (this is the argument of [14, Proposition 2.2], see also [15, Theorem 3.12]). □

To apply c) we use the following result of Abramovich.

Theorem 4.2 ([1, Theorem 0.1])**.** *Let $\Gamma \subseteq \mathrm{PSL}_2(\mathbb{Z})$ be a congruence subgroup of index D. Then $\operatorname{gon}_{\mathbb{C}} X_\Gamma \ge \frac{7}{800} D$.*

The constant comes from the Li-Yau inequality and the bound $\lambda_1 \ge 21/100$ of Luo, Rudnick and Sarnak [29] for the smallest positive eigenvalue of the Laplacian (see [1, Sections 1.5 and 1.6]). As $[\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma}_\Delta(N)] = \psi(N) i_\Delta$, where $\psi(N) = N \prod_{p \mid N}(1 + 1/p)$, it follows that

$$\operatorname{gon}_{\mathbb{C}} X_\Delta(N) \ge \frac{7}{800}\, \psi(N)\, i_\Delta. \tag{4.2}$$

5. Cusps, elliptic points and modularity

We now show that the correspondence identity forces an automorphism to preserve the cusps and the elliptic points. For $\ell \ge 5$ these are characterized by the multiplicities of the points in $T_\ell(P)$ [14, Theorem 2.4]. We use the divisors $T_\ell^n(P)$ instead, which also works for $\ell = 2$ and $\ell = 3$ (these primes are also treated in [15, Lemma 3.2], with a different argument for the elliptic points).

Lemma 5.1. *Let $\ell \nmid N$ be a prime, let u be an automorphism of $X_\Delta(N)_{\overline{\mathbb{Q}}}$ which satisfies the correspondence identity at ℓ, and let σ be a lift of σ_ℓ. Then*

$$T_\ell^n(uP) = u^{\sigma^n}\left(T_\ell^n(P)\right) \quad \text{for all } n \geq 1 \text{ and all } P \in X_\Delta(N)(\overline{\mathbb{Q}}), \tag{5.1}$$

as an equality of divisors.

Proof. Since T_ℓ is defined over $\mathbb{Q}$, applying σ^j to (4.1) gives $T_\ell \circ u^{\sigma^j} = u^{\sigma^{j+1}} \circ T_\ell$ for all $j \geq 0$, and the claim follows by induction on n. □

Lemma 5.2. *Let $\ell \nmid N$ be a prime and let P be a non-cuspidal point of $X_\Delta(N)$. Then*

$$T_\ell^n(P) = \sum_{k=0}^{\lfloor n/2 \rfloor} c_{n,k}\, T_{\ell^{n-2k}}^{\mathrm{cyc}}\left(\langle \ell \rangle^k P\right)$$

for some non-negative integers $c_{n,k}$ with $c_{n,0} = 1$.

Proof. Write $P = (E, s)$. The divisor $T_\ell^n(P)$ is the sum of the points $(E/K_n, s_{K_n})$ over all the chains $0 = K_0 \subset K_1 \subset \cdots \subset K_n$ of subgroups of E with $[K_i : K_{i-1}] = \ell$. A subgroup K of E of order ℓ^n is isomorphic to $\mathbb{Z}/\ell^{n-k}\mathbb{Z} \times \mathbb{Z}/\ell^k\mathbb{Z}$ for some $0 \leq k \leq n/2$, and then K contains $E[\ell^k]$. Since $E/E[\ell^k] \simeq E$ via multiplication by ℓ^k, which maps s to $\ell^k s$, we have $(E/K, s_K) \simeq (E/\ell^k K, (\ell^k s)_{\ell^k K})$, and $K \mapsto \ell^k K$ is a bijection from the subgroups of this type to the cyclic subgroups of E of order ℓ^{n-2k}. The number of chains ending in K depends only on the isomorphism type of K, which proves the claim, with $c_{n,k}$ the number of chains of subgroups with successive quotients of order ℓ in $\mathbb{Z}/\ell^{n-k}\mathbb{Z} \times \mathbb{Z}/\ell^k\mathbb{Z}$. As a cyclic group has only one such chain, $c_{n,0} = 1$. □

Lemma 5.3. *Let $\ell \nmid N$ be a prime and let u be an automorphism of $X_\Delta(N)_{\overline{\mathbb{Q}}}$ which satisfies the correspondence identity at ℓ. Then u maps cusps to cusps.*

Proof. Let c be a cusp. The support of $T_\ell^n(c)$ consists of cusps, so by Lemma 5.1 the support of $T_\ell^n(uc)$ is contained in the finite set $\bigcup_\tau u^\tau(\text{cusps})$, where τ runs over $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (the automorphism u has finitely many conjugates). If $uc = (E, s)$ were not a cusp, then by Lemma 5.2 the support of $T_\ell^n(uc)$ would contain all the points $(E/C, s_C)$ with C cyclic of order ℓ^n, and as n grows these have infinitely many different j-invariants, which is a contradiction. □

For elliptic points the support of $T_\ell^n(P)$ is not enough, as different cyclic subgroups often have isomorphic quotients when ℓ splits into principal primes in the CM field of E, so we compare multiplicities. For example, we compute that on $X(1)$ with $\ell = 2$ the number of points in the support of $T_2^n(P)$ grows at the same rate for the non-elliptic point $j = -3375$ as for the elliptic point $j = 1728$ (see `recheck_lemmaE.py`). For a prime $\ell \nmid N$, a non-cuspidal point P of $X_\Delta(N)$, $n \geq 1$ and $e \in \{2, 3\}$ put

$$\nu_e(P, n) = \#\left\{R : \mathrm{mult}_R\, T_\ell^n(P) \not\equiv 0 \pmod{e}\right\}.$$

We use the following facts about isogenies between elliptic curves with CM, see [27] or [40, Sections 2.7, 2.9 and 2.10, Lemma 6 and its proof, and Remark 8]. Let ℓ be a prime. For an elliptic curve E with CM, let $d(E)$ be the ℓ-adic valuation of the conductor of the order $\mathrm{End}(E)$, and call an ℓ-isogeny $E \to E'$ *descending* if $d(E') = d(E) + 1$ and *ascending* if $d(E') = d(E) - 1$. Every ℓ-isogeny changes d by at most 1, and the dual of a descending ℓ-isogeny is ascending. At least $\ell - 1$ of the $\ell + 1$ isogenies of degree ℓ from E are descending, and if $d(E) \geq 1$, exactly one is ascending and the remaining ℓ are descending.

For an elliptic curve E over $\overline{\mathbb{Q}}$ and $n \geq 1$ we call a cyclic subgroup C of E of order ℓ^n *descending* if E does not have CM, or if E has CM and all the ℓ-isogenies in the sequence $E \to E/C[\ell] \to \cdots \to E/C$ are descending.

Lemma 5.4. *Let ℓ be a prime, let E be an elliptic curve over $\overline{\mathbb{Q}}$ and let $n \geq 1$.*

a) *There are at least $(\ell-1)\ell^{n-1}$ descending cyclic subgroups of E of order ℓ^n.*
b) *Let C be a descending cyclic subgroup of E of order ℓ^n, and let C' be a cyclic subgroup of E of order ℓ^m with $m \leq n$ such that $E/C \simeq E/C'$. Then $m = n$ and $C' = \beta C$ for some $\beta \in \mathrm{Aut}(E)$.*
c) *Let C be a descending cyclic subgroup of E of order ℓ^n. Then $\mathrm{Aut}(E/C) = \{\pm 1\}$, and $\beta C \neq C$ for all $\beta \in \mathrm{Aut}(E) \setminus \{\pm 1\}$.*

Proof. Suppose first that E does not have CM. Then all the $(\ell+1)\ell^{n-1}$ cyclic subgroups of order ℓ^n are descending, and $\mathrm{Aut}(E) = \mathrm{Aut}(E/C) = \{\pm 1\}$, which proves a) and c). In b), composing $E \to E/C \simeq E/C'$ with the dual of $E \to E/C'$ gives an endomorphism of E of degree ℓ^{n+m}, i.e. multiplication by $\pm\ell^{(n+m)/2}$, whose kernel contains the cyclic group C of order ℓ^n only if $m = n$, and then $C' = C$.

Suppose now that E has CM. Let $1 \leq i < n$ and let C_i be a descending cyclic subgroup of E of order ℓ^i. Then $d(E/C_i) = d(E) + i \geq 1$, and the unique ascending ℓ-isogeny from E/C_i is the dual of the last isogeny in $E \to \cdots \to E/C_i$, so the ℓ descending ℓ-isogenies from E/C_i correspond to descending cyclic subgroups of E of order ℓ^{i+1} containing C_i. Together with the $\ell - 1$ descending isogenies from E this proves a). If C is descending, then $d(E/C) = d(E) + n$, while $d(E/C') < d(E) + n$ for every cyclic subgroup C' of order ℓ^m with $m < n$ and for every cyclic subgroup C' of order ℓ^n that is not descending. Hence in b) we have $m = n$ and C' is descending, and following the unique ascending isogenies back from E/C and E/C' identifies the two sequences of isogenies, so $C' = \beta C$ for some $\beta \in \mathrm{Aut}(E)$. As $d(E/C) \geq 1$, the order $\mathrm{End}(E/C)$ is not maximal, so $\mathrm{Aut}(E/C) = \{\pm 1\}$. Finally, if $\beta \in \mathrm{Aut}(E) \setminus \{\pm 1\}$, then $\mathrm{End}(E) = \mathbb{Z}[\beta]$, so a subgroup C with $\beta C = C$ is an $\mathrm{End}(E)$-submodule. Then $\mathrm{End}(E)$ acts on E/C, so $d(E/C) \leq d(E)$, and C is not descending. □

Lemma 5.5. *Let $\ell \nmid N$ be a prime, let P be a non-cuspidal point of $X_\Delta(N)$ and let $e \in \{2, 3\}$.*

a) *If $e(P) = e$, then $\nu_e(P, n) \leq 2(\lfloor n/2 \rfloor + 1)$.*
b) *If $e(P) \neq e$, then $\nu_e(P, n) \geq (\ell-1)\ell^{n-1}/3$.*

Proof. Write $P = (E, s)$. We use the decomposition of Lemma 5.2.

a) Let α be an element of $\mathrm{Aut}(E, s)$ whose image generates $\mathrm{Aut}(E, s)/\{\pm 1\}$, a group of order e. The curve E has CM by $\mathcal{O} = \mathbb{Z}[i]$ or $\mathbb{Z}[\zeta_3]$, and α permutes the cyclic subgroups of E. Since $(E/C, s_C) \simeq (E/\alpha C, s_{\alpha C})$ and the orbits of $\langle\alpha\rangle$ have size e or 1, the multiplicity of every point R in $T_{\ell^m}^{\mathrm{cyc}}(\langle\ell\rangle^k P)$ is congruent modulo e to the number of α-stable cyclic subgroups C of order ℓ^m with $(E/C, s_C) = R$. Note that $\langle\ell\rangle^k P$ has the same automorphisms as P. An α-stable cyclic subgroup of $E[\ell^m] \simeq \mathcal{O}/\ell^m\mathcal{O}$ is an $\mathcal{O}$-submodule. For $m = 0$ there is only the trivial subgroup, and for $m \geq 1$ there are 2 such subgroups of order ℓ^m if ℓ splits in $\mathcal{O}$, at most 1 if ℓ ramifies (and none for $m \geq 2$), and none if ℓ is inert. It follows that each of the $\lfloor n/2 \rfloor + 1$ terms contributes at most 2 points of multiplicity not divisible by e.

b) Let C be a descending cyclic subgroup of E of order ℓ^n. By Lemma 5.4 b), the point $(E/C, s_C)$ does not occur in the terms of Lemma 5.2 with $k \geq 1$, and it occurs in $T_{\ell^n}^{\mathrm{cyc}}(P)$ only as $(E/\beta C, s_{\beta C})$ with $\beta \in \mathrm{Aut}(E)$. As $\mathrm{Aut}(E/C) = \{\pm 1\}$ by Lemma 5.4 c), we have

$(E/\beta C, s_{\beta C}) \simeq (E/C, s_C)$ if and only if $\beta \in \mathrm{Aut}(E,s)$, and by Lemma 5.4 c) the group $\mathrm{Aut}(E,s)/\{\pm 1\}$ acts freely on the descending subgroups. We conclude that the multiplicity of $(E/C, s_C)$ in $T_\ell^n(P)$ is exactly $e(P)$, which is not divisible by e. By Lemma 5.4 a), there are at least $(\ell-1)\ell^{n-1}/e(P) \geq (\ell-1)\ell^{n-1}/3$ such points. □

Theorem 5.6. *Suppose that there is a prime $\ell \nmid N$ such that one of the conditions a), b) or c) of Proposition 4.1 holds for $X_\Delta(N)$. Then every automorphism of $X_\Delta(N)$ is modular.*

Proof. Let u be an automorphism of $X_\Delta(N)_{\overline{\mathbb{Q}}}$. By Proposition 4.1, u satisfies the correspondence identity at ℓ. By Lemma 5.3, u maps cusps to cusps. By Lemma 5.1 we have $\nu_e(uP, n) = \nu_e(P, n)$ for all n, $e \in \{2, 3\}$ and all non-cuspidal P, so it follows from Lemma 5.5 that $e(uP) = e(P)$. Hence u induces an automorphism of $Y_\Delta(N) = \overline{\Gamma}_\Delta(N)\backslash\mathcal{H}$ which preserves the elliptic points and their orders, i.e. an automorphism of the orbifold $Y_\Delta(N)$. As $\mathcal{H}$ is simply connected, $\mathcal{H} \to Y_\Delta(N)$ is its universal orbifold covering, with group $\overline{\Gamma}_\Delta(N)$, so u lifts to an automorphism γ of $\mathcal{H}$ with $\gamma\overline{\Gamma}_\Delta(N)\gamma^{-1} = \overline{\Gamma}_\Delta(N)$ (see also [13, Proposition 3.1]). Thus $\gamma \in \mathcal{N}(\Gamma_\Delta(N))$ and u is modular. □

Remark 5.7. For $N \geq 4$ the group $\overline{\Gamma}_1(N)$ is torsion-free, so $X_1(N)$ has no elliptic points and Lemma 5.5 is not needed for $X_1(N)$.

