On the automorphism group of quotient modular curves

Francesc Bars*and Tarun Dalal

Abstract

In this article, we determine the automorphism group of all the quotient modular curves of the modular curve $X_0(pq)$, where p, q are two distinct primes. In obtaining such results, we provide different insights to compute the automorphism group for any quotient modular curve, which are very effective when the level of the curve is square-free. In particular, in the case where the level of the quotient curve is non square-free, we would mention that we present an unfamiliar automorphism of order 3 for the genus 4 curve $X_0^*(25 \cdot 11)$ defined over $\mathbb{Q}[\sqrt{5}]$.

1 Introduction

Kenku and Momose in [KM88], determined the automorphism group of all modular curves $X_0(N)$ with genus > 1, except for $N = 63$, which was solved by Elkies in [Elk90], and $N = 108$ in [Har14].

For the modular curve $X_0^+(N) := X_0(N)/\langle w_N \rangle$, where w_N denotes the Fricke involution, in [BaHa03] Baker and Hasegawa determined the automorphism group when N is a prime. When N is the square of a prime, the automorphism group of $X_0^+(N)$ was studied in [Gon16].

Later González and the first author in [BaGo21] determined the automorphism group for the modular curves $X_0^*(N) = X_0(N)/B(N)$, with N square-free, where $B(N)$ is the group of the Atkin-Lehner involutions w_d with $d||N$ (i.e., $d|N$ and $(d, N/d) = 1$) of the modular curve $X_0(N)$.

The present paper is the first in this direction, where we determine the automorphism group for $X_0(N)/W_N$ with W_N a non-trivial subgroup of $B(N)$ such that genus$(X_0(N)/W_N) \geq 2$ and provide first insights to determine the automorphism group of $X_0^*(N)$ with N a fixed non square-free positive integer. In particular, we extend the results of [BaHa03] in the sense that, as applications of the techniques presented, we determine the automorphism group of $X_0(N)/W_N$ when N is a product of two different primes and W_N is any non-trivial subgroup of $B(N)$. Another generalization of the results of [BaHa03] and [Gon16] for the Cartan subgroups can be found in the recent paper of Dose, Lido and Mercuri (cf. [DLM22]).

First, observe that $B(N)/W_N$ is always a commutative subgroup of $Aut(X_0(N)/W_N)$, the automorphism group of $X_0(N)/W_N$. Following the case of $X_0(N)$, one can ask whether $B(N)/W_N$ will coincide with $Aut(X_0(N)/W_N)$ for almost all N with $4 \nmid N$ and $9 \nmid N$ (cf. [AtLe70, Theorem 8], [KM88, Theorem 0.1], [BaGo21, Theorem 2] and [Lan01, §3, Corollary]). We call any $u \in Aut(X_0(N)/W_N) \setminus (B(N)/W_N)$ a non Atkin-Lehner type automorphism of the quotient modular curve $X_0(N)/W_N$. In particular, if any $u \in Aut(X_0(N)/W_N)$ commutes with an element $w \in B(N)/W_N$, then it induces a non-trivial automorphism for the

*First author is supported by PID2020-116542GB-I00

quotient curve $X_0(N)/\langle W_N, w\rangle$. Unfortunately, such commutative situation only works without any problem in the case when the $\overline{\mathbb{Q}}$-decomposition on isogeny factors of the Jacobian of $X_0(N)/W_N$ has no repeated factors, see §3.

In general, if the Jacobian decomposition does not involve abelian varieties associated to modular forms with complex multiplication, we can control the decomposition of the Jacobian over a number field. Concretely, we know the smallest number field K where all automorphisms are defined (§2) and control the repeated factors in the K-isogeny decomposition of the Jacobian. Thus, in the case when repeated factors appear (under the assumption that no CM modular form appears), we provide in §3 different results following ideas of Baker and Hasegawa in [BaHa03] and of González and the first author in [BaGo20] and [BaGo21], in §4 following results by computing automorphisms via the canonical model (which is also known as Petri's model) as explained, and in §5 following ideas of Hasegawa in [Has97] and ad-hoc results for particular quotient curves.

In particular, we derive

Theorem 1. *Consider $C = X_0(N)/W_N$ a quotient modular curve of genus $g_N^{W_N}$, write by g_N^* the genus of $X_0^*(N)$. Then $Aut(X_0(N)/W_N) = B(N)/W_N$ in the following situations:*

(i) (Corollary 23 in text) N is an odd square-free natural number such that the Jacobian decomposition of C over $\mathbb{Q}$ has no repeated factors with $\operatorname{Gon}(X_0^*(N)) > 3$ *(where* $\operatorname{Gon}(X_0^*(N))$ *denotes the gonality of $X_0^*(N)$) and satisfies $g_N^{W_N} > dg_N^* + (d-1)5$, where $d := |B(N)/W_N|$.*

(ii) (Corollary 17 in text) $N = Mp$ is a square-free natural number with p prime, and $W_N = \langle w_d \mid d||M\rangle$ such that $g_M^* = 0$ and $g_N^{W_N} \geq 2$.

(iii) (Corollary 36 in text) N is square-free natural number with $N \geq 645$ and $M|N$ with $W_N = B(M)$.

We remark that for a fixed square-free level N and subgroup W_N such that the Jacobian of $X_0(N)/W_N$ has no repeated factors in the $\mathbb{Q}$-decomposition, it is computationally manageable to compute its automorphism group as we indicate in §3 with few examples.

For levels that are products of two or three primes we can go further in general (results corresponding to main results in §6 and §7 respectively).

Theorem 2. *[Theorem 37, Theorem 38 in text] Consider $C = X_0(N)/W_N$ a quotient modular curve with $N = pq$, where p,q are two different primes with $g_N^{W_N} \geq 2$ and $W_N = \langle w_d\rangle$ with $d|pq$, and denote the curve C by (N, d). Then $Aut((N, d)) = B(N)/\langle w_d\rangle$ except for the following quotient curves whose automorphism group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ where we have new involutions because they are hyperelliptic or bielliptic curves:*

$$(57, 57), (74, 74), (77, 77), (85, 85), (91, 91), (111, 111), (143, 143)$$

$$(57, 3), (58, 29), (142, 71).$$

Theorem 3. *Consider $C = X_0(N)/W_N$ a quotient modular curve with $N = pqr$, where p,q and r are three different primes with $g_N^{W_N} \geq 2$.*

(i) (Proposition 40 in text) Assume that $g_r^* = 0$ and consider $W_N = \langle w_{qp}, w_r\rangle$, and denote such quotient curve C by $(N; r)$. Then $Aut(C) = B(N)/\langle w_{qp}, w_r\rangle$ except for

$(102; 2), (114; 2), (138; 2), (165; 11), (195; 3), (195; 5), (238; 2), (154; 2), (231; 7), (285; 3), (286; 2),$

where all such exceptions correspond to hyperelliptic or bielliptic curves, and in each case the automorphism group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(ii) (Proposition 41 in text) Assume that $g_r^* = 0$ and $W_N = \langle w_{pq} \rangle$, then $Aut(C) = B(N)/W_N$.

(iii) (Proposition 42 in text) Assume $W_N = \langle w_p \rangle$ or $W_N = \langle w_p, w_q \rangle$, then $Aut(C) = B(N)/W_N$, except for the hyperelliptic or bielliptic curves: $X_0(190)/\langle w_5, w_{19} \rangle$, $X_0(138)/\langle w_3, w_{23} \rangle$, $X_0(130)/\langle w_2, w_{13} \rangle$, $X_0(114)/\langle w_2, w_{19} \rangle$ and $X_0(102)/\langle w_3, w_{17} \rangle$ with automorphism group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

The proof of Theorem 1(iii), Theorem 2 and Theorem 3 heavily depends on whether there is a map between $Aut(X_0(N)/W_N)$ and $Aut(X_0(N)/\langle W_N, w \rangle)$ for a certain Atkin-Lehner involution $w \in B(N) \setminus W_N$. We prove that such map exists for certain cases (cf. Theorem 34 for the precise statement in a concrete situation).

