Chapter 3

Automorphisms of Cartan curves

This chapter is the result of a joint work with Valerio Dose and Pietro Mercuri

We study the automorphisms of modular curves associated to Cartan subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ and certain subgroups of their normalizers. We prove that if n is large enough, all the automorphisms are induced by the ramified covering of the complex upper half-plane. We get new results for non-split curves of prime level $p \geq 13$: the curve $X_{\mathrm{ns}}^{+}(p)$ has no non-trivial automorphisms, whereas the curve $X_{\mathrm{ns}}(p)$ has exactly one non-trivial automorphism. Moreover, as an immediate consequence of our results we compute the automorphism group of $X_0^*(n) := X_0(n)/W$, where W is the group generated by the Atkin-Lehner involutions of $X_0(n)$ and n is a large enough square.

3.1 Introduction

Since the 1970s many efforts have been made to determine automorphisms of modular curves and in particular to establish whether a modular curve has other automorphisms besides the expected ones. Indeed, infinitely many automorphisms naturally arise when the curve has genus zero or one. Moreover, since the components of modular curves over $\mathbb{C}$ can be seen as compactification of quotients of the complex upper half-plane $\mathbb{H}$, some automorphisms of $\mathbb{H}$ induce automorphisms of the quotient modular curve. Such automorphisms are called *modular* and their determination is a purely group theoretic problem.

The focus has been classically placed on the modular curves $X_0(n)$ associated to a Borel subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ (e.g., upper triangular matrices), with n a positive integer. For these curves, modular automorphisms played an important role in the development of the theory of modular curves. They were determined in the seminal paper [4], with a small gap which was later filled in a couple of different ways (see [2], [14]). Meanwhile, a complete picture about the remaining automorphisms of $X_0(n)$ has been painted through the decades by the works [83], [85], [60], [42], [52]. Also some works in this century (e.g., [5], [74], [47]) took on the case of the modular curves $X_0(p)/\langle w_p\rangle$ and $X_0(p^2)/\langle w_{p^2}\rangle$, where w_p and w_{p^2} are the Atkin-Lehner involutions of the respective modular curve.

More recently, great interest has been generated in modular curves associated to different subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, in particular to normalizers of Cartan subgroups for $n = p$ prime. This is mainly due to the fact that rational points on these curves help classifying rational elliptic curves whose associated Galois representation modulo p is not surjective. This is directly linked to a question formulated by Serre (also known as *uniformity conjecture*) in the 1970s ([92]). After the works [72], on the Borel case, and [17], [18], on the *split* Cartan case, the only part of this problem left to understand nowadays is equivalent to asking whether, for almost every prime p, the modular curve $X_{\mathrm{ns}}^+(p)$ associated to the normalizer of a *non-split* Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ has other rational points besides the expected ones, namely the CM points of class number one. Such equivalence led to a certain amount of research driven towards computing equations and finding rational points of modular curves associated to non-split Cartan subgroups and their normalizers (see for example [12], [13], [10], [35], [36], [75]).

A curious connection between the problem of determining rational points and the one of determining automorphisms in a modular curve is given by the fact that in the case of the Borel modular curves $X_0(p)$ of genus at least 2, the sole occurrence of unexpected rational points ($p = 37$) in the setting of Serre's uniformity conjecture, happens in the presence of an unexpected automorphism of the corresponding modular curve. A further connection is made in [37], where is proven that, for almost every prime p, the absence of unexpected rational points of the curve $X_{\mathrm{ns}}^+(p)$ implies the absence of unexpected rational automorphisms of the modular curve $X_{\mathrm{ns}}(p)$ associated to a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

The first work centered on automorphisms of non-split Cartan modular curves has been [35], in which the existence of an unexpected automorphism of $X_{\mathrm{ns}}(11)$ is proven. Some partial results on the automorphisms of $X_{\mathrm{ns}}(p)$ and $X_{\mathrm{ns}}^+(p)$, for almost every prime p, were proven in [37], while in [48] the full determination of the automorphism group is obtained for low primes ($p \leq 31$).

In the present work we complete the results in [37] about the prime level case. Moreover, we extend the analysis to every composite level n, where we can define Cartan subgroups of mixed split/non-split type. The scope of our study concerns Cartan subgroups and also a specific subgroup of their normalizer in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ which we call *Cartan-plus* subgroup. However, in most cases, for example when n is odd, a Cartan-plus subgroup actually coincides with the normalizer of the relative Cartan subgroup. We prove the following result:

Theorem 3.6.15. *Let $n \geq 10^{400}$ be an integer and let $H < \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be either a Cartan or a Cartan-plus subgroup. Then every automorphism of X_H is modular, hence we have*

$$\mathrm{Aut}(X_H) \cong \begin{cases} N'/H' \times \mathbb{Z}/2\mathbb{Z}, & \text{if } n \equiv 2 \bmod 4 \text{ and } H \text{ is a Cartan-plus split at } 2,\\ N'/H', & \text{otherwise,} \end{cases}$$

where $N' < \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ is the normalizer of $H' := H \cap \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$.

It may be interesting to note that the modular curve associated to a Cartan-plus subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ which is split at every prime dividing n is isomorphic to the modular curve $X_0^*(n^2) := X_0(n^2)/W$, where W is the group generated by Atkin-Lehner involutions of the Borel curve $X_0(n^2)$.

In the case $n = p^e$, where p is a prime number, we can refine the techniques developed and obtain a more complete result:

Theorem 3.6.17. *Let p be a prime number and let e be a positive integer. If $p^e > 11$ and $p^e \notin \{3^3, 2^4, 2^5, 2^6\}$, then all the automorphisms of $X_{\mathrm{ns}}(p^e), X_{\mathrm{ns}}^+(p^e), X_{\mathrm{s}}(p^e)$ and $X_{\mathrm{s}}^+(p^e)$ are modular and*

$$\mathrm{Aut}(X_{\mathrm{ns}}(p^e)) \cong \mathbb{Z}/2\mathbb{Z}, \qquad \mathrm{Aut}(X_{\mathrm{ns}}^+(p^e)) \cong \{1\},$$

$$\mathrm{Aut}(X_{\mathrm{s}}(p^e)) \cong \begin{cases} (\mathbb{Z}/8\mathbb{Z})^2 \rtimes (\mathbb{Z}/2\mathbb{Z}), & \text{if } p = 2,\\ \mathbb{Z}/3\mathbb{Z} \times S_3, & \text{if } p = 3,\\ \mathbb{Z}/2\mathbb{Z}, & \text{if } p > 3, \end{cases} \qquad \mathrm{Aut}(X_{\mathrm{s}}^+(p^e)) \cong \begin{cases} \mathbb{Z}/8\mathbb{Z}, & \text{if } p = 2,\\ \mathbb{Z}/3\mathbb{Z}, & \text{if } p = 3,\\ \{1\}, & \text{if } p > 3, \end{cases}$$

where the above semidirect product $(\mathbb{Z}/8\mathbb{Z})^2 \rtimes \mathbb{Z}/2\mathbb{Z}$ is described in Remark 3.6.16.

Corollary 3.6.18. *Let $p \geq 13$ be a prime number. Then the group of automorphisms of $X_{\mathrm{ns}}^+(p)$ is trivial and the group of automorphisms of $X_{\mathrm{ns}}(p)$ has order 2.*

The main technical novelty of our proofs is a thorough analysis of the action of Hecke operators on very general modular curves. This allows us to prove results about automorphisms without exploiting and worrying about the field of definition of the cusps and CM points which has been instead instrumental for determining automorphisms of modular curves throughout the literature in the past. We also give à la Chen results to describe jacobians of Cartan modular curves in terms of jacobians of Borel modular curves and we give an explicit upper bound on the dimension of the CM part of the jacobian of Borel modular curves. The structure of the paper is the following.

In Section 3.2 we define modular curves associated to general subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ and we give an equivalent condition to the fact that a point of a modular curves branches in the covering of the curve by $\mathbb{H}$.

In Section 3.3 we study the action of Hecke operators on modular curves. In particular we focus on the action on the cusps and the other points which could branch in the covering by $\mathbb{H}$. Such points are associated to elliptic curves with j-invariant equal to 0 or 1728.

In Section 3.4 we define Cartan and Cartan-plus subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ for every positive integer n. We also define the relative modular curves of composite level. Then we prove that the jacobian of a Cartan modular curve is a quotient of the jacobian of some Borel modular curve. When $n = p^e$, this is done applying the techniques of [26] and [39] to a previously unexplored case, and for n general we combine these results. We also extend the results of [26] to the case of even level.

In Section 3.5 we prove that all the automorphisms of Cartan modular curves must be defined on a compositum of quadratic fields when the level n is large enough. To do this, we use a geometrical criterion that we can apply by bounding the dimension of the CM part of the jacobian of Cartan modular curves. This last step is obtained using the isogenies of Section 3.4 and computing explicit bounds for the CM part of the jacobians of Borel modular curves. Furthermore, we refine the results in the case $n = p^e$, with p prime.

Finally, in Section 3.6 we prove the results stated above about automorphisms. The main idea is to show that each automorphism must preserve the cusps and the set of branching points of the covering by $\mathbb{H}$. This implies that there are no non-modular automorphisms. Thus, we compute the modular automorphisms to complete the analysis. We first concentrate on Cartan modular curves of general level n. Then we adapt the strategy to the case $n = p^e$, with p prime, giving the complete result for $X_{\mathrm{ns}}(p)$ and $X_{\mathrm{ns}}^+(p)$, and improving the result we obtained for the general level in the cases of $X_{\mathrm{s}}^+(p^e)$, $X_{\mathrm{ns}}(p^e)$ and $X_{\mathrm{ns}}^+(p^e)$. To treat some of the small level cases, we use the criterion of [48] which we verify through an algorithm implemented in MAGMA ([69]) which is available at [70].

As we did for the case of level $n = p^e$, with p prime, the result on Cartan modular curves of composite level can be sharpened, with our techniques, for levels with a specific type of factorization. However, certain cases remain out of the reach of the strategy described in this work, for example when we are not able to apply the criterion of [48] and either the curve has low gonality (e.g., $X_{\mathrm{ns}}(16)$, $X_{\mathrm{ns}}^+(16)$, $X_{\mathrm{ns}}^+(27)$) or its jacobian has a large CM part relative to its dimension (see Remark 3.5.11 for the example with the lowest level).

3.2 Modular curves

Let n be a positive integer. We denote by $Y(n)$ the (coarse if $n < 3$) moduli space that parametrizes pairs (E, ϕ) where E is an elliptic curve over a $\mathbb{Q}$-scheme S and $\phi\colon (\mathbb{Z}/n\mathbb{Z})^2_S \to E[n]$ is an isomorphism of S-group schemes. We denote by $X(n)$ the compactification of $Y(n)$ and we call $X(n)$ the *modular curve of full level n*.

Every matrix $\gamma \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ gives an automorphism of the constant group scheme $(\mathbb{Z}/n\mathbb{Z})^2_S$, hence γ acts on $Y(n)$ sending (E, ϕ) to $(E, \phi \circ \gamma)$. This defines an action of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ on $Y(n)$ that extends uniquely to $X(n)$. For each subgroup H of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, let X_H be the quotient $X(n)/H$. By [32, IV.6.7], X_H has good reduction over each prime that does not divide n and the smooth model of $Y_H = Y(n)/H$ over $\mathbb{Z}[1/n]$ is a coarse moduli space for *elliptic curves with H-structure*, i.e., the equivalence classes of pairs (E, ϕ) where E is an elliptic curve over a $\mathbb{Z}[1/n]$-scheme S and $\phi\colon (\mathbb{Z}/n\mathbb{Z})^2_S \to E[n]$ is an isomorphism of S-group schemes, and the equivalence relation is given by:

$$(3.2.1)\ \ (E, \phi) \sim_H (E', \phi') \iff (\phi')^{-1} \circ \iota|_{E[n]} \circ \phi = h, \text{ for some } h \in H \text{ and } \iota\colon E \xrightarrow{\sim} E'.$$

In particular, for every algebraically closed field K of characteristic $p \nmid n$, we have a bijection between $Y_H(K)$ and the set of elliptic curves over K with H-structure.

Remark 3.2.2. Since -1 is an automorphism of every elliptic curve, then for every H, the curve X_H is isomorphic to $X_{\pm H}$, where $\pm H := \{\pm \mathrm{Id}\}\cdot H < \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Hence, the equivalence relation (3.2.1) can be written as follows

$$(E, \phi) \sim_H (E', \phi') \iff (\phi')^{-1} \circ \iota|_{E[n]} \circ \phi = h, \text{ for some } h \in \pm H \text{ and } \iota\colon E \xrightarrow{\sim} E'.$$

Let $\mathbb{H}$ be the complex upper half-plane $\{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}$, let $\mathbb{H}^\pm = \mathbb{C} - \mathbb{R}$ and moreover let $\overline{\mathbb{H}} = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ and $\overline{\mathbb{H}}^\pm = \mathbb{H}^\pm \cup \mathbb{P}^1(\mathbb{Q})$ be their "compactifications". The group $\mathrm{GL}_2(\mathbb{Z})$ acts on $\mathbb{H}$, $\mathbb{H}^\pm$, $\overline{\mathbb{H}}$ and $\overline{\mathbb{H}}^\pm$ by Möbius transformations. Moreover, every g in $\mathrm{GL}_2(\mathbb{Z})$ acts on pairs $(z, \gamma H) \in \mathbb{H}^\pm \times (\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})/H)$ as $(g(z), \bar{g}\gamma H)$, where $g(z)$ is the image of z under the Möbius transformation given by g and $\bar{g}$ is the reduction of g mod n. This action gives canonical isomorphisms of Riemann surfaces

$$\mathrm{GL}_2(\mathbb{Z})\backslash\big(\mathbb{H}^\pm \times (\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})/H)\big) \longrightarrow Y_H(\mathbb{C}), \tag{3.2.2.1}$$

$$\mathrm{GL}_2(\mathbb{Z})\backslash\big(\overline{\mathbb{H}}^\pm \times (\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})/H)\big) \longrightarrow X_H(\mathbb{C}). \tag{3.2.2.2}$$

The isomorphism (3.2.2.1) is equivalent to that one described in [32, IV.5.3] and is given by $\mathrm{GL}_2(\mathbb{Z})(\tau, \gamma H) \mapsto (E_\tau, \phi_\tau \circ \gamma)$, where E_τ is the elliptic curve $\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$ and $\phi_\tau\colon (\mathbb{Z}/n\mathbb{Z})^2_{\mathbb{C}} \to E_\tau[n]$ is the unique isomorphism such that

$$\phi_\tau \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{n}, \quad \phi_\tau \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{\tau}{n}.$$

The isomorphism (3.2.2.2) is just the extension of the previous one to the compactifications. For each subgroup H of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, we define

$$\Gamma_H := \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \pmod{n} \text{ lies in } H\}.$$

If $\det H \neq (\mathbb{Z}/n\mathbb{Z})^\times$, then $X_H(\mathbb{C})$ is not connected: the number of connected components is $[(\mathbb{Z}/n\mathbb{Z})^\times : \det(H)]$ and, for each connected component $X_H^{cc}(\mathbb{C})$, there are isomorphisms of Riemann surfaces

$$\Gamma_{gHg^{-1}}\backslash\overline{\mathbb{H}} \longrightarrow X_H^{cc}(\mathbb{C}), \quad \Gamma_{gHg^{-1}}\backslash\mathbb{H} \longrightarrow Y_H^{cc}(\mathbb{C}), \tag{3.2.3}$$

for some g in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. In particular, if $\det H = (\mathbb{Z}/n\mathbb{Z})^\times$, then Y_H and X_H are geometrically connected curves defined over $\mathbb{Q}$.

The following proposition about the morphisms (3.2.3) is used in Section 3.6. We say that an automorphism of an elliptic curve is *non-trivial* if it is different from ±Id.

Proposition 3.2.4. *Let n be a positive integer, let H be a subgroup of* $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$*, let g be in* $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ *and consider the composition*

$$\begin{tikzcd}
\mathbb{H} \arrow[r] \arrow[rr, bend right] & \Gamma_{gHg^{-1}}\backslash\mathbb{H} \arrow[r, hook] & Y_H(\mathbb{C}),
\end{tikzcd}$$

where the left map is the natural projection and the right map is in (3.2.3). Then a point $(E,\phi) \in Y_H(\mathbb{C})$ is a branch point for such composition if and only if there is a non-trivial automorphism u of E such that $\phi^{-1} \circ u|_{E[n]} \circ \phi \in \pm H$. If this happens, then each point $\tau \in \mathbb{H}$ projecting to (E,ϕ) has ramification index $\#\mathrm{Aut}(E)/2$.

Proof. By Remark 3.2.2 we can suppose that H contains $-\mathrm{Id}$. Instead of looking at a map $\mathbb{H} \to Y_H(\mathbb{C})$ parametrizing a single component of Y_H, we can work with the canonical map

$$\begin{tikzcd}
\mathbb{H}^{\pm} \times \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \arrow[r, "\pi"] \arrow[rr, bend right] & Y(n)(\mathbb{C}) \arrow[r, "\pi_H"] & Y_H(\mathbb{C}).
\end{tikzcd}$$

Up to substituting n with $3n$ and H with its preimage under $\mathrm{GL}_2(\mathbb{Z}/3n\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, we can suppose that $n \geq 3$. This implies that π is an (unramified) covering map, hence the ramification index of the $\pi_H \circ \pi$ in a point (τ, γ) is equal to the ramification index of π_H in the point $\pi(\tau,\gamma)$. Hence, we only need to look at the ramification points of π_H. A point $(E,\phi) \in Y_H(\mathbb{C})$ is a branch point for π_H if and only if the fiber $\pi_H^{-1}(E,\phi)$ has cardinality smaller than $\deg \pi_H = \#H/2$. The modular interpretation of Y_H and $Y(n)$ implies that

$$\pi_H^{-1}(E,\phi) = \big\{(E, u|_{E[n]}\circ\phi\circ h) : h \in H, u \in \mathrm{Aut}(E)\big\}/\mathrm{Aut}(E), \tag{3.2.5}$$

where $v \in \mathrm{Aut}(E)$ acts sending (E,ψ) to $(E, v|_{E[n]}\circ\psi)$. Since $n \geq 3$, the map that sends u to $\phi^{-1}\circ u|_{E[n]}\circ\phi$ gives an inclusion $\mathrm{Aut}(E) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, hence, by (3.2.5), we have

$$\#\pi_H^{-1}(E,\phi) = \#\Big((H{\cdot}\mathrm{Aut}(E))/\mathrm{Aut}(E)\Big) = \#\Big(H/(H\cap\mathrm{Aut}(E))\Big).$$

The group $\mathrm{Aut}(E)$ always contains the multiplication by -1 and is cyclic of order $2, 4$ or 6. Finally, there are two options for $\mathrm{Aut}(E)\cap H$:

- $\mathrm{Aut}(E)\cap H$ only contains $\pm\mathrm{Id}$ and (E,ϕ) is not a branch point;
- $\mathrm{Aut}(E)\cap H$ has order equal to $\#\mathrm{Aut}(E) > 2$, in this case (E,ϕ) is a branch point and, since the map π_H is Galois, every point in $\pi_H^{-1}(E,\phi)$ has ramification index equal to $\deg(\pi_H)/\#\pi_H^{-1}(E,\phi) = \#\mathrm{Aut}(E)/2$.