6. The CM part of $J_\Delta(N)$

We now bound the dimension of the CM part of $S_2(N, \chi)$ for all characters χ. For the trivial character, a formula for the dimension of the CM part of $J_0(N)$ is [25, Lemma 1.5], and an explicit bound of the form $N^{1/2+o(1)}$ is [14, Proposition 4.2].

6.1. **Hecke characters.** The following description of CM newforms is well known, see [35, Theorem 3.4, Remark 3.5, and Theorem 4.5 and its proof].

Proposition 6.1. *Let F be an imaginary quadratic field of discriminant $-D$, and let ξ be a Hecke character of F of conductor $\mathfrak{f}$ such that $\xi((\alpha)) = \alpha$ for all $\alpha \in \mathcal{O}_F$ with $\alpha \equiv 1 \pmod{\ }^\times \mathfrak{f}$. Then*

$$f_\xi = \sum_{\mathfrak{a}} \xi(\mathfrak{a}) q^{N(\mathfrak{a})},$$

the sum running over the integral ideals of $\mathcal{O}_F$ coprime to $\mathfrak{f}$, is a newform in $S_2(D \cdot N(\mathfrak{f}), \chi)$, where $\chi(n) = \varepsilon_F(n)\xi((n))/n$ for integers n coprime to $DN(\mathfrak{f})$. Every newform of weight 2 with CM by F is equal to f_ξ for exactly one such ξ.

For ξ as in Proposition 6.1, the function $\omega(n) = \xi((n))/n$ is a Dirichlet character modulo $f = \mathfrak{f} \cap \mathbb{Z}$, and $\chi = \varepsilon_F\omega$. As χ is even and ε_F is odd, ω is odd. For a prime p we denote by ω_p the character of $\mathbb{Z}_p^\times$ corresponding to the p-part of ω, and by $\mathfrak{f}_p = \mathfrak{f}\mathcal{O}_{F,p}$ the p-part of $\mathfrak{f}$.

Lemma 6.2. *Let F be an imaginary quadratic field of discriminant $-D$, let $\mathfrak{f}$ be an ideal of $\mathcal{O}_F$ and let ω be an odd Dirichlet character whose conductor divides $\mathfrak{f} \cap \mathbb{Z}$. For a prime p let $e_p(\mathfrak{f}_p, \omega_p)$ be the number of characters of $\mathcal{O}_{F,p}^\times$ of conductor exactly $\mathfrak{f}_p$ whose restriction to $\mathbb{Z}_p^\times$ is ω_p^{-1}. Then the number of Hecke characters ξ as in Proposition 6.1 with conductor $\mathfrak{f}$ and with $\xi((n)) = n\omega(n)$ for all integers n coprime to $\mathfrak{f}$ is*

$$h(-D) \prod_{p \mid N(\mathfrak{f})} e_p(\mathfrak{f}_p, \omega_p)$$

if $D > 4$, and at most this number if $D \in \{3, 4\}$.

Proof. We view ξ as a character of $\mathbb{A}_F^\times/F^\times$ whose restriction to $(F\otimes\mathbb{R})^\times=\mathbb{C}^\times$ is $z\mapsto z^{-1}$. Its restriction to $\widehat{\mathcal{O}}_F^\times=\prod_{\mathfrak{p}}\mathcal{O}_{F,\mathfrak{p}}^\times$ is a product of local characters $\xi_\mathfrak{p}$, whose conductors give $\mathfrak{f}$. As ξ is trivial on $F^\times$, we have $\prod_{\mathfrak{p}}\xi_\mathfrak{p}(u)=u$ for all $u\in\mathcal{O}_F^\times$. Conversely, every character of $\widehat{\mathcal{O}}_F^\times$ satisfying this condition extends to exactly $h(-D)$ characters ξ of $\mathbb{A}_F^\times/F^\times$ with the given restriction to $\mathbb{C}^\times$, as $\mathbb{A}_F^\times/(F^\times\mathbb{C}^\times\widehat{\mathcal{O}}_F^\times)$ is the class group of F. Evaluating ξ on the principal idele generated by an integer n coprime to $\mathfrak{f}$ shows that the condition $\xi((n))=n\omega(n)$ is equivalent to $\prod_{\mathfrak{p}|p}\xi_\mathfrak{p}|_{\mathbb{Z}_p^\times}=\omega_p^{-1}$ for all p. If $D>4$, then $\mathcal{O}_F^\times=\{\pm1\}$ and the unit condition $\prod_{\mathfrak{p}}\xi_\mathfrak{p}(-1)=-1$ follows from $\prod_p\omega_p(-1)=\omega(-1)=-1$. This proves the claim for $D>4$, and for $D\in\{3,4\}$ we obtain an upper bound by dropping the conditions coming from the units of order 4 and 6. □

The local numbers $e_p(\mathfrak{f}_p,\omega_p)$ of Lemma 6.2 are computed by inclusion-exclusion. Let s_p be the conductor exponent of ω_p, let $\mathfrak{g}$ be an ideal of $\mathcal{O}_{F,p}$ and let $p^v\mathbb{Z}_p=\mathfrak{g}\cap\mathbb{Z}_p$. Denote by $U(\mathfrak{g})$ the kernel of the reduction map $\mathcal{O}_{F,p}^\times\to(\mathcal{O}_{F,p}/\mathfrak{g})^\times$ (so $U(\mathcal{O}_{F,p})=\mathcal{O}_{F,p}^\times$), and by $U(p^v)$ the kernel of $\mathbb{Z}_p^\times\to(\mathbb{Z}/p^v\mathbb{Z})^\times$. Since $\mathbb{Z}_p^\times/U(p^v)$ injects into $\mathcal{O}_{F,p}^\times/U(\mathfrak{g})$, the number of characters of $\mathcal{O}_{F,p}^\times$ that are trivial on $U(\mathfrak{g})$ and restrict to ω_p^{-1} is

$$r(\mathfrak{g})=\frac{\#\left(\mathcal{O}_{F,p}^\times/U(\mathfrak{g})\right)}{\varphi(p^v)}\ \text{ if } s_p\le v,\qquad \text{and 0 otherwise.}$$

Explicitly, if p splits in F and $\mathfrak{g}=\mathfrak{p}^x\overline{\mathfrak{p}}^y$, then $v=\max\{x,y\}$ and the numerator is $\varphi(p^x)\varphi(p^y)$, where $\varphi(1)=1$. If p is inert and $\mathfrak{g}=p^x\mathcal{O}_{F,p}$, then $v=x$ and the numerator is $p^{2x}-p^{2x-2}$ for $x\ge1$. If p ramifies and $\mathfrak{g}=\mathfrak{p}^x$, then $v=\lceil x/2\rceil$ and the numerator is p^x-p^{x-1} for $x\ge1$. In both cases the numerator is 1 for $x=0$. It follows that

$$e_p(\mathfrak{f}_p,\omega_p)=\sum_{\mathfrak{g}}\mu(\mathfrak{f}_p\mathfrak{g}^{-1})\,r(\mathfrak{g}),$$

the sum running over the ideals $\mathfrak{g}\mid\mathfrak{f}_p$ with $\mathfrak{f}_p\mathfrak{g}^{-1}$ square-free.

Proposition 6.3. *Let χ be an even Dirichlet character modulo N. For a fundamental discriminant $-D$ with $D\mid N$ and a prime $p\mid N$, let $s_p(D,\chi)$ be the conductor exponent of the character $\chi_p\varepsilon_{F,p}$ of $\mathbb{Z}_p^\times$, where $F=\mathbb{Q}(\sqrt{-D})$ and χ_p and $\varepsilon_{F,p}$ are the p-components of χ and ε_F, and put*

$$E_p(D,\chi)=\sum_{\mathfrak{f}_p}e_p(\mathfrak{f}_p)\left(v_p(N)-v_p(D)-n_p(\mathfrak{f}_p)+1\right),$$

where $n_p(\mathfrak{f}_p)=v_p(N(\mathfrak{f}_p))$, the sum runs over the ideals $\mathfrak{f}_p$ of $\mathcal{O}_{F,p}$ with $v_p(D)+n_p(\mathfrak{f}_p)\le v_p(N)$, and $e_p(\mathfrak{f}_p)$ is computed with $s_p=s_p(D,\chi)$. Then

$$\dim S_2(N,\chi)^{\mathrm{CM}}\le B(\chi):=\sum_D h(-D)\prod_{p\mid N}E_p(D,\chi),$$

where the sum runs over the fundamental discriminants $-D$ with $D\mid N$. For $D>4$ the contribution of the forms with CM by $\mathbb{Q}(\sqrt{-D})$ is equal to the corresponding term on the right.

Proof. By Proposition 6.1, a CM newform f_ξ of level $M\mid N$ contributes to $S_2(N,\chi)$ if and only if χ is induced by its nebentypus $\varepsilon_F\omega$, i.e. $\omega_p=\chi_p\varepsilon_{F,p}$ on $\mathbb{Z}_p^\times$ for all p, and in that

case it contributes $\prod_p(v_p(N)-v_p(M)+1)$ dimensions. As $M = D\cdot N(\mathfrak{f})$, the claim follows from Lemma 6.2. □

Note that $E_p(D,\chi)$ depends on χ only through $s_p(D,\chi)$, which is determined by the *local type* of χ at p: for odd p the conductor exponent of χ_p, together with whether χ_p is the quadratic character if its conductor exponent is 1, and for $p=2$ the pair (u,k) such that $\chi_2 = \chi_{-4}^u\psi$ with ψ trivial on -1 of order 2^k. It depends on D only through $v_p(D)$, the splitting of p in F and $\varepsilon_{F,p}$. This makes $B(\chi)$ easy to compute (see `cmV.py` and `cm_exact.c`).

As a check of Proposition 6.3, we compared $B(\chi)$ with the dimensions of the subspaces of $S_2(N,\chi)$ on which $T_q = 0$ for the primes q up to some bound that are inert in F, which contain the forms with CM by F, at all levels $N \le 200$ and at 24 levels between 216 and 1728, and found no contradiction (see `recheck_V.m`).

6.2. **A uniform bound.** Let $M(N)$ be the maximum of $\dim S_2(N,\chi)^{\mathrm{CM}}$ over the even characters χ modulo N.

Lemma 6.4. *Suppose that* $2M(N) < g(X_0(N))-1$. *Then* $X_\Delta(N)$ *satisfies* (CM) *for every* Δ.

Proof. We have $g_{\mathrm{CM}}(\Delta) = \sum_{\chi\in\Delta^\perp}\dim S_2(N,\chi)^{\mathrm{CM}} \le i_\Delta M(N)$, and by the Riemann-Hurwitz formula for $X_\Delta(N)\to X_0(N)$ we have $g_\Delta - 1 \ge i_\Delta(g(X_0(N))-1)$. □

Lemma 6.5. *For every fundamental discriminant* $-D<0$ *we have* $h(-D) \le \sqrt{D}(\log D + 2)/\pi$.