Finally, for non-square free levels we derive some insights in §4, the more remarkable are:

Proposition 4. *Consider the quotient curves $X_0(p^k q)/\langle w_{p^k} \rangle$ and $X_0^*(p^k q)$ with p, q two different primes and $k \geq 1$ and assume that $g_{p^k}^* = 0$. Then*

(i) (Corollary 19 in text) Any non-trivial automorphism of $X_0(p^k q)/\langle w_{p^k} \rangle$ over $\mathbb{Q}$ different from w_q induces a non-trivial automorphism of $X_0^*(p^k q)$.

(ii) (Lemma 25 in text) $Aut(X_0^*(275)) \cong S_3$, where an element of order three is defined over $\mathbb{Q}[\sqrt{5}]$, corresponding to a non Atkin-Lehner type automorphism of order 3.

All the codes to verify the computations in this paper can be found at `https://github.com/FrancescBars/Files-on-Automorphism-Quotient-Curves`.

The paper is organized as follows: In §2, we discuss various techniques for computing the field of definition of automorphisms of quotient modular curves. In §3, we discuss some initial techniques to compute the automorphism group and prove Theorem 1(ii), Proposition 4(i). In §3.1, we prove Theorem 1(i). In §4, we discuss how to compute the automorphism group by reduction modulo primes of good reduction and prove Proposition 4(ii), Proposition 4(iii). In §5, by studying the reduction at bad primes, we establish an exact sequence between the automorphism groups of certain quotient modular curves and prove Theorem 1(iii). Finally, in §6 we prove Theorem 2, and in §7 we prove Theorem 3.

2 On the field of definition of the automorphism group

In order to compute the automorphisms of a curve, we first need to decide what is the field of definition of the automorphisms. The main objective of this section is to discuss how to compute the field of definition of automorphisms of quotient modular curves.

As usual, for a smooth, proper curve X over a number field k we denote by $Aut(X)$ the automorphism group of X and by $Aut_k(X)$ the automorphisms of X defined over k.

We first recall the following general results.

Lemma 5. *[BaHa03, Lemma 2.1] Let X be a smooth proper and geometrically connected algebraic curve of genus $g \geq 2$ over a field k, and let $J(X)$ be its Jacobian variety over k. Then $Aut_k(X)$ injects into $End_k(J(X))$.*

Theorem 6. *[Rib75, Corollary 1.4] Let A be a semistable abelian variety over the rationals. Then every endomorphism of A is defined over the rationals.*

Now assume that N is a natural number and let $B(N)$ denote the group of automorphisms of $X_0(N)$ generated by the Atkin-Lehner involutions. For any subgroup $W_N \le B(N)$, consider the quotient modular curve $X_0(N)/W_N$. Clearly, we have a natural inclusion

$$B(N)/W_N \le Aut_{\mathbb{Q}}(X_0(N)/W_N).$$

Furthermore, for a fixed number field K and $w \in B(N)/W_N$, if w commutes with all elements of $Aut_K(X_0(N)/W_N)$, then we have an exact sequence:

$$1 \to \langle w \rangle \to Aut_K(X_0(N)/W_N) \to Aut_K(X_0(N)/\langle W_N, w\rangle).$$

We now study the automorphism group of quotient modular curves inside its Jacobian. Recall that the Jacobian $J_0(N)$ of $X_0(N)$ decomposes over $\mathbb{Q}$ as

$$J_0(N) \sim_{\mathbb{Q}} \prod_{f \in \mathrm{New}_N/G_{\mathbb{Q}}} A_f \cdot \prod_{\substack{M|N \\ M<N}} \prod_{f \in \mathrm{New}_M/G_{\mathbb{Q}}} A_f^{n_f}, \tag{2.1}$$

where n_f is the number of positive divisors of $\frac{N}{M}$ (for any field F, the notation $\sim_F$ denotes “isogenous over F”).

Let $J_0^{W_N}(N)$ (resp., $J_0^*(N)$) denote the Jacobian of the quotient curve $X_0^{W_N}(N) := X_0(N)/W_N$ (resp., $X_0^*(N)$). We have the Jacobian decomposition

$$J_0^{W_N}(N) \sim_{\mathbb{Q}} \prod_{f \in \mathrm{New}_N^{W_N}/G_{\mathbb{Q}}} A_f \cdot \prod_{\substack{M|N \\ M<N}} \prod_{f \in \mathrm{New}_M^{W_N}/G_{\mathbb{Q}}} A_f^{m_f}, \tag{2.2}$$

where $0 < m_f \le n_f$ and $f \in \mathrm{New}_N^{W_N}$ (resp., $f \in \mathrm{New}_M^{W_N}$) means $f \in \mathrm{New}_N$ (resp., $f \in \mathrm{New}_M$) such that $f|w_d = f$ for all $w_d \in W_N$ (resp., for all $w_d \in W_N$ with $d|M$). Hence

$$End(J_0^{W_N}(N)) \otimes \mathbb{Q} = \prod_{f \in \mathrm{New}_N^{W_N}/G_{\mathbb{Q}}} K_f \cdot \prod_{\substack{M|N \\ M<N}} \prod_{f \in \mathrm{New}_M^{W_N}/G_{\mathbb{Q}}} M_{m_f}(K_f), \tag{2.3}$$

where K_f denote the totally real number field associated to f.

Proposition 7. *[BaHa03, Proposition 2.4] Let X be an algebraic curve over $\mathbb{Q}$ of genus ≥ 1. If the Jacobian variety $J(X)$ is semistable over $\mathbb{Q}$, then every automorphism of X is defined over $\mathbb{Q}$. Furthermore, if $End(Jac(X)) \otimes \mathbb{Q}$ is a product of totally real fields, then $Aut(X)$ is an elementary abelian 2-group i.e $Aut(X) \cong \mathbb{Z}/2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/2\mathbb{Z}$.*

When N is square-free, as consequences of Proposition 7, we obtain the following results.

Theorem 8. *([Rib75, Proposition 3.1]) For any square-free integer N, the Jacobian variety $J_0(N)$ is a semistable over $\mathbb{Q}$. Consequently, $J_0^{W_N}(N)$ is also semistable over $\mathbb{Q}$ and every automorphism of $X_0(N)/W_N$ is defined over $\mathbb{Q}$ for any subgroup $W_N \le B(N)$.*

Proof. Since N square-free, $J_0(N)$ is semi-stable over $\mathbb{Q}$ by [Rib75, Proposition 3.1] (which refers to [DeRa72, Theorem 6.9, DeRa-144]). Now the result follows from the fact that any $\mathbb{Q}$-isogeny factor of $J_0^{W_N}(N)$ appears in $J_0(N)$. □

Corollary 9 ([BaHa03]). *Let N be a square-free integer and suppose the decomposition of $J_0^{W_N}(N)$ over $\mathbb{Q}$ has no repeated factors (i.e., $m_f = 1$ for all f appearing in the product (2.2)). Then $End(J_0^{W_N}(N)) \otimes \mathbb{Q}$ is a product of totally real fields, thus $Aut(X_0(N)/W_N)$ is a 2-abelian group. In particular if $W_N = B(N)$, then $J_0^{B(N)}(N)$ has no repeated factors, thus $Aut(X_0^*(N))$ is a 2-abelian group.*

Proof. The endomorphism ring (tensored by $\mathbb{Q}$) for each $\mathbb{Q}$-isogeny factor A_f of $J_0(N)$ (in particular for $J_0^{W_N}(N)$) is a totally real number field (cf. [Rib80, (3.9), Theorem 5.1] or [MuPa08, Corollary 4.2]). Now by Proposition 7 we conclude the first statement. Finally, $J_0^{B(N)}(N)$ has no repeated $\mathbb{Q}$-isogeny factors by [BaHa03, before Corollary 2.6] (see [Rib80]). □

Therefore when N is square-free, every automorphism of $X_0(N)/W_N$ is defined over $\mathbb{Q}$, i.e., $Aut_{\mathbb{Q}}(X_0(N)/W_N) = Aut(X_0(N)/W_N)$.