□

3.3 Hecke operators

Let n be a positive integer and let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. For every prime $\ell \nmid n$, there is a divisor $D_\ell \subset X_H \times X_H$ inducing the ℓ-th Hecke operator

$$T_\ell \colon \mathrm{Div}(X_H) \to \mathrm{Div}(X_H), \quad T_\ell \colon \mathrm{Jac}(X_H) \to \mathrm{Jac}(X_H).$$

On $Y_H(\mathbb{C})$, it is described by

$$T_\ell(E,\phi) = \sum_{0 \subsetneq C \subsetneq E[\ell]} (E/C, \pi_C \circ \phi), \tag{3.3.1}$$

where $\pi_C \colon E \to E/C$ is the natural projection. Now we recall the definition of T_ℓ. Let H_ℓ be the subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\ell\mathbb{Z})$ containing the matrices whose reduction modulo n lies in H and whose reduction modulo ℓ is an upper triangular matrix. Given a $\mathbb{Z}[\frac{1}{n\ell}]$-scheme S and an elliptic curve E/S with H_ℓ-structure $\phi \colon (\mathbb{Z}/n\ell\mathbb{Z})^2 \to E[n\ell]$, we have two ways of constructing an elliptic curve over S with H-structure:

- The n-torsion subgroup of $(\mathbb{Z}/n\ell\mathbb{Z})^2$ is canonically isomorphic, via the Chinese Remainder Theorem, to $(\mathbb{Z}/n\mathbb{Z})^2$ and the restriction of ϕ to this subgroup gives an isomorphism $\phi|_{(\mathbb{Z}/n\mathbb{Z})^2} \colon (\mathbb{Z}/n\mathbb{Z})^2 \to E[n]$. One can check that the class of

$(E,\phi|_{(\mathbb{Z}/n\mathbb{Z})^2})$ modulo $\sim_H$ does not depend on the choice of the representative (E,ϕ) in the equivalence class defined by $\sim_{H_\ell}$, hence

$$\mathrm{pr}(E,\phi) := (E,\phi|_{(\mathbb{Z}/n\mathbb{Z})^2})$$

is a well defined elliptic curve over S with H-structure.

- The subgroup $C \subset E[\ell]$ generated by $\phi(\begin{smallmatrix} n \\ 0 \end{smallmatrix})$ is a subgroup of E of order ℓ and E/C is an elliptic curve over S. Denoting by $\pi_C \colon E \to E/C$ the natural projection, we have that
$$\mathrm{qt}(E,\phi) := (E/C, \pi_C \circ \phi|_{(\mathbb{Z}/n\mathbb{Z})^2})$$
is a well defined elliptic curve over S with H-structure.

These two constructions define natural transformations between the functor of elliptic curves with H_ℓ-structure and the functor of elliptic curves with H-structure restricted to schemes over $\mathbb{Z}[\frac{1}{n\ell}]$. We get induced morphisms between the coarse moduli spaces Y_{H_ℓ} and $(Y_H)_{\mathbb{Z}[\frac{1}{n\ell}]}$ that can be extended by smoothness to the compactifications:

$$\mathrm{pr}, \mathrm{qt} \colon X_{H_\ell} \longrightarrow (X_H)_{\mathbb{Z}[\frac{1}{n\ell}]}.$$

The image of X_{H_ℓ} under the map $(\mathrm{pr},\mathrm{qt})$ defines a divisor inside $(X_H)_{\mathbb{Z}[\frac{1}{n\ell}]} \times (X_H)_{\mathbb{Z}[\frac{1}{n\ell}]}$. Since X_H is smooth over $\mathbb{Z}[\frac{1}{n}]$, this divisor extends uniquely to $D_\ell \subset X_H \times X_H$ whose irreducible components project surjectively on each factor X_H. This correspondence induces the operator $T_\ell = \mathrm{qt}_* \circ \mathrm{pr}^*$ and the definitions of qt and pr imply the equality (3.3.1).

The reduction of T_ℓ modulo ℓ is described by a celebrated theorem of Eichler and Shimura. To state this theorem in the full generality, we recall the definition of diamond operators. Let $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, then the matrix $(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix})$ normalizes H, hence

$$\langle a \rangle (E,\phi) := (E, \phi \circ (\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}))$$

defines an automorphism of the functor of elliptic curves with H-structure. So $\langle a \rangle$ induces an automorphism of the coarse moduli space Y_H and it extends to an automorphism of the compactification X_H. Eichler-Shimura Relation is nowadays a common knowledge, but in the literature is often stated in a different form than we need. The proof of [38, Theorem 8.7.2] can be directly adapted to our case, and another proof is in [94, Theorem 7.9 and Corollary 7.10]. We use the result in the following form.

Theorem (Eichler-Shimura Relation). *Let n be a positive integer, let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, let ℓ be a prime number not dividing n, let $\overline{X}_H$ be the reduction of X_H modulo ℓ, let $\overline{T}_\ell, \overline{\langle \ell \rangle} \colon \mathrm{Div}(\overline{X}_H) \to \mathrm{Div}(\overline{X}_H)$ be the reduction of the Hecke operator T_ℓ*

and of the diamond operator $\langle \ell \rangle$ *and let* $\mathrm{Frob}_\ell \colon \overline{X}_H \to \overline{X}_H$ *be the Frobenius morphism. Then*

$$\overline{T}_\ell = (\mathrm{Frob}_\ell)_* + \overline{\langle \ell \rangle}_* \circ (\mathrm{Frob}_\ell)^*.$$

Notice that in general X_H is not geometrically connected and if X' is a component of $\overline{X}_H$, the Frobenius morphism $\overline{X}_H \to \overline{X}_H$ may not restrict to a morphishm $X' \to X'$. Analogously, if x is a point on X', the divisor $T_\ell(x)$ may be not supported on X'. We are interested in Eichler-Shimura Relation because, as already pointed out in [60, Lemma 2.6], it implies that, in certain cases, Hecke operators commute with automorphisms of modular curves.

Proposition 3.3.2. *Let* n *be a positive integer, let* $H < \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ *be a subgroup containing the scalar matrices and such that* $\det H = (\mathbb{Z}/n\mathbb{Z})^\times$*. Let* ℓ *be a prime not dividing* n *and let* $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *be a Frobenius element at* ℓ*. Then, for any automorphism* u *of* X_H *defined over a compositum of quadratic fields, in* $\mathrm{End}(\mathrm{Jac}(X_H))$ *we have*

$$T_\ell \circ u = u^\sigma \circ T_\ell, \tag{3.3.3}$$

where we identify u *and* u^σ *with their pushforward on* $\mathrm{Jac}(X_H)$*. Moreover, if the gonality of* $X_H(\mathbb{C})$ *is greater than* $2(\ell+1)$*, then (3.3.3) holds at level of divisors.*

Proof. Let $J := \mathrm{Jac}(X_H)$, let $\mathrm{Frob}_\ell \colon \overline{X}_H \to \overline{X}_H$ be the Frobenius morphism and let ϕ_ℓ be the Frobenius generator of $\mathrm{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell)$. Let $D \in \mathrm{Div}(\overline{X}_H)$ and let $\bar{u}$ be the reduction of u modulo ℓ. Using Eichler-Shimura Relation, we have

$$\begin{aligned}\overline{T}_\ell \circ \bar{u}(D) =& ((\mathrm{Frob}_\ell)_* + (\mathrm{Frob}_\ell)^*) \circ \bar{u}(D) = (\mathrm{Frob}_\ell)_* \bar{u}(D) + (\mathrm{Frob}_\ell)^* \bar{u}(D) = \\ =& \bar{u}^{\phi_\ell} (\mathrm{Frob}_\ell)_*(D) + \bar{u}^{\phi_\ell^{-1}} (\mathrm{Frob}_\ell)^*(D) = \overline{u^\sigma} (\mathrm{Frob}_\ell)_*(D) + \overline{u^{\sigma^{-1}}} (\mathrm{Frob}_\ell)^*(D).\end{aligned}$$

Now, since u is defined over a compositum of quadratic fields, the Galois automorphisms σ and σ^{-1} act in the same way on u. This implies that the last term in the previous chain of equalities is equal to $\overline{u^\sigma} \circ \overline{T}_\ell(D)$ obtaining $\overline{T}_\ell \circ \bar{u} = \overline{u^\sigma} \circ \overline{T}_\ell$ in $\mathrm{End}(J_{\mathbb{F}_\ell})$.

Since J has good reduction at ℓ, the natural map $\mathrm{End}(J) \to \mathrm{End}(J_{\mathbb{F}_\ell})$ is injective, hence (3.3.3) holds in $\mathrm{End}(J)$. This means that, for any two points P and Q in $X_H(\mathbb{C})$, the divisor $D := (T_\ell u - u^\sigma T_\ell)(P - Q)$ is principal. Hence, either D is the zero divisor or is the divisor of a non-constant rational function on X_H of degree at most $2(\ell+1)$.

Now we suppose that the gonality of X_H exceeds $2(\ell+1)$. In this case, there are no non-constant rational functions on X_H of degree at most $2(\ell+1)$, hence D is the zero divisor. This gives the following equality of divisors:

$$T_\ell u(P) + u^\sigma T_\ell(Q) = u^\sigma T_\ell(P) + T_\ell u(Q).$$

For every point P, we can choose Q such that the supports of $T_\ell u(P)$ and $T_\ell u(Q)$ are disjoint, and, therefore, last equality implies $T_\ell u(P) = u^\sigma T_\ell(P)$ as divisors. Up to a base change to $\mathbb{C}$, each divisor on X_H is a sum of points with integer coefficients, hence we conclude that (3.3.3) holds at level of divisors. □

Multiple points in the image of Hecke operators

In the proofs of Section 3.6 we look at points $P \in X_H(\mathbb{C})$ and primes ℓ such that $T_\ell(P)$ is not a sum of distinct points. In this subsection we study this phenomenon. When P is a cusp, we have the following result.

Proposition 3.3.4. *Let n be a positive integer and let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Let ℓ be a prime number not dividing n, let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be a Frobenius element at ℓ and let $C \in X_H(\overline{\mathbb{Q}})$ be a cusp. Then*

$$T_\ell(C) = C^\sigma + \ell\,\langle \ell \rangle (C^{\sigma^{-1}}).$$

Proof. The divisor $T_\ell(C) = \mathrm{qt}_*\mathrm{pr}^*(C)$ is supported on the cusps because both the maps $\mathrm{pr}, \mathrm{qt}\colon X_{H_\ell} \to X_H$ send non-cuspidal points to non-cuspidal points and cusps to cusps. If we fix a prime ideal $\mathfrak{l}$ in the algebraic integers such that $\mathfrak{l} \mid \ell$, then, by [32, IV.3.4], each cusp in $X_H(\overline{\mathbb{Q}})$ reduces to a different point modulo $\mathfrak{l}$. Thus, it is enough to prove that $T_\ell(C)$ is congruent to $C^\sigma + \ell\,\langle \ell \rangle (C^{\sigma^{-1}})$ modulo $\mathfrak{l}$, and this is true by Eichler-Shimura Relation. □

We need a criterion to characterize the points $(E, \phi) \in Y_H(\mathbb{C})$ such that their image via T_ℓ contains a point with multiplicity at least 2. It is given by the following lemma.

Lemma 3.3.5. *Let n be a positive integer, let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ and let ℓ be a prime not dividing n. For all points $(E, \phi), (E, \phi') \in Y_H(\mathbb{C})$ and all positive integers $m \geq 2$, the following are equivalent:*

1. *$T_\ell(E, \phi)$ contains (E', ϕ') with multiplicity m;*
2. *there are m isogenies $\alpha_1, \dots, \alpha_m \colon E \to E'$ of degree ℓ with distinct kernels such that $(\phi')^{-1} \circ \alpha_j|_{E[n]} \circ \phi$ lies in $\pm H$, for every $j = 1, \dots, m$;*
3. *there are m endomorphisms $\beta_1 = \ell, \beta_2, \dots, \beta_m$ of E' of degree ℓ^2 and an isogeny $\alpha\colon E' \to E$ of degree ℓ such that:*

P1 *$\beta_i \neq u \circ \beta_j$, for $i, j = 1, \dots, m$, such that $i \neq j$ and for each $u \in \mathrm{Aut}(E')$;*

P2 *$\ker \alpha \subset \ker \beta_j$, for every j in $\{1, \dots, m\}$;*

P3 *the matrices $\ell^{-1}\phi^{-1}\circ\alpha|_{E'[n]}\circ\phi'$ and $\ell^{-1}(\phi')^{-1}\circ\beta_j|_{E'[n]}\circ\phi'$ lie in $\pm H$, for every j in $\{1,\dots,m\}$, where ℓ^{-1} is the inverse of the scalar matrix $\ell \bmod n$.*

Proof. The equivalence between (1) and (2) follows by definition of Hecke operator. Now we prove the equivalence between (2) and (3). Let $\alpha_1,\dots,\alpha_m$ be isogenies of degree ℓ with distinct kernels, then it is enough to take α equal to the dual of α_1 and $\beta_j = \alpha_j\circ\alpha$, for $j = 1,\dots,m$. Conversely, if $\beta_1,\dots,\beta_m$ respect the three properties above, then, for every $j = 1,\dots,m$, we can take α_j to be the unique isogeny such that $\beta_j = \alpha_j\circ\alpha$. □

From now on we denote by $\rho = e^{\frac{2\pi i}{3}}$ the primitive third root of unity contained in $\mathbb{H}$. Moreover, for every $\tau \in \mathbb{H}$, we denote by E_τ the elliptic curve $\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$. The following result proves that if $T_\ell(E,\phi)$ shows certain multiplicities, then E has complex multiplication by $\mathbb{Q}(i)$ or $\mathbb{Q}(\rho)$.

Proposition 3.3.6. *Let n be a positive integer, let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, let ℓ be a prime not dividing n and let (E,ϕ) be a $\mathbb{C}$-point of Y_H. Then:*

1. *the points in the image $T_\ell(E,\phi)$ have multiplicity at most 3;*
2. *if $T_\ell(E,\phi)$ contains a point with multiplicity 3, then $\mathrm{End}(E)$ contains $\mathbb{Z}[\ell^2\rho]$;*
3. *if $\ell \geq 5$ and*

$$T_\ell(E,\phi) = 2(P_1+\ldots+P_{\frac{\ell+1}{2}}) \quad \text{or} \quad T_\ell(E,\phi) = 2(P_1+\ldots+P_{\frac{\ell-1}{2}}) + P_{\frac{\ell+1}{2}} + P_{\frac{\ell+3}{2}},$$

for $P_1,\dots,P_{\frac{\ell+3}{2}} \in Y_H(\mathbb{C})$ distinct points, then $\mathrm{End}(E)$ contains $\mathbb{Z}[\ell^2 i]$.

Proof. Parts (1) and (2).

First we prove that if $T_\ell(E,\phi)$ contains a point with multiplicity at least 3, then $\mathrm{End}(E)$ contains $\mathbb{Z}[\ell^2\rho]$. Let $(E',\phi') \in Y_H(\mathbb{C})$ such that $T_\ell(E,\phi) \geq 3(E',\phi')$, then there are isogenies $\alpha\colon E' \to E$ and $\beta_1 = \ell, \beta_2, \beta_3\colon E' \to E'$ as in Lemma 3.3.5 and, consequently, $\mathrm{End}(E')$ and $\mathrm{End}(E)$ are orders in a quadratic field K, with ring of integers $\mathcal{O}_K$. Since $\ker(\alpha)$ is non-trivial and it is contained in $\ker(\beta_j)$, for every $j = 1,2,3$, the ideal of $\mathrm{End}(E')$ generated by β_1, β_2, β_3 is non-trivial. Using that $\mathrm{End}(E') \subset \mathcal{O}_K$ is a finite extension of rings, we deduce that the ideal of $\mathcal{O}_K$ generated by β_1, β_2, β_3 is non-trivial as well. The ideals $\beta_1\mathcal{O}_K$, $\beta_2\mathcal{O}_K$ and $\beta_3\mathcal{O}_K$ of $\mathcal{O}_K$ have norm ℓ^2 and if they are three distinct ideals, then there are two distinct primes $\mathfrak{l}_1, \mathfrak{l}_2 \subset \ell\mathcal{O}_K$ such that, up to reordering, $\beta_1\mathcal{O}_K = \mathfrak{l}_1\mathfrak{l}_2$, $\beta_2\mathcal{O}_K = \mathfrak{l}_2^2$, $\beta_3\mathcal{O}_K = \mathfrak{l}_1^2$, implying that the ideal of $\mathcal{O}_K$ generated by $\beta_1, \beta_2, \beta_3$ is the whole $\mathcal{O}_K$, contradiction. Hence the ideals $\beta_1\mathcal{O}_K$, $\beta_2\mathcal{O}_K$ and $\beta_3\mathcal{O}_K$ cannot be distinct.

If $K \notin \{\mathbb{Q}(i), \mathbb{Q}(\rho)\}$, then $\mathcal{O}_K^\times = \{\pm 1\}$, hence $\beta_k\mathcal{O}_K = \beta_j\mathcal{O}_K$ implies $\beta_k = \pm\beta_j$, which is absurd by condition **P1** in Lemma 3.3.5. Hence either $K = \mathbb{Q}(i)$ or $K = \mathbb{Q}(\rho)$.

Then $\mathcal{O}_K = \mathbb{Z}[u]$ with $u \in \{i, \rho\}$ and $\mathrm{End}(E') = \mathbb{Z}[mu]$ for some positive integer $m > 0$. Condition **P1** in Lemma 3.3.5 implies that the ideals of $\mathrm{End}(E')$ generated by β_1, β_2 and β_3 are distinct and we have just proven that their extensions to $\mathbb{Z}[u]$ are not distinct. We know that ideal extension gives a bijection between ideals in $\mathbb{Z}[mu]$ with index coprime to m and ideals in $\mathbb{Z}[u]$ with index coprime to m, hence $\ell^2 = [\mathcal{O}_K : \beta_j \mathcal{O}_K]$ is not coprime to m. Therefore $\ell \mid m$ and $\mathrm{End}(E') \subset \mathbb{Z}[\ell u]$. Hence β_2 and β_3 are elements of $\mathbb{Z}[\ell u]$ having norm equal to ℓ^2 and the only elements of this kind are $\{\pm\ell, \pm\ell u, \pm\ell u^2\}$. If $K = \mathbb{Q}(i)$, then $\beta_1, \beta_2, \beta_3 \in \{\pm\ell, \pm\ell i\}$, contradicting $\beta_k \neq \pm\beta_j$, for $k \neq j$. If $K = \mathbb{Q}(\rho)$, the only possibility, up to reordering, is $\beta_2 = \pm\rho\ell$ and $\beta_3 = \pm\rho^2\ell$ and consequently $m = \ell$. Finally, since there is an isogeny $E' \to E$ of degree ℓ, we have $\mathbb{Z}[\ell^2\rho] \subset \mathrm{End}(E)$.