Proof. For $D = 3,4$ this is checked directly. For $D>4$ we have $h(-D) = \sqrt{D}L(1,\varepsilon_F)/\pi$, and partial summation, using that the partial sums of ε_F are bounded by $D/2$, gives $|L(1,\varepsilon_F)| \le \sum_{n\le D} 1/n + 1 \le \log D + 2$. □

To obtain a bound which is uniform in χ, we use a cruder count of the characters. Every ideal $\mathfrak{f}_p$ of $\mathcal{O}_{F,p}$ can be written uniquely as $p^i\mathfrak{g}$, where $\mathfrak{g}$ is *primitive*, i.e. not divisible by p, and one checks that $e_p(\mathfrak{f}_p) \le r(\mathfrak{f}_p) = \rho(p^i)$ if $s_p \le i + v_p(N(\mathfrak{g}))$, where $\rho(1)=1$ and $\rho(p^i) = p^i(1-\varepsilon_F(p)/p)$ for $i\ge 1$. For a prime p with $p^e \parallel N$, integers $\delta, s \ge 0$ and a splitting type τ of p let

$$L_p(e,\delta,\tau,s) = \sum_{\substack{\delta+2i+j\le e\\ i+j\ge s}} \rho(p^i)\,a(p^j)\,(e-\delta-2i-j+1),$$

where ρ is computed with $\varepsilon_F(p) = 1,-1,0$ according to τ and $a(p^j)$ is the number of primitive ideals of norm p^j (an empty sum is 0). Then $E_p(D,\chi) \le L_p(e, v_p(D), \tau, s_p(D,\chi))$, where τ is the splitting type of p in F. The exponent $s_p(D,\chi)$ depends only on the local type t of χ at p and on the character $\varepsilon = \varepsilon_{F,p}$, and we denote it by $s(t,\varepsilon)$. The possible pairs (τ,ε) for $\delta = v_p(D)$ are the following. For $\delta = 0$, τ is split or inert and $\varepsilon = 1$. For odd p and $\delta = 1$, τ is ramified and ε is the quadratic character of $\mathbb{Z}_p^\times$. For $p=2$ and $\delta\in\{2,3\}$, τ is ramified, and $\varepsilon = \chi_{-4}$ if $\delta = 2$ and $\varepsilon\in\{\chi_8,\chi_{-8}\}$ if $\delta = 3$. Let

$$\Lambda_p(e) = \max_t \sum_\delta p^{\delta/2} \max_{(\tau,\varepsilon)} L_p(e,\delta,\tau,s(t,\varepsilon)),$$

where δ runs over $\{0,1\}$ for odd p and over $\{0,2,3\}$ for $p=2$, and (τ,ε) over the pairs just described. Note that for $\delta = 3$ both characters $\chi_{\pm 8}$ are needed, as they can give

different values of $s(t,\varepsilon)$ (for example $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-6})$ for $\chi_2=\chi_8$). Since $h(-D)\le \sqrt{D}(\log N+2)/\pi$ by Lemma 6.5, $\sqrt{D}=\prod_p p^{v_p(D)/2}$, and each D is determined by the valuations $v_p(D)$ for $p\mid N$, we obtain

$$M(N)\le \frac{\log N+2}{\pi}\prod_{p^e\|N}\Lambda_p(e). \tag{6.1}$$

For an odd prime p we have $\Lambda_p(1)=\max\{4,2+\sqrt{p}\}$ and $\Lambda_p(2)=p+5+3\sqrt{p}$. To see this, let $c\le e$ be the conductor exponent of χ_p and let ε be the quadratic character of $\mathbb{Z}_p^\times$. Then $s(t,1)=c$, while $s(t,\varepsilon)=0$ if $\chi_p=\varepsilon$ and $s(t,\varepsilon)=\max\{c,1\}$ otherwise. For $\delta=0$ the maximum over τ is attained when p splits, and $L_p(1,0,\tau,c)=4,2$ for $c=0,1$ and $L_p(2,0,\tau,c)=p+8,p+5,2$ for $c=0,1,2$. For $\delta=1$ we have $L_p(1,1,\tau,s)=1,0$ for $s=0$ and $s\ge 1$, and $L_p(2,1,\tau,s)=3,1,0$ for $s=0$, $s=1$ and $s\ge 2$. Hence the sum in the definition of $\Lambda_p(1)$ is 4 if χ_p is trivial, $2+\sqrt{p}$ if $\chi_p=\varepsilon$ and 2 otherwise, and the sum in the definition of $\Lambda_p(2)$ is $p+8+\sqrt{p}$ if χ_p is trivial, $p+5+3\sqrt{p}$ if $\chi_p=\varepsilon$, $p+5+\sqrt{p}$ if $c=1$ and $\chi_p\ne\varepsilon$, and 2 if $c=2$. As $2\sqrt{p}>3$, the claim follows. The function `Lam` in `cmlocal.py` computes $\Lambda_p(e)$ for all p and e.

By [12, Theorem 3.1.1], $g(X_0(N))-1=\frac{\psi(N)}{12}-\frac{\nu_2}{4}-\frac{\nu_3}{3}-\frac{\nu_\infty}{2}$, where $\nu_2,\nu_3\le 2^{\omega(N)}$ [12, Corollary 3.7.2] are the numbers of elliptic points of order 2 and 3 and $\nu_\infty=\prod_{p^e\|N}\nu_\infty(p^e)$ is the number of cusps. Combining this with (6.1), it follows that the assumption of Lemma 6.4 holds whenever

$$G(N):=\frac{24}{\pi}(\log N+2)\prod_{p^e\|N}\frac{\Lambda_p(e)}{\psi(p^e)}+7\prod_{p^e\|N}\frac{2}{\psi(p^e)}+6\prod_{p^e\|N}\frac{\nu_\infty(p^e)}{\psi(p^e)}<1.$$

For a prime p and $e\ge 1$ put $\kappa(p,e)=\Lambda_p(e)/\psi(p^e)$ and $\theta(p,e)=\kappa(p,e)(1+\frac{e\log p}{2})$.

Lemma 6.6. *Let $e\ge 1$. For every odd prime q we have*

$$\kappa(q,e)\le U(q,e):=\frac{(e+1)^2+2e}{1-1/q}\,q^{-e/2},$$

and $\kappa(2,e)\le 2((e+1)^2+4e)2^{-e/2}$.

Proof. Let q be an odd prime. We drop the condition $i+j\ge s$ in L_q, and use that $\rho(q^i)\le q^i$ if q splits or ramifies and $\rho(q^i)\le q^i(1+1/q)$ if q is inert. For $\delta=0$ and q split, the sum over j for fixed i is $(e-2i+1)^2$, so the split term is at most $(e+1)^2q^{\lfloor e/2\rfloor}/(1-1/q)$. For q inert only $j=0$ occurs, and the inert term is at most $(e+1)(1+1/q)q^{\lfloor e/2\rfloor}/(1-1/q)$, which is smaller. The ramified term (with its factor $\sqrt{q}$) is at most $2eq^{e/2}/(1-1/q)$. As $\Lambda_q(e)$ is at most the sum of the term for $\delta=0$ and the ramified term, and $\psi(q^e)\ge q^e$, it follows that $\kappa(q,e)\le U(q,e)$. The bound for $\kappa(2,e)$ is proved in the same way. □

Lemma 6.7. *For all primes $q\ge 11$ and all $e\ge 1$ we have $\theta(q,e)<1$ and $\theta(q,e)\le\theta(q,1)$.*

Proof. As $\Lambda_q(1)=2+\sqrt{q}$, the function $\theta(q,1)=\frac{2+\sqrt{q}}{q+1}(1+\frac{\log q}{2})$ is decreasing for $q\ge 11$, and $\theta(11,1)=0.9742\ldots$. Hence it is enough to show that $\theta(q,e)\le\theta(q,1)$ for $e\ge 2$. For $11\le q<2000$ and $2\le e\le 25$ we compute the exact values of $\Lambda_q(e)$ (see `review_dfs_bounds.sage`, where interval arithmetic is used), and the largest value of $\theta(q,e)/\theta(q,1)$ is $\theta(11,2)/\theta(11,1)=0.6856\ldots$. Suppose now that $q\ge 2000$ or $e\ge 26$. As $\frac{2+\sqrt{q}}{q+1}\ge q^{-1/2}$,

$\frac{1}{1-1/q} \le \frac{11}{10}$ and $1 + \frac{e\log q}{2} \le e(1 + \frac{\log q}{2})$, it follows from Lemma 6.6 that

$$\frac{\theta(q,e)}{\theta(q,1)} \le R(q,e) := \frac{11}{10}\, e\,(e^2+4e+1)\, q^{-(e-1)/2}.$$

The function $R(q,e)$ is decreasing in q, and it is decreasing in $e \ge 2$, as both fractions in

$$\frac{R(q,e+1)}{R(q,e)} = \frac{e+1}{e} \cdot \frac{e^2+6e+6}{e^2+4e+1} \cdot q^{-1/2}$$

are decreasing in e, so this ratio is at most $\frac{3}{2} \cdot \frac{22}{13} \cdot 11^{-1/2} < 1$. Hence $\theta(q,e)/\theta(q,1) \le \max\{R(2000,2), R(11,26)\} < 0.64$. □

Proposition 6.8. *The set $\mathcal{S}$ of integers $N \ge 2$ with $G(N) \ge 1$ is finite. It has* 2 370 285 *elements, the largest being* 266 378 112 000.

Proof. As $\log N + 2 \le 2\prod_{p^e \| N}(1 + \frac{e\log p}{2})$, we have

$$G(N) \le \frac{48}{\pi} \prod_{p^e \| N} \theta(p,e) + 7 \prod_{p^e \| N} \frac{2}{\psi(p^e)} + 6 \prod_{p^e \| N} \frac{\nu_\infty(p^e)}{\psi(p^e)}.$$

By Lemma 6.7, multiplying N by a power of a prime $q \ge 11$ not dividing N does not increase this upper bound for G. Note that $\theta(q,e) \le \theta(q,1)$ is equivalent to $\kappa(q,e)(2 + e\log q) \le \kappa(q,1)(2+\log q)$, so for such q the exponent $e = 1$ gives the largest value of $G(Nq^e)$, and one checks directly that $G(Nq)$ is decreasing in $q \ge 11$.

This reduces the determination of $\mathcal{S}$ to a finite depth-first search over the factorizations of N, with the primes in increasing order. The primes $2, 3, 5, 7$ can increase the first term, but only by the factors $\sup_e \theta(p,e)$, which are less than 3.786, 2.491, 1.454 and 1.146, respectively. While some of these primes can still be added to N, we abandon a branch when the bound for G, with its first term multiplied by the factors of the primes that can still be added, is less than 1. Once all the primes that can still be added are at least 11, we abandon a branch when $G(Nq) < 1$ for the smallest admissible next prime q. Exponents $e \ge 60$ can be excluded, as the worst case is $p = 2$ and $e = 60$, which gives, by Lemma 6.6,

$$G(N) < \frac{48}{\pi} \cdot 16 \cdot 2\left(61^2 + 240\right) 2^{-30}(1 + 30\log 2) + 7 \cdot 2^{-59} + 6 \cdot 2^{-30} < 0.04,$$

where 16 bounds the product of the factors $\max\{1, \sup_e \theta(p,e)\}$ for $p \in \{2,3,5,7\}$. Similarly, prime powers $q^e > 10^{40}$ with $q \ge 11$ and $e < 60$ can be excluded, as $U(q,e)(1 + \frac{e\log q}{2}) \le \frac{11}{10} \cdot 3718 \cdot x^{-1/2}(1 + \frac{1}{2}\log x)$ with $x = q^e$, which gives $G(N) < 5 \cdot 10^{-13}$. We compute the resulting set, obtaining the stated numbers (see `cm_general_dfs.py`). A second implementation of the search using interval arithmetic, which keeps N whenever the upper end of the interval for $G(N)$ is at least 1, gives the same set (see `review_dfs_interval.sage`). □

Proposition 6.9. *The assumption of Lemma 6.4 holds for all $N > 200$ except for the* 3 *square-free values $N \in \{213, 285, 429\}$ and the following* 55 *values:*

207, 216, 225, 240, 243, 252, 256, 279, 288, 300, 320, 324, 336, 351,
360, 363, 375, 378, 384, 392, 400, 432, 441, 480, 486, 504, 512, 540,
567, 576, 600, 640, 648, 675, 720, 756, 768, 784, 800, 864, 900, 972,
1024, 1080, 1152, 1296, 1440, 1536, 1728, 2304, 2592, 3072, 3456, 4608, 6912.

Proof. By Proposition 6.8 we only need to consider $N \in \mathcal{S}$. For each such N we compute the maximum of $B(\chi)$ from Proposition 6.3 over all the tuples of local types that are realized by even characters modulo N, using a branch and bound search, with exact class numbers for $D \le 10^7$ and the bound of Lemma 6.5 for larger D. We find that $2\max B(\chi) < g(X_0(N)) - 1$ for all $N \in \mathcal{S}$ except for 134 values, and that 58 of these are larger than 200 (see `cm_exact.c`). A second implementation using only integer arithmetic gives the same 134 values (see `review_cm_exact_integer.c`). Note that the parity of χ matters here: a type in which $\chi_p \varepsilon_{F,p}$ is unramified at every p would force $\chi = \varepsilon_F$, which is odd. We do not claim that the assumption of Lemma 6.4 fails at the levels listed above, only that the bound $\max_\chi B(\chi)$ is not good enough to prove it. □

At the 55 levels of Proposition 6.9 we check (CM) for each Δ separately. By Proposition 6.3, the curve $X_\Delta(N)$ satisfies (CM) if

$$\sum_{\chi \in \Delta^\perp} (2B(\chi) - \dim S_2(N,\chi)) < -1. \tag{6.2}$$

Proposition 6.10. *Let N be one of the 55 levels of Proposition 6.9. Then (6.2) holds for all Δ with $i_\Delta \ge 2$, except for 63 subgroups Δ at 26 of these levels, all of which have $i_\Delta \in \{2,3,4\}$. At the remaining 29 levels, including $N = 6912$, it holds for all Δ with $i_\Delta \ge 2$.*

Proof. We compute the left-hand side of (6.2), using the Cohen-Oesterlé formula [10] for $\dim S_2(N,\chi)$, for all the subgroups Δ (see `perdelta.m` and `cmV_table.py`). □

7. Proof of Theorem 1.1 for $N > 200$

For some levels we check the conditions of Proposition 4.1 directly, as follows. For each Galois orbit of even characters χ modulo N we compute $S_2(N,\chi)$ using modular symbols and the subspace $W_\chi \subseteq S_2(N,\chi)$ obtained as the sum, over the imaginary quadratic fields F whose discriminant divides N, of the joint kernels of the Hecke operators T_q for the primes $q \le 60$ with $q \nmid N$ that are inert in F. The space W_χ is stable under the Hecke operators and contains the CM part of $S_2(N,\chi)$. We also compute the traces of $\langle \ell \rangle^{-1} T_\ell^2$ on $S_2(N,\chi)$ and on W_χ for the primes $\ell \le 37$ with $\ell \nmid N$. These traces lie in $\mathbb{Q}(\chi)$ and need not be the same for all the characters of an orbit (for $N = 25$, $\ell = 2$ and χ of order 5 they are $(3 \pm \sqrt{5})/2$), so each orbit contributes the trace from $\mathbb{Q}(\chi)$ to $\mathbb{Q}$ of these numbers. Summing over the orbits in $\Delta^\perp$, this gives an upper bound for $g_{\mathrm{CM}}(\Delta)$, the exact value of S_ℓ and an upper bound for S_ℓ^{CM}, so we can check the conditions a), b) and c) of Proposition 4.1 for every Δ (using (4.2) for c)). We call this computation the *scan* of level N (see `xdelta.m`).