On the other hand, for any arbitrary positive integer N there is an injective mapping

$$Aut(X_0(N)/W_N) \hookrightarrow End_{\overline{\mathbb{Q}}}(J_0^{W_N}(N)) \otimes \mathbb{Q}.$$

Moreover, we know the decomposition of $J_0^{W_N}(N)$ over $\overline{\mathbb{Q}}$. The following proposition gives us a criterion to check when the automorphisms of $X_0(N)/W_N$ are defined over $\mathbb{Q}$.

Proposition 10. *([BaGo20, Proposition 2.4, Remark 2.5]) Let A be a modular abelian variety defined over $\mathbb{Q}$ such that $A \sim_{\mathbb{Q}} \prod_{i=1}^{m} A_{f_i}^{n_i}$ for some $f_i \in New_{N_i}$, where A_{f_i} are pairwise non-isogenous over $\mathbb{Q}$. All endomorphisms of A are defined over $\mathbb{Q}$ if and only if, for every non trivial quadratic Dirichlet character χ, the newform $f_i \otimes \chi$ is different from any Galois conjugate of f_j for all i and j.*

Moreover, for any quadratic Dirichlet character χ attached to the quadratic number field $F = \mathbb{Q}(\sqrt{D})$, the abelian varieties A_f and $A_f \otimes \chi$ are isogenous over F.

Remark 11. *Take A_f with $f \in New_M$ the Shimura abelian variety defined over $\mathbb{Q}$ associated to a modular form f with $dim(A_f) > 1$. A lot of authors studied the $\overline{\mathbb{Q}}$-decomposition of A_f as isogeny factors, see for example [Pyl04] and references therein. Recall that if $f \neq f \otimes \chi$ for all χ quadratic Dirichlet character (i.e. f has no CM), then A_f, in order to have a one dimensional quotient, need to satisfy that $a_p(f)^2 \in \mathbb{Z}$ for any prime p, where $a_p(f)$ denotes the p-th term of the q-expansion of the modular form f, see [Pyl04].*

The following result will be very useful for computing the field of definition of automorphisms of a quotient modular curve.

Corollary 12. *Write $J_0^{W_N}(N) \sim_{\mathbb{Q}} \prod_{i=1}^{m} A_{f_i}^{n_{f_i}}$, and assume that each f_i has no inner twist (i.e $f_i \otimes \chi \neq f_i'$ for any Dirichlet character χ and Galois conjugate f_i' of f_i). List all the quadratic twists involving the different f_i's by $f_i \otimes \chi_{i,j} = f_j$ (for $i \neq j$) with quadratic field $K_{i,j}$ associated to $\chi_{i,j}$, and denote by K the composition of all $K_{i,j}$. Then any $u \in Aut(X_0(N)/W_N)$ is defined over K, thus $Aut(X_0(N)/W_N) = Aut_K(X_0(N)/W_N)$.*

Proof. Consider $u \in Aut(X_0(N)/W_N)$, then naturally u can be considered as an element of $End(J_0^{W_N}(N))$. It is well-known that if f_i does not have any inner twists, then the abelian variety A_{f_i} is simple over $\overline{\mathbb{Q}}$ (if f_i has no inner twists, then the twisting group of f_i (as defined in [MuPa08, Page 19] or [Rib80, Page 48]) is trivial, consequently, $End_{\bar{\mathbb{Q}}}(A_{f_i})$ is a field and this forces that A_{f_i} is simple over $\bar{\mathbb{Q}}$ (cf. [MuPa08, Corollary 4.2 and the proof]).) Thus by Proposition 10, we have $End_{\mathbb{Q}}(A_{f_i}) = End_{\overline{\mathbb{Q}}}(A_{f_i})$. If A_{f_i} and A_{f_j} are isogenous over $\overline{\mathbb{Q}}$ but not over $\mathbb{Q}$, then there exists a Dirichlet character χ such that $A_{f_i} = A_{f_j} \otimes \chi$ [BGGP05, Proposition 4.2]. In particular, $A_{f_i} \sim_{K_{i,j}} A_{f_j}$ (i.e., A_{f_i} and A_{f_j} are isogenous over $K_{i,j}$). Therefore the automorphism u should keep A_{f_i} invariant over K. Now the result follows from the fact that the isogeny decomposition of $J_0^{W_N}(N)$ remains the same for any extension of K in $\overline{\mathbb{Q}}$. □

3 Insights on involutions of $X_0(N)/W_N$

In this section we discuss various techniques to compute the automorphisms of quotient modular curves. Consider the quotient modular curve $X_0(N)/W_N$ of genus $g_N^{W_N}$. Clearly, $B(N)/W_N$ is an abelian subgroup of $Aut_{\mathbb{Q}}(X_0(N)/W_N)$ given only by involutions. Moreover, such involutions are modular in the sense that they are obtained from the normalizer of $\langle \Gamma_0(N), W_N\rangle$ in $\mathrm{PSL}_2(\mathbb{R})$.

In the case when $g_N^{W_N} \geq 3$ and $X_0(N)/W_N$ is not hyperelliptic, by Petri's theorem we can obtain the canonical model of this curve given by an explicit system of quadratic or cubic equations in $\mathbb{P}^{g_N^{W_N}-1}$ which is easily computable. If there are no repeated factors (over $\mathbb{Q}$) in $J_0^{W_N}(N)$, then any possible involution (over $\mathbb{Q}$) can be computed as mentioned in [BaGo19, Page 2947]. Such procedure will cover all automorphism groups when N is square-free.

Recall that for a non-hyperelliptic curve X defined over $\mathbb{C}$ with genus $g > 2$, the image of the canonical map $X \to \mathbb{P}^{g-1}$ is the common zero locus of a set of homogeneous polynomials of degree 2 and 3, when $g > 3$, or of a homogenous polynomial of degree 4, if $g = 3$.

More precisely, assume that X is defined over $\mathbb{Q}$ and choose a basis $\omega_1, \cdots, \omega_g$ of $\Omega^1_{X/\mathbb{Q}}$. For any integer $i \geq 2$, let us denote by $\mathcal{L}_i$ the $\mathbb{Q}$-vector space of homogeneous polynomials $Q \in \mathbb{Q}[x_1, \cdots, x_g]$ of degree i that satisfy $Q(\omega_1, \cdots, \omega_g) = 0$. Of course, $\dim \mathcal{L}_i \leq \dim \mathcal{L}_{i+1}$ because one has $x_j \cdot Q \in \mathcal{L}_{i+1}$ for all $Q \in \mathcal{L}_i$ and for $1 \leq j \leq g$.