Finally, we suppose that $(E, \phi) \in Y_H(\mathbb{C})$ and (E', ϕ') appears in $T_\ell(E, \phi)$ with multiplicity at least 4. Then, by what we have just proven, $\mathrm{End}(E') = \mathbb{Z}[\ell\rho]$. Hence, there are exactly 3 elements in $\mathrm{End}(E')$, up to sign, with norm equal to ℓ^2 and we cannot find elements $\beta_1, \ldots, \beta_4$ satisfying the properties of Lemma 3.3.5. This contradiction concludes the proof of Parts (1) and (2).

Part (3).

Let τ be an element of $\mathbb{H}$ such that $E = E_\tau$. Then

$$T_\ell(E, \phi) = (E_{\frac{\tau}{\ell}}, \phi_0) + (E_{\frac{\tau+1}{\ell}}, \phi_1) + \ldots + (E_{\frac{\tau+\ell-1}{\ell}}, \phi_{\ell-1}) + (E_{\ell\tau}, \phi_\ell),$$

for suitable $\phi_0, \ldots, \phi_\ell$. The hypothesis on $T_\ell(E, \phi)$ implies that we can find three distinct integers $r_1, r_2, r_3 \in \{0, \ldots, \ell-1\}$, with corresponding

$$\tau_1 := (\tau + r_1)/\ell, \quad \tau_2 := (\tau + r_2)/\ell, \quad \tau_3 := (\tau + r_3)/\ell, \tag{3.3.7}$$

such that (E_{τ_1}, ϕ_{r_1}), (E_{τ_2}, ϕ_{r_2}) and (E_{τ_3}, ϕ_{r_3}) appear in $T_\ell(E, \phi)$ with multiplicity at least 2. In particular by Lemma 3.3.5 we see that $\mathrm{End}(E_{\tau_k})$ contains a non-trivial element of degree ℓ^2, for $k = 1, 2, 3$, hence E_{τ_k} and E have CM over some quadratic imaginary field $K \subset \mathbb{C}$. Therefore $\tau \in K$ and there are $a, b \in \mathbb{Q}$ such that

$$\tau^2 = a\tau + b. \tag{3.3.8}$$

Hence $\mathrm{End}(E_{\tau_1})$, $\mathrm{End}(E_{\tau_2})$ and $\mathrm{End}(E_{\tau_3})$ are naturally subrings of $\mathcal{O}_K$ the ring of integers of K. We denote by $\mathcal{I}$ their intersection.

Now, we prove that $\mathcal{I} \subset \mathbb{Z} + \ell\mathcal{O}_K$. Let $\lambda \in \mathcal{I}$. We know that λ defines an element in the endomorphism ring of E_{τ_1}, E_{τ_2} and E_{τ_3} if and only if the lattices

$$\mathbb{Z} + \mathbb{Z}\tau_1, \quad \mathbb{Z} + \mathbb{Z}\tau_2 \quad \text{and} \quad \mathbb{Z} + \mathbb{Z}\tau_3 \tag{3.3.9}$$

are stable under the multiplication by λ. In particular $\lambda = \lambda \cdot 1$ lies in all these lattices and in their intersection $\mathbb{Z}+\mathbb{Z}\tau$, hence $\lambda = x + y\tau$, for $x, y \in \mathbb{Z}$. Then, all the lattices in

(3.3.9) are stable also under the multiplication by $\mu := y\tau$ and consequently

$$\mu\tau_1 \in \mathbb{Z} + \mathbb{Z}\tau_1, \quad \mu\tau_2 \in \mathbb{Z} + \mathbb{Z}\tau_2, \quad \mu\tau_3 \in \mathbb{Z} + \mathbb{Z}\tau_3.$$

Then, using (3.3.7) and (3.3.8), we deduce that ay and by lie in $\mathbb{Z}$ and that the polynomial

$$p(t) := -yt^2 - yat + yb \in \mathbb{Z}[t]$$

has the property $p(r_1) \equiv p(r_2) \equiv p(r_3) \equiv 0 \bmod \ell$. Since r_1, r_2 and r_3 are pairwise distinct modulo ℓ, we deduce that y, ay and by are divisible by ℓ and consequently

$$\mu^2 = (y\tau)^2 = ay^2\tau + by^2 = ay\mu + by^2 \in ay\mathcal{O}_K + by\mathcal{O}_K \subset \ell\mathcal{O}_K.$$

If $y = 0$ or if the ideal $\ell\mathcal{O}_K$ is radical, we deduce that μ lies in $\ell\mathcal{O}_K$ and consequently $\lambda = x + \mu$ lies in $\mathbb{Z} + \ell\mathcal{O}_K$. If $y \neq 0$ and $\ell\mathcal{O}_K$ factors as $\mathfrak{l}^2$, for a prime ideal $\mathfrak{l} \mid \ell$, then the norm of μ is equal to by^2 which is a multiple of ℓ^2, hence μ lies in $\mathfrak{l}^2 = \ell\mathcal{O}_K$ and, as before, λ lies in $\mathbb{Z} + \ell\mathcal{O}_K$.

Let a_1, a_2, a_3 be positive integers such that $\mathrm{End}(E_{\tau_k}) = \mathbb{Z} + a_k\mathcal{O}_K$, for $k = 1, 2, 3$. Then $\mathbb{Z} + \mathrm{lcm}(a_1, a_2, a_3)\mathcal{O}_K = \mathcal{I} \subset \mathbb{Z} + \ell\mathcal{O}_K$. Hence $\ell \mid \mathrm{lcm}(a_1, a_2, a_3)$, i.e., we can suppose, up to renaming τ_1, τ_2, τ_3, that $\mathrm{End}(E_{\tau_1})$ is contained in $\mathbb{Z}+\ell\mathcal{O}_K$. Let $\beta_1 = \ell, \beta_2$ be endomorphisms of E_{τ_1} satisfying the properties of Lemma 3.3.5. We write $\mathcal{O}_K = \mathbb{Z}[\gamma]$, for a suitable γ, and $\beta_2 = z + w\gamma$. Since $\mathrm{End}(E_{\tau_1}) \subset \mathbb{Z} + \ell\mathcal{O}_K$, then w is multiple of ℓ and, since the norm of β_2 is ℓ^2, we deduce that z is multiple of ℓ as well. Hence $\beta_2 \in \ell\mathcal{O}_K$ and $\beta_2 = u\ell$ for some $u \in \mathcal{O}_K^\times$. Since $\beta_2 \neq \pm\beta_1 = \pm\ell$, we deduce that $\mathcal{O}_K$ has non-trivial units, hence either $K = \mathbb{Q}(i)$ or $K = \mathbb{Q}(\rho)$.

We suppose by contradiction that $K = \mathbb{Q}(\rho)$. Then we have that $u \in \{\pm\rho, \pm\rho^2\}$ and $\mathbb{Z}[\beta_2] = \mathbb{Z}[\ell\rho] \subset \mathrm{End}(E_{\tau_1})$. Since $\beta_2 \notin \ell\mathrm{End}(E_{\tau_1})^\times$ by property **P1** of Lemma 3.3.5, we deduce that $\mathrm{End}(E_{\tau_1}) \neq \mathbb{Z}[\rho]$, hence $\mathrm{End}(E_{\tau_1}) = \mathbb{Z}[\ell\rho]$. In particular $u^2\ell \in \mathrm{End}(E_{\tau_1})$ and the third condition in Lemma 3.3.5 is satisfied by (E, ϕ), (E_{τ_1}, ϕ_{r_1}), α, β_1, β_2 together with $\beta_3 := u^2\ell$. Hence the point (E_{τ_1}, ϕ_{r_1}) appears with multiplicity 3 in $T_\ell(E, \phi)$ which is impossible. Thus, $K = \mathbb{Q}(i)$ and $\beta_2 = \pm\ell i$. Hence $\mathrm{End}(E_{\tau_1})$ contains $\mathbb{Z}[\ell i]$ and, since there is an isogeny of degree ℓ between E and E_{τ_1}, then $\mathrm{End}(E)$ contains $\mathbb{Z}[\ell^2 i]$. □

The following proposition characterizes when $\phi^{-1} \circ \tau|_{E_\tau[n]} \circ \phi$ belongs to $\pm H$, for $\tau = \rho, i$, in terms of the multiplicities shown in the divisor $T_\ell(E_\tau, \phi)$.

Proposition 3.3.10. *Let n be a positive integer, let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ and let ℓ be a prime not dividing n.*

1. *Let $(E_\rho, \phi) \in Y_H(\mathbb{C})$. The matrix $\phi^{-1} \circ \rho|_{E_\rho[n]} \circ \phi$ lies in $\pm H$ if and only if the divisor $T_\ell(E_\rho, \phi)$ contains a point with multiplicity 3.*

2. *Let $(E_i, \phi) \in Y_H(\mathbb{C})$. If $\ell > 2$: The matrix $\phi^{-1} \circ i|_{E_i[n]} \circ \phi$ lies in $\pm H$ if and only if there are distinct points $P_1, \ldots, P_{\frac{\ell+3}{2}} \in Y_H(\mathbb{C})$ such that*

$$\begin{aligned} T_\ell(E_i, \phi) &= 2(P_1 + \ldots + P_{\frac{\ell+1}{2}}) \\ &\quad \textit{or} \\ T_\ell(E_i, \phi) &= 2(P_1 + \ldots + P_{\frac{\ell-1}{2}}) + P_{\frac{\ell+1}{2}} + P_{\frac{\ell+3}{2}}. \end{aligned} \tag{3.3.11}$$

If $\ell = 2$: The matrix $\phi^{-1} \circ i|_{E_i[n]} \circ \phi$ lies in $\pm H$ if and only if there are two distinct points $P_1, P_2 \in Y_H(\mathbb{C})$ such that

$$T_2(E_i, \phi) = 2P_1 + P_2.$$

Proof. Part (1).

If $C \subset E_\rho[\ell]$ is a subgroup of order ℓ, then ρC and $\rho^2 C$ are subgroups of order ℓ as well and there are two unique isomorphisms u, v that make the following diagrams commutative:

$$\begin{tikzcd} E_\rho \arrow[r, "\rho"] \arrow[d, "\pi_C"] & E_\rho, \arrow[d, "\pi_{\rho C}"] \\ E_\rho/C \arrow[r, "u"] & E_\rho/\rho C, \end{tikzcd} \qquad \begin{tikzcd} E_\rho \arrow[r, "\rho^2"] \arrow[d, "\pi_C"] & E_\rho \arrow[d, "\pi_{\rho^2 C}"] \\ E_\rho/C \arrow[r, "v"] & E_\rho/\rho^2 C. \end{tikzcd}$$

We have that $\rho C = C$ if and only if ρ is an endomorphism of E_ρ/C, which is in turn equivalent to $\mathrm{Aut}(E_\rho/C) \neq \{\pm 1\}$ or $\mathrm{End}(E_\rho/C) = \mathbb{Z}[\rho]$ and, since the class number of $\mathbb{Z}[\rho]$ is equal to 1, this is equivalent to $E_\rho/C \cong E_\rho$. Hence, if $\rho C \neq C$, then $\mathrm{Aut}(E_\rho/C) = \{\pm 1\}$ and, using that π_C and $\pi_{\rho C}$ are bijections on the n-torsion subgroups, we have

$$\begin{aligned} (E_\rho/C, \pi_C \circ \phi) = (E_\rho/\rho C, \pi_{\rho C} \circ \phi) &\iff (\pi_{\rho C}|_{E_\rho[n]} \circ \phi)^{-1} \circ u|_{(E_\rho/C)[n]} \circ (\pi_C|_{E_\rho[n]} \circ \phi) \in \pm H \\ &\iff \phi^{-1} \circ \rho|_{E_\rho[n]} \circ \phi \in \pm H. \end{aligned} \tag{3.3.11.1}$$

Analogously, $\rho^2 C \neq C$ if and only if $\mathrm{Aut}(E_\rho/C) = \{\pm 1\}$ and when this happens

$$(E_\rho/C, \pi_C \circ \phi) = (E_\rho/\rho^2 C, \pi_{\rho^2 C} \circ \phi) \iff \phi^{-1} \circ \rho|_{E_\rho[n]} \circ \phi \in \pm H. \tag{3.3.12}$$

Since the endomorphism ρ does not act as a scalar on $E_\rho[\ell]$, there are at most two non-trivial subgroups of $E_\rho[\ell]$ that are ρ-stable. In particular we can take a non-trivial subgroup C_0 such that C_0, ρC_0 and $\rho^2 C_0$ are pairwise distinct.

If $\phi^{-1} \circ \rho|_{E_\rho[n]} \circ \phi$ lies in $\pm H$, then, by (3.3.11.1) and (3.3.12),

$$T_\ell(E_\rho, \phi) \geq (E_\rho/C_0, \pi_{C_0} \circ \phi) + (E_\rho/\rho C_0, \pi_{\rho C_0} \circ \phi) + (E_\rho/\rho^2 C_0, \pi_{\rho^2 C_0} \circ \phi) = 3(E_\rho/C_0, \pi_{C_0} \circ \phi).$$

Conversely, if $T_\ell(E_\rho,\phi)$ contains a point with multiplicity 3, there are three pairwise distinct subgroups $C_1, C_2, C_3 \subset E_\rho[\ell]$ of order ℓ such that

$$(E_\rho/C_1, \pi_{C_1}\circ\phi) = (E_\rho/C_2, \pi_{C_2}\circ\phi) = (E_\rho/C_3, \pi_{C_3}\circ\phi).$$

If one of the C_j is ρ-stable, then $E_\rho/C_1 \cong E_\rho/C_2 \cong E_\rho/C_3 \cong E_\rho$, and C_1, C_2, C_3 are all ρ-stable, contradicting that there are at most two non-trivial ρ-stable subgroups of $E_\rho[\ell]$. In particular $\mathbb{Z}[\rho] \supsetneq \mathrm{End}(E_\rho/C_1)$ and since E/C_1 is ℓ-isogenous to E_ρ we deduce that $\mathrm{End}(E_\rho/C_1) = \mathbb{Z}[\ell\rho]$. Hence, the only endomorphisms of E_ρ/C_1 having degree ℓ^2 are $\pm\ell, \pm\rho\ell, \pm\rho^2\ell$ and so there are at most three subgroups $C \subset E_\rho[\ell]$ of order ℓ such that E_ρ/C is isomorphic to E_ρ/C_1, namely: $C_1, \rho C_1$ and $\rho^2 C_1$. We deduce that, up to reordering, $C_2 = \rho C_1$ hence, by (3.3.11.1), $\phi^{-1}\circ\rho|_{E_\rho[n]}\circ\phi$ lies in $\pm H$.

Part (2).

If $C \subset E_i[\ell]$ is a subgroup of order ℓ, then iC is another subgroup of order ℓ and there is a unique isomorphism u that makes the following diagram commutative:

$$\begin{tikzcd}
E_i \arrow[r, "i"] \arrow[d, "\pi_C"] & E_i \arrow[d, "\pi_{iC}"] \\
E_i/C \arrow[r, "u"] & E_i/iC.
\end{tikzcd}$$

We have that $iC = C$ if and only if $\mathrm{End}(E_i/C) = \mathbb{Z}[i]$ if and only if $\mathrm{Aut}(E_i/C) \neq \{\pm 1\}$. Hence, if $iC \neq C$, then $\mathrm{Aut}(E_i/C) = \{\pm 1\}$ and, using that π_C and π_{iC} are bijections on the n-torsion subgroups, we have

(3.3.13)

$$\begin{aligned}
(E_i/C, \pi_C\circ\phi) = (E_i/iC, \pi_{iC}\circ\phi) \quad &\iff \quad (\pi_{iC}\circ\phi)^{-1}\circ u|_{(E_i/C)[n]}\circ(\pi_C\circ\phi) \in \pm H \\
&\iff \quad \phi^{-1}\circ i|_{E_i[n]}\circ\phi \in \pm H.
\end{aligned}$$

The endomorphism i does not act as multiplication by a scalar on $E_i[\ell]$. For each subgroup $C \subset E_i[\ell]$ of order ℓ, except at most two, we have $C \neq iC$. Hence, there are subgroups $C_1, \ldots, C_{\frac{\ell+3}{2}} \subset E_i$ of order ℓ such that $\{C_1, iC_1, \ldots, C_{\frac{\ell-1}{2}}, iC_{\frac{\ell-1}{2}}, C_{\frac{\ell+1}{2}}, C_{\frac{\ell+3}{2}}\}$ is the set of all the $\ell+1$ subgroups of order ℓ of E_i.

If $\phi^{-1}\circ i|_{E_i[n]}\circ\phi$ lies in $\pm H$, then, by (3.3.13), we have

$$T_\ell(E_i,\phi) = \sum_{k=1}^{\frac{\ell-1}{2}} 2(E_i/C_k, \pi_{C_k}\circ\phi) + (E_i/C_{\frac{\ell+1}{2}}, \pi_{C_{\frac{\ell+1}{2}}}\circ\phi) + (E_i/C_{\frac{\ell+3}{2}}, \pi_{C_{\frac{\ell+3}{2}}}\circ\phi),$$

and no point appears with multiplicity greater than 2 because of Proposition 3.3.6.

Now we assume that (3.3.11) holds. If $\ell = 3$, there are $C_1, C_2 \subset E_i$ subgroups of order 3 such that E_i/C_1 is not isomorphic to E_i/C_2 and C_1, iC_1, C_2, iC_2 are all the subgroups of E_i of order 3. Hence Equation (3.3.11) implies that, up to renaming,

$$(E_i/C_1, \pi_{C_1} \circ \phi) = (E_i/iC_1, \pi_{iC_1} \circ \phi),$$

and by (3.3.13), we have that $\phi^{-1} \circ i|_{E_i[n]} \circ \phi$ lies in $\pm H$. The case $\ell = 2$ is similar to $\ell = 3$. We now suppose $\ell \geq 5$, so there are more repetitions in Equation (3.3.11). There are at most two possible subgroups C such that $iC = C$. Hence Equation (3.3.11) implies the existence of a subgroup $C_0 \subset E_i[\ell]$ such that $(E_i/C_0, \pi_{C_0} \circ \phi)$ has multiplicity 2 in $T_\ell(E_i, \phi)$ and $C_0 \neq iC_0$. It follows that E_i/C_0 is not isomorphic to E_i, thus $\mathrm{End}(E_i/C_0) = \mathbb{Z}[\ell i]$, and this implies that $\pm\ell$ and $\pm\ell i$ are the only elements of $\mathrm{End}(E_i/C_0)$ having degree ℓ^2. Hence, if C is a subgroup of $E_i[\ell]$ of order ℓ such that E_i/C is isomorphic to E_i/C_0, then $C \in \{C_0, iC_0\}$. Since $(E_i/C_0, \pi_{C_0} \circ \phi)$ has multiplicity 2, we have

$$(E_i/C_0, \pi_{C_0} \circ \phi) = (E_i/iC_0, \pi_{iC_0} \circ \phi),$$

and by (3.3.13), we have that $\phi^{-1} \circ i|_{E_i[n]} \circ \phi$ lies in $\pm H$. □

3.4 Cartan modular curves and their jacobians

We give the definition of Cartan modular curves following [93, Appendix A.5]. Let $n{>}1$ be an integer and let A be a free commutative étale $\mathbb{Z}/n\mathbb{Z}$-algebra of rank 2. For each prime $p \mid n$, we have that A/pA is isomorphic either to $\mathbb{F}_p \times \mathbb{F}_p$ or to $\mathbb{F}_{p^2}$: in the former case we say that A is *split* at p, in the latter we say that A is *non-split* at p. Moreover, for every assignment of each prime $p|n$ to split or non-split, there is a unique, up to isomorphism, algebra A which is split or non-split at every $p \mid n$ accordingly to the assignment.