Proposition 7.1. *In each of the following cases, the scan shows that $X_\Delta(N)$ satisfies one of the conditions of Proposition 4.1.*

a) $200 < N \le 500$ *and* $i_\Delta \le 3$, *or* $200 < N \le 500$ *is square-free and Δ is arbitrary.*

b) *N is one of the 22 levels*

$$216, 225, 256, 288, 320, 384, 432, 512, 576, 648, 675,$$
$$768, 864, 1024, 1152, 1296, 1536, 1728, 2304, 2592, 3456, 4608$$

and $i_\Delta \le 4$.

c) *$N > 500$ is not one of the levels in b), either N is one of the levels of Proposition 6.9 or $7\psi(N) \le 1600(\ell+1)$ for the smallest prime $\ell \nmid N$, and $\Delta = (\mathbb{Z}/N\mathbb{Z})^\times$. There are 113 such levels, the largest being 6912.*

The largest of these computations is the case $N = 6912$ and $\Delta = (\mathbb{Z}/6912\mathbb{Z})^\times$ in c), where $g(X_0(6912)) = 1081$ and the upper bound for g_{CM} is 236. At $N = 4608$ the two subgroups Δ of index 2 left over by Proposition 6.10 give curves of genus 1409 with CM parts of dimension at most 392 and 428.

Lemma 7.2. *Let ℓ be the smallest prime not dividing N.*

a) *If $\ell \geq 13$, then $7\psi(N) > 1600(\ell+1)$.*
b) *If $N > 500$, then $7\psi(N) > 800(\ell+1)$, and $7\psi(N) > 1600(\ell+1)$ unless $N \leq 840$. There are 105 values $N > 500$ with $7\psi(N) \leq 1600(\ell+1)$.*
c) *If $200 < N \leq 500$ and $N \neq 210$, then $7\psi(N) > 400(\ell+1)$.*

Proof. If $\ell \geq 13$, then N is divisible by $P_\ell = \prod_{p<\ell} p$, so $\psi(N) \geq \psi(P_\ell)$. For $\ell = 13$ we have $7\psi(2310) = 48384 > 1600 \cdot 14$, and if ℓ' is the prime following ℓ, then $\psi(P_{\ell'})/(\ell'+1) = \frac{(\ell+1)^2}{\ell'+1} \cdot \frac{\psi(P_\ell)}{\ell+1}$, where $(\ell+1)^2 > \ell'+1$ by Bertrand's postulate. This proves a). If $\ell \leq 11$, then a failure of one of the inequalities in b) or c) implies $N \leq \psi(N) \leq 1600 \cdot 12/7 < 2743$, and we check all $N < 2743$ directly (see `gon_general.py` and `review_gonality.sage`). □

Proof of Theorem 1.1 for $N > 200$. Let $N > 200$ and let Δ be such that $g_\Delta \geq 2$. By Theorem 5.6 it is enough to show that $X_\Delta(N)$ satisfies one of the conditions a), b) or c) of Proposition 4.1.

Suppose first that $i_\Delta = 1$, i.e. $X_\Delta(N) = X_0(N)$. If $N \leq 500$ or N is one of the levels of Proposition 7.1 b) or c), this follows from Proposition 7.1. Otherwise $N > 500$ is not one of the levels of Proposition 7.1 c), so by the definition of that list N is not one of the levels of Proposition 6.9 and $7\psi(N) > 1600(\ell+1)$. Hence $X_0(N)$ satisfies (CM) by Proposition 6.9 and Lemma 6.4, and $\operatorname{gon}_{\mathbb{C}} X_0(N) > 2(\ell+1)$ by (4.2), so condition c) holds.

Suppose now that $i_\Delta \geq 2$. We first show that $X_\Delta(N)$ satisfies (CM), or directly one of the conditions of Proposition 4.1. If N is not one of the 58 levels of Proposition 6.9, then (CM) holds by Lemma 6.4. If $N \in \{213, 285, 429\}$, one of the conditions holds by Proposition 7.1 a). If N is one of the 55 levels of Proposition 6.9, then (CM) holds by Proposition 6.10, except for 63 subgroups Δ with $i_\Delta \leq 4$. We check that each of these is covered by Proposition 7.1 a) or b), comparing the subgroups as sets of residues (see `check_large.py`).

It remains to prove the correspondence identity when (CM) holds. If $N > 500$, then $\operatorname{gon}_{\mathbb{C}} X_\Delta(N) \geq \frac{7}{800}\psi(N) \cdot 2 > 2(\ell+1)$ by (4.2) and Lemma 7.2 b), so c) holds. If $200 < N \leq 500$, $i_\Delta \geq 4$ and $N \neq 210$, then c) holds by Lemma 7.2 c). Finally, if $200 < N \leq 500$ and either $i_\Delta \leq 3$ or $N = 210$, one of the conditions holds by Proposition 7.1 a). □

8. Levels $N \leq 200$

For $N \leq 12$ all the curves $X_\Delta(N)$ have genus at most 1. We compute the scan of Section 7 for all $13 \leq N \leq 200$. There are 1449 curves $X_\Delta(N)$ of genus at least 2 with $13 \leq N \leq 200$, and 1362 of them satisfy one of the conditions of Proposition 4.1, so all their automorphisms are modular by Theorem 5.6. As a check of the method, the curves of levels 37, 63 and 108 that fail the conditions are exactly the curves of these levels in Theorem 1.1. The remaining 87 curves are the following.

a) The 37 curves $X_0(N)$ with

$$N \in \{22, 23, 26, 28, 29, 30, 31, 33, 34, 35, 37, 38, 39, 40, 42, 43, 44, 45, 48,$$
$$50, 54, 56, 57, 60, 61, 63, 64, 72, 80, 81, 84, 96, 98, 100, 108, 128, 144\}.$$

By [34, 25, 16, 18], all their automorphisms are modular, except for $N \in \{37, 63, 108\}$ (see also [18, Section 2], where this is verified by computation for all $N \leq 200$).

b) The 8 curves $X_1(N)$ with $N \in \{13, 16, 18, 20, 21, 22, 24, 30\}$.

c) The 42 curves listed in Table 1.

8.1. **Automorphism groups of explicit models.** For the hyperelliptic curves $X_1(13)$, $X_1(16)$, $X_1(18)$ and $X_{\{\pm1,\pm8\}}(21)$ and the plane quartic $X_1(20)$ we compute the automorphism group of an explicit model over $\overline{\mathbb{Q}}$ directly. For the other curves we work over finite fields. Let $X = X_\Delta(N)$, let $g = g_\Delta$ and let $\ell \equiv 1 \pmod N$ be a prime. We compute the canonical model of $X_{\mathbb{F}_\ell}$ as in [18, Section 2]. Let $f_1, \dots, f_g$ be a basis of $S_2(\Gamma_\Delta(N))$ in echelon form with integral q-expansions. The differentials $f_i(q)\,dq/q$ extend to the smooth model of X over $\mathbb{Z}_{(\ell)}$, and q is a local parameter at the cusp ∞ also modulo ℓ, so the reductions of the f_i, which we check to be linearly independent, are the q-expansions of a basis of the differentials of $X_{\mathbb{F}_\ell}$. A homogeneous polynomial relation of degree d between them is a relation between modular forms of weight $2d$ modulo ℓ, so it is enough to check it up to the Sturm bound $2d\psi(N)i_\Delta/12$. If the quadrics through the canonical image define a curve, they generate its ideal, and otherwise the ideal is generated by quadrics and cubics [38]. For $g = 3$ we compute the quartic relation instead. We check that there are $(g-2)(g-3)/2$ quadrics, and not $(g-1)(g-2)/2$ as for a hyperelliptic reduction, that the resulting curve has genus g, and that $\#X(\mathbb{F}_\ell) = \ell + 1 - \operatorname{tr} T_\ell$ (see `canon2.m`, `review_manuscript_reduction.m` and `review_manuscript_logs.py`).

Let π be the Frobenius endomorphism of $J = J_\Delta(N)_{\mathbb{F}_\ell}$, which acts semisimply on the Tate module of J by a theorem of Tate [41], and let k be the least common multiple of the orders of the roots of unity among the ratios of the eigenvalues of π. An endomorphism of $J_{\overline{\mathbb{F}}_\ell}$ is defined over $\mathbb{F}_{\ell^m}$ if and only if it commutes with π^m, and every endomorphism is defined over some $\mathbb{F}_{\ell^m}$ with $k \mid m$. As π is semisimple, the commutant of π^m in the endomorphisms of the Tate module is then equal to the commutant of π^k, so all the endomorphisms of $J_{\overline{\mathbb{F}}_\ell}$ are defined over $\mathbb{F}_{\ell^k}$. If ζ_m is one of these ratios, then $\varphi(m) \leq 4g^2$, and we determine k by checking all such m (in all our cases $g \leq 10$, and then $m \leq 1680$). As $\operatorname{Aut}(X_{\overline{\mathbb{F}}_\ell})$ acts faithfully on $J_{\overline{\mathbb{F}}_\ell}$ [11, Theorem 1.13], every automorphism of $X_{\overline{\mathbb{F}}_\ell}$ is defined over $\mathbb{F}_{\ell^k}$, and we compute the automorphism group of $X_{\mathbb{F}_{\ell^k}}$ with Magma. Since the reduction map $\operatorname{Aut}(X_{\overline{\mathbb{Q}}}) \to \operatorname{Aut}(X_{\overline{\mathbb{F}}_\ell})$ is injective [11, Theorem 1.11], we obtain an upper bound for $\#\operatorname{Aut}(X_{\overline{\mathbb{Q}}})$. On the other hand, we compute the order of the group of modular automorphisms from explicit matrices normalizing $\Gamma_\Delta(N)$: the diamond operators, the Atkin-Lehner matrices and the matrices $\left(\begin{smallmatrix} 1 & 1/h \\ 0 & 1 \end{smallmatrix}\right)$ with $h \mid 24$ and $h^2 \mid N$ that normalize $\Gamma_\Delta(N)$, and for $N = 49, 50$ the normalizers described in Remark 8.1. When the two numbers agree, all the automorphisms of X are modular. Note that for this we do not need to know that these matrices generate the whole normalizer.

We do this for the 8 curves in b) and for 29 of the curves in c) (see Table 1). In all cases except $X_{\Delta_{37}}(37)$ the two numbers agree (see `canon2.m` and `normalizer.m`). For $X_{\Delta_{37}}(37)$ we obtain 12 automorphisms, of which 6 are modular, in agreement with [23, Theorem 4.4].

Remark 8.1. Let $N = 49$ and $\Delta = \{x : x \equiv \pm 1 \pmod 7\}$. Conjugation by $\left(\begin{smallmatrix} 7 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ maps $\Gamma_\Delta(49)$ to $\pm\Gamma(7)$, so $X_\Delta(49)$ is isomorphic to $X(7)$, the Klein quartic, and all its 168 automorphisms are modular (see [17]). Similarly, for $N = 50$ and $\Delta = \{x : x \equiv \pm 1$

(mod 5)}, conjugation by $\begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix}$ maps $\Gamma_\Delta(50)$ to $\pm(\Gamma(5) \cap \Gamma_0(2))$, and $X_\Delta(50)$ has 120 modular automorphisms by Section 10 (see Table 2). As $X_\Delta(50)$ has genus 4 and at most 120 automorphisms (by the computation over $\mathbb{F}_{101}$ above), all its automorphisms are modular, and $X_\Delta(50)$ is Bring's curve. In both cases the normalizer of $\Gamma_\Delta(N)$ is not contained in the normalizer of $\Gamma_0(N)$.

8.2. **A descent argument.** For the remaining 12 curves in Table 1 the computation of the automorphism group over a finite field takes too long, and we use the following lemma instead.

Lemma 8.2. *Let $\Delta \subsetneq \Delta'$ be subgroups of $(\mathbb{Z}/N\mathbb{Z})^\times$ containing -1 and put $H = \Delta'/\Delta$, so $X_{\Delta'}(N) = X_\Delta(N)/H$. Suppose that $g(X_{\Delta'}(N)) \geq 2$. Let J^H be the image of $J_{\Delta'}(N)$ in $J_\Delta(N)$ and let A be the abelian subvariety of $J_\Delta(N)$ corresponding to the characters in $\Delta^\perp \setminus \Delta'^\perp$. Suppose that one of the following holds:*

a) $\mathrm{Hom}(J^H_{\overline{\mathbb{Q}}}, A_{\overline{\mathbb{Q}}}) = 0$,

b) *H has order 2 and $2 \dim S < g_\Delta - 1$, where S is the sum of the isotypic components of $J_\Delta(N)_{\overline{\mathbb{Q}}}$ that occur both in J^H and in A.*

Then H is a normal subgroup of $\mathrm{Aut}(X_\Delta(N)_{\overline{\mathbb{Q}}})$, so every automorphism of $X_\Delta(N)$ induces an automorphism of $X_{\Delta'}(N)$. If moreover all the automorphisms of $X_{\Delta'}(N)$ are modular, then all the automorphisms of $X_\Delta(N)$ are modular.

Proof. Let $X = X_\Delta(N)$ and $Y = X_{\Delta'}(N)$, and let u be an automorphism of $X_{\overline{\mathbb{Q}}}$.