If $g = 3$, then $\dim \mathcal{L}_2 = \dim \mathcal{L}_3 = 0$ and $\dim \mathcal{L}_4 = 1$. Any generator of $\mathcal{L}_4$ provides an equation for X. On the other hand, for $g > 3$, $\dim \mathcal{L}_2 = (g-2)(g-3)/2 > 0$ and a basis of $\mathcal{L}_2 \bigoplus \mathcal{L}_3$ provides a system of equations for X. When X is neither trigonal nor a smooth plane quintic ($g = 6$), it suffices to take a basis of $\mathcal{L}_2$.

As before, assume that $J_0^{W_N}(N) \overset{\mathbb{Q}}{\sim} A_{h_1}^{k_1} \times \cdots \times A_{h_n}^{k_n}$ for some normalized eigenforms $h_1, \cdots, h_k \in S_2^{W_N}(N)$. These abelian varieties A_{h_i} are simple and pairwise nonisogenous over $\mathbb{Q}$ and, any automorphism u of $X_0(N)/W_N$ defined over $\mathbb{Q}$ leaves each $A_{h_i}^{k_i}$ stable. In the case when N is square-free and $k_i = 1$ for all i, any non trivial automorphism u of $X_0(N)/W_N$ is an involution defined over $\mathbb{Q}$. Thus u acts on $\Omega^1_{A_{h_i}}$ as the product by -1 or the identity.

Choose a basis $\{\omega_1, \cdots, \omega_{g_N^{W_N}}\}$ of $\Omega^1_{(X_0(N)/W_N)/\mathbb{Q}}$ obtained as the ordered union of bases of all $\Omega^1_{A_{h_i}^{k_i}/\mathbb{Q}}$. Assume that N is square-free, and $k_i = 1$ for all i. Under these assumptions all non-trivial automorphisms of $X_0(N)/W_N$ are involutions defined over $\mathbb{Q}$. An involution u of $X_0(N)/W_N$ induces a linear map $u^* : \Omega^1_{(X_0(N)/W_N)/\mathbb{Q}} \to \Omega^1_{(X_0(N)/W_N)/\mathbb{Q}}$ sending $(\omega_1, \cdots, \omega_{g_N^{W_N}})$ to $(\varepsilon_1\omega_1, \cdots, \varepsilon_{g_N^{W_N}}\omega_{g_N^{W_N}})$ with $\varepsilon_i = \pm 1$ for all $i \leq g_N^{W_N}$ and satisfy

$$Q(\varepsilon_1 x_1, \cdots, \varepsilon_{g_N^{W_N}} x_{g_N^{W_N}}) \in \mathcal{L}_i \text{ for all } Q \in \mathcal{L}_i \text{ and for all } i \geq 2\,. \tag{3.1}$$

The genus of the quotient curve $X_0(N)/\langle W_N, u\rangle$ is the cardinality of the set $\mathcal{I} = \{i\colon \varepsilon_i = 1\}$ and $\{\omega_j\}_{j\in\mathcal{I}}$ is a basis of the pullback of the regular differentials of the quotient curve. For any linear map u^* as above satisfying condition (3.1), only one of the two maps $\pm u^*$ comes from an involution of the curve, because we are assuming that X is non-hyperelliptic. Therefore, we can determine the Automorphism group of non-hyperelliptic $X_0(N)/W_N$ for N square-free, under the assumption that its Jacobian decomposition over $\mathbb{Q}$ has no repeated factors. We present here two such examples. The Mathematica codes to verify the following computations can be found in `github.com/FrancescBars/Mathematica-files-on-Automorphism-Quotient-Curves`.

For simplicity of notations, instead of writting a $\mathbb{Q}$-isogeny Jacobian decomposition of $J_0^{W_N}(N)$ by $\prod A_{f_i}^{n_i}$, we will write it by $\sum (dim(A_{f_i})_{d_i,f_i})^{n_i}$, where d_i denotes the notation of the modular form f_i as in [LMFDB] when $dim(A_{f_i}) \geq 2$, and d_i denotes the Cremona level (cf. [Cre]) of the elliptic curve corresponding to the modular form f_i when $dim(A_{f_i}) = 1$.

Example 13. *Consider the genus* 5 *quotient modular curve* $C := X_0(210)/\langle w_2, w_3, w_5\rangle$. *Since* $N = 210$ *is square-free, all automorphisms of* C *are defined over* $\mathbb{Q}$. *The Jacobian decomposition of* C *over* $\mathbb{Q}$ *is given by*

$$1_{E14a,f_1} + 1_{E35a,f_2} + 2_{105.2.a.b,f_3} + 1_{E210d,f_4}$$

and any automorphism of C *acts as an automorphism on each factor as* ±1. *Since* C *is non-hyperelliptic, we consider the following canonical model of* C *in* $(x : y : z : t : s) \in \mathbb{P}^4$*:*

$$-1260s^2 - 1575t^2 - 1815tx + 480x^2 + 1059ty + 15xy - 1179tz + 900xz - 135yz = 0,$$

$$-900s^2 - 9225t^2 - 3225tx + 2685ty + 1185xy + 480y^2 + 315tz + 540xz - 1305yz = 0,$$

$$-600s^2 + 2850t^2 - 1150tx + 790ty - 210xy - 2790tz + 360xz - 30yz + 480z^2 = 0.$$

From the canonical model we can easily conclude that the only non-trivial automorphism of C *is given by* w_7 *which acts as* $x \leftrightarrow -x$, $y \leftrightarrow -y$, $(z,t) \leftrightarrow (-z,-t)$ *and* $s \leftrightarrow s$, *implying that* $Aut(C) = \{id, w_7\}$.

Example 14. *Consider the genus* 10 *quotient modular curve* $C := X_0(210)/\langle w_6, w_{10}, w_{15}\rangle$. *Since* $N = 210$ *is square-free, all automorphisms of* C *are defined over* $\mathbb{Q}$. *The Jacobian decomposition of* C *over* $\mathbb{Q}$ *is given by*

$$1_{E14a,f_1} + 1_{E21a,f_2} + 1_{E35a,f_3} + 2_{35.2.a.b,f_4} + 1_{E105a,f_5} + 2_{105.2.a.b,f_6} + 1_{E210d,f_7} + 1_{E210e,f_8}$$

and any automorphism of C *acts as an automorphism on each factor as* ±1. *Since* C *is non-hyperelliptic, by constructing a canonical model of* C *in* $(x_1 : \ldots : x_{10}) \in \mathbb{P}^9$ *it can be easily verified that all automorphism of* C *corresponds to* $B(210)/\langle w_6, w_{10}\rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

For the general case when N is not necessarily square-free (recall here that the automorphisms may not be defined over $\mathbb{Q}$), if $w \in Aut(X_0(N)/W_N)$ commutes with $B(N)/W_N$ then it induces an automorphism of $X_0^*(N)$.

Lemma 15. *Let* N *be a positive integer and let* W_N *be a subgroup of* $B(N)$. *Assume that the Jacobian decomposition of* $X_0(N)/W_N$ *over* $\mathbb{Q}$ *has no repeated factors. Then any* $w \in Aut_{\mathbb{Q}}(X_0(N)/W_N) \setminus (B(N)/W_N)$ *induces a non-trivial automorphism of* $X_0^*(N)$ *defined over* $\mathbb{Q}$.