We fix a $\mathbb{Z}/n\mathbb{Z}$-basis of A and, consequently, we identify the automorphism group of A, as $\mathbb{Z}/n\mathbb{Z}$-module, with $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. The group $A^\times$ of the units of A acts on A by multiplication, giving an embedding of $A^\times$ inside $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. A subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ which is the image of such an embedding is called a *Cartan subgroup.* The normalizer of $A^\times$ inside $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ contains all the matrices representing automorphisms of the ring A, hence $H := \langle A^\times, \mathrm{Aut}_{\mathrm{Ring}}(A)\rangle$ is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ that contains $A^\times$ as normal subgroup. We call every such an H a *Cartan-plus subgroup* of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. The natural map $\mathrm{Aut}_{\mathrm{Ring}}(A) \to \prod_{p|n} \mathrm{Aut}_{\mathrm{Ring}}(A \otimes \mathbb{F}_p)$ is an isomorphism, hence $\mathrm{Aut}_{\mathrm{Ring}}(A)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{\omega(n)}$, where $\omega(n)$ is the number of prime divisors of n. In particular, given A, the Cartan subgroup has index $2^{\omega(n)}$ inside the Cartan-plus subgroup. Moreover, if n is odd, the Cartan-plus is equal to the normalizer of the Cartan subgroup inside $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. We call *Cartan modular curves* the modular curves associated to Cartan subgroups or to Cartan-plus subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.

When $n = p^e$ is a prime power, we use the following notation:

- $X_{\mathrm{ns}}^{+}(p^e) := X_H$, if H is a Cartan-plus subgroup non-split at p;
- $X_{\mathrm{ns}}(p^e) := X_H$, if H is a Cartan subgroup non-split at p;
- $X_{\mathrm{s}}^{+}(p^e) := X_H$, if H is a Cartan-plus subgroup split at p;
- $X_{\mathrm{s}}(p^e) := X_H$, if H is a Cartan subgroup split at p.

Remark 3.4.1. If H_1 and H_2 are two conjugate subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, then the corresponding modular curves X_{H_1} and X_{H_2} are isomorphic. Moreover, given two Cartan or two Cartan-plus subgroups C_1 and C_2 of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ with the same assignment of each prime $p \mid n$ to split or non-split, then C_1 and C_2 are conjugate, so $X_{C_1} \cong X_{C_2}$. This implies that the above definitions are unambiguous.

We want to understand the structure, up to isogeny, of the jacobian of the Cartan modular curves. This is achieved using Chen's isogenies (see [25], [39],[26]). Let p be a prime and let e be a positive integer. We give an analogue of [26, Theorem 1.1] involving the jacobian of $X_{\mathrm{ns}}(p^e)$ for every p, and, to do this, we extend the analysis in [26] to the case $p = 2$. In order to state our result, we choose a non-square element $\xi \in (\mathbb{Z}/p^e\mathbb{Z})^\times$ when p is odd and define the following subgroups of $\mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$ for every prime p:

$$C_{\mathrm{s}}(p^e) := \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}, a, d \in (\mathbb{Z}/p^e\mathbb{Z})^\times \right\};$$

$$C_{\mathrm{s}}^{+}(p^e) := C_{\mathrm{s}} \cup \left\{ \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}, b, c \in (\mathbb{Z}/p^e\mathbb{Z})^\times \right\};$$

$$C_{\mathrm{ns}}(2^e) := \left\{ \begin{pmatrix} a & b \\ b & a+b \end{pmatrix}, a, b \in \mathbb{Z}/2^e\mathbb{Z}, (a,b) \not\equiv (0,0) \bmod 2 \right\};$$

$$C_{\mathrm{ns}}^{+}(2^e) := C_{\mathrm{ns}}(2^e) \cup \left\{ \begin{pmatrix} a & a-b \\ b & -a \end{pmatrix}, a, b \in \mathbb{Z}/2^e\mathbb{Z}, (a,b) \not\equiv (0,0) \bmod 2 \right\};$$

$$C_{\mathrm{ns}}(p^e) := \left\{ \begin{pmatrix} a & b\xi \\ b & a \end{pmatrix}, a, b \in \mathbb{Z}/p^e\mathbb{Z}, (a,b) \not\equiv (0,0) \bmod p \right\}, \quad \text{if } p \text{ is odd;}$$

$$C_{\mathrm{ns}}^{+}(p^e) := C_{\mathrm{ns}}(p^e) \cup \left\{ \begin{pmatrix} a & b\xi \\ -b & -a \end{pmatrix}, a, b \in \mathbb{Z}/p^e\mathbb{Z}, (a,b) \not\equiv (0,0) \bmod p \right\}, \quad \text{if } p \text{ is odd;}$$

$$B_r(p^e) := \left\{ \begin{pmatrix} a & bp^r \\ cp^{r+1} & d \end{pmatrix}, a, b, c, d \in \mathbb{Z}/p^e\mathbb{Z}, \quad ad \not\equiv 0 \bmod p \right\}, \quad \text{for } r = 0, 1, \ldots, e-1;$$

$$T_r(p^e) := \left\{ \begin{pmatrix} a & bp^r \\ cp^r & d \end{pmatrix}, a, b, c, d \in \mathbb{Z}/p^e\mathbb{Z}, ad - bcp^{2r} \in (\mathbb{Z}/p^e\mathbb{Z})^\times \right\}, \quad \text{for } r = 0, 1, \ldots, e.$$

We remark that $T_e(p^e) = C_{\mathrm{s}}(p^e)$ and that $C_{\mathrm{s}}(p^e), C_{\mathrm{ns}}(p^e)$ are respectively a split and a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$ and $C^+_{\mathrm{s}}(p^e), C^+_{\mathrm{ns}}(p^e)$ are the corresponding Cartan-plus subgroups.

Proposition 3.4.2. *Let p be a prime, let e be a positive integer and let $G = \mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$. We have the following isomorphism of $\mathbb{Q}$-representations of G:*

$$\mathbb{Q}[G/C_{\mathrm{ns}}(p^e)] \oplus \bigoplus_{r=0}^{e-1} 2\mathbb{Q}[G/B_r(p^e)] \cong \mathbb{Q}[G/C_{\mathrm{s}}(p^e)] \oplus \bigoplus_{r=0}^{e-1} 2\mathbb{Q}[G/T_r(p^e)]. \tag{3.4.3}$$

Proof. We follow the same strategy as in [26]. It is enough to prove that the representation on the right hand side has the same character as the representation on the left hand side. For every subgroup $H \subset G$, let χ_H be the character of the representation $\mathbb{Q}[G/H]$. If $p = 2$, the character χ_H for the groups appearing in the statement is computed in the Appendix of this article. If p is odd and H has the form B_r, T_r or C_{s}, the character χ_H is given in [26, Tables 3 and 4]; if p is odd and $H = C_{\mathrm{ns}}(p^e)$, then

$$\chi_H(g) = \begin{cases} (p-1)p^{2e-1}, & \text{if } g \text{ is a scalar matrix (type } I \text{ in [26, Tables 3, 4]),} \\ 2p^{2\mu}, & \text{if } g \text{ is a conjugate of } \left(\begin{smallmatrix} \alpha & \xi\beta p^{\mu} \\ \beta p^{\mu} & \alpha \end{smallmatrix}\right)\text{, with } \beta \in (\mathbb{Z}/p^e\mathbb{Z})^\times \\ & \text{ and } 0 \le \mu < e-1 \text{ (types } RI'_{\mu} \text{ and } T' \text{ in [26, Tables 3, 4]),} \\ 0, & \text{otherwise.} \end{cases}$$

The characters of the representations in Equation (3.4.3) are sums of the previous characters. A straightforward computation proves the proposition. □

As explained in [39, Théorème 2 and the discussion below it], the representation theoretic result in Proposition 3.4.2, together with the isomorphisms of modular curves $X_{B_r(p^e)} \cong X_0(p^{2r+1})$ and $X_{T_r(p^e)} \cong X_{C_{\mathrm{s}}}(p^r) \cong X_0(p^{2r})$, implies the following proposition on jacobians of modular curves.

Proposition 3.4.4. *Let p be a prime, let e be a positive integer and let $J_{\mathrm{ns}}(p^e)$ be the jacobian of $X_{\mathrm{ns}}(p^e)$. We have the following isogenies over $\mathbb{Q}$:*

$$J_{\mathrm{ns}}(p^e) \times \prod_{r=0}^{e-1} J_0(p^{2r+1})^2 \sim J_0(p^{2e}) \times \prod_{r=0}^{e-1} J_0(p^{2r})^2, \qquad J_{\mathrm{ns}}(p^e) \sim \prod_{r=1}^{e} J_0^{\mathrm{new}}(p^{2r}).$$

For jacobians of Cartan curves of composite level we have the following theorem.

Theorem 3.4.5. *Let $n > 1$ be an integer and let $H < \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be a Cartan or a Cartan-plus subgroup. Then the jacobian of X_H is a quotient of $J_0(n^2)$.*

Proof. Since all the Cartan-plus subgroups contain a Cartan subgroup, we can suppose that H is a Cartan subgroup. Let a, b be positive integers such that $n = ab$ and such that H is split at all primes dividing a and non-split at all the primes dividing b. If $b = 1$, then $X_H(n) \cong X_0(n^2)$. Thus, we suppose that $b > 1$. Let $b = p_1^{e_1} \cdots p_k^{e_k}$ be the prime factorization of b and for each $j = 1, \ldots, k$, we set $G_j := \mathrm{GL}_2(\mathbb{Z}/p_j^{e_j}\mathbb{Z})$ and $H_j := C_{\mathrm{ns}}(p_j^{e_j}) < G_j$. Moreover we set $G := \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ and $G_{\mathrm{s}} := \mathrm{GL}_2(\mathbb{Z}/a\mathbb{Z})$, and we choose a totally split Cartan subgroup $H_{\mathrm{s}} < G_{\mathrm{s}}$. Chinese Remainder Theorem gives an identification between G and $G_{\mathrm{s}} \times \prod_{j=1}^k G_j$ sending H to a conjugate of $H_s \times \prod_{j=1}^k H_j$.

Instead of working with G-representations up to isomorphism, it is easier to work inside the representation ring of G, namely the Grothendieck ring of the category of finite-dimensional G-representations, where we can take differences of representations. By Proposition 3.4.2 we have the following equality in the representation ring of G_j over $\mathbb{Q}$:

$$\mathbb{Q}\big[G_j/H_j\big] = \mathbb{Q}\big[G_j/K_j(p_j^{2e_j})\big] + 2\sum_{i=0}^{2e_j-1}(-1)^i\mathbb{Q}\big[G_j/K_j(p_j^i)\big],$$

where $K_j(p_j^{2r}) := T_r(p_j^{e_j})$ for $r = 0, \ldots, e_j$, and $K_j(p_j^{2r+1}) := B_r(p_j^{e_j})$ for $r = 0, \ldots, e_j - 1$. Interpreting G_j-representations as G-representations via the reduction modulo $p_j^{e_j}$ map, the above equality also holds in the representation ring of G over $\mathbb{Q}$. We now get information about the representation $\mathbb{Q}[G/H]$ by taking the tensor product of the above identities, for $j = 1, \ldots, k$, and using that, for all the groups $\mathcal{G}_1, \mathcal{G}_2$ and all the subgroups $\mathcal{H}_i < \mathcal{G}_i$, we have the isomorphisms of $(\mathcal{G}_1 \times \mathcal{G}_2)$-representations

$$\mathbb{Q}[\mathcal{G}_1/\mathcal{H}_1] \otimes \mathbb{Q}[\mathcal{G}_2/\mathcal{H}_2] \cong \mathbb{Q}[(\mathcal{G}_1 \times \mathcal{G}_2)/(\mathcal{H}_1 \times \mathcal{H}_2)].$$

Denoting by $\otimes$ the product in the representation ring of G over $\mathbb{Q}$, we have

$$\begin{aligned}\mathbb{Q}\big[G/H\big] &= \mathbb{Q}\big[G_{\mathrm{s}}/H_s\big] \otimes \bigotimes_{j=1}^k \mathbb{Q}\big[G_j/H_j\big] \\ &= \mathbb{Q}\big[G_{\mathrm{s}}/H_s\big] \otimes \bigotimes_{j=1}^k \left(\mathbb{Q}\big[G_j/K_j(p_j^{2e_j})\big] + 2\sum_{i=0}^{2e_j-1}(-1)^i\mathbb{Q}\big[G_j/K_j(p_j^i)\big]\right) \\ &= \sum_{d \mid b^2} \varepsilon(d)m(d)\mathbb{Q}\big[G/K(d)\big],\end{aligned} \tag{3.4.6}$$

where, for every $d = p_1^{f_1} \cdots p_k^{f_k}$ dividing b^2, we have

$$\varepsilon(d) := (-1)^{f_1 + \ldots + f_k}, \quad m(d) := 2^{\#\{j : f_j \neq 2e_j\}}, \quad K(d) := H_s \times \prod_{j=1}^k K_j(p_j^{f_j}) < G.$$

As explained in [39], Equation (3.4.6) implies the following equality in the Grothendieck group of the category of abelian varieties over $\mathbb{Q}$ up to isogeny:

$$\mathrm{Jac}(X_H) \sim \prod_{d|b^2} \mathrm{Jac}(X_{K(d)})^{\varepsilon(d)m(d)}.$$

Denoting by $U(m)$ the Borel subgroup $\{(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix})\} < \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, we notice that a $K_j(p_j^i)$-structure on an elliptic curve E is equivalent to a $U(p_j^i)$-structure on E and a H_s-structure is equivalent to a $U(a^2)$-structure. Therefore, a $K(d)$-structure on an elliptic curve E is equivalent to a $U(a^2d)$-structure on E. Hence the modular curve $X_{K(d)}$ is isomorphic to $X_0(a^2d)$ and consequently

$$\mathrm{Jac}(X_H) \sim \prod_{d|b^2} J_0(a^2d)^{\varepsilon(d)m(d)}.$$

Using $J_0(a^2d) \sim \prod_{m|a^2d} J_0^{\mathrm{new}}(m)^{\sigma_0\left(\frac{a^2d}{m}\right)}$, where $\sigma_0(n)$ is the number of divisors of n, one can compute that

$$\mathrm{Jac}(X_H) \sim \prod_{d|b^2} J_0(a^2d)^{\varepsilon(d)m(d)} \sim \prod_{\substack{c|a^2 \\ d|b}} J_0^{\mathrm{new}}(cd^2)^{\sigma_0\left(\frac{a^2}{c}\right)}. \tag{3.4.7}$$

Hence, in the Grothendieck group of the category of abelian varieties over $\mathbb{Q}$ up to isogeny, $\mathrm{Jac}(X_H)$ is equal to an abelian subvariety of $J_0(n^2)$. This proves the theorem. □

Remark 3.4.8. In [26], Chen deals with Cartan curves and Cartan subroups whose level is an odd prime power. Using the computations in our Appendix, Theorem 1.1 in [26] (and therefore all the results contained in the paper), can be extended to the cases of level 2^e, for e a positive integer. Notice that $C_{\mathrm{s}}^{+}(2^e)$ is different from the normalizer of $C_{\mathrm{s}}(2^e)$ and that, substituting $C_{\mathrm{s}}^{+}(p^e)$ with the normalizer of $C_{\mathrm{s}}(p^e)$, Theorem 1.1 in [26] wouldn't extend to the case of level 2^e.

Now we give a lower bound for the genus of Cartan modular curves: we show that for every $\varepsilon > 0$ the genus of a Cartan modular curve of level n big enough is larger than $n^{2-\varepsilon}$.

Proposition 3.4.9. *Let $n \geq 10^5$ be an integer and let $H < \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be either a Cartan or a Cartan-plus subgroup. Denoting by $g(\Gamma_H)$ the genus of X_H we have*

$$g(\Gamma_H) > 0.01\frac{n^{2-\frac{0.96}{\log\log n}}}{\log\log n}.$$

Proof. Since $\det(H) = (\mathbb{Z}/n\mathbb{Z})^\times$, then $X_H = \Gamma_H\backslash\overline{\mathbb{H}}$. Given a congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ containing $-\mathrm{Id}$, we denote by $d(\Gamma)$ the index $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$. Moreover, we denote by $\varepsilon_\infty(\Gamma)$ the number of cusps of $\Gamma\backslash\overline{\mathbb{H}}$ and by $\varepsilon_2(\Gamma)$, respectively $\varepsilon_3(\Gamma)$, the number of elliptic points of period 2, respectively 3, of $\Gamma\backslash\overline{\mathbb{H}}$. Then, by [38, Theorem 3.1.1], the genus of $\Gamma\backslash\overline{\mathbb{H}}$ is

$$g(\Gamma) = 1 + \frac{d(\Gamma)}{12} - \frac{\varepsilon_2(\Gamma)}{4} - \frac{\varepsilon_3(\Gamma)}{3} - \frac{\varepsilon_\infty(\Gamma)}{2}. \tag{3.4.10}$$

The numbers $d(\Gamma), \varepsilon_\infty(\Gamma), \varepsilon_2(\Gamma)$ and $\varepsilon_3(\Gamma)$ are multiplicative with the following meaning: Given two coprime integers n_1, n_2 and two congruence subgroups $\Gamma_1, \Gamma_2 < \mathrm{SL}_2(\mathbb{Z})$ of level n_1 and n_2 respectively, both containing $-\mathrm{Id}$, then

$$\begin{aligned} d(\Gamma_1 \cap \Gamma_2) &= d(\Gamma_1)d(\Gamma_2), & \varepsilon_\infty(\Gamma_1 \cap \Gamma_2) &= \varepsilon_\infty(\Gamma_1)\varepsilon_\infty(\Gamma_2), \\ \varepsilon_2(\Gamma_1 \cap \Gamma_2) &= \varepsilon_2(\Gamma_1)\varepsilon_2(\Gamma_2), & \varepsilon_3(\Gamma_1 \cap \Gamma_2) &= \varepsilon_3(\Gamma_1)\varepsilon_3(\Gamma_2). \end{aligned} \tag{3.4.11}$$

Let $n = p_1^{e_1} \cdots p_k^{e_k}$ the prime factorization of n and we denote by H_j the reduction of H modulo $p_j^{e_j}$. Then each H_j is either a Cartan or a Cartan-plus subgroup and, under the isomorphism $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \cong \prod_{j=1}^k \mathrm{GL}_2(\mathbb{Z}/p_j^{e_j}\mathbb{Z})$, we have $H \cong \prod_{j=1}^k H_j$ and therefore $\Gamma_H = \bigcap_{j=1}^k \Gamma_{H_j}$. Last equation, together with the multiplicativity and (3.4.10), implies that we can estimate the genus of X_H estimating the quantities $d(\Gamma_H), \varepsilon_\infty(\Gamma_H), \varepsilon_2(\Gamma_H)$ and $\varepsilon_3(\Gamma_H)$ for $n = p^e$. We write these values in Table 3.1 (see [38] and [36] for the split case and [11] for the non-split case).