Suppose first that a) holds. Then u maps J^H to itself, as the projection of $u(J^H)$ to A is zero. Since H acts trivially on J^H, so does uHu^{-1}. Let G be the group of automorphisms of X acting trivially on J^H. Then $H \subseteq G$. If $v \in G \setminus H$, then $Y \to X/\langle H, v\rangle$ is a map of degree at least 2 between curves of the same genus $g(Y) \geq 2$ (as J^H is contained in the image of the Jacobian of $X/\langle H, v\rangle$), which is impossible by the Riemann-Hurwitz formula. Hence $G = H$ and $uHu^{-1} \subseteq H$.

Suppose now that b) holds, and let δ be the non-trivial element of H. The automorphism u preserves every isotypic component B of $J_\Delta(N)_{\overline{\mathbb{Q}}}$. If B is not contained in S, then B is contained in J^H or in A, and δ acts on B as 1 or -1, respectively, and so does $u\delta u^{-1}$. Hence $u\delta u^{-1}\delta^{-1}$ acts trivially on an abelian subvariety of dimension $g_\Delta - \dim S > (g_\Delta + 1)/2$, so it is trivial by Lemma 3.3.

In both cases H is normal, so u induces an automorphism $\overline{u}$ of Y. Suppose that $\overline{u}$ is modular. Then $\overline{u}$ maps cusps to cusps and preserves the orders of elliptic points of Y, and hence u maps cusps to cusps. For a non-cuspidal point P of X with image $\overline{P}$ in Y we have $e(P) = e(\overline{P})/\#\mathrm{Stab}_H(P)$, and $\#\mathrm{Stab}_H(uP) = \#\mathrm{Stab}_H(P)$ as $uHu^{-1} = H$. Hence u preserves the orders of the elliptic points of X, and we conclude as in the proof of Theorem 5.6 that u is modular. □

We verify the conditions of Lemma 8.2 as follows. The number $a_p(f)^2/\chi_f(p)$ does not change if we replace f by a twist, and it is replaced by its conjugate if we replace f by a Galois conjugate. Hence, if the $\mathbb{Q}$-characteristic polynomials of $\langle p\rangle^{-1}T_p^2$ on J^H and on A are coprime for some prime $p \nmid N$, then by [36] J^H and A have no common isogeny factor without CM. This does not exclude common CM factors, as two CM newforms with the same CM field always give isogenous factors over $\overline{\mathbb{Q}}$, even if their Hecke eigenvalues at a prime split in the CM field are different. Hence, for each imaginary quadratic field F whose

discriminant divides N, we also compute an upper bound for the dimension of the part with CM by F of J^H and of A, as in Section 7. If no field F occurs on both sides, condition a) holds.

We compute that the 12 curves in Table 1 marked with a letter satisfy the corresponding condition of Lemma 8.2 for the indicated Δ' (see `recheck_c4.m`). For $N = 128$ and $N = 144$ both sides have CM by $\mathbb{Q}(i)$ and by $\mathbb{Q}(\sqrt{-3})$, respectively, and we use b). As the parts of J^H and A without CM have no common isogeny factor, S is contained in the part with CM by this field, which gives $\dim S \le 7$ and $\dim S \le 8$, while $g_\Delta = 17$ and $g_\Delta = 25$, respectively. In all cases the automorphisms of $X_{\Delta'}(N)$ are modular, either by [25] (when $X_{\Delta'}(N) = X_0(N)$) or by the scan (for $N = 75$).

9. The exceptional curves

By Sections 7 and 8, all the automorphisms of the curves $X_\Delta(N)$ with $g_\Delta \ge 2$ are modular, except possibly for the curves in Theorem 1.1. The curves $X_0(37)$, $X_0(63)$ and $X_0(108)$ have non-modular automorphisms by [34, 16, 18], and $X_{\Delta_{37}}(37)$ by [23, Theorem 4.4] (see also Section 8.1). It remains to deal with $X_{\Delta_{63}}(63)$.

Proposition 9.1. *Let $X = X_{\Delta_{63}}(63)$ and $Y = X_0(63)$, and let δ be the non-trivial diamond operator on X. Then X has genus 9, the map $X \to Y$ is étale, δ is central in $\mathrm{Aut}(X_{\overline{\mathbb{Q}}})$, and $\mathrm{Aut}(X_{\overline{\mathbb{Q}}})/\langle\delta\rangle \simeq \mathrm{Aut}(Y_{\overline{\mathbb{Q}}}) \simeq S_4 \times \mathbb{Z}/2\mathbb{Z}$. In particular $\#\mathrm{Aut}(X_{\overline{\mathbb{Q}}}) = 96$, and exactly 48 of these automorphisms are modular.*

Proof. We have $g(X) = 9$ and $g(Y) = 5$, so $X \to Y$ is étale by the Riemann-Hurwitz formula. We compute that $J_0(63)$ and the part A of $J_\Delta(63)$ corresponding to the quadratic character of conductor 21 satisfy condition a) of Lemma 8.2 (with $\Delta' = (\mathbb{Z}/63\mathbb{Z})^\times$), so δ is central and $\mathrm{Aut}(X_{\overline{\mathbb{Q}}})/\langle\delta\rangle$ embeds into $\mathrm{Aut}(Y_{\overline{\mathbb{Q}}})$, which has order 48 by [16]. This gives $\#\mathrm{Aut}(X_{\overline{\mathbb{Q}}}) \le 96$.

For the lower bound, we need to show that every automorphism of Y lifts to X. The cover $X \to Y$ corresponds to a non-zero element $\eta \in J_0(63)[2]$, and an automorphism a of $Y_{\overline{\mathbb{Q}}}$ lifts to $X_{\overline{\mathbb{Q}}}$ if and only if $a^*\eta = \eta$. We compute the canonical models of X and Y over $\mathbb{F}_{127^2}$ and find that $\#\mathrm{Aut}(X_{\overline{\mathbb{F}}_{127}}) = 96$, that the reduction of δ is central in $\mathrm{Aut}(X_{\overline{\mathbb{F}}_{127}})$ and that $\#\mathrm{Aut}(Y_{\overline{\mathbb{F}}_{127}}) = 48$, where by the method of Section 8.1 all the geometric automorphisms are defined over $\mathbb{F}_{127^2}$ (see `review_xdelta63.m` and `review_frobenius_fields.m`). It follows that every automorphism of $Y_{\overline{\mathbb{F}}_{127}}$ lifts to $X_{\overline{\mathbb{F}}_{127}}$, i.e. fixes the reduction $\overline{\eta}$ of η. The reduction map $\mathrm{Aut}(Y_{\overline{\mathbb{Q}}}) \to \mathrm{Aut}(Y_{\overline{\mathbb{F}}_{127}})$ is injective, hence bijective, and reduction is injective on $J_0(63)[2]$ and compatible with the action of automorphisms. Hence $a^*\eta = \eta$ for all $a \in \mathrm{Aut}(Y_{\overline{\mathbb{Q}}})$, and every automorphism of Y has exactly 2 lifts to X.

Finally, 48 of the automorphisms of X are modular, as we find 48 distinct cosets of explicit matrices normalizing $\Gamma_{\Delta_{63}}(63)$ (see `normalizer.m`). Conversely, a modular automorphism of X descends to a modular, hence cusp-preserving, automorphism of Y, and exactly 24 automorphisms of Y preserve the set of cusps (see `x063.m`). As each of them has 2 lifts, there are at most 48 modular automorphisms of X. □

Remark 9.2. If an automorphism $\overline{u}$ of $X_0(N)$ lifts to an automorphism u of $X_\Delta(N)$, then u normalizes the group of diamond operators, so if u is modular, then so is $\overline{u}$ (as $\overline{\Gamma}_0(N)$ consists of the elements of $\mathcal{N}(\Gamma_\Delta(N))$ that induce diamond operators). Hence, by Theorem 1.1, the non-modular automorphisms of $X_0(63)$ lift to no curve $X_\Delta(63)$ other than $X_{\Delta_{63}}(63)$, and those of $X_0(108)$ lift to no curve $X_\Delta(108)$ with $\Delta \ne (\mathbb{Z}/108\mathbb{Z})^\times$.

Remark 9.3. The argument of [30] for square-free N contains the following errors, which we found by checking it against the computations of Section 8. In the treatment of $N = 37$, it is claimed that the class of the divisor $(0_i) - (0_1)$ of two cusps on $X_{\Delta_{37}}(37)$ has order 7 in $J_{\Delta_{37}}(37)(\mathbb{Q})$. We compute, by reduction modulo $3, 5, 7, 11$ and 13, that it has order 21, and the claimed contradiction disappears. This is consistent with the existence of the non-modular automorphisms of $X_{\Delta_{37}}(37)$ found in [23]. Furthermore, the group generated by the diamond operators and the Atkin-Lehner involutions w_p, $p \mid N$, which is used throughout [30], is not a subgroup of $\mathrm{Aut}(X_\Delta(N))$ when some w_p does not normalize $\Gamma_\Delta(N)$ (the same problem in [20] was pointed out in [22, Remark 2.4]). For square-free $N \leq 70$ this first happens for $N = 65$ (see also [23, Example 1.5]).

Proof of Theorem 1.1, Corollary 1.2 and Corollary 1.3. Theorem 1.1 follows from Sections 7 and 8 and Proposition 9.1. By Theorem 1.1, every automorphism of $X_1(N)$ is modular, i.e. $\mathrm{Aut}(X_1(N)_{\overline{\mathbb{Q}}}) \simeq \mathcal{N}(\Gamma_1(N))/\overline{\Gamma}_1(N)$. For $\Delta = \{\pm 1\}$ and $N \neq 4$ we have $h'_\Delta = 1$ (see the paragraph after Theorem 10.6), and $\iota_Q(\Delta) = \Delta$ for all $Q \parallel N$. Hence, by Theorem 10.6, the normalizer of $\Gamma_1(N)$ in $\mathrm{PSL}_2(\mathbb{R})$ is generated by $\Gamma_0(N)$ and the Atkin-Lehner matrices, as was proved in [26, 28]. This proves Corollary 1.2, as $\Gamma_0(N)/\pm\Gamma_1(N)$ has order $\varphi(N)/2$ and the Atkin-Lehner matrices generate a group of order $2^{\omega(N)}$ modulo $\Gamma_0(N)$. Corollary 1.3 follows directly from Theorem 1.1. □

10. The order of the automorphism group

If $g_\Delta \geq 2$ and $X_\Delta(N)$ is not one of the five curves of Theorem 1.1, then all the automorphisms of $X_\Delta(N)$ are modular by Theorem 1.1, so

$$\#\,\mathrm{Aut}(X_\Delta(N)_{\overline{\mathbb{Q}}}) = [\mathcal{N}(\Gamma_\Delta(N)) : \overline{\Gamma}_\Delta(N)].$$

For $X_1(N)$ this index is given by Corollary 1.2. The five curves of Theorem 1.1, in the order in which they are listed there, have 4, 48, 216, 12 and 96 automorphisms, of which 2, 24, 108, 6 and 48 are modular. We now determine the index for every Δ.

Let ε_Δ be the greatest common divisor of N and of the integers $d^2 - 1$ with $d \bmod N \in \Delta$, and let

$$h_\Delta = \prod_{p \mid N} p^{\min\{v_p(\varepsilon_\Delta), \lfloor v_p(N)/2 \rfloor\}}, \qquad n_\Delta = \frac{N}{h_\Delta^2}.$$

Let $h(N)$ be the largest divisor of 24 whose square divides N. Every unit modulo a divisor of 24 squares to 1, so $\gcd(N, 24)$ divides ε_Δ, and hence $h(N)$ divides h_Δ. One easily checks that $h_\Delta = h(N)$ unless one of the following holds:

i) $p^2 \mid N$ and $d \equiv \pm 1 \pmod{p}$ for all $d \in \Delta$, for some prime $p \geq 5$,
ii) $3^4 \mid N$ and $d \equiv \pm 1 \pmod{9}$ for all $d \in \Delta$,
iii) $2^8 \mid N$ and $d \equiv \pm 1 \pmod{8}$ for all $d \in \Delta$.

We first compute the $\mathbb{Z}$-span of $\Gamma_\Delta(N)$. We denote by E_{ij} the matrix units in $M_2(\mathbb{Z})$.

Lemma 10.1. *Let $L \subseteq M_2(\mathbb{Z})$ be the $\mathbb{Z}$-span of $\Gamma_\Delta(N)$. Then*

$$L = \mathbb{Z} + \mathbb{Z}E_{12} + N\mathbb{Z}E_{21} + \varepsilon_\Delta\mathbb{Z}E_{22}.$$

Every $g \in \mathrm{SL}_2(\mathbb{R})$ which normalizes $\Gamma_\Delta(N)$ is of the form $g = \lambda A$ with $\lambda \in \mathbb{R}^\times$ and $A \in M_2(\mathbb{Z})$ primitive, and then $ALA^{-1} = L$.

Proof. As $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $U = \begin{pmatrix} 1 & 0 \\ N & 1 \end{pmatrix}$ lie in $\Gamma_\Delta(N)$, the span L contains $E_{12} = T - 1$, $NE_{21} = U - 1$, $NE_{11} = (T-1)(U-1)$ and $NE_{22} = N - NE_{11}$. For $\gamma = \begin{pmatrix} x & y \\ Nz & t \end{pmatrix} \in \Gamma_\Delta(N)$ it also contains $\gamma - x - yE_{12} - zNE_{21} = (t-x)E_{22}$, where $t - x \equiv t^{-1}(t^2 - 1) \pmod N$. As $x \equiv t^{-1} \equiv t \pmod{\varepsilon_\Delta}$ for all such γ, the first claim follows.