Proof. Write $J_0^{W_N}(N) \sim_{\mathbb{Q}} \prod_{i=1}^m A_{f_i}$. Note that $Aut_{\mathbb{Q}}(X_0(N)/W_N) \subset \prod_{i=1}^m End_{\mathbb{Q}}(A_{f_i})$. Since the isomorphisms of each factor $End_{\mathbb{Q}}(A_{f_i}) \otimes \mathbb{Q}$ correspond to a totally real field K_i and the only finite order elements in K_i are $\{\pm 1\}$, we obtain that $Aut_{\mathbb{Q}}(X_0(N)/W_N)$ is an abelian 2-group. Therefore any $w \in Aut_{\mathbb{Q}}(X_0(N)/W_N) \setminus (B(N)/W_N)$ commutes with all elements of $B(N)/W_N$. Consequently, w induces a non-trivial involution of $X_0^*(N)$. □

When N is square-free, by the work of the first author and González, we know the structure of the automorphism group of $X_0^*(N)$. More precisely, we have

Theorem 16. *[BaGo21, Theorem 1,Theorem 2] Let* N *be a square-free integer such that the curve* $X_0^*(N)$ *has genus* > 2 *and it is not bielliptic*[1].

Then, the group $Aut(X_0^*(N))$ *is non-trivial if and only if* $N = 366, 645$. *In both cases, the order of this group is 2 and the genus of the quotient curve by the non trivial involution is 2.*

As a consequence of Lemma 15 and Theorem 16, we obtain the following result.

[1] i.e. $N \notin \{178, 183, 246, 249, 258, 290, 303, 318, 370, 430, 455, 510\}$.

Corollary 17. *Let N be a square-free positive integer and p be a prime such that $(p, N) = 1$ and $g_N^* = 0$* [2]*. Consider the concrete subgroup $\mathcal{W} := \langle w_d \mid d||N\rangle \subset B(Np)$, in particular, $\langle \mathcal{W}, w_p\rangle = B(Np)$. If $g_N^{\mathcal{W}} \geq 2$, then we have an exact sequence*

$$1 \to \langle w_p\rangle \to Aut(X_0(Np)/\mathcal{W}) \to Aut(X_0^*(Np)).$$

Furthermore, if $g_{Np}^* > 2$, then $Aut(X_0(Np)/\mathcal{W}) = \{id, w_p\}$ for

$$Np \notin \{178, 183, 246, 249, 258, 290, 303, 318, 366, 370, 430, 455, 510, 645\}.$$

Proof. Since N is square-free, all the automorphisms of $X_0(N)/\mathcal{W}$ and $X_0^*(N)$ are defined over $\mathbb{Q}$. Consider the Jacobian decomposition of $X_0(N)/\mathcal{W}$ over $\mathbb{Q}$:

$$J_0^{\mathcal{W}}(Np) \sim_{\mathbb{Q}} \prod_{i=1}^{k} A_{f_i}^{n_i}, \tag{3.2}$$

where f_i is a weight 2 newform of level l_i with $l_i|Np$ and $n_i \geq 1$ is an integer. If possible, let $p \nmid l_i$ for some i and let f_i be a newform of level l_i appearing in the Jacobian decomposition (3.2). Let $l_i = \prod_{j=1}^{k_i} p_j$ be the prime factorization of l_i. By definition of $\mathcal{W}$, we have $w_{p_j} \in \mathcal{W}$ for $j = 1, \dots, k$. Since f_i appears in the Jacobian decomposition of $J_0^{\mathcal{W}}(Np)$, all w_{p_j,l_i}'s (here w_{p_j,l_i} denotes the p_j-th Atkin-Lehner operator acting on level l_i and w_{p_j} denotes the p_j-th Atkin-Lehner operator acting on level Np) acts as $+1$ on f_i (the ± 1 action of the Atkin-Lehner involution w_{p_j,l_i} acting on a modular form f_i of level l_i remains unchanged for all the liftings of f_i at level Ml_i with $(M, l_i) = 1$, i.e. w_{p_j,Ml_i} acts exactly in the same way as w_{p_j,l_i} for each lift of f_i at level Ml_i [AtLe70]). By [BaGo20, Lemma 2.1,Proposition 2.2], f_i can be lifted to a weight 2 cuspform for $\langle \Gamma_0(N), B(N)\rangle$ (since f_i has level l_i and N/l_i is a product of distinct primes coprime with l_i, we can lift f_i to an old form in $\Gamma_0(N)$ such that $w_{\tilde{\ell}}$ acts as $+1$ for each prime $\tilde{\ell}$ with $\tilde{\ell}|N/l_i$, and w_ℓ at level N acts in the same way as w_{ℓ,l_i} at level l_i for each prime ℓ dividing l_j) . This contradicts the assumption that $g_N^* = 0$.

Hence $p|l_i$ for all i. Consider a cuspform f_i of level $l_i = pl'$ appearing in the Jacobian decomposition (3.2). Let $l' = \prod_{j=1}^{s} q_j$ be the prime decomposition of l'. Since $w_{q_j} \in \mathcal{W}$, each Atkin-Lehner involution w_{q_j,l_i} acts as $+1$ on f_i (the argument is similar as before). By [BaGo20, Lemma 2.1, Proposition 2.2], f_i can be uniquely lifted to a weight 2 cuspform for $\langle \Gamma_0(pN), \mathcal{W}\rangle$ (since f_i has level $l_i = pl'$ and N/l_i is a product of distinct primes coprime with l_i, we can lift f_i to an old form in $\Gamma_0(Np)$ such that w_ℓ acts as $+1$ for each prime ℓ with $\ell|N/l_i$ and w_{q_j} acts as $+1$ for each prime q_j dividing l', thus such lift becomes a cuspform for $\langle \Gamma_0(pN), \mathcal{W}\rangle$, furthermore such lift is unique up to multiple by constants when N is square-free (cf. loc.cit.)). Therefore $n_i = 1$ for all i, i.e., the decomposition of $J_0^{\mathcal{W}}(Np)$ over $\mathbb{Q}$ has no repeated factors. By Corollary 9, $Aut(X_0(N)/\mathcal{W})$ is an abelian group. Now the first part follows from Lemma 15.

The second part follows from the first part and Theorem 16. □

We now discuss some criteria to compute the automorphism group of $X_0(N)/W_N$ when N is not necessarily square-free.

Lemma 18. *Let K be a number field, N be a positive integer and W_N be a subgroup of $B(N)$. Assume that each $w_d \in B(N)/W_N$ acts as ± 1 on each repeated factor appearing in the Jacobian decomposition of $X_0(N)/W_N$ over K (where $\pm$ depends only on d and the repeated factor). Then any $w \in Aut_K(X_0(N)/W_N) \setminus (B(N)/W_N)$ induces a non-trivial automorphism of $X_0^*(N)$ over K.*

[2] Recall that $g_N^* = 0$ for N in the list: 2, 3, 5, 6,7, 10,11, 13, 14, 15, 17, 19, 21, 22, 23, 26, 29, 30, 31, 33, 34, 35, 38, 39, 41, 42, 46, 47, 51, 55, 59, 62, 66, 69, 70, 71, 78, 87, 94, 95, 105, 110, 119.

Proof. Take $w \in Aut_K(X_0(N)/W_N)$, then naturally w can be considered as an element of $End_K(J_0^{W_N}(N))$. Let $J_0^{W_N}(N) \sim_K \prod_{i=1}^m A_{f_i}^{m_i}$ be the decomposition of the Jacobian over K, where the factors A_{f_i}'s are pairwise non-isogenous over K. Then each $A_{f_i}^{m_i}$ remains stable under the action of w. Since w_d acts as ± 1 on each repeated factor, we have that in each factor w commutes with w_d. Therefore $w \circ w_d = w_d \circ w$ in the group $Aut_K(X_0(N)/W_N)$. Since $X_0(N)/W_N \to X_0^*(N)$ is a Galois cover given by w_d's, we conclude that w induces a non-trivial automorphism in $X_0^*(N)$. □

Corollary 19. *Let p, q be two distinct primes and $k \geq 2$ be an integer such that the genus of $X_0^*(p^k)$ is zero* [3]*. Then any non-trivial $w \in Aut_{\mathbb{Q}}(X_0(p^k q)/\langle w_{p^k}\rangle)$ with $w \neq w_q$ induces a non-trivial automorphism of $X_0^*(p^k q)$ over $\mathbb{Q}$.*

Moreover, assume that for any two non-$\mathbb{Q}$-isogeny factors A_{f_i} and A_{f_j} of the Jacobian of $X_0(p^k q)/\langle w_{p^k}\rangle$ which are isogenous over $\overline{\mathbb{Q}}$, the involution w_q acts as +1 on both factors or exactly as -1 on both factors. Then, any non-trivial $w \in Aut(X_0(p^k q)/\langle w_{p^k}\rangle)$ with $w \neq w_q$ induces a non-trivial automorphism of $X_0^*(p^k q)$.