Table 3.1: Degree, elliptic points and cusps for prime power levels.

H	$d(\Gamma_H)$	$\varepsilon_2(\Gamma_H)$	$\varepsilon_3(\Gamma_H)$	$\varepsilon_\infty(\Gamma_H)$
$C_{\mathrm{s}}(p^e)$	$p^{2e-1}(p{+}1)$	2 if $p \equiv 1\,(4)$ 0 if $p \not\equiv 1\,(4)$	2 if $p \equiv 1\,(3)$ 0 if $p \not\equiv 1\,(3)$	$p^{e-1}(p{+}1)$
$C_{\mathrm{s}}^+(p^e)$	$\frac{p^{2e-1}(p+1)}{2}$	2^{e-1} if $p = 2$ $1{+}\frac{p^{e-1}(p-1)}{2}$ if $p \equiv 1\,(4)$ $\frac{p^{e-1}(p+1)}{2}$ if $p \equiv 3\,(4)$	1 if $p \equiv 1\,(3)$ 0 if $p \not\equiv 1\,(3)$	2 if $p^e = 2$ $\frac{p^{e-1}(p+1)}{2}$
$C_{\mathrm{ns}}(p^e)$	$p^{2e-1}(p{-}1)$	0 if $p \not\equiv 3\,(4)$ 2 if $p \equiv 3\,(4)$	0 if $p \not\equiv 2\,(3)$ 2 if $p \equiv 2\,(3)$	$p^{e-1}(p{-}1)$
$C_{\mathrm{ns}}^+(p^e)$	$\frac{p^{2e-1}(p-1)}{2}$	2^{e-1} if $p = 2$ $\frac{p^{e-1}(p-1)}{2}$ if $p \equiv 1\,(4)$ $1{+}\frac{p^{e-1}(p+1)}{2}$ if $p \equiv 3\,(4)$	0 if $p \not\equiv 2\,(3)$ 1 if $p \equiv 2\,(3)$	1 if $p^e = 2$ $\frac{p^{e-1}(p-1)}{2}$

The table implies that for every prime p_j dividing n with exponent e_j we have

$$d(\Gamma_{H_j}) \geq \tfrac{1}{2}p_j^{2e_j}(1-\tfrac{1}{p_j}), \quad \varepsilon_2(\Gamma_{H_j}) \leq p_j^{e_j}, \quad \varepsilon_3(\Gamma_{H_j}) \leq 2, \quad \varepsilon_\infty(\Gamma_{H_j}) \leq p_j^{e_j}(1+\tfrac{1}{p_j}).$$

These inequalities and the multiplicativity (3.4.11) imply the following estimates for $n \geq 15$:

$$d(\Gamma_H) \geq \frac{n\phi(n)}{2^{\omega(n)}} > \frac{n^2}{4.4\,\log\log(n)2^{\omega(n)}} \geq \frac{n^2}{4.4\,\log\log(n)2^{1.3841\frac{\log n}{\log\log n}}} > \frac{n^{2-\frac{0.96}{\log\log n}}}{4.4\,\log\log n},$$

$$\varepsilon_2(\Gamma_H) \leq n, \quad \varepsilon_3(\Gamma_H) \leq 2^{\omega(n)} \leq n, \quad \varepsilon_\infty(\Gamma_H) \leq n\prod_{j=1}^{k}(1+\tfrac{1}{p_j}) \leq \sigma_1(n) \leq 2.59n\log\log n,$$

where $\phi(n)$ is Euler's totient function which is estimated using [89, Theorem 15], $\omega(n) = k$ is the number of prime divisors of n which is estimated as in [87, Théorème 11], and $\sigma_1(n)$ is the sum of positive divisors of n which is estimated as in [55, Theorem 1]. For $n \geq 10^5$, substituting in (3.4.10), we get

$$g(\Gamma_H) > 1 + \frac{n^{2-\frac{0.96}{\log\log n}}}{52.8\,\log\log n} - \frac{n}{3} - \frac{n}{4} - 1.3n\log\log n \geq 0.01\frac{n^{2-\frac{0.96}{\log\log n}}}{\log\log n}.$$

□

3.5 Field of definition of automorphisms

In this section we prove that, when the level is large enough, every automorphism of the modular curve X_H associated to a subgroup H of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ is defined over the compositum of some quadratic fields, and in some cases we find explicitly this field.

Whenever K is a field, X is a variety over K, and F is an extension of K, we write $\mathrm{Aut}_F(X)$ for the set of automorphisms of X defined over F; analogously we use the notations $\mathrm{End}_F(X)$ and $\mathrm{Hom}_F(X,Y)$ for X and Y being abelian varieties over K. Whenever we omit the dependency on the field, we mean automorphisms (or endomorphisms) defined over the algebraic closure of K; in particular when X is a modular curve the "group of the automorphisms of X" is $\mathrm{Aut}_{\overline{\mathbb{Q}}}(X)$ or equivalently $\mathrm{Aut}_{\mathbb{C}}(X)$. We start with a straightforward generalization of [60, Lemma 1.4].

Lemma 3.5.1. *Let K be a perfect field with algebraic closure $\overline{K}$, let X be a smooth projective and geometrically connected curve defined over K of genus $g(X)$ and let $\mathrm{Jac}(X)$ be its jacobian variety. We suppose that there are two abelian varieties A_1 and A_2 over K such that $\mathrm{Hom}_{\overline{K}}(A_1, A_2) = 0$ and such that $\mathrm{Jac}(X)$ is isogenous to $A_1 \times_K A_2$. If*

$$g(X) > 2\dim(A_2) + 1,$$

and if $F \subset \overline{K}$ is an extension of K such that $\mathrm{End}_{\overline{K}}(A_1) = \mathrm{End}_F(A_1)$, then every automorphism of X over $\overline{K}$ can be defined over F.

Proof. We fix isogenies $\varphi\colon \mathrm{Jac}(X) \to A_1 \times_K A_2$ and $\tilde{\varphi}\colon A_1 \times_K A_2 \to \mathrm{Jac}(X)$ whose compositions are multiplications by an integer. Let $u \in \mathrm{Aut}_{\overline{K}}(X)$ and $\sigma \in \mathrm{Gal}(\overline{K}/F)$ and consider the automorphism $v := u^\sigma \circ u^{-1}$. Let Y be the quotient of X by the subgroup of automorphisms generated by v (which is finite since $g(X) \geq 2$) and let $\mathrm{Jac}(Y)$ be the jacobian of Y. Using φ and the equality $\mathrm{Hom}_{\overline{K}}(A_1, A_2) = 0$, we can identify $u_*, u_*^\sigma \in \mathrm{Aut}_{\overline{K}}(\mathrm{Jac}(X))$ respectively with

$$(u_1, u_2), (u_1^\sigma, u_2^\sigma) \in \left(\mathrm{End}_{\overline{K}}(A_1 \times_K A_2) \otimes \mathbb{Q}\right)^\times \cong \left(\mathrm{End}_{\overline{K}}(A_1) \otimes \mathbb{Q}\right)^\times \times \left(\mathrm{End}_{\overline{K}}(A_2) \otimes \mathbb{Q}\right)^\times.$$

Since $\mathrm{End}_{\overline{K}}(A_1) = \mathrm{End}_F(A_1)$, then $u_1 = u_1^\sigma$, and $v_* = (\mathrm{id}, v_2)$. This implies that there is a morphism of abelian varieties $A_1 \to \mathrm{Jac}(Y)$ with finite kernel, namely the composition of the natural inclusion $A_1 \to A_1 \times_K A_2$, the isogeny $\tilde{\varphi}$ and the map $\mathrm{Jac}(X) \to \mathrm{Jac}(Y)$. In particular, denoting by $g(Y)$ the genus of Y, we have

$$g(X) - \dim(A_2) = \dim(A_1) \leq g(Y).$$

Hence, by the Riemann-Hurwitz formula applied to the projection $X \to Y$, we have

$$\dim(A_1) + \dim(A_2) - 1 \geq d(g(Y) - 1) \geq d \dim(A_1) - d,$$

where d is the order of v. If $d > 1$, we get $\dim(A_1) \leq \dim(A_2) + 1$, which is impossible by hypothesis. Hence $d = 1$ and v is the identity. This implies that $u^\sigma = u$, for every $\sigma \in \mathrm{Gal}(\overline{K}/F)$, i.e., since K is perfect, $u \in \mathrm{Aut}_F(X)$. □

Every abelian variety A over a number field K, is isogenous over $\mathbb{C}$ to a product of geometrically simple abelian varieties. We denote by A^{C} the CM part of A that is the product, with multiplicities, of the simple abelian varieties in the decomposition of A with complex multiplication and we denote by A^{N} the non-CM part of A defined analogously. The CM part and the non-CM part of A are unique only up to isogeny and are defined over K. We want to apply Lemma 3.5.1 to the case $A_1 = \mathrm{Jac}(X)^{\mathrm{N}}$ and $A_2 = \mathrm{Jac}(X)^{\mathrm{C}}$. Hence, we are interested in an upper bound on the dimension of the CM part of the jacobian of Cartan modular curves. By Theorem 3.4.5, it is enough to know an upper bound in the case $X = X_0(n)$.

Proposition 3.5.2. *For every integer $n > 1$, the dimension $g_0^{\mathrm{C}}(n)$ of the CM part of $J_0(n)$ satisfies*

$$g_0^{\mathrm{C}}(n) \leq 9 \log(n)^2 n^{\frac{1}{2} + \frac{2.816}{\log\log n}}.$$

Proof. For every positive integer k, let $J_0^{\mathrm{new}}(k)$ be the new part of $J_0(k)$ and let $\sigma_0(k)$ be the number of positive divisors of k. Then we have a canonical isogeny

$$J_0(n) \sim \prod_{d|n} J_0^{\mathrm{new}}(d)^{\sigma_0(n/d)}.$$

Denoting by $g_0^{\mathrm{new,C}}(d)$ the dimension of the CM part of $J_0^{\mathrm{new}}(d)$, we also have

$$g_0^{\mathrm{C}}(n) = \sum_{d|n} \sigma_0(n/d) g_0^{\mathrm{new,C}}(d). \tag{3.5.3}$$

We know that $J_0^{\mathrm{new}}(d)$ is isogenous over $\mathbb{Q}$ to $\prod_{[f]} A_f$, where $[f]$ is the Galois orbit of the newform f (see [38, Chapter 6]). By [95, Proposition 1.6], A_f has non-trivial CM part if and only if A_f is isogenous over $\mathbb{C}$ to the product of finitely many copies of an elliptic curve with CM by an imaginary quadratic field K, which is in turn equivalent to the existence of an ideal $\mathfrak{m}$ of $\mathcal{O}_K$ and a primitive Grössencharacter λ of K defined modulo $\mathfrak{m}$ such that $f = f_\lambda$ (see [96, Section 4] for the definition of Grössencharacter and the definition of the modular form associated to a Grössencharacter), the nebentypus ε_λ is trivial (see [96, Lemma 3]) and $d = |\Delta_K||\mathfrak{m}|$, where Δ_K is the discriminant of K and $|\mathfrak{m}|$ is the norm of the ideal $\mathfrak{m}$. This implies that $g_0^{\mathrm{new,C}}(d)$ is equal to the number of such triples $(K, \mathfrak{m}, \lambda)$. For every choice of K and $\mathfrak{m}$, the set of primitive Grössencharacters of K defined modulo $\mathfrak{m}$ is a subset of the set of Grössencharacters of K defined modulo $\mathfrak{m}$. If this set is not empty, then there is at least one Grössencharacter λ_0 and all other Grössencharacters are given by $\lambda_0\chi$, for χ a character of the group

$$\widetilde{\mathrm{Cl}}_{\mathfrak{m}}(K) := \frac{\{\text{fractional ideals of } \mathcal{O}_K \text{ coprime to } \mathfrak{m}\}}{\{(\alpha) : \exists a \in \mathbb{Z} \text{ coprime to } \mathfrak{m} \text{ such that } \alpha \equiv a \bmod \mathfrak{m}\}}.$$

Thus, for given K and $\mathfrak{m}$, the cardinality of $\widetilde{\mathrm{Cl}}_{\mathfrak{m}}(K)$ is larger than the number of triples $(K, \mathfrak{m}, \lambda)$ we are interested in, hence

$$g_0^{\mathrm{new,C}}(d) \leq \sum_{|\Delta_K||\mathfrak{m}|=d} \#\widetilde{\mathrm{Cl}}_{\mathfrak{m}}(K)\,. \tag{3.5.4}$$

To give a bound on $\widetilde{\mathrm{Cl}}_{\mathfrak{m}}(K)$ we look at the following short exact sequence

$$1 \longrightarrow \frac{(\mathcal{O}_K/\mathfrak{m})^\times}{\mathcal{O}_K^\times \cdot (\mathbb{Z}/(\mathbb{Z}\cap\mathfrak{m}))^\times} \longrightarrow \widetilde{\mathrm{Cl}}_{\mathfrak{m}}(K) \longrightarrow \mathrm{Cl}(K) \longrightarrow 0,$$

where $\mathrm{Cl}(K)$ is the class group of K and we write $\mathcal{O}_K^\times$ and $(\mathbb{Z}/(\mathbb{Z}\cap\mathfrak{m}))^\times$ in place of their natural image inside $(\mathcal{O}_K/\mathfrak{m})^\times$. We write $\mathfrak{m} = \prod_p \mathfrak{m}_p$ for p varying in the set of rational primes and $\mathfrak{m}_p$ being a product of primes of $\mathcal{O}_K$ dividing p. Thus the above short exact sequence gives

$$\begin{aligned}\#\widetilde{\mathrm{Cl}}_{\mathfrak{m}}(K) \le \#\mathrm{Cl}(K)\cdot\#\Big(\frac{(\mathcal{O}_K/\mathfrak{m})^\times}{(\mathbb{Z}/(\mathbb{Z}\cap\mathfrak{m}))^\times}\Big) &= \#\mathrm{Cl}(K)\prod_{p\,\mid\,|\mathfrak{m}|}\#\Big(\frac{(\mathcal{O}_K/\mathfrak{m}_p)^\times}{(\mathbb{Z}/(\mathbb{Z}\cap\mathfrak{m}_p))^\times}\Big) \le\\ \le 3\log(|\Delta_K|)\sqrt{|\Delta_K|}\prod_{p\,\mid\,|\mathfrak{m}|}\Big((1+\tfrac{1}{p})|\mathfrak{m}_p|^{1/2}\Big) &= 3\log(|\Delta_K|)\sqrt{|\Delta_K||\mathfrak{m}|}\prod_{p\,\mid\,|\mathfrak{m}|}(1+\tfrac{1}{p}),\end{aligned}$$

where the class number of K is estimated using [81, Theorem 8.10 and Lemma 8.16] and the bound on the cardinality of $(\mathcal{O}_K/\mathfrak{m}_p)^\times/(\mathbb{Z}/(\mathbb{Z}\cap\mathfrak{m}_p))^\times$ is trivial after factoring $\mathfrak{m}_p$. Substituting in (3.5.4), we have

$$g_0^{\mathrm{new,C}}(d) \le \sum_{|\Delta_K||\mathfrak{m}|=d}\Big(3\sqrt{d}\log(|\Delta_K|)\prod_{p|\,|\mathfrak{m}|}(1+\tfrac{1}{p})\Big).$$

Let $M_d := \#\Big\{(K,\mathfrak{m}) : |\Delta_K||\mathfrak{m}| = d\Big\}$ and for $m \in \mathbb{Z}_{\ge 1}$, we denote by $\sigma_1(m)$ the sum of the positive divisors of m. We have $\sigma_1(m) < 3m\log m$, for each $m \ge 2$ (see [55, Theorem 1] if $m \ge 7$, it is trivial in the remaining cases). Then

$$g_0^{\mathrm{new,C}}(d) \le 3M_d\sqrt{d}\log(d)\prod_{p|d}(1+\tfrac{1}{p}) \le 3M_d\sqrt{d}\log(d)\tfrac{\sigma_1(d)}{d} \le 9M_d\sqrt{d}\log(d)^2.$$

Substituting in (3.5.3), we get

$$\begin{aligned}g_0^{\mathrm{C}}(n) &\le 9\sum_{d|n}\sigma_0(n/d)M_d\sqrt{d}\log(d)^2 \le 9\sqrt{n}\log(n)^2\sum_{d|n}M_d\sigma_0(n/d) \le\\ &\le 9\sqrt{n}\log(n)^2\#\Big\{(K,\mathfrak{m},d) : |\Delta_K||\mathfrak{m}|d \text{ divides } n\Big\}.\end{aligned}\tag{3.5.5}$$

Writing the prime factorization $n = \prod_{i=1}^r p_i^{e_i}$, we know that an imaginary quadratic field K with discriminant dividing n must be $K = \mathbb{Q}(\sqrt{-\prod_{i=1}^r p_i^{\varepsilon_i}})$, with $\varepsilon \in \{0,1\}^r$. Hence

$$\begin{aligned}\#\Big\{(K,\mathfrak{m},d) : |\Delta_K||\mathfrak{m}|d \text{ divides } n\Big\} &\le \sum_{\varepsilon\in\{0,1\}^r}\#\Big\{(\mathfrak{m},d) : |\Delta_K||\mathfrak{m}|d \text{ divides } n\Big\} \le\\ \le \sum_{\substack{\varepsilon\in\{0,1\}^r\\ m\in\mathbb{Z}_{>0}}}\#\Big\{\mathfrak{m}\subset\mathcal{O}_K : |\mathfrak{m}| = m\Big\}\cdot\#\Big\{d\in\mathbb{Z}_{>0} &: dm\prod_{i=1}^r p_i^{\varepsilon_i} \text{ divides } n\Big\}.\end{aligned}$$

We have the factorizations $m = \prod_{i=1}^r p_i^{f_i}$ and $d = \prod_{i=1}^r p_i^{c_i}$, where $f_i, c_i \in \{0,1,\dots,e_i\}$, for $i = 1,\dots,r$, and we denote by f the r-tuple whose components are the f_i's and similarly we define c. Then the number of ideals $\mathfrak{m}$ in $\mathcal{O}_K$ having norm m is less than $\prod_{i=1}^r(f_i{+}1)$ which is equal to the number of pairs (a,b) of elements of $\mathbb{Z}_{\ge 0}^r$ such that

$a+b=f$. Hence we get

$$\#\Big\{(K,\mathfrak{m},d):|\Delta_K||\mathfrak{m}|d \text{ divides } n\Big\}\leq\#\Big\{(\varepsilon,a,b,c)\in\{0,1\}^r\times(\mathbb{Z}^r_{\geq 0})^3\colon \varepsilon_i+a_i+b_i+c_i\leq e_i\Big\}\leq$$

$$\leq\prod_{i=1}^r\Big(\#\Big\{(a_i,b_i,c_i)\in\mathbb{Z}^3_{\geq 0}: a_i+b_i+c_i\leq e_i\Big\}+\#\Big\{(a_i,b_i,c_i)\in\mathbb{Z}^3_{\geq 0}: a_i+b_i+c_i\leq e_i-1\Big\}\Big)\leq$$

$$\leq\prod_{i=1}^r\left(\binom{e_i+3}{3}+\binom{e_i+2}{3}\right)\leq\prod_{i=1}^r\frac{(e_i+2)(e_i+1)^2}{2}.$$

Notice that $\sigma_0(n)=\prod_{i=1}^r(e_i+1)$ is the number of positive divisors of n and that the product $\prod_{i=1}^r\frac{(e_i+2)(e_i+1)}{2}$ is the number of triples (d_1,d_2,d_3) of positive integers such that $d_1d_2d_3=n$. Using the upper bounds, contained in [82] and [88], for these two quantities, we get

$$\#\Big\{(K,\mathfrak{m},d):|\Delta_K||\mathfrak{m}|d \text{ divides } n\Big\}\leq n^{\frac{1.538\log 2}{\log\log n}}n^{\frac{1.592\log 3}{\log\log n}}\leq n^{\frac{2.816}{\log\log n}}.$$

Substituting in (3.5.5) we find

$$g_0^{\mathrm{C}}(n)\leq 9\sqrt{n}\log(n)^2n^{\frac{2.816}{\log\log n}}=9\log(n)^2n^{\frac{1}{2}+\frac{2.816}{\log\log n}}.$$

□

When the level is a prime power, the previous upper bound is easier and smaller.