Let $g \in \mathrm{SL}_2(\mathbb{R})$ normalize $\Gamma_\Delta(N)$. Then $gLg^{-1} = L$, and the entries of $gE_{12}g^{-1}$, $g(NE_{21})g^{-1}$ and $g(NE_{11})g^{-1}$ show that $Nxy \in \mathbb{Z}$ for any two entries x, y of g. Hence $g = \lambda A$ with $\lambda \in \mathbb{R}^\times$ and $A \in M_2(\mathbb{Z})$ primitive, and $ALA^{-1} = gLg^{-1} = L$. □

Let p be a prime. We use the tree of $\mathrm{PGL}_2(\mathbb{Q}_p)$ [39, Chapter II, Section 1], whose vertices are the classes $[\Lambda]$ of $\mathbb{Z}_p$-lattices $\Lambda \subset \mathbb{Q}_p^2$ up to multiplication by $\mathbb{Q}_p^\times$, and on which $\mathrm{GL}_2(\mathbb{Q}_p)$ acts by isometries. The vertices $e_s = [\mathbb{Z}_p \oplus p^s\mathbb{Z}_p]$, $s \in \mathbb{Z}$, form a line. Every vertex x has a unique closest vertex $e_{F(x)}$ on this line, and we denote by $i(x)$ the distance between them. Then $d(x, e_s) = i(x) + |F(x) - s|$. A vertex x with $i(x) = i \geq 1$ and $F(x) = F$ is the class of $g_x\mathbb{Z}_p^2$ for a matrix $g_x = \begin{pmatrix} p^{i-F} & u \\ 0 & 1 \end{pmatrix}$ with $v_p(u) = -F$.

Lemma 10.2. *Let p be a prime and let $0 \leq j \leq \nu$ be integers. Put $k = \min\{j, \lfloor \nu/2 \rfloor\}$ and*

$$L_p = \mathbb{Z}_p + \mathbb{Z}_pE_{12} + p^\nu\mathbb{Z}_pE_{21} + p^j\mathbb{Z}_pE_{22}.$$

Let $\mathcal{X}$ be the set of vertices $[\Lambda]$ with $L_p\Lambda \subseteq \Lambda$, and let $\mathcal{C}$ be the set of vertices x such that all the vertices at distance at most k from x lie in $\mathcal{X}$. Then $\mathcal{C} = \{e_s : k \leq s \leq \nu - k\}$.

Proof. Computing $g_x^{-1}Yg_x$ for $Y = E_{12}, p^\nu E_{21}, p^j E_{22}$ shows that

$$\mathcal{X} = \{x : 0 \leq F(x) \leq \nu \text{ and } i(x) \leq \min\{j, F(x), \nu - F(x)\}\}.$$

If $k \leq s \leq \nu - k$ and $d(y, e_s) \leq k$, then $i(y) + |F(y) - s| \leq k \leq j$, which implies $y \in \mathcal{X}$, so $e_s \in \mathcal{C}$. If $s < k$ or $s > \nu - k$, then e_s is at distance at most k from $e_{-1} \notin \mathcal{X}$ or from $e_{\nu+1} \notin \mathcal{X}$. If $x \in \mathcal{X}$ and $i(x) \geq 1$, let $m = \min\{j, F(x), \nu - F(x)\}$. Then $m \leq k$, and a vertex y with $F(y) = F(x)$ and $i(y) = m + 1$ on a ray from $e_{F(x)}$ through x is not in $\mathcal{X}$ and satisfies $d(x, y) = m + 1 - i(x) \leq k$, so $x \notin \mathcal{C}$. □

Proposition 10.3. *Every element of $\mathcal{N}(\Gamma_\Delta(N))$ is the image of a matrix*

$$\frac{1}{\sqrt{e}} \begin{pmatrix} ae & b/h_\Delta \\ Nc/h_\Delta & de \end{pmatrix} \quad \text{with } a, b, c, d \in \mathbb{Z},\ e \parallel n_\Delta \text{ and } ade^2 - bcn_\Delta = e.$$

For $\Delta = (\mathbb{Z}/N\mathbb{Z})^\times$ this is one half of Newman's description of the normalizer of $\Gamma_0(N)$ (see [2]). For the groups generated by $\Gamma_0(N)$ and some Atkin-Lehner involutions, which contain $\Gamma_0(N)$, the normalizers were determined by Bars and Dalal [5] when $4 \nmid N$ and $9 \nmid N$.

Proof. Let $g \in \mathrm{SL}_2(\mathbb{R})$ normalize $\Gamma_\Delta(N)$, and let L be the $\mathbb{Z}$-span of $\Gamma_\Delta(N)$. By Lemma 10.1, $g = \lambda A$ with $\lambda \in \mathbb{R}^\times$ and $A \in M_2(\mathbb{Z})$ primitive such that $ALA^{-1} = L$. Fix a prime p and put $\nu = v_p(N)$, $j = v_p(\varepsilon_\Delta)$ and $k = \min\{j, \lfloor \nu/2 \rfloor\} = v_p(h_\Delta)$. As $\varepsilon_\Delta \mid N$, we have $j \leq \nu$, and $L \otimes \mathbb{Z}_p$ is the ring L_p of Lemma 10.2. Hence $AL_pA^{-1} = L_p$, so A preserves the set $\mathcal{X}$ of Lemma 10.2, and hence the set $\mathcal{C}$ and the set $\{e_k, e_{\nu-k}\}$ of the endpoints of $\mathcal{C}$.

Let $D = \begin{pmatrix} h_\Delta & 0 \\ 0 & 1 \end{pmatrix}$ and $B = DAD^{-1}$. As D maps e_s to e_{s-k}, the matrix B preserves $\{e_0, e_{\nu-2k}\}$. If B fixes e_0, then we may rescale B to lie in $\mathrm{GL}_2(\mathbb{Z}_p)$, and as B also fixes

$e_{\nu-2k}$, its lower left entry is then divisible by $p^{\nu-2k}$. Otherwise $w^{-1}B$ fixes e_0 and $e_{\nu-2k}$, where $w = \begin{pmatrix} 0 & -1 \\ p^{\nu-2k} & 0 \end{pmatrix}$ interchanges these two vertices.

Let B_0 be the primitive integral multiple of B with positive determinant e. By the above, for every prime p either $p \nmid e$ and $p^{v_p(n_\Delta)}$ divides the lower left entry of B_0, or $v_p(e) = v_p(n_\Delta)$ and $p^{v_p(n_\Delta)}$ divides the lower left entry and both diagonal entries of B_0. Hence $e \parallel n_\Delta$ and $B_0 = \begin{pmatrix} ae & b \\ n_\Delta c & de \end{pmatrix}$ with $ade^2 - bcn_\Delta = e$, and $g = \pm e^{-1/2} D^{-1} B_0 D$ is of the stated form. □

We will use the following conjugation formulas in the proofs of Corollary 10.5 and Theorem 10.6.

Lemma 10.4. *Let h and n be positive integers, let $Q \parallel n$, and let $W = \begin{pmatrix} QA & B \\ nC & QE \end{pmatrix}$ be an integral matrix with $\det W = Q$. Let $x = \begin{pmatrix} a & h\beta \\ hn\gamma & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ with $\beta, \gamma \in \mathbb{Z}$ and $a \equiv d \pmod h$, and let y_{ij} be the entries of $y = WxW^{-1}$. Then*

$$\begin{aligned} y_{12} &= AB(d-a) + h\left(QA^2\beta - \tfrac{n}{Q}B^2\gamma\right), \\ y_{21} &= nCE(a-d) + hn\left(QE^2\gamma - \tfrac{n}{Q}C^2\beta\right), \\ y_{22} &= d + \tfrac{n}{Q}BC(d-a) + hn(AC\beta - BE\gamma). \end{aligned}$$

In particular $y \in \mathrm{SL}_2(\mathbb{Z})$, $h \mid y_{12}$ and $hn \mid y_{21}$. For every prime p we have $y_{22} \equiv d \pmod{p^{v_p(hn)}}$ if $p \nmid Q$, and $y_{22} \equiv a \pmod{p^{v_p(hn)}}$ if $p \mid Q$.

Proof. The formulas follow from a direct computation, using $W^{-1} = Q^{-1}\begin{pmatrix} QE & -B \\ -nC & QA \end{pmatrix}$ and $QAE - \frac{n}{Q}BC = 1$. They show that y_{12}, y_{21} and y_{22} are integers, and so is $y_{11} = a + d - y_{22}$. Let p be a prime and $m = v_p(hn)$. If $p \nmid Q$, then $v_p(n/Q) = v_p(n)$, and as $h \mid d - a$, we obtain $y_{22} \equiv d \pmod{p^m}$. If $p \mid Q$, then $v_p(Q) = v_p(n)$, and as $\frac{n}{Q}BC = QAE - 1$, we obtain $y_{22} \equiv a + QAE(d-a) \equiv a \pmod{p^m}$. □

Corollary 10.5. *Suppose that $g_\Delta \geq 2$, that $X_\Delta(N)$ is not one of the curves of Theorem 1.1 and that $h_\Delta = h(N)$. Then $\mathcal{N}(\Gamma_\Delta(N))$ is contained in the normalizer of $\Gamma_0(N)$, and*

$$\#\operatorname{Aut}(X_\Delta(N)_{\overline{\mathbb{Q}}}) = i_\Delta \cdot s_\Delta,$$

where s_Δ is the number of elements of $\mathcal{N}(\Gamma_0(N))/\overline{\Gamma}_0(N)$ that normalize $\overline{\Gamma}_\Delta(N)$. If in addition $4 \nmid N$ and $9 \nmid N$, then s_Δ is the number of $Q \parallel N$ such that $\iota_Q(\Delta) = \Delta$, where ι_Q is the automorphism of $(\mathbb{Z}/N\mathbb{Z})^\times$ such that $\iota_Q(d) \equiv d^{-1} \pmod Q$ and $\iota_Q(d) \equiv d \pmod{N/Q}$.

Proof. Put $H = h_\Delta$ and $D = \begin{pmatrix} H & 0 \\ 0 & 1 \end{pmatrix}$. By Proposition 10.3, every element of $\mathcal{N}(\Gamma_\Delta(N))$ is the image of $\frac{1}{\sqrt{e}}D^{-1}WD$ for an integral matrix $W = \begin{pmatrix} eA & B \\ n_\Delta C & eE \end{pmatrix}$ with $e \parallel n_\Delta$ and $\det W = e$. Let $\gamma = \begin{pmatrix} x & y \\ Nz & t \end{pmatrix} \in \Gamma_0(N)$. As $H = h(N)$ divides 24, we have $t^2 \equiv 1 \pmod H$, and as $xt \equiv 1 \pmod N$, it follows that $x \equiv t \pmod H$. As $N = H^2 n_\Delta$, we may apply Lemma 10.4 to W and $D\gamma D^{-1} = \begin{pmatrix} x & Hy \\ Hn_\Delta z & t \end{pmatrix}$, with $h = H$, $n = n_\Delta$ and $Q = e$.

It shows that $WD\gamma D^{-1}W^{-1}$ lies in $\mathrm{SL}_2(\mathbb{Z})$, and that its upper right entry is divisible by H and its lower left entry by N/H. Hence $D^{-1}WD\gamma D^{-1}W^{-1}D \in \Gamma_0(N)$, so $\mathcal{N}(\Gamma_\Delta(N))$ is contained in $\mathcal{N}(\Gamma_0(N))$. As $\Gamma_\Delta(N)$ is a normal subgroup of $\Gamma_0(N)$ of index i_Δ, the formula for $\#\operatorname{Aut}(X_\Delta(N)_{\overline{\mathbb{Q}}})$ follows from Theorem 1.1.

If $4 \nmid N$ and $9 \nmid N$, then $H = h(N) = 1$ and $n_\Delta = N$, so every element of $\mathcal{N}(\Gamma_\Delta(N))$ which is not in $\overline{\Gamma}_0(N)$ is the image of $\frac{1}{\sqrt{Q}}W$ for an integral matrix $W = \begin{pmatrix} QA & B \\ NC & QE \end{pmatrix}$ with $Q \parallel N$, $Q > 1$ and $\det W = Q$, and the matrices of this form with the same Q lie in the same coset of $\overline{\Gamma}_0(N)$. For γ as above, Lemma 10.4 with $h = 1$ and $n = N$ shows that the lower right entry of $W\gamma W^{-1}$ is congruent to $x \equiv t^{-1}$ modulo Q and to t modulo N/Q, so $W\Gamma_\Delta(N)W^{-1} = \Gamma_{\iota_Q(\Delta)}(N)$ (see also [23, Lemma 1.3]). This proves the last claim. □

For general Δ we need a refinement of h_Δ. For a positive integer h with $h^2 \mid N$ let U_h be the kernel of the reduction map $(\mathbb{Z}/N\mathbb{Z})^\times \to (\mathbb{Z}/(N/h)\mathbb{Z})^\times$. As N/h is divisible by every prime divisor of N, the group U_h has order h, and by the Chinese remainder theorem $U_{h_1}U_{h_2} = U_{\mathrm{lcm}(h_1,h_2)}$. Let h'_Δ be the largest positive integer h such that

$$h^2 \mid N, \qquad d^2 \equiv 1 \pmod{h} \text{ for all } d \in \Delta \qquad \text{and} \qquad U_h \subseteq \Delta.$$

The set of such h contains 1 and is closed under taking least common multiples, so every such h divides h'_Δ. Note that h'_Δ divides h_Δ, as $h'_\Delta \mid \varepsilon_\Delta$ and $(h'_\Delta)^2 \mid N$. Put $n'_\Delta = N/(h'_\Delta)^2$ and let $\overline{\Delta}$ be the image of Δ in $(\mathbb{Z}/(N/h'_\Delta)\mathbb{Z})^\times$. For $Q \parallel n'_\Delta$ let ι_Q be the automorphism of $(\mathbb{Z}/(N/h'_\Delta)\mathbb{Z})^\times$ such that $\iota_Q(d) \equiv d^{-1} \pmod{p^{v_p(N/h'_\Delta)}}$ for the primes $p \mid Q$ and $\iota_Q(d) \equiv d \pmod{p^{v_p(N/h'_\Delta)}}$ for the other primes p. If $h'_\Delta = 1$, this is the automorphism ι_Q of Corollary 10.5.