Proof. We show that for any number field K, the Atkin-Lehner involution w_q acts as ± 1 on the repeated factors appearing in the Jacobian decomposition of $X_0(p^k q)/\langle w_{p^k}\rangle$ over K. Then the result follows from Lemma 18.

First consider the Jacobian decomposition over $\mathbb{Q}$ (we take $K = \mathbb{Q}$).

Assume that a factor A_{f_i} appears in such decomposition corresponding to a newform f_i of level l with $l | p^k q$. If $q \nmid l$, then by [BaGo20, Lemma 2.1,Prop.2.2] we can lift f_i to level p^k which is fixed by w_{p^k}, this contradicts the assumption that $g_{p^k}^* = 0$. Therefore $q | l$, and write $l = qp^s$ for some non-negative integer s.

The newform f_i has level qp^s. Let $w_{p^s, qp^s}(f_i) = \epsilon \cdot f_i$ (recall that w_{p^s,qp^s} denotes the p^s-th Atkin-Lehner operator on level qp^s, and $\epsilon = 1$ when $s = 0$). Let S_{f_i} be the vector subspace of $S_2(\Gamma_0(p^k q))$ generated by the $k-s+1$ linearly independent eigenforms $\{f(z), f(pz), \ldots, f(p^{k-s}z)\}$. Then using the similar arguments as in the proof of [BaGo20, Proposition 2.2], we get that the dimension n_{f_i} of the vector space $S_2(\Gamma_0(p^k q))^{\langle w_p^k\rangle} \cap S_{f_i}$ is

$$n_{f_i} = \begin{cases} \frac{k-s+1}{2} & \text{if } k-s \text{ is odd,} \\ \frac{k-s+1-\epsilon}{2} & \text{if } k-s \text{ is even.} \end{cases} \tag{3.3}$$

In particular, this dimension encodes the number of repeated factors for A_{f_i} at level $p^k q$ that appears in the Jacobian decomposition of $X_0(p^k q)/\langle w_{p^k}\rangle$. Also, note that if $w_{q,qp^s}(f_i) = \delta_{f_i} f_i$ (recall that $\delta_{f_i} \in \{\pm 1\}$), then for any $g \in S_2(\Gamma_0(p^k q))^{\langle w_p^k\rangle} \cap S_{f_i}$, we have $w_q(g) = \delta_{f_i} g$ (i.e., the action of w_q on every element of $S_2(\Gamma_0(p^k q))^{\langle w_p^k\rangle} \cap S_{f_i}$ is same as the action of w_{q,qp^s} on f_i). Consequently, w_q acts as ± 1 on the repeated factor corresponding to A_{f_i} appearing in the Jacobian decomposition of $X_0(p^k q)/\langle w_{p^k}\rangle$. This concludes the proof for $K = \mathbb{Q}$.

Consider now that A_{f_i} and A_{f_j} non $\mathbb{Q}$-isogeny factors that are isogenous over $\overline{\mathbb{Q}}$. By [BGGP05, Proposition.4.2] they are isogenous in a quadratic twist in a quadratic number field K by its Dirichlet character $f_i \otimes \chi \cong f_j$, but from the above argument, one has level qp^{k_1} and the other qp^{k_2} and because the action of w_q remains unchanged by hypothesis, we obtain the result arguing as in the rational field case. □

We give an example where we apply Corollary 19 to compute the automorphism group.

Example 20. *We have $Aut(X_0^*(245)) \cong Aut(X_0^*(147)) \cong \mathbb{Z}/2\mathbb{Z}$ and all the automorphisms are defined over $\mathbb{Q}$. Moreover, for $p \in \{3, 5\}$, $Aut_{\mathbb{Q}}(X_0(49 \cdot p)/\langle w_{49}\rangle) \cong \langle w_p\rangle$, and $Aut(X_0(49 \cdot p)/\langle w_{49}\rangle) = Aut_{\mathbb{Q}[\sqrt{-7}]}(X_0(49 \cdot p)/\langle w_{49}\rangle)$.*

[3] Recall $g_{p^k}^* = 0$ with $k \geq 2$ iff $p^k \in \{4, 8, 9, 16, 25, 27, 32, 49\}$

Proof. First observe that $X_0^*(7^2 \cdot 3)$ is a hyperelliptic curve of genus 2 with the hyperelliptic involution defined over $\mathbb{Q}$. The Jacobian decomposition is given by $J_0^*(147) \sim^{\mathbb{Q}} 2_{147.2.a.d}$. The dimension two factor does not break into two elliptic curves in the algebraic closure (cf. [Pyl04]) and the corresponding modular form does not have CM. Thus by Corollary 12, all automorphisms of $X_0^*(7^2 \cdot 3)$ are defined over $\mathbb{Q}$, and by Magma we see that the only non-trivial automorphism over $\mathbb{Q}$ is the hyperelliptic involution. Hence $Aut(X_0^*(7^2 \cdot 3)) \cong \mathbb{Z}/2\mathbb{Z}$. On the other hand, the curve $X_0^*(49 \cdot 5)$ is bielliptic with bielliptic involution defined over $\mathbb{Q}$ (cf. [BaGo20, Propositiom 5.1]). The Jacobian decompositions over $\mathbb{Q}$ of the curve is given by

$$J_0^*(245) \sim^{\mathbb{Q}} 1_{E35a,f_1} + 2_{245.2.a.e}.$$

By a similar argument as previous, we get that all automorphisms of $X_0^*(245)$ are defined over $\mathbb{Q}$ and one can easily check that (by constructing an explicit model using Petri's theorem as discussed earlier) the automorphism group is $\mathbb{Z}/2\mathbb{Z}$, given by the bielliptic involution(cf, [BaGo21, Lemma 2]).

For the quotient curves $X_0(147)/\langle w_{49}\rangle$ and $X_0(245)/\langle w_{49}\rangle$, the $\mathbb{Q}$-decompositions of the Jacobian are given by:

$$J_0^{\langle w_{49}\rangle}(147) \sim_{\mathbb{Q}} 1_{E21a,g_1} + 1_{E147b,g2} + 2_{147.2.a.d,g_3=g} + 2_{147.2.a.e,g_4}$$

$$J_0^{\langle w_{49}\rangle}(245) \sim_{\mathbb{Q}} 1_{E35a,f_1} + 2_{35.2.a.b,f_2} + 2_{245.2.a.e,f_3=h} + 2_{245.2.a.f,f_4} + 2_{245.2.a.h,f_5}.$$

The cusp forms appearing in the above Jacobian decomposition have no inner twist, but $h \otimes \chi_{\mathbb{Q}[\sqrt{-7}]} = f_4$ and $g \otimes \chi_{\mathbb{Q}[\sqrt{-7}]} = g_4$. Therefore, all the automorphisms of such quotient modular curves are defined over $\mathbb{Q}[\sqrt{-7}]$.