Proposition 3.5.6. *For every prime p and positive integer e, the dimension $g_0^{\mathrm{C}}(p^e)$ of the CM part of $J_0(p^e)$ satisfies*

$$g_0^{\mathrm{C}}(p^e)\leq\begin{cases}13\sqrt{2^e} & \text{if } p=2,\\ 0 & \text{if } p\equiv 1 \bmod 4,\\ 5.5\sqrt{p^e}\log p & \text{if } p\equiv 3 \bmod 4.\end{cases}$$

The proof follows the same steps of the previous proposition and is simplified by the fact that there are few quadratic imaginary fields K whose discriminant divides p^e. More precisely: there are two fields when $p=2$, there are no fields if $p\equiv 1$ mod 4 and there is only one field if $p\equiv 3$ mod 4. We now give an upper bound for the field of definition of the automorphisms of a Cartan modular curve of large enough level.

Proposition 3.5.7. *Let $n\geq 10^{400}$ be an integer and let $H<\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be either a Cartan or a Cartan-plus subgroup. Then every automorphism of X_H is defined over the compositum of all the quadratic fields whose discriminant divides n.*

Proof. Let J_H be the jacobian of X_H and let J_H^{C} and J_H^{N} be the CM part and the non-CM part of J_H respectively. By Lemma 3.5.1, it is enough to prove that $2\dim(J_H^{\mathrm{C}})+1$ is smaller than the genus of X_H and that every endomorphism of J_H^{N} is defined over the compositum of all the quadratic fields whose discriminant divides n. The latter is true because, by Theorem 3.4.5, J_H^{N} is a quotient of $J_0(n^2)^{\mathrm{N}}$ and by [60, Proposition 1.3] every endomorphism of $J_0(n^2)^{\mathrm{N}}$ is defined over the compositum of all the quadratic fields whose discriminant divides n. By Theorem 3.4.5 J_H^{C} is a quotient of $J_0(n^2)^{\mathrm{C}}$ hence we can use Proposition 3.5.2 to bound the $\dim(J_H^{\mathrm{C}})$; this, together with the bound for the genus $g(X_H)$ of X_H given in Proposition 3.4.9, implies the inequality we need when $n \geq 10^{400}$:

$$2\dim(J_H^{\mathrm{C}})+1 \leq 2\dim(J_0(n^2)^{\mathrm{C}})+1 \leq 73\log(n)^2 n^{1+\frac{5.632}{\log\log n}} < \frac{n^{2-\frac{0.96}{\log\log n}}}{100\log\log n} < g(X_H).$$

□

Proposition 3.5.7 can be made sharper when n is a prime power.

Proposition 3.5.8. *Let p be a prime and e a positive integer and let X be a curve associated to a Cartan or a Cartan-plus subgroup of level p^e. If the genus of X is at least 2, then every automorphism of X is defined over the field*

$$K_p = \begin{cases} \mathbb{Q}(i,\sqrt{2}), & \text{if } p = 2,\\ \mathbb{Q}\left(\sqrt{p}\right), & \text{if } p \equiv 1 \bmod 4,\\ \mathbb{Q}\left(\sqrt{-p}\right), & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

A strategy of proof is the same of Proposition 3.5.7:

(I) give an upper bound for $\dim(\mathrm{Jac}(X)^{\mathrm{C}})$;

(II) give a lower bound for the genus;

(III) apply [60, Proposition 1.3] and Theorem 3.4.5 to deduce that the endomorphisms of $\mathrm{Jac}(X)^{\mathrm{N}}$ are defined over K_p;

(IV) apply Lemma 3.5.1.

In particular in the case of $X_{\mathrm{ns}}(p^e)$ and $X_{\mathrm{ns}}^{+}(p^e)$, when $p^e > 600$, the propositions 3.4.4 and 3.5.6 and Table 3.1 give bounds in ((I)) and ((II)) that are sharp enough for ((IV)). If $p^e \leq 600$, the bounds in Proposition 3.5.6 are sometimes not sharp enough. In these cases we can compute explicitly the CM part and notice that only a factor of it of low dimension has endomorphisms defined over a field bigger than K_p: whenever a CM factor is a rational elliptic curve, we know by CM theory that its endomorphisms are defined over K_p and it can be discarded from the count. This is done in the MAGMA script available at [70]. The case $X_{\mathrm{s}}(p^e) \cong X_0(p^{2e})$ follows from [60, Corollary 1.14] and the case $X_{\mathrm{s}}^+(p^e) \cong X_0(p^{2e})$ follows from the following proposition.

Proposition 3.5.9. *Let p be a prime and e a positive integer. If the genus of $X_0^*(p^e)$ is at least 2, then every automorphism of $X_0^*(p^e)$ is defined over the field*

$$K_p = \begin{cases} \mathbb{Q}(i, \sqrt{2}), & \text{if } p = 2, \\ \mathbb{Q}\left(\sqrt{p}\right), & \text{if } p \equiv 1 \bmod 4, \\ \mathbb{Q}\left(\sqrt{-p}\right), & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

Again, one can apply the same strategy used for Propositions 3.5.7 and 3.5.8, together with the MAGMA script available at [70]. In particular we need a lower bound for the genus of $X_0^*(p^e)$. Since we do not know an explicit reference giving a formula for this genus, we write it in the following remark.

Remark 3.5.10. Given a positive integer n, let $X_0^+(n)$ be the quotient of $X_0(n)$ by the n-th Atkin-Lehner operator. This curve is equal to $X_0^*(n)$ when n is the power of a prime.

In [84, Equation 9] there is a formula for the genus $g_0^+(n)$ of $X_0^+(n)$ when n is prime. When $n = p^{2e}$ with p prime, we can compute $g_0^+(n)$ using Table 3.1 since $X_0^+(n)$ is isomorphic to a split Cartan curve. For general n, [84, Equation 9] can be easily generalized applying Riemann-Hurwitz formula to the natural map $X_0(n) \to X_0^+(n)$ and counting the number of fixed points of the n-th Atkin-Lehner operator. This gives

$$g_0^+(n) = \begin{cases} 0, & \text{if } n \in \{1,2,3,4\}, \\ \frac{1+g_0(n)}{2} - \frac{h(-n)+h(-4n)}{4}, & \text{if } n \geq 5 \text{ is odd}, \\ \frac{1+g_0(n)}{2} - \frac{h(-4n)}{4}, & \text{if } n \geq 5 \text{ is even}, \end{cases}$$

where $g_0(n)$ is the genus of $X_0(n)$ and $h(D)$ is the class number of the quadratic order with discriminant D, with the convention $h(D) = 0$ if D is a square or if $D \equiv 2, 3 \bmod 4$.

Remark 3.5.11. We are not always able to prove that every automorphism of a Cartan modular curve is defined over a compositum of quadratic fields. For example, an analogue of Section 3.4.7 for Cartan-plus curves, proved using Chen's isogeny in [26], implies that the jacobian of the totally non-split Cartan-plus curve X of level 48 contains $J_0^{\mathrm{new},*}(48^2)$. Since there are two CM (weight 2) newforms of level 48^2 of degree 2 and invariant under the action of both the Atkin-Lehner operators w_9 and w_{256}, then the jacobian $J_0^{\mathrm{new},*}(48^2)$ has a CM part of dimension at least 4 whose endomorphisms could be defined over a field bigger than the compositum of quadratic fields. This prevents us from applying Lemma 3.5.1 in ((IV)) of the strategy above, because the genus of X is 9 (see Table 3.1).

3.6 Automorphisms

In this section we treat our main problem, namely to determine the automorphisms of certain modular curves X_H over $\mathbb{C}$ for a subgroup H of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. We restrict our attention to X_H geometrically connected, i.e., $\det(H) = (\mathbb{Z}/n\mathbb{Z})^\times$. Every automorphism we are interested in induces an automorphism of the Riemann surface $X_H(\mathbb{C}) = \Gamma_H\backslash\overline{\mathbb{H}}$ and, since it is compact, each of these automorphisms comes from an automorphism of the algebraic curve $(X_H)_{\mathbb{C}}$. Let $\mathbb{P}\colon \mathrm{GL}_2^+(\mathbb{Q}) \to \mathrm{PGL}_2^+(\mathbb{Q})$ be the natural map. Each matrix $m \in \mathrm{PGL}_2^+(\mathbb{Q})$ defines a Möbius transformation $m\colon \overline{\mathbb{H}} \to \overline{\mathbb{H}}$ and such an automorphism of the Riemann surface $\overline{\mathbb{H}}$ pushes down to an automorphism of $\Gamma_H\backslash\overline{\mathbb{H}}$ if and only if m normalizes $\mathbb{P}(\Gamma_H)$.

Definition 3.6.1. Let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ such that $\det(H) = (\mathbb{Z}/n\mathbb{Z})^\times$. An automorphism of X_H defined over $\mathbb{C}$ is *modular* if its action on $X_H(\mathbb{C}) = \Gamma_H\backslash\overline{\mathbb{H}}$ is described by a Möbius transformation associated to a matrix $m \in \mathrm{PGL}_2^+(\mathbb{Q})$ normalizing $\mathbb{P}(\Gamma_H)$.

When H has surjective determinant, $\mathrm{Aut}(X_H)$ contains the subgroup of modular automorphisms which is isomorphic to $\mathcal{N}/\mathbb{P}(\Gamma_H)$, where $\mathcal{N}$ is the normalizer of $\mathbb{P}(\Gamma_H)$ inside $\mathrm{PGL}_2^+(\mathbb{Q})$.

Remark 3.6.2. Notice that we can define modular automorphisms of Y_H looking at $\mathrm{PGL}_2^+(\mathbb{R})$, instead of $\mathrm{PGL}_2^+(\mathbb{Q})$, as follows: an automorphism ι of $Y_H(\mathbb{C}) = \Gamma_H\backslash\mathbb{H}$ is *modular* if there is a matrix $m \in \mathrm{PGL}_2^+(\mathbb{R})$ that normalizes the image of Γ_H in $\mathrm{PGL}_2^+(\mathbb{R})$ and hence defines a Möbius transformation $m\colon \mathbb{H} \to \mathbb{H}$ that pushes down to ι. This is equivalent to the previous definition. Indeed if $\tilde{m} \in \mathrm{GL}_2^+(\mathbb{R})$ is a lift of m, then $\tilde{m}$ normalizes $\Gamma_{\pm H} = (\mathbb{R}^\times\Gamma_H) \cap \mathrm{SL}_2(\mathbb{R})$, hence conjugation by $\tilde{m}$ preserves the set of $\mathbb{Q}$-linear combinations of matrices in $\Gamma_{\pm H}$, which is equal to the set of matrices with entries in $\mathbb{Q}$. Looking at the conjugates by $\tilde{m}$ of the matrices $\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right)$, we easily deduce that $\tilde{m}$ is a real multiple of a matrix in $\mathrm{GL}_2(\mathbb{Q})$, and consequently m lies in $\mathrm{PGL}_2^+(\mathbb{Q})$.

In other words: every modular automorphism of $Y_H(\mathbb{C})$ extends to a modular automorphism of X_H and, conversely, every modular automorphism of X_H preserves the set of cusps, hence restricts to a modular automorphism of $Y_H(\mathbb{C})$.

If an automorphism is modular, then it preserves the set of cusps and also the set of branch points for the map $\mathbb{H} \to \Gamma_H\backslash\mathbb{H}$. The converse is also true.

Lemma 3.6.3. *Let n be a positive integer and let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ such that $\det(H) = (\mathbb{Z}/n\mathbb{Z})^\times$. An automorphism of X_H defined over $\mathbb{C}$ is modular if and only if it preserves the set of cusps and the set of branch points for the map $\mathbb{H} \to \Gamma_H\backslash\mathbb{H} = Y_H(\mathbb{C})$.*

Proof. We prove that an automorphism u of X_H is modular if it preserves the set of cusps and the set of branch points for the map $\mathbb{H} \to \Gamma_H \backslash \mathbb{H} = Y_H(\mathbb{C})$. Since u preserves the set of the cusps, then it restricts to an automorphism of $Y_H(\mathbb{C})$. Moreover, since u preserves $\mathcal{B}$, then it induces an automorphism $\tilde{u}$ of $Y_H(\mathbb{C}) - \mathcal{B}$. Since $\det(H) = (\mathbb{Z}/n\mathbb{Z})^\times$, the map

$$\tilde{\pi}\colon \mathbb{H} - \pi^{-1}(\mathcal{B}) \longrightarrow Y_H(\mathbb{C}) - \mathcal{B}$$

is a covering map and the pushforward $\tilde{\pi}_*$ sends the fundamental group $\pi_1(\mathbb{H} - \pi^{-1}(\mathcal{B}))$ to the subgroup of $\pi_1(Y_H(\mathbb{C}) - \mathcal{B})$ generated by the loops running around a point in $\mathcal{B}$. Since $\tilde{u}$ extends to $u\colon Y_H(\mathbb{C}) \to Y_H(\mathbb{C})$, the image, under $\tilde{u}$, of a loop running around a point in $\mathcal{B}$ is still a loop running around a point in $\mathcal{B}$. Hence, $\tilde{u}_*$ sends $\tilde{\pi}_*(\pi_1(\mathbb{H} - \pi^{-1}(\mathcal{B})))$ into itself and consequently $\tilde{u}$ lifts to an automorphism $\tilde{v}$ of $\mathbb{H} - \pi^{-1}(\mathcal{B})$. Again, since $\tilde{u}$ extends to $u\colon Y_H(\mathbb{C}) \to Y_H(\mathbb{C})$, then $\tilde{v}$ extends to an automorphism $v\colon \mathbb{H} \to \mathbb{H}$ as well.

We know that $\mathrm{Aut}(\mathbb{H}) = \mathrm{PGL}_2^+(\mathbb{R})$, hence v is a Möbius transformation given by a matrix $m \in \mathrm{PGL}_2^+(\mathbb{R})$ and, since it passes to the quotient, m belongs to the normalizer of the image of Γ_H in $\mathrm{PGL}_2^+(\mathbb{R})$. Hence the restriction of u to Y_H is modular and, by Remark 3.6.2, u itself is modular. □

In the following two propositions, we give sufficient conditions for an automorphism to preserve the set of cusps and the set of branch points.

Proposition 3.6.4. *Let n be a positive integer and let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ containing the scalar matrices and such that $\det(H) = (\mathbb{Z}/n\mathbb{Z})^\times$. Let $\mathrm{gon}(X_H)$ be the gonality of X_H. If there is a prime ℓ not dividing n such that $5 \le \ell < \frac{1}{2}\mathrm{gon}(X_H) - 1$, then every automorphism of X_H defined over a compositum of quadratic fields preserves the set of cusps.*

Proof. Let u be an automorphism of X_H defined over the compositum L of some quadratic fields and let $C \in X_H(\mathbb{C})$ be a cusp. Then the propositions 3.3.2 and 3.3.4 imply

$$T_\ell u(C) = u^\sigma T_\ell(C) = \ell u^\sigma \langle \ell \rangle (C^{\sigma^{-1}}) + u^\sigma(C^\sigma),$$

where $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ is a Frobenius element at ℓ. Since $\ell \ge 5$, then $T_\ell u(C)$ contains a point of multiplicity at least 4 and, by Part (1) of Proposition 3.3.6, this implies that $u(C)$ must be a cusp. □

Proposition 3.6.5. *Let n be a positive integer and let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ containing the scalar matrices and such that $\det(H) = (\mathbb{Z}/n\mathbb{Z})^\times$. Let $\mathrm{gon}(X_H)$ be the gonality of X_H. If there are two prime numbers $\ell_1 < \ell_2$ not dividing n and such that $5 \le \ell_2 < \frac{1}{2}\mathrm{gon}(X_H) - 1$, then every automorphism of X_H defined over a compositum of quadratic fields preserves the set of branch points of the map $\mathbb{H} \to \Gamma_H \backslash \mathbb{H} = Y_H(\mathbb{C})$.*

Proof. Let L be a compositum of quadratic fields and let $\sigma_1, \sigma_2 \in \mathrm{Gal}(L/\mathbb{Q})$ be Frobenius elements at the primes ℓ_1 and ℓ_2 respectively. Let u be an automorphism of X_H defined over L and let $P = (E, \phi) \in Y_H(\mathbb{C})$ be a branch point for the map $\mathbb{H} \to \Gamma_H \backslash \mathbb{H} = Y_H(\mathbb{C})$. Applying Proposition 3.6.4 with $\ell = \ell_2 \geq 5$, we deduce that u sends non-cuspidal points to non-cuspidal points, hence we can write $u(P) = (E', \phi')$ for some elliptic curve $E'/\mathbb{C}$. Proposition 3.3.2 implies that

$$T_{\ell_1} u(P) = u^{\sigma_1} T_{\ell_1}(P) \quad \text{and} \quad T_{\ell_2} u(P) = u^{\sigma_2} T_{\ell_2}(P). \tag{3.6.6}$$

Since, up to isomorphism, the only elliptic curves over $\mathbb{C}$ with non-trivial automorphisms are E_i and E_ρ, Proposition 3.2.4 implies that there are only two possibilities: $E = E_i$ or $E = E_\rho$.