For a positive integer n let $\Gamma_0(n)^+$ be the group generated by $\Gamma_0(n)$ and its Atkin-Lehner matrices. Zemel [42, Corollary 2.6] showed that $\mathcal{N}(\Gamma_\Delta(N))$ is contained in a group $\Gamma_0^{*,\sigma}(N)$, where σ is the integer h'_Δ (his σ_H for $H = \Delta$), and by [42, Remark 1.10] this group is $D'^{-1}\Gamma_0(n'_\Delta)^+D'$, with D' as in the theorem below. He also described $\mathcal{N}(\Gamma_\Delta(N))$ as the set of elements of this group that satisfy a congruence condition. The following theorem makes this condition explicit and gives the index. For completeness we give a short proof, which uses Proposition 10.3 and Lemma 10.4.

Theorem 10.6. *Let $D' = \begin{pmatrix} h'_\Delta & 0 \\ 0 & 1 \end{pmatrix}$ and let S_Δ be the set of $Q \parallel n'_\Delta$ such that $\iota_Q(\overline{\Delta}) = \overline{\Delta}$. Then $\mathcal{N}(\Gamma_\Delta(N))$ is the image in $\mathrm{PSL}_2(\mathbb{R})$ of the matrices $\frac{1}{\sqrt{Q}}D'^{-1}WD'$ with*

$$W = \begin{pmatrix} Qa & b \\ n'_\Delta c & Qd \end{pmatrix}, \quad a, b, c, d \in \mathbb{Z},\ Q \in S_\Delta \text{ and } adQ^2 - bcn'_\Delta = Q.$$

In particular

$$[\mathcal{N}(\Gamma_\Delta(N)) : \overline{\Gamma}_\Delta(N)] = i_\Delta \cdot \frac{\psi(N)}{\psi(n'_\Delta)} \cdot \#S_\Delta,$$

where $\psi(m) = m\prod_{p\mid m}(1 + 1/p)$ is the index of $\Gamma_0(m)$ in $\mathrm{SL}_2(\mathbb{Z})$.

Proof. Write $h = h'_\Delta$ and $n = n'_\Delta$, so $N = h^2n$, and let $\Gamma' = D'\Gamma_\Delta(N)D'^{-1}$. Then Γ' consists of the matrices

$$x = \begin{pmatrix} a & h\beta \\ hn\gamma & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \quad \text{with } d \bmod N \in \Delta.$$

For such x we have $ad \equiv 1 \pmod{N}$, and as $d^2 \equiv 1 \pmod{h}$, it follows that $a \equiv d \pmod{h}$.

Let $W = \begin{pmatrix} QA & B \\ nC & QE \end{pmatrix}$ be an integral matrix with $Q \parallel n$ and $\det W = Q$, and let $y = WxW^{-1}$. By Lemma 10.4, $y \in \mathrm{SL}_2(\mathbb{Z})$, $h \mid y_{12}$ and $hn \mid y_{21}$, and as $hn = N/h$ and $a \equiv d^{-1} \pmod{N}$, we have $y_{22} \equiv \iota_Q(d) \pmod{N/h}$. As $U_h \subseteq \Delta$, a unit modulo N lies in Δ if and only if its reduction modulo N/h lies in $\overline{\Delta}$, so $y \in \Gamma'$ if and only if $\iota_Q(d) \in \overline{\Delta}$. When x runs over Γ', d mod N runs over all of Δ, and hence $W\Gamma'W^{-1} \subseteq \Gamma'$ if and only if $Q \in S_\Delta$. The same holds for W^{-1}, which is a multiple of a matrix of the same form with the same Q. This proves that the matrices of the theorem normalize $\Gamma_\Delta(N)$, and that $\frac{1}{\sqrt{Q}} D'^{-1} W D'$ does not normalize $\Gamma_\Delta(N)$ if $Q \notin S_\Delta$.

Now let $g \in \mathcal{N}(\Gamma_\Delta(N))$, and put $H = h_\Delta$ and $D = \begin{pmatrix} H & 0 \\ 0 & 1 \end{pmatrix}$. By Proposition 10.3, g is the image of $\frac{1}{\sqrt{e}} D^{-1} W D$ for an integral matrix $W = \begin{pmatrix} eA & B \\ n_\Delta C & eE \end{pmatrix}$ with $e \parallel n_\Delta$ and $\det W = e$. The matrix W normalizes $D\Gamma_\Delta(N)D^{-1}$, which contains $\begin{pmatrix} 1 & H\beta \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ (N/H)\gamma & 1 \end{pmatrix}$ for all $\beta, \gamma \in \mathbb{Z}$. The formula for y_{22} in Lemma 10.4, with H, n_Δ and e in place of h, n and Q, shows that $1 + (N/H)AC\beta$ and $1 - (N/H)BE\gamma$ lie in Δ for all $\beta, \gamma \in \mathbb{Z}$. As N/H is divisible by every prime divisor of N, it follows that $U_{h_1} \subseteq \Delta$ for $h_1 = H/\gcd(H, AC, BE)$. Since $H^2 \mid N$ and $H \mid \varepsilon_\Delta$, the integer h_1 satisfies the three conditions in the definition of h'_Δ, so $h_1 \mid h$, i.e. $t = H/h$ divides both AC and BE.

Let p be a prime divisor of t and $k = v_p(t)$. We use that $eAE - \frac{n_\Delta}{e} BC = 1$, as $\det W = e$. If $p \nmid AE$, then p^k divides B and C, and hence $p \nmid e$. If $p \mid AE$, then $p \nmid BC$, so p^k divides A and E, and $p \mid e$ or $p \nmid n_\Delta$, as otherwise p would divide both AE and $\frac{n_\Delta}{e}$, and hence 1. Let t_2 be the product of the $p^{v_p(t)}$ over the prime divisors p of t with $p \mid AE$, and put $Q' = t_2^2 e$. As $n = t^2 n_\Delta$, it follows that $Q' \parallel n$ and that

$$W' = t_2 \begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix}^{-1} W \begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} t_2 eA & t_2 B/t \\ t_2 t n_\Delta C & t_2 eE \end{pmatrix}$$

is an integral matrix of determinant Q', whose diagonal entries are divisible by Q' and whose lower left entry is divisible by n. As $D = \begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix} D'$, the element g is the image of $\frac{1}{\sqrt{Q'}} D'^{-1} W' D'$, and $Q' \in S_\Delta$ by the first part of the proof. This proves the first claim.

The matrices W of the theorem are primitive, as $Qad - \frac{n}{Q} bc = 1$, so Q is determined by the image of $\frac{1}{\sqrt{Q}} W$ in $\mathrm{PSL}_2(\mathbb{R})$. Such matrices exist for every $Q \parallel n$, as $\gcd(Q, n/Q) = 1$, and a direct computation shows that $W_1 W_2^{-1} \in \Gamma_0(n)$ if W_1 and W_2 have the same Q. Hence $\mathcal{N}(\Gamma_\Delta(N))$ contains $D'^{-1}\overline{\Gamma}_0(n)D'$ with index $\#S_\Delta$. The group $D'\Gamma_0(N)D'^{-1}$ consists of the matrices in $\mathrm{SL}_2(\mathbb{Z})$ whose upper right entry is divisible by h and whose lower left entry is divisible by hn, so it is contained in $\Gamma_0(n)$, and it has index $\psi(N)$ in $\mathrm{SL}_2(\mathbb{Z})$, as conjugation by D' preserves hyperbolic area. Hence $[D'^{-1}\Gamma_0(n)D' : \Gamma_0(N)] = \psi(N)/\psi(n)$, and as $[\Gamma_0(N) : \Gamma_\Delta(N)] = i_\Delta$, the formula for the index follows. □

For $\Delta = (\mathbb{Z}/N\mathbb{Z})^\times$ we have $h'_\Delta = h(N)$ and S_Δ consists of all $Q \parallel n'_\Delta$, and Theorem 10.6 is Newman's description of the normalizer of $\Gamma_0(N)$ (see [2]). For $\Delta = \{\pm 1\}$ and $N \neq 4$ we have $h'_\Delta = 1$, as U_h has order h and $U_2 = \{1, 1 + N/2\}$ is contained in $\{\pm 1\}$ only for $N = 4$, and Theorem 10.6 is the description of the normalizer of $\Gamma_1(N)$ from [26, 28]. Zemel

[42, Theorems 3.1 and 3.8] determined the normalizers explicitly when Δ is the kernel of the reduction map $(\mathbb{Z}/N\mathbb{Z})^\times \to (\mathbb{Z}/N_0\mathbb{Z})^\times$ for some $N_0 \mid N$, and when Δ is the m-torsion subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times$. Note that $\mathcal{N}(\Gamma_\Delta(N))$ is contained in the normalizer of $\Gamma_0(N)$ if $h_\Delta = h(N)$ (Corollary 10.5), but not in general.

Corollary 10.7. *Suppose that $g_\Delta \geq 2$ and that $X_\Delta(N)$ is not one of the curves of Theorem 1.1. Then*

$$\#\operatorname{Aut}(X_\Delta(N)_{\overline{\mathbb{Q}}}) = i_\Delta \cdot \frac{\psi(N)}{\psi(n'_\Delta)} \cdot \#S_\Delta.$$

Proof. This follows from Theorem 1.1 and Theorem 10.6. □

We have formalized Proposition 10.3 and the claims of Corollary 10.5 about $\mathcal{N}(\Gamma_\Delta(N))$ and its index in Lean 4 with Mathlib [33], as `newman_delta`, `normG_GammaDeltaR_le_Norm0`, `card_BG_GammaDeltaR` and `card_BG_GammaDeltaR_of_not_dvd`, and Theorem 10.6 as `mem_normG_GammaDeltaR_iff` and `card_BG_GammaDeltaR_hStar`, where h'_Δ is `hStar`. The formalization also proves that $\mathcal{N}(\Gamma_\Delta(N))$ is contained in the normalizer of $\Gamma_0(N)$ if and only if h'_Δ divides $h(N)$ (`normG_GammaDeltaR_le_Norm0_iff`). The formalization also contains the claim that $h_\Delta = h(N)$ unless one of i), ii) and iii) holds (`hDelta_eq_hPart_iff`), the description of the normalizer of $\Gamma_1(N)$ from [26, 28] together with the order $2^{\omega(N)}\varphi(N)/2$ of Corollary 1.2 (`normG_pmGamma1R` and `card_BG_pmGamma1R`), and the index for $X(M)$ used in Remark 10.8 (`card_BG_GammaDeltaR_sq`).

As a check of Theorem 10.6, we also computed the index directly. The matrices of Proposition 10.3 form the group $M_\Delta = D^{-1}\Gamma_0(n_\Delta)^+ D$, where $D = \begin{pmatrix} h_\Delta & 0 \\ 0 & 1 \end{pmatrix}$. Every element of M_Δ is a multiple of a primitive integral matrix whose determinant divides N (for the normalizer of any group Γ_H of level n, the analogous statement with n in place of N is [15, Proposition 4.3]), so every coset $\overline{\Gamma}_0(N)g$ in $\mathcal{N}(\Gamma_\Delta(N))$ contains a multiple of a matrix σH, where σ runs over a fixed set of representatives of $\Gamma_0(N)\backslash \mathrm{SL}_2(\mathbb{Z})$ and H over the matrices $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ with $ad \mid N$, $0 \leq b < d$ and $\gcd(a,b,d) = 1$ (that this computes the index is `relIndex_normG_eq_card_sigmaH` in [33]). We test all these matrices for the 4397 curves $X_\Delta(N)$ with $N \leq 400$ and $g_\Delta \geq 2$ (see `aut_orders.py`), and in all cases the index agrees with Theorem 10.6 (see `index_formula_check.py`) and every normalizing matrix σH has the form of Proposition 10.3. Among the 1449 curves with $N \leq 200$ there are 58 with $h_\Delta \neq h(N)$, and for 28 of them $\mathcal{N}(\Gamma_\Delta(N))$ is not contained in $\mathcal{N}(\Gamma_0(N))$. We list these 28 curves in Table 2. For the 30 curves of Table 1 whose automorphism groups we computed in Section 8.1, the two computations give the same number of modular automorphisms.