Observe that the operator w_3 acts on the $\mathbb{Q}$-decomposition of $J_0^{\langle w_{49}\rangle}(147)$ as follows: on the dimension 2 factor corresponding to the modular form g it acts as $+1$ and on the dimension two factor corresponding to the modular form g_4 it acts as -1. Thus the automorphisms of $X_0(147)/\langle w_{49}\rangle$ defined over $\mathbb{Q}[\sqrt{-7}]$ are not necessarily coming from an automorphism of $X_0^*(147)$. A similar argument holds in the case 245.

Since $g_{49}^* = 0$, by Corollary 19, any (non-trivial) non Atkin-Lehner type automorphism of $X_0(245)/\langle w_{49}\rangle$ over $\mathbb{Q}$ maps to the bielliptic involution of $X_0^*(245)$. Since the Jacobian decomposition of $X_0(245)/\langle w_{49}\rangle$ over $\mathbb{Q}$ has no repeated factors, every element of the group $Aut_{\mathbb{Q}}(X_0(245)/\langle w_{49}\rangle)$ is an involution. We need to check whether the bielliptic involution of $X_0^*(245)$ lifts to an automorphism of $X_0(245)/\langle w_{49}\rangle$. If such lift exists, then it acts as $+1$ on $E35a$ and -1 on $2_{245.2.a.e,h}$ (or vice-versa). Now using the canonical model it is easy to check that no such lift is possible (the Mathematica files for verifying the computations can be found in `https://github.com/FrancescBars/Files-on-Automorphism-Quotient-Curves`). Therefore, $Aut_{\mathbb{Q}}(X_0(245)/\langle w_{49}\rangle) = \{id, w_5\}$. A similar argument holds for $N = 147$. □

3.1 N odd square-free and no repeated factors in $J_0^{W_N}(N)$

In this section, we present a criterion to compute the automorphism group of quotient modular curves of odd level.

Proposition 21. *Let N be a square-free positive integer and $W \leq B(N)$ such that $X_0(N)/W$ is non-hyperelliptic with $g := g(X_0(N)/W) \geq 3$ and that the Jacobian decomposition of $X_0(N)/W$ over $\mathbb{Q}$ has no repeated factors. If u is any non-trivial involution of $X_0(N)/W$, then $u(\infty) \neq \infty$.*

In particular, if $u \notin B(N)/W$, then $u(\infty)$ is not a cusp.

Proof. By Theorem 8, u is defined over $\mathbb{Q}$ and the eigenvalues of u on $S_2(\langle\Gamma_0(N), W\rangle)$ are ± 1. If all the eigenvalues are $+1$, then $u = id$ on $X_0(N)/W$. On the other hand, if all the eigenvalues are -1, then $X_0(N)/W$ is hyperelliptic and u is the hyperelliptic involution.

Thus $+1$ and -1 both are eigenvalues of u. There are differentials $\omega_1, \omega_2 \in H^0(X_0(N)/W, \Omega^1)$ such that $u^*\omega_1 = \omega_1$ and $u^*\omega_2 = -\omega_2$, which are normalized eigendifferentials under the action of the Hecke algebra. The q-expansion at ∞ of ω_i is of the form

$$\omega_i = \big(\sum_{j=1}^{\infty} a_{i,j} q^j\big)\frac{dq}{q},$$

where $a_{i,1} = 1$ for $i \in \{1, 2\}$.

This implies that $\omega = \omega_1 + \omega_2$ does not vanish at ∞ but $u^*\omega = \omega_1 - \omega_2$ vanishes at ∞. This shows that $u(\infty) \neq \infty$. This proves the first part.

Since N is square-free, the Atkin-Lehner involutions act transitively on the cusps. If $u(\infty)$ is a cusp, then there exists $w \in B(N)/W$ such that $u(\infty) = w(\infty)$, i.e., $wu(\infty) = \infty$. By the first part, we conclude that $u \in B(N)/W$. The result follows. □

Proposition 22. *Assume that N is an odd square-free positive integer and $W \leq B(N)$ such that $X_0(N)/W$ is non-hyperelliptic with $g := g(X_0(N)/W) \geq 3$ and that the Jacobian decomposition of $X_0(N)/W$ over $\mathbb{Q}$ has no repeated factors. If $u \notin B(N)/W$ is a non-trivial involution of $X_0(N)/W$, then the $\mathbb{Q}$-gonality of $X_0(N)/W$ is ≤ 6.*

Proof. Since u is defined over $\mathbb{Q}$, by Eichler-Shimura congruence we have

$$uT_l = T_l u \text{ on } Jac(X_0(N)/W), \text{ for any prime } l \nmid N. \tag{3.4}$$

In particular, we have

$$uT_2 = T_2 u \text{ on } Jac(X_0(N)/W). \tag{3.5}$$

From Proposition 21, we know that $Q = u(\infty)$ is not a cusp. Let $P \in Y_0(N)$ such that $\pi_W(P) = u(\infty)$, where π_W is the natural projection mapping $\pi_W : X_0(N) \to X_0(N)/W$.

Since P is not a cusp, there exists an elliptic curve E defined over $\bar{\mathbb{Q}}$ and an N-cyclic subgroup C_N of $E(\bar{\mathbb{Q}})$ such that $P = (E, C_N)$. If $w_d \in W$, then

$$w_d(P) = (E/C_d, (E[d] + C_N)/C_d),$$

where C_d denotes the d-th cyclic subgroup of C_N, i.e., $C_d = C_N \cap E[d]$.

Let $S \in X_0(N)/W$ be a non cuspidal point. Consider the divisor

$$D_S := (uT_2 - T_2 u)(\infty - S).$$

From (3.5) we see that D_S is linearly equivalent to zero. If D_S is identically zero then

$$uT_2(\infty) + T_2 u(S) = uT_2(S) + T_2 u(\infty). \tag{3.6}$$

Since all the points in the support of $T_2(\infty)$ are cusps and all the points in the support of $T_2(S)$ are noncuspidal, applying u to both sides of (3.6) we see that there is no cancellation between the points in the support of $uT_2(\infty)$ and $uT_2(S)$. Therefore (3.6) implies $uT_2(\infty) = T_2 u(\infty)$, i.e., $3(Q) = T_2(Q)$. Recall that

$$T_2(Q) = \sum_{i=1}^{3} \pi_W((E/G_i, (C_N + G_i)/G_i)),$$

where G_i, $1 \leq i \leq 3$, are the 2-cyclic subgroups of $E[2]$.

If $3(Q) = T_2(Q)$, then each elliptic curve E/G_i is isomorphic to E/C_d for some $d|N$ such that $w_d \in W$. Therefore, E has CM by a quadratic order $\mathcal{O}$ of discriminant D with odd conductor. Moreover, this property holds for all elliptic curves E/C_d with $d|N$ such that $w_d \in W$ and also for all elliptic curves E/G_i.

From the proof of [BaGo21, Proposition 2], we know that for every elliptic curve E with CM by the order of discriminant D with odd conductor, there is at least a 2-subgroup G of $E[2]$ such that the discriminant of the order $End(E/G)$ has even conductor. Therefore $T_2(Q) \neq 3(Q)$, i.e., D_S is not identically zero.

Since $u(\infty)$ is not a cusp, taking $S = u(\infty)$, we see that D_S is a divisor of a non-constant function which is difference of effective rational degree 6 divisors. Thus the $\mathbb{Q}$-gonality of $X_0(N)/W$ is at most 6. □

As an immediate consequence of Proposition 22 and Castelnuovo-Severi's inequality, we obtain the following result which will be helpful for computing the automorphism group of quotient modular curves of higher genus.