Firstly we treat the case $P = (E_\rho, \phi)$. Since P is a branch point, by Proposition 3.2.4, we know that $\phi^{-1} \circ \rho|_{E_\rho[n]} \circ \phi \in H$. Hence, we can apply Part (1) of Proposition 3.3.10, for each $k \in \{1, 2\}$, which gives

$$T_{\ell_k}(E', \phi') = T_{\ell_k} u(P) = u^{\sigma_k} T_{\ell_k}(P) \geq 3P_1, \tag{3.6.7}$$

for some point $P_1 \in Y_H(\mathbb{C})$. Because of last inequality, we can apply Proposition 3.3.6 Part (2) to obtain that $\mathbb{Z}[\ell_1^2 \rho]$ and $\mathbb{Z}[\ell_2^2 \rho]$ are both contained in $\mathrm{End}(E')$ which implies $\mathrm{End}(E') = \mathbb{Z}[\rho]$. Since the class group of $\mathbb{Z}[\rho]$ is trivial, we have $E' \cong E_\rho$. Again by Inequality (3.6.7), Proposition 3.3.10 Part (1) implies that $\phi'^{-1} \circ \rho|_{E_\rho[n]} \circ \phi' \in H$. By Proposition 3.2.4, we conclude that $u(P)$ is a branch point associated to the elliptic curve E_ρ.

Now, we consider $P = (E_i, \phi)$. Since P is a branch point, by Proposition 3.2.4, we know that $\phi^{-1} \circ i|_{E_i[n]} \circ \phi \in H$. Hence, by Proposition 3.3.10 Part (2), one of the following two possibilities happens

$$\begin{aligned} &T_{\ell_2} u(P) = u^{\sigma_2} T_{\ell_2}(P) = 2(P_1 + \ldots + P_{\frac{\ell_2+1}{2}}) \quad \text{or} \\ &T_{\ell_2} u(P) = u^{\sigma_2} T_{\ell_2}(P) = 2(P_1 + \ldots + P_{\frac{\ell_2-1}{2}}) + P_{\frac{\ell_2+1}{2}} + P_{\frac{\ell_2+3}{2}}, \end{aligned} \tag{3.6.8}$$

with $P_1, \ldots, P_{\frac{\ell_2+3}{2}}$ being distinct points in $Y_H(\mathbb{C})$. This equation implies that the hypotheses of Proposition 3.3.6 Part (3) are satisfied, hence $\mathbb{Z}[\ell_2^2 i]$ is contained in $\mathrm{End}(E')$. We now prove, distinguishing three cases, that $\mathbb{Z}[\ell_1^2 i]$ is contained in $\mathrm{End}(E')$. If $\ell_1 \geq 5$, we can apply the same argument used for ℓ_2. If $\ell_1 = 2$ or $\ell_1 = 3$, by Proposition 3.3.10 Part (2) and Equation (3.6.6), there is a point $(E'', \phi'') \in Y_H(\mathbb{C})$ such that

$$T_{\ell_1}(E', \phi') = T_{\ell_1} u(P) = u^{\sigma_1} T_{\ell_1}(P) \geq 2(E'', \phi''). \tag{3.6.9}$$

If $\ell_1 = 3$, Lemma 3.3.5 implies that E'' has an endomorphism $\beta \neq \pm 3$ having degree 9. Since E'' is isogenous to E', we know that $\mathrm{End}(E'') \subset \mathbb{Z}[i]$, hence $\beta = \pm 3i$. Using that

E' and E'' are 3-isogenous, we see that

$$\mathrm{End}(E') \supset \mathbb{Z} + 3\mathrm{End}(E'') \supset \mathbb{Z} + 3\mathbb{Z}[\beta] = \mathbb{Z}[9i].$$

If $\ell_1 = 2$, Inequality (3.6.9) and Lemma 3.3.5 imply that E'' has an endomorphism $\beta \neq \pm 2$ having degree 4. Since E'' is isogenous to E', we know that $\mathrm{End}(E'') \subset \mathbb{Z}[i]$, hence $\beta = \pm 2i$ or $\beta = \pm 1 \pm i$. Using that E' and E'' are 2-isogenous, we see that

$$\mathrm{End}(E') \supset \mathbb{Z} + 2\mathrm{End}(E'') \supset \mathbb{Z} + 2\mathbb{Z}[\beta] \supset \mathbb{Z}[4i].$$

We proved that both $\mathbb{Z}[\ell_1^2 i]$ and $\mathbb{Z}[\ell_2^2 i]$ are contained in $\mathrm{End}(E')$, hence $\mathrm{End}(E') = \mathbb{Z}[i]$ and, since the class group of $\mathbb{Z}[i]$ is trivial, we deduce that $E' \cong E_i$. By Equation (3.6.8), the hypotheses of Proposition 3.3.10 Part (2) are satisfied, hence $\phi'^{-1} \circ i|_{E_i[n]} \circ \phi' \in H$ and, by Proposition 3.2.4, we conclude that $u(P)$ is a branch point. □

Propositions 3.6.4 and 3.6.5, together with Lemma 3.6.3, imply the following Corollary, which gives a concise sufficient condition to exclude the presence of non-modular automorphisms.

Corollary 3.6.10. *Let n be a positive integer let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ containing the scalar matrices and such that $\det(H) = (\mathbb{Z}/n\mathbb{Z})^\times$ and let $\mathrm{gon}(X_H)$ be the gonality of X_H. If there are two primes $\ell_1 < \ell_2$ not dividing n such that $5 \leq \ell_2 < \frac{1}{2}\mathrm{gon}(X_H) - 1$, then every automorphism of X_H defined over a compositum of quadratic fields is modular.*

We still need to determine which are the modular automorphisms of a modular curve X_H for Cartan and Cartan-plus subgroups H of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Since in these cases we have $\det(H) = (\mathbb{Z}/n\mathbb{Z})^\times$, then Y_H also parametrizes pairs $[E, \phi]$ such that the Weil pairing of $(\phi\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right), \phi\left(\begin{smallmatrix}0\\1\end{smallmatrix}\right))$ is fixed, up to the action of $H \cap \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$. With this interpretation, every matrix $\gamma \in \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ that normalizes $H \cap \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ defines an automorphism of Y_H sending $[E, \phi] \mapsto [E, \phi \circ \gamma]$: such an automorphism is modular, induced by a lift of γ in $\mathrm{SL}_2(\mathbb{Z})$. Next proposition implies that these are all the modular automorphisms except when $n \equiv 2 \bmod 4$ and H is a Cartan-plus which is split at 2. We now suppose we are in this last case and we construct another modular automorphism. Letting $n = 2n'$, we have

$$H = H_2 \times H_{n'} \subset \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/n'\mathbb{Z}) = \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}),$$

where H_2 and $H_{n'}$ are the images of H in $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ and $\mathrm{GL}_2(\mathbb{Z}/n'\mathbb{Z})$ respectively. Since we are assuming that H_2 is a split Cartan-plus subgroup, there are three possibilities for H_2 (all conjugated) and, depending on them, we define

$$\gamma_0 := \begin{cases} \left(\begin{smallmatrix}3&1\\1&1\end{smallmatrix}\right), & \text{if } H_2 = \{\mathrm{Id}, \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)\}, \\ \left(\begin{smallmatrix}2&1\\2&2\end{smallmatrix}\right), & \text{if } H_2 = \{\mathrm{Id}, \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)\}, \\ \left(\begin{smallmatrix}2&2\\1&2\end{smallmatrix}\right), & \text{if } H_2 = \{\mathrm{Id}, \left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)\}. \end{cases} \tag{3.6.11}$$

Since the projection $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/2n\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/n'\mathbb{Z})$ is surjective and since $\det(H_{n'}) = (\mathbb{Z}/n'\mathbb{Z})^\times$, there exists

$$(3.6.12) \qquad \gamma_1 \in \mathrm{SL}_2(\mathbb{Z}) \quad \text{such that} \quad \gamma_1 \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \pmod 4 \quad \text{and} \quad \gamma_0\gamma_1 \ (\mathrm{mod}\ \tfrac{n}{2}) \in H_{\frac{n}{2}}.$$

The matrix $\mathbb{P}(\gamma_0\gamma_1)$ lies in the normalizer $\mathcal{N}$ of $\mathbb{P}(\Gamma_H)$ inside $\mathrm{PGL}_2^+(\mathbb{Q})$ and we have that $\mathbb{P}(\gamma_0\gamma_1)^2 \in \mathbb{P}(\Gamma_H)$, hence $\mathbb{P}(\gamma_0\gamma_1)$ induces an involution on X_H. Since $\mathbb{P}(\gamma_0\gamma_1)$ is not in $\mathbb{P}(\mathrm{SL}_2(\mathbb{Z}))$, the modular automorphism defined by $\gamma_0\gamma_1$ is not of the form $[E, \phi] \mapsto [E, \phi \circ \gamma]$ with $\gamma \in \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$.

Proposition 3.6.13. *Let n be a positive integer and let $H < \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be either a Cartan subgroup or a Cartan-plus subgroup. Let $N' < \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ be the normalizer of the group $H' := H \cap \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ and let $\mathcal{N}$ be the normalizer of $\mathbb{P}(\Gamma_H)$ in $\mathrm{PGL}_2^+(\mathbb{Q})$. If $n \equiv 2 \bmod 4$ and H is a Cartan-plus split at 2, then, for every choice of γ_0 and γ_1 as in (3.6.11) and (3.6.12), $\mathcal{N}$ is generated by $\mathbb{P}(\Gamma_{N'})$ and $\mathbb{P}(\gamma_0\gamma_1)$. Otherwise $\mathcal{N}$ is $\mathbb{P}(\Gamma_{N'})$.*

Proof. Let $\tilde{\mathcal{N}} < \mathrm{GL}_2^+(\mathbb{Q})$ be the normalizer of $\mathbb{Q}^\times\Gamma_H$, or, equivalently, the normalizer of Γ_H (each matrix normalizing $\mathbb{Q}^\times\Gamma_H$ also normalizes $(\mathbb{Q}^\times\Gamma_H) \cap \mathrm{SL}_2(\mathbb{Q}) = \Gamma_H$, and since scalar matrices commute with everything, each matrix normalizing Γ_H also normalizes $\mathbb{Q}^\times\Gamma_H$). The statement of the proposition is equivalent to

$$\tilde{\mathcal{N}} = \mathbb{Q}^\times\Gamma_{N'} \quad \text{or} \quad \tilde{\mathcal{N}} = \mathbb{Q}^\times\langle\gamma_0\gamma_1, \Gamma_{N'}\rangle,$$

depending on the case. The inclusions $\supseteq$ are trivial, hence we prove the other inclusions. Since the normalizer of Γ_H inside $\mathrm{SL}_2(\mathbb{Z})$ is $\Gamma_{N'}$, it is enough to show that

$$\tilde{\mathcal{N}} \subseteq \mathbb{Q}^\times\mathrm{SL}_2(\mathbb{Z}) \quad \text{or} \quad \tilde{\mathcal{N}} \subseteq \mathbb{Q}^\times\mathrm{SL}_2(\mathbb{Z}) \cup \gamma_0\gamma_1\mathbb{Q}^\times\mathrm{SL}_2(\mathbb{Z}),$$

depending on the case. We suppose that $\tilde{\mathcal{N}}$ contains a matrix $m = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ not lying in $\mathbb{Q}^\times\mathrm{SL}_2(\mathbb{Z})$: it is enough to prove, with this assumption, that $n \equiv 2 \bmod 4$ and H is a Cartan-plus subgroup split at 2 and $m \in \gamma_0\gamma_1\mathbb{Q}^\times\mathrm{SL}_2(\mathbb{Z})$.

Up to multiplication by a scalar matrix, we can suppose that $a, b, c, d \in \mathbb{Z}$ and that $\gcd(a, b, c, d) = 1$. Since $m \notin \mathbb{Q}^\times\mathrm{SL}_2(\mathbb{Z})$, then $\det(m) \neq 1$. Let p be a prime dividing $\det(m)$, let $\lambda_1 = \left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right), \lambda_2 = \left(\begin{smallmatrix} b \\ d \end{smallmatrix}\right) \in \mathbb{Z}^2$ and let $\Lambda \subset \mathbb{Z}^2$ be the lattice generated by λ_1, λ_2. By definition of $\tilde{\mathcal{N}}$, for every $\gamma \in \Gamma_H$ there is $\gamma' = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \in \Gamma_H$ such that $\gamma m = m\gamma'$. Hence, looking at the columns of γm, we get $\gamma\lambda_1 = x\lambda_1 + z\lambda_2$ and $\gamma\lambda_2 = y\lambda_1 + w\lambda_2$. Since γ is arbitrary and $\gamma' \in \mathrm{SL}_2(\mathbb{Z})$, we have

$$\Gamma_H\Lambda = \Lambda.$$

Let $\overline{\Lambda}$ be the image of Λ under the quotient map $\mathbb{Z}^2 \to \mathbb{F}_p^2$. Since at least one of a, b, c, d is not multiple of p, we know that $\overline{\Lambda} \neq \{0\}$ and since $\det(m)$ is multiple of p, we know that $\overline{\Lambda} \neq \mathbb{F}_p^2$. Hence $\overline{\Lambda}$ is a line inside $\mathbb{F}_p^2$ which is left invariant by every matrix in the image $\overline{\Gamma}_H$ of Γ_H in $\mathrm{GL}_2(\mathbb{F}_p)$. This implies that $\overline{\Gamma}_H$ is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$, thus p divides the level n and $\overline{\Gamma}_H = \overline{H} \cap \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, where $\overline{H}$ is the image of H in $\mathrm{GL}_2(\mathbb{F}_p)$. We deduce that either H is a Cartan group split at p or $p = 2$ and H is a Cartan-plus group split at p.

First we suppose that H is a Cartan group split at p. Let p^e be the maximum power of p dividing n. Up to conjugacy, the image of H in $\mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$ is $\{\left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right)\}$, hence, for every $\gamma \in \Gamma_H$, we have

$$m^{-1}\gamma m = \tfrac{1}{\det(m)} \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right) \gamma \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right) \pmod{p^e}.$$

Applying this to $\gamma = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$ and $\gamma = \left(\begin{smallmatrix} 1 & 0 \\ n & 1 \end{smallmatrix}\right)$, we see that since $\det(m)$ is multiple of p, then a, b, c, d are all multiples of p, which is a contradiction.

This contradiction implies that the only prime dividing $\det(m)$ is 2 and H is a Cartan-plus group split at 2. Let 2^e be the maximum power of 2 dividing n. Up to conjugacy, the image of H in $\mathrm{GL}_2(\mathbb{Z}/2^e\mathbb{Z})$ is $\{\left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & * \\ * & 0 \end{smallmatrix}\right)\}$. In particular the image of H in $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ is $\{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)\}$, hence $\overline{\Lambda} = \langle \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right) \rangle$ is the only $\overline{\Gamma}_H$-invariant line. In other words the columns $\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right), \left(\begin{smallmatrix} b \\ d \end{smallmatrix}\right)$ of m span $\langle \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right) \rangle$ in $\mathbb{F}_2^2$ and with a similar argument we see that the rows $(a\,b), (c\,d)$ of m span $\langle (1\,1) \rangle$ in $\mathbb{F}_2^2$. Hence $m \equiv \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right) \pmod 2$. For every $\gamma \in \Gamma_H$, we have

$$m^{-1}\gamma m \pmod{2^e} \in \{\left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & * \\ * & 0 \end{smallmatrix}\right)\}. \tag{3.6.14}$$

When $\gamma = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$, we see that $m^{-1}\gamma m \equiv \left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right) \pmod{2^e}$ is not possible because both c and d are odd, hence $m^{-1}\gamma m \equiv \left(\begin{smallmatrix} 0 & * \\ * & 0 \end{smallmatrix}\right) \pmod{2^e}$ and, by explicit computations, we deduce that $\det(m) = 2$ and $n \equiv 2 \bmod 4$. Finally, since $m \equiv \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right) \pmod 2$ and $\det(m) = 2$, we see that $(\gamma_0\gamma_1)^{-1}m \in \mathrm{SL}_2(\mathbb{Z})$. □

We now prove the main results of this paper.

Theorem 3.6.15. *Let $n \geq 10^{400}$ be an integer and let $H < \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be either a Cartan or a Cartan-plus subgroup. Then every automorphism of X_H is modular, hence we have*

$$\mathrm{Aut}(X_H) \cong \begin{cases} N'/H' \times \mathbb{Z}/2\mathbb{Z}, & \text{if } n \equiv 2 \bmod 4 \text{ and } H \text{ is a Cartan-plus split at } 2, \\ N'/H', & \text{otherwise,} \end{cases}$$

where $N' < \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ is the normalizer of $H' := H \cap \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$.