Remark 10.8. Many of the curves in Table 2 are of the form $X_1(M, N/M)$. If $M^2 \mid N$ and $\Delta = \{d : d \equiv \pm 1 \pmod{N/M}\}$, then conjugation by $\begin{pmatrix} M & 0 \\ 0 & 1 \end{pmatrix}$ maps $\Gamma_\Delta(N)$ to $\pm(\Gamma(M) \cap \Gamma_1(N/M))$, so $X_\Delta(N)$ is isomorphic to $X_1(M, N/M)$, and to $X(M)$ if $N = M^2$. In the latter case $h'_\Delta = M$ and $n'_\Delta = 1$, and Corollary 10.7 gives $\#\operatorname{Aut}(X(M)_{\overline{\mathbb{Q}}}) = i_\Delta\psi(M^2) = \#\mathrm{PSL}_2(\mathbb{Z}/M\mathbb{Z})$ for $M \geq 7$, which was proved by Bars, Kontogeorgis and Xarles [6, Theorem 4]. The curves $X_\Delta(49) \simeq X(7)$ and $X_\Delta(50) \simeq X_1(5, 10)$ of Remark 8.1 are the first two entries of Table 2.

11. Tables

In Table 1 we list the 42 curves $X_\Delta(N)$ with $\Delta \neq \{\pm 1\}, (\mathbb{Z}/N\mathbb{Z})^\times$, $N \leq 200$ and $g_\Delta \geq 2$ that do not satisfy any of the conditions of Proposition 4.1. The group Δ is generated by -1 and the elements listed in the second column. In the last column, a number m means that $X_\Delta(N)$ has m automorphisms, all of them modular, computed as in Section 8.1 (for $N = 37$ and $N = 63$ we write 12/6 and 96/48, as only half of the automorphisms are modular, see Section 8.1 and Proposition 9.1). An entry m, a) or m, b) means that we use the corresponding condition of Lemma 8.2, with $\Delta' = (\mathbb{Z}/N\mathbb{Z})^\times$, except for $N = 75$ (marked a)*), where $\Delta' = \langle \pm 1, 4, 26 \rangle$, and that $X_\Delta(N)$ has m automorphisms by Section 10.

Table 1. The intermediate curves with $N \leq 200$ not covered by Proposition 4.1

N	Δ	i_Δ	g_Δ		N	Δ	i_Δ	g_Δ	
21	13, 8	3	3	12	45	34, 44	2	5	48
24	17, 7	2	3	8	48	19, 47	2	7	32
24	23, 5	2	3	8	48	25, 17, 31	2	7	32
25	7	5	4	10	48	25, 47	4	13	64, a)
26	17	2	4	8	48	37, 47	2	5	96
26	21	3	4	12	49	27	3	3	168
28	13, 15	3	4	36	50	29	2	4	120
28	19	2	4	8	54	35	3	10	108
30	19, 11	2	5	16	56	31, 29	2	9	32
31	26	5	6	10	60	43, 11	2	15	16, a)
32	17, 31	4	5	32	63	59, 37	2	9	96/48
33	29	2	5	8	64	25, 63	2	5	192
36	17, 19	3	7	36	69	44	2	13	8, a)
36	23	2	3	48	72	23, 53	2	13	48, a)
37	8	3	4	12/6	72	47, 37	2	9	192
40	37, 31	2	7	8	72	47	4	25	96, a)
40	39, 21	4	9	64, a)	75	59	4	17	240, a)*
40	9, 21, 31	2	5	32	96	43, 95	2	17	128, a)
42	5	2	9	16	120	7, 71, 61	2	33	64, a)
44	7	2	8	8	128	25, 127	2	17	256, b)
					144	11, 71	2	25	576, b)
					192	91, 191	2	41	384, a)

In Table 2 we list the 28 curves $X_\Delta(N)$ with $N \leq 200$ and $g_\Delta \geq 2$ for which $\mathcal{N}(\Gamma_\Delta(N))$ is not contained in the normalizer of $\Gamma_0(N)$ (see Section 10). As before, Δ is generated by -1 and the elements listed in the second column. The column $i_\Delta s_\Delta$ gives the number of automorphisms induced by the normalizer of $\Gamma_0(N)$, in the notation of Corollary 10.5, and the last column gives $\#\operatorname{Aut}(X_\Delta(N)_{\overline{\mathbb{Q}}}) = [\mathcal{N}(\Gamma_\Delta(N)) : \overline{\Gamma}_\Delta(N)]$.

References

[1] D. Abramovich, *A linear lower bound on the gonality of modular curves*, Internat. Math. Res. Notices, (1996), pp. 1005–1011. 1, 4.2, 4

[2] M. Akbaş and D. Singerman, *The normalizer of* $\Gamma_0(N)$ *in* $\mathrm{PSL}(2,\mathbb{R})$, Glasgow Math. J., 32 (1990), pp. 317–327. 10, 10

TABLE 2. The curves with $N \leq 200$ whose normalizer is not contained in the normalizer of $\Gamma_0(N)$

N	Δ	i_Δ	g_Δ	$i_\Delta s_\Delta$	$\#\operatorname{Aut}$	N	Δ	i_Δ	g_Δ	$i_\Delta s_\Delta$	$\#\operatorname{Aut}$
49	27	3	3	6	168	150	29	4	73	32	480
50	29	2	4	8	120	162	17	3	46	108	648
75	4	2	9	8	120	169	12	6	50	12	1092
75	59	4	17	16	240	175	4	2	29	8	120
81	8	3	10	54	324	175	11	4	57	16	240
98	13	3	19	12	336	175	6	6	85	24	360
100	9	2	13	24	360	175	34	12	169	48	720
100	19	4	31	16	240	196	13	3	49	36	1008
121	10	5	26	10	660	196	27	6	109	24	672
125	4	2	16	4	100	200	9, 11	2	37	32	480
125	24	10	76	20	500	200	9	4	85	16	240
147	8	3	33	12	336	200	11	4	85	16	240
147	20	6	65	24	672	200	19	4	73	64	960
150	11	2	37	16	240	200	39	8	169	32	480

[3] F. BARS, *On quadratic points of classical modular curves*, in Number theory related to modular curves—Momose memorial volume, vol. 701 of Contemp. Math., Amer. Math. Soc., Providence, RI, 2018, pp. 17–34. We use the numbering of `https://arxiv.org/abs/1308.3267v2`. 1

[4] F. BARS AND T. DALAL, *On the automorphism group of quotient modular curves*, J. Algebra, 672 (2025), pp. 334–378. 1

[5] ———, *The modular automorphisms of quotient modular curves*, Mathematika, 72 (2026). `https://doi.org/10.1112/mtk.70065`. 1, 10

[6] F. BARS, A. KONTOGEORGIS, AND X. XARLES, *Bielliptic and hyperelliptic modular curves $X(N)$ and the group* $\operatorname{Aut}(X(N))$, Acta Arith., 161 (2013), pp. 283–299. We use the numbering of `https://arxiv.org/abs/1207.2273v2`. 10.8

[7] C. BIRKENHAKE AND H. LANGE, *Complex abelian varieties*, vol. 302 of Grundlehren der Mathematischen Wissenschaften, Springer-Verlag, Berlin, second ed., 2004. 4

[8] A. R. BOOKER, M. LEE, AND A. STRÖMBERGSSON, *Twist-minimal trace formulas and the Selberg eigenvalue conjecture*, J. Lond. Math. Soc. (2), 102 (2020), pp. 1067–1134. We use the numbering of `https://arxiv.org/abs/1803.06016v2`. 3

[9] W. BOSMA, J. CANNON, AND C. PLAYOUST, *The Magma algebra system. I. The user language*, J. Symbolic Comput., 24 (1997), pp. 235–265. 1, 2

[10] H. COHEN AND J. OESTERLÉ, *Dimensions des espaces de formes modulaires*, in Modular functions of one variable, VI, vol. 627 of Lecture Notes in Math., Springer, 1977, pp. 69–78. 6.2

[11] P. DELIGNE AND D. MUMFORD, *The irreducibility of the space of curves of given genus*, Inst. Hautes Études Sci. Publ. Math., (1969), pp. 75–109. 8.1

[12] F. DIAMOND AND J. SHURMAN, *A first course in modular forms*, vol. 228 of Graduate Texts in Mathematics, Springer-Verlag, New York, 2005. 3, 3, 6.2

[13] V. DOSE, *On the automorphisms of the nonsplit Cartan modular curves of prime level*, Nagoya Math. J., 224 (2016), pp. 74–92. 5

[14] V. DOSE, G. LIDO, AND P. MERCURI, *Automorphisms of Cartan modular curves of prime and composite level*, Algebra Number Theory, 16 (2022), pp. 1423–1461. We use the numbering of `https://arxiv.org/abs/2005.09009v2`. 1, 3, 4, 5, 6

[15] V. DOSE, G. M. LIDO, AND P. MERCURI, *Automorphisms of general modular curves*, 2026. preprint, `https://arxiv.org/abs/2610.08998v1`. 1, 1, 3, 4, 5, 10

[16] N. D. ELKIES, *The automorphism group of the modular curve $X_0(63)$*, Compositio Math., 74 (1990), pp. 203–208. 1, 1, 8, 9, 9

[17] ———, *The Klein quartic in number theory*, in The eightfold way, vol. 35 of Math. Sci. Res. Inst. Publ., Cambridge Univ. Press, Cambridge, 1999, pp. 51–101. 8.1
[18] M. Harrison, *A new automorphism of $X_0(108)$*, 2014. preprint, `https://arxiv.org/abs/1108.5595v3`. 1, 1, 8, 8.1, 9
[19] B.-H. Im, D. Jeon, and C. H. Kim, *Normalizers of intermediate congruence subgroups of the Hecke subgroups*, Open Math., 15 (2017), pp. 787–799. 1
[20] N. Ishii and F. Momose, *Hyperelliptic modular curves*, Tsukuba J. Math., 15 (1991), pp. 413–423. 1, 9.3
[21] D. Jeon, *Automorphism groups of hyperelliptic modular curves*, Proc. Japan Acad. Ser. A Math. Sci., 91 (2015), pp. 95–100. 1
[22] D. Jeon and C. H. Kim, *On the arithmetic of certain modular curves*, Acta Arith., 130 (2007), pp. 181–193. 1, 9.3
[23] D. Jeon, C. H. Kim, and A. Schweizer, *Bielliptic intermediate modular curves*, J. Pure Appl. Algebra, 224 (2020), pp. 272–299. 1, 1, 1, 2, 8.1, 9, 9.3, 10
[24] S. Kamienny, *On the automorphism groups of some modular curves*, Math. Proc. Cambridge Philos. Soc., 134 (2003), pp. 61–64. 1
[25] M. A. Kenku and F. Momose, *Automorphism groups of the modular curves $X_0(N)$*, Compositio Math., 65 (1988), pp. 51–80. 1, 1, 3, 6, 8, 8.2
[26] C. H. Kim and J. K. Koo, *The normalizer of $\Gamma_1(N)$ in $\mathrm{PSL}_2(\mathbb{R})$*, Comm. Algebra, 28 (2000), pp. 5303–5310. 1, 1, 1, 9, 10, 10
[27] D. Kohel, *Endomorphism rings of elliptic curves over finite fields*, PhD thesis, University of California, Berkeley, 1996. 5
[28] M.-L. Lang, *Normalizer of $\Gamma_1(m)$*, J. Number Theory, 86 (2001), pp. 50–60. 1, 1, 1, 9, 10, 10
[29] W. Luo, Z. Rudnick, and P. Sarnak, *On Selberg's eigenvalue conjecture*, Geom. Funct. Anal., 5 (1995), pp. 387–401. 4
[30] F. Momose, *Automorphism groups of the modular curves $X_1(N)$*. unpublished preprint. 1, 1, 1, 9.3
[31] ———, *On the l-adic representations attached to modular forms*, J. Fac. Sci. Univ. Tokyo Sect. IA Math., 28 (1981), pp. 89–109. 3
[32] D. Mumford, *Abelian varieties*, vol. 5 of Tata Institute of Fundamental Research Studies in Mathematics, Oxford University Press, 1970. 4
[33] F. Najman, *Normalizers of congruence subgroups in Lean 4*, 2026. `https://github.com/F-Najman/normalizer-lean`, revision `1f4c27e`. 1, 10
[34] A. P. Ogg, *Über die Automorphismengruppe von $X_0(N)$*, Math. Ann., 228 (1977), pp. 279–292. 1, 1, 8, 9
[35] K. A. Ribet, *Galois representations attached to eigenforms with Nebentypus*, in Modular functions of one variable, V, vol. 601 of Lecture Notes in Math., Springer, 1977, pp. 17–51. 6.1
[36] ———, *Twists of modular forms and endomorphisms of abelian varieties*, Math. Ann., 253 (1980), pp. 43–62. 8.2
[37] ———, *On l-adic representations attached to modular forms. II*, Glasgow Math. J., 27 (1985), pp. 185–194. 3
[38] B. Saint-Donat, *On Petri's analysis of the linear system of quadrics through a canonical curve*, Math. Ann., 206 (1973), pp. 157–175. 8.1
[39] J.-P. Serre, *Trees*, Springer-Verlag, Berlin-New York, 1980. 10
[40] A. V. Sutherland, *Isogeny volcanoes*, in ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium, vol. 1 of Open Book Ser., Math. Sci. Publ., Berkeley, CA, 2013, pp. 507–530. 5
[41] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math., 2 (1966), pp. 134–144. 8.1
[42] S. Zemel, *Normalizers of congruence groups in $\mathrm{SL}_2(\mathbb{R})$ and automorphisms of lattices*, Int. J. Number Theory, 13 (2017), pp. 1275–1300. We use the numbering of `https://arxiv.org/abs/1512.07547v2`. 1, 10, 10

University of Zagreb Faculty of Science, Department of Mathematics, Bijenička Cesta 30, 10000 Zagreb, Croatia
Email address: `fnajman@math.hr`