Proof. Let $\mathcal{N}$ be the normalizer of $\mathbb{P}(\Gamma_H)$ inside $\mathrm{PGL}_2^+(\mathbb{Q})$. By Proposition 3.6.13 we have

$$\mathcal{N}/\mathbb{P}(\Gamma_H)\cong \begin{cases} \mathbb{P}(\Gamma_{N'})/\mathbb{P}(\Gamma_H)\times\mathbb{Z}/2\mathbb{Z}, & \text{if } n\equiv 2 \bmod 4 \text{ and } H \text{ is a Cartan-plus split at } 2,\\ \mathbb{P}(\Gamma_{N'})/\mathbb{P}(\Gamma_H), & \text{otherwise,}\end{cases}$$

where the first case is true because $\mathbb{P}(\gamma_0\gamma_1\Gamma_H)$ has order 2 in $\mathcal{N}/\mathbb{P}(\Gamma_H)$ and commutes with every element in $\mathbb{P}(\Gamma_{N'})/\mathbb{P}(\Gamma_H)$. Since $\mathbb{P}(\Gamma_{N'})/\mathbb{P}(\Gamma_H)\cong\mathbb{P}(\Gamma_{N'})/\mathbb{P}(\Gamma_{H'})\cong N'/H'$, it is enough to prove that every automorphism of X_H is modular. For $n\geq 10^{400}$ every automorphism is defined over the compositum of some quadratic fields by Proposition 3.5.7. We can bound the gonality $\mathrm{gon}(X_H)$ of X_H using [1] and, with the same estimates used in the proof of Proposition 3.4.9, we have

$$\mathrm{gon}(X_H)\geq\frac{7}{800}[\mathrm{SL}_2(\mathbb{Z}):\Gamma_H]\geq\frac{7n^2}{800(\omega(n)+1)2^{\omega(n)}}>10n.$$

So, there are at least two primes $\ell_1<\ell_2$ not dividing n with $5\leq\ell_2<\frac{1}{2}\mathrm{gon}(X_H)-1$. By Corollary 3.6.10, we can conclude that every automorphism is modular. □

Remark 3.6.16. One can determine the groups N'/H' in all cases. Indeed, let $n=\prod_{i=1}^r p_i^{e_i}$ be any positive integer with its prime factorization, let $H<\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be either a Cartan or a Cartan-plus subgroup and let $N'<\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ be the normalizer of the group $H':=H\cap\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$. By Chinese Remainder Theorem we have

$$H'\cong\prod_{i=1}^r H_i' \quad\text{and}\quad N'\cong\prod_{i=1}^r N_i' \quad\text{inside}\quad \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})\cong\prod_{i=1}^r\mathrm{SL}_2(\mathbb{Z}/p^{e_i}\mathbb{Z}),$$

where H_i' is the image of H' in $\mathrm{SL}_2(\mathbb{Z}/p^{e_i}\mathbb{Z})$ and $N_i'<\mathrm{SL}_2(\mathbb{Z}/p^{e_i}\mathbb{Z})$ is the normalizer of H_i'. Hence the knowledge of N'/H' for $H\in\{C_{\mathrm{ns}}(p^e),C_{\mathrm{ns}}(p^e),C_{\mathrm{s}}(p^e),C_{\mathrm{s}}^+(p^e)\}$ allows to compute the group N'/H' for every Cartan or Cartan-plus subgroup H of level n not necessarily a prime power. Explicit computations give the following:

- if $H=C_{\mathrm{ns}}(p^e)$, then $N'/H'\cong\mathbb{Z}/2\mathbb{Z}$, since $N'=C_{\mathrm{ns}}^+(p^e)\cap\mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})$;
- if $p^e\neq 3$ and $H=C_{\mathrm{ns}}^+(p^e)$, then $N'/H'\cong\{1\}$;
- if $H=C_{\mathrm{ns}}^+(3)$, then $N'/H'\cong\langle\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)\rangle\cong\mathbb{Z}/3\mathbb{Z}$;
- if $p\neq 2,3$ and $H=C_{\mathrm{s}}(p^e)$, then $N'/H'\cong\langle\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)\rangle\cong\mathbb{Z}/2\mathbb{Z}$;
- if $e\geq 2$ and $H=C_{\mathrm{s}}(3^e)$, then

$$N'/H'\cong\left\langle\left(\begin{smallmatrix}1&3^{e-1}\\-3^{e-1}&1\end{smallmatrix}\right)\right\rangle\times\left\langle\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right),\left(\begin{smallmatrix}1&3^{e-1}\\3^{e-1}&1\end{smallmatrix}\right)\right\rangle\cong\mathbb{Z}/3\mathbb{Z}\times S_3,$$

  where S_3 is the symmetric group acting on three elements;

- if $e \geq 5$ and $H = C_{\mathrm{s}}(2^e)$, then
$$N'/H' \cong \left\langle \left(\begin{smallmatrix} 1 & 2^{e-3} \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ -2^{e-3} & 1 \end{smallmatrix}\right) \right\rangle \rtimes \left\langle \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \right\rangle \cong (\mathbb{Z}/8\mathbb{Z})^2 \rtimes_{\varphi} (\mathbb{Z}/2\mathbb{Z}),$$
where $(\varphi(1))\,(x,y) = (y,x)$; this group is labeled as $(128,67)$ in MAGMA, [50];

- if $p^e \in \{3, 2, 2^2, 2^3\}$ and $H = C_{\mathrm{s}}(p^e)$, then $N'/H' \cong \mathrm{PSL}_2(\mathbb{Z}/p^e\mathbb{Z})$, since we have $N' = \mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})$;

- if $H = C_{\mathrm{s}}(2^4)$, then $N'/H' \cong \left\langle \left(\begin{smallmatrix} -1 & 6 \\ 6 & -5 \end{smallmatrix}\right), \left(\begin{smallmatrix} 4 & 9 \\ 7 & -4 \end{smallmatrix}\right) \right\rangle \rtimes \left\langle \left(\begin{smallmatrix} 1 & -2 \\ 0 & 1 \end{smallmatrix}\right) \right\rangle \cong D_8 \rtimes_{\varphi} (\mathbb{Z}/8\mathbb{Z})$, where $D_8 \cong \mathbb{Z}/8\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ is the dihedral group of order 16 and $(\varphi(1))\,(1,0) = (5,0)$ and $(\varphi(1))\,(0,1) = (3,1)$; moreover N'/H' is labeled as $(128,68)$ in MAGMA, [50];

- if $p \neq 2,3$ and $p^e \neq 5$ and $H = C_{\mathrm{s}}^{+}(p^e)$ then $N'/H' \cong \{1\}$;

- if $H = C_{\mathrm{s}}^{+}(5)$, then $N'/H' \cong \langle \left(\begin{smallmatrix} 1 & 2 \\ 1 & 3 \end{smallmatrix}\right) \rangle \cong \mathbb{Z}/3\mathbb{Z}$;

- if $e \geq 2$ and $H = C_{\mathrm{s}}^{+}(3^e)$, then $N'/H' \cong \langle \begin{pmatrix} 1 & -3^{e-1} \\ 3^{e-1} & 1 \end{pmatrix} \rangle \cong \mathbb{Z}/3\mathbb{Z}$;

- if $H = C_{\mathrm{s}}^{+}(3)$, then $N'/H' \cong \langle \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right) \rangle \cong \mathbb{Z}/2\mathbb{Z}$;

- if $e \geq 6$ and $H = C_{\mathrm{s}}^{+}(2^e)$, then $N'/H' \cong \langle \begin{pmatrix} 1 & -2^{e-3} \\ 2^{e-3} & 1 \end{pmatrix} \rangle \cong \mathbb{Z}/8\mathbb{Z}$;

- if $H = C_{\mathrm{s}}^{+}(2)$, then $N'/H' \cong \{1\}$;

- if $H = C_{\mathrm{s}}^{+}(2^2)$, then $N'/H' \cong \langle \left(\begin{smallmatrix} 1 & 2 \\ 2 & 1 \end{smallmatrix}\right) \rangle \cong \mathbb{Z}/2\mathbb{Z}$;

- if $H = C_{\mathrm{s}}^{+}(2^3)$, then $N'/H' \cong \langle \left(\begin{smallmatrix} 1 & -2 \\ 2 & -3 \end{smallmatrix}\right) \rangle \cong \mathbb{Z}/4\mathbb{Z}$;

- if $H = C_{\mathrm{s}}^{+}(2^4)$, then $N'/H' \cong \langle \left(\begin{smallmatrix} 1 & 6 \\ 2 & -3 \end{smallmatrix}\right) \rangle \cong \mathbb{Z}/8\mathbb{Z}$;

- if $H = C_{\mathrm{s}}^{+}(2^5)$, then $N'/H' \cong \langle \left(\begin{smallmatrix} 1 & -4 \\ 4 & -15 \end{smallmatrix}\right) \rangle \cong \mathbb{Z}/8\mathbb{Z}$.

Recall that the groups N'/H' computed for $H = C_{\mathrm{s}}(p^e)$ are the same determined in [4], [2], [14], in the setting of Borel modular curves.

For Cartan modular curves of prime power level we make Theorem 3.6.15 more precise.

Theorem 3.6.17. *Let p be a prime number and let e be a positive integer. If $p^e > 11$ and $p^e \notin \{3^3, 2^4, 2^5, 2^6\}$, then all the automorphisms of $X_{\mathrm{ns}}(p^e), X_{\mathrm{ns}}^{+}(p^e), X_{\mathrm{s}}(p^e)$ and $X_{\mathrm{s}}^{+}(p^e)$ are modular and*

$$\mathrm{Aut}(X_{\mathrm{ns}}(p^e)) \cong \mathbb{Z}/2\mathbb{Z}, \qquad \mathrm{Aut}(X_{\mathrm{ns}}^{+}(p^e)) \cong \{1\},$$

$$\mathrm{Aut}(X_{\mathrm{s}}(p^e)) \cong \begin{cases} (\mathbb{Z}/8\mathbb{Z})^2 \rtimes (\mathbb{Z}/2\mathbb{Z}), & \text{if } p = 2, \\ \mathbb{Z}/3\mathbb{Z} \times S_3, & \text{if } p = 3, \\ \mathbb{Z}/2\mathbb{Z}, & \text{if } p > 3, \end{cases} \qquad \mathrm{Aut}(X_{\mathrm{s}}^{+}(p^e)) \cong \begin{cases} \mathbb{Z}/8\mathbb{Z}, & \text{if } p = 2, \\ \mathbb{Z}/3\mathbb{Z}, & \text{if } p = 3, \\ \{1\}, & \text{if } p > 3, \end{cases}$$

where the above semidirect product $(\mathbb{Z}/8\mathbb{Z})^2 \rtimes \mathbb{Z}/2\mathbb{Z}$ is described in Remark 3.6.16.

Proof. We first treat the case $p^e > 49$ with $p^e \neq 2^6 = 64$. Up to conjugacy we can assume that $H \in \{C_{\mathrm{s}}(p^e), C_{\mathrm{s}}^+(p^e), C_{\mathrm{ns}}(p^e), C_{\mathrm{ns}}^+(p^e)\}$ where these groups are the subgroups of $\mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$ defined in Chapter 3.4 and $X_H \in \{X_{\mathrm{ns}}(p^e), X_{\mathrm{ns}}^+(p^e), X_{\mathrm{s}}(p^e), X_{\mathrm{s}}^+(p^e)\}$ is the corresponding associated modular curve. By [1, Theorem 0.1] and Table 3.1, for $p^e > 87$, we have the following lower bounds for the gonality of X_H:

$$\mathrm{gon}(X_H) \geq \frac{7}{800}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_H] \geq \frac{7}{800}\frac{p^{2e}(1-\frac{1}{p})}{2} > \frac{7 \cdot 87^2}{3200} > 16.$$

Hence there are two primes $\ell_1 < \ell_2$, different from p, such that $5 \leq \ell_2 < \frac{1}{2}\mathrm{gon}(X_H) - 1$: we can take $\ell_1 = 3$, $\ell_2 = 7$ if $p \in \{2, 5\}$ and $\ell_1 = 2$, $\ell_2 = 5$ otherwise. With a similar computation one can show that $\mathrm{gon}(X_H) > 12$, for $49 < p^e \leq 87$, if $p^e \neq 64$ and we can take $\ell_1 \in \{2, 3\}$, $\ell_2 = 5$. Applying Corollary 3.6.10 we deduce that all the automorphisms of X_H defined over a compositum of quadratic fields are modular, hence, by Proposition 3.5.8, all the automorphisms of X_H are modular. Finally, we can use Proposition 3.6.13 and Remark 3.6.16 to obtain the group of modular automorphisms.

We now assume $11 < p^e \leq 49$. All the cases $X_{\mathrm{s}}(p^e) \cong X_0(p^{2e})$ are treated in [60], all the cases $X_{\mathrm{s}}^+(p)$ are treated in [47] and the cases $X_{\mathrm{ns}}(p)$, $X_{\mathrm{ns}}^+(p)$, for $13 \leq p \leq 31$, are treated in [48]. The remaining cases $X_{\mathrm{s}}^+(25)$, $X_{\mathrm{s}}^+(49)$ and $X_{\mathrm{ns}}(p^e)$, $X_{\mathrm{ns}}^+(p^e)$, for $p^e = 25, 37, 41, 43, 47, 49$, are treated in the MAGMA script available at [70]. □

Last theorem can be specialized to the prime level case, obtaining new results for non-split Cartan curves. The split cases are treated in [47] and [60].

Corollary 3.6.18. *Let $p \geq 13$ be a prime number. Then the group of automorphisms of $X_{\mathrm{ns}}^+(p)$ is trivial and the group of automorphisms of $X_{\mathrm{ns}}(p)$ has order 2.*

Remark 3.6.19. Theorem 3.6.17 implies that, for p^{2e} big enough, all the automorphisms of $X_0^*(p^{2e}) \cong X_{\mathrm{s}}^+(p^e)$ are modular, extending [5] and [47] that treat the cases $X_0^*(p)$ and $X_0^*(p^2)$. Our techniques (in particular Lemma 3.6.5) cannot be generalized to the case $X_0^*(p^e)$ with e odd, because some of the branch points of the natural map $\mathbb{H} \to Y_0^+(p^e)$ have the form $\{(E, C), (E/C, E[p^e]/C)\}$ with $E \neq E_i, E_\rho$. Anyway, the techniques used in [47, Lemmas 4, 5, 6], together with Proposition 3.5.9, can be used to prove the modularity of all elements in $\mathrm{Aut}(X_0^*(p^e))$, without restrictions on e, for all but finitely many cases.

3.7 Appendix

Let $G := \mathrm{GL}_2(\mathbb{Z}/2^e\mathbb{Z})$. For each $H < G$, let $\chi_H : G \to \mathbb{Q}$ be the character of the representation $\mathbb{Q}[G/H]$. The entry (γ, H) of the table below is $\chi_H(\gamma)$. Every element of G is conjugated to a unique element appearing in the first column, hence the table determines the characters χ_H for H appearing in Proposition 3.4.2 or in [26, Theorem 1.1]. In the first column we have $\lambda, a \in (\mathbb{Z}/2^e\mathbb{Z})^\times$, $b \in (\mathbb{Z}/2^e\mathbb{Z})$, $k \in \{1, \dots, e{-}1\}$, and $u \in (\mathbb{Z}/2^{e-k}\mathbb{Z})^\times$.

Proving that the first column contains every conjugacy class of $\mathrm{GL}_2(\mathbb{Z}/2^e\mathbb{Z})$ exactly once is rather easy, yet cumbersome, using the following lemma.

Lemma 3.7.1. *Let $M \in \mathrm{M}_{2\times 2}(\mathbb{Z}/2^e\mathbb{Z})$. If $M \equiv \left(\begin{smallmatrix} 0 & * \\ 1 & * \end{smallmatrix}\right) \bmod 2$ or $M \equiv \left(\begin{smallmatrix} * & 1 \\ * & 0 \end{smallmatrix}\right) \bmod 2$, then there are unique elements $a, b \in \mathbb{Z}/2^e\mathbb{Z}$ such that M is conjugated to $\left(\begin{smallmatrix} 0 & a \\ 1 & b \end{smallmatrix}\right)$. If $M \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \bmod 2$ or $M \equiv \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) \bmod 2$, then there are unique elements $\lambda_1, \lambda_2 \in \mathbb{Z}/2^e\mathbb{Z}$, the first odd and the second even, such that M is conjugated to $\left(\begin{smallmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{smallmatrix}\right)$*

Proof. The cases $M \equiv \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) \bmod 2$ and $M \equiv \left(\begin{smallmatrix} * & 1 \\ * & 0 \end{smallmatrix}\right) \bmod 2$ can be reduced to the remaining cases by considering $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)^{-1} M \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Let V be the module made of column vectors in $(\mathbb{Z}/2^e\mathbb{Z})^2$ with standard basis e_1, e_2 and let $F_M \colon V \to V$ be the multiplication by M.

If $M \equiv \left(\begin{smallmatrix} 0 & * \\ 1 & * \end{smallmatrix}\right) \bmod 2$ we notice that $e_1, F_M(e_1)$ are a basis of V when we reduce modulo 2, hence they are a basis of V. In the basis $B = (e_1, F_M(e_1))$ we have

$$M \sim F_M^B = \left(\begin{smallmatrix} 0 & a \\ 1 & b \end{smallmatrix}\right)$$

for some a, b, that are unique since $a = -\det(M)$ and $b = \mathrm{tr}(M)$.

Finally the case $M \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \bmod 2$. The uniqueness result is motivated by the fact that λ_1, λ_2 are the only roots of $\det(M - \lambda\mathrm{Id})$. The existence part is a Hensel argument. Let $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and let us lift for example e_1 to an eigenvector:

$$\begin{aligned} &F_M(e_1 + \lambda) = (a + \lambda b)e_1 + (c + \lambda d)e_2 \quad \in \langle e_1 + \lambda e_2 \rangle \quad \iff \\ &\lambda(a + \lambda b) = c + \lambda d \quad \iff b\lambda^2 + (a - d)\lambda - c = 0 \end{aligned}$$

and last equation has a unique zero because the polynomial $p(\lambda) = b\lambda^2 + (a - d)\lambda - c$ satisfies $p(0) \equiv 0, p'(0) \not\equiv 0$ modulo 2. With the same argument we can lift e_2 to an eigenvector. □

In order to fill Table 3.2 we use that

$$\mathbb{Q}[G/H] = \bigoplus gH \cdot \mathbb{Q} \quad \text{and} \quad \forall \gamma \in G : \quad \rho_H(\gamma)(gH) = \gamma g H$$

hence, in basis $\{gH\}$ the matrix $\rho_H(\gamma)$ is a permutation matrix and consequently

$$\chi_H(\gamma) = \mathrm{tr}(\rho_H(\gamma)) = \#\{gH : \gamma g H = gH\} = \frac{\#\{g : \gamma g \in gH\}}{\#H} = \frac{\#\{g : g^{-1}\gamma g \in H\}}{\#H} .$$

Table 3.2: Character table.

	$B_r, r \geq 0$	T_0	$T_r, r > 0$	C_s	C_s^+	C_{ns}	C_{ns}^+
$\lambda\mathrm{Id}$	$3{\cdot}2^{2r}$	1	$3{\cdot}2^{2r-1}$	$3{\cdot}2^{2e-1}$	$3{\cdot}2^{2e-2}$	2^{2e-1}	2^{2e-2}
$\left(\begin{smallmatrix} 0 & a \\ 1 & b \end{smallmatrix}\right)$ b odd	0	1	0	0	0	2	1
$\left(\begin{smallmatrix} 0 & a \\ 1 & b \end{smallmatrix}\right)$ b even	1 if $r{=}0$ 0 if $r{>}0$	1	0	0	2^{e-1} if $b{=}0$ 0 if $b{\neq}0$	0	2^{e-1} if $b{=}0$ 0 if $b{\neq}0$
$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda+2^k u \end{pmatrix}$	$3{\cdot}2^{2r}$ if $r{<}k$ 2^{2k+1} if $r{\geq}k$	1	$3{\cdot}2^{2r-1}$ if $r{\leq}k$ 2^{2k+1} if $r{>}k$	2^{2k+1}	2^{2k}	0	0
$\begin{pmatrix} \lambda & 2^k u \\ 2^k & \lambda \end{pmatrix}$	$3{\cdot}2^{2r}$ if $r{<}k$ 2^{2r} if $r{=}k$ 0 if $r{>}k$	1	$3{\cdot}2^{2r-1}$ if $r{\leq}k$ 0 if $r{>}k$	0	0	0	0
$\begin{pmatrix} \lambda & 2^k u \\ 2^k & \lambda+2^k \end{pmatrix}$	$3{\cdot}2^{2r}$ if $r{<}k$ 0 if $r{\geq}k$	1	$3{\cdot}2^{2r-1}$ if $r{\leq}k$ 0 if $r{>}k$	0	0	2^{2k+1}	2^{2k}
$\begin{pmatrix} \lambda & 2^k u \\ 2^k & \lambda+2^{k+1} \end{pmatrix}$	$3{\cdot}2^{2r}$ if $r{<}k$ 2^{2r} if $r{=}k$ 0 if $r{>}k$	1	$3{\cdot}2^{2r-1}$ if $r{\leq}k$ 0 if $r{>}k$	0	0	0	0