Corollary 23. *Assume that N is an odd square-free positive integer and $W \leq B(N)$ such that $\mathrm{Gon}(X_0^*(N)) > 3$ (where $\mathrm{Gon}(X_0^*(N))$ denotes the gonality of $X_0^*(N)$) and that the Jacobian decomposition of $X_0(N)/W$ over $\mathbb{Q}$ has no repeated factors. Let g^* (resp., g) denote the genus of $X_0^*(N)$ (resp., $X_0(N)/W$) and $d := |B(N)/W|$. If $g > d \cdot g^* + (d-1) \cdot 5$, then $Aut(X_0(N)/W) = B(N)/W$.*

Proof. By Corollary 9, we have $Aut(X_0(N)/W) \cong \mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}$. Recall that there is a degree d mapping $f_1 : X_0(N)/W \to X_0^*(N)$ defined over $\mathbb{Q}$. By Proposition 22 (note that the assumption $\mathrm{Gon}(X_0^*(N)) > 3$ implies that $X_0(N)/W$ is non-hyperelliptic and $g \geq 3$), if $u \notin B(N)/W$ is any non trivial involution of $X_0(N)/W$, then the $\mathbb{Q}$-gonality of $X_0(N)/W$ is ≤ 6. Let $f_2 : X_0(N)/W \to \mathbb{P}^1$ be a mapping of degree $d' \leq 6$. If possible let f_1 and f_2 factor through a common map $f_3 : X_0(N)/W \to Y$ of degree > 1. Since f_2 factors through f_3, we have $\mathrm{Gon}(Y) \leq 3$. On the other hand since f_1 factors through f_3, we have $3 < \mathrm{Gon}(X_0^*(N)) \leq \mathrm{Gon}(Y)$, which is a contradiction (the values of N such that $\mathrm{Gon}(X_0^*(N)) \leq 3$ can be found in [HaHa96] and [HaSh00]). Thus the mappings f_1, f_2 do not factor through a common map. By Castelnuovo-Severi's inequality we must have

$$g \leq d \cdot g(X_0^*(645)) + (d-1) \cdot 5,$$

which is a contradiction. Thus $Aut(X_0(N)/W) = B(N)/W$. □

We now discuss an application of Corollary 23.

Corollary 24. *$Aut(X_0(645)/\langle w_3, w_5\rangle) = \langle w_{43}\rangle$.*

Proof. Note that $g(X_0(645)/\langle w_3, w_5\rangle) = 21$, $g(X_0^*(645)) = 5$, $\mathrm{Gon}(X_0^*(645)) > 3$ (cf. [HaSh00, Theorem 1]) and the Jacobian decomposition of $X_0(645)/\langle w_3, w_5\rangle$ over $\mathbb{Q}$ has no repeated factors. Since $g(X_0(645)/\langle w_3, w_5\rangle) > 2g(X_0^*(645)) + 5$, by Corollary 23 (with $d = 2$) we conclude that $Aut(X_0(645)/\langle w_3, w_5\rangle) = B(645)/\langle w_3, w_5\rangle = \langle w_{43}\rangle$. □

4 A computation bound for $|Aut(X_0(N)/W_N)|$

In this section we discuss how to compute the automorphism group by obtaining an explicitly computable upper bound on it. Throughout the section we always assume that $g(X_0(N)/W_N) \geq$

2. Recall that $B(N)/W_N \leq Aut(X_0(N)/W_N)$, moreover for $p \nmid N$ we have an injective map

$$\iota : Aut(X_0(N)/W_N) \hookrightarrow Aut(\overline{X_0(N)/W_N}),$$

where $\overline{X_0(N)/W_N}$ denote the reduction mod p of the curve $X_0(N)/W_N$. More concretely, if we consider all automorphisms of $X_0(N)/W_N$ defined over a number field K, then for each prime $\mathfrak{p}$ of K with $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ (recall that $p \nmid N$), we have an injective map

$$\iota_K : Aut_K(X_0(N)/W_N) \hookrightarrow Aut_{\mathcal{O}_K/\mathfrak{p}}(\overline{X_0(N)/W_N}).$$

The Magma code "`X0NQuotient(N,[WN])`" gives a model for the quotient curve $X_0(N)/W_N$ over $\mathbb{Q}$ (here "`WN`" should be replaced by the integers d_i's such that w_{d_i}'s generate W_N). In many cases this model is a good model to study the mod p reduction for some prime $p \nmid N$. However, in some cases this built-in model is not good to study the mod p reduction for some $p \nmid N$, in those cases, using Magma we construct a good model of $X_0(N)/W_N$. Then the Magma code

"`#Automorphisms(ChangeRing(X0NQuotient(N,[WN]),GF(q)))`"

computes the number of automorphisms of $X_0(N)/W_N$ modulo p over the finite field $GF(q = p^z)$ for some prime $p \nmid N$ and $z \in \mathbb{N}$. Thus we obtain an upper bound for $|Aut(X_0(N)/W_N)|$ and if it coincides with $|B(N)/W_N|$ then we obtain $Aut(X_0(N)/W_N) = B(N)/W_N$. By abuse notations we denote $Aut_{\mathbb{F}_{p^z}}(\overline{X_0(N)/W_N})$ by $Aut_{\mathbb{F}_{p^z}}(X_0(N)/W_N)$.

Following the notations of §3, suppose that the Jacobian decomposition of $X_0(p^k q)/\langle w_{p^k}\rangle$ is of the form $\sum(dim(A_{f_i})_{d_i,f_i})^{n_i}$. Since we are interested in the action of w_q on the modular forms appearing the Jacobian decomposition, we write $\sum(dim(A_{f_i})_{d_i,f_i,t_i})^{n_i}$ instead of $\sum(dim(A_{f_i})_{d_i,f_i})^{n_i}$, where t_i denotes the action of w_q on the modular form f_i.

We now discuss an interesting example.

Lemma 25. *We have $Aut_{\mathbb{Q}}(X_0^*(275)) \cong \mathbb{Z}/2\mathbb{Z}$, $Aut(X_0^*(275)) = Aut_{\mathbb{Q}[\sqrt{5}]}(X_0^*(275)) \cong S_3$, $Aut_{\mathbb{Q}}(X_0(275)/w_{25}) = \{id, w_{11}\}$. Moreover, there is an exact sequence:*

$$1 \to \{id, w_{11}\} \to Aut(X_0(275)/w_{25}) = Aut_{\mathbb{Q}[\sqrt{5}]}(X_0(275)/w_{25}) \to Aut(X_0^*(275)).$$

Proof. The Jacobian decomposition of $X_0(275)/\langle w_{25}\rangle$ over $\mathbb{Q}$ is given by

$$J_0^{(25)}(275) \sim^{\mathbb{Q}} (1_{E11a,g_1,-1})^2 + 1_{E55a,g_2,1} + 2_{55.2.a.b,g_3,-1} + 1_{E275a,g_4,1} +$$

$$1_{E275b,g_5,-1} + 2_{275.2.a.e,g_6,1} + 2_{275.2.a.f,g_7,-1} + 2_{275.2.a.h,g_8,-1}.$$

The cusp forms g_i's have only the inner twist $g_8 \otimes \chi_{\mathbb{Q}[\sqrt{5}]} = g_8$, and the quadratic twists correspond to $g_2 \otimes \chi_{\mathbb{Q}[\sqrt{5}]} = g_4$, $g_1 \otimes \chi_{\mathbb{Q}[\sqrt{5}]} = g_5$ and $g_6 \otimes \chi_{\mathbb{Q}[\sqrt{5}]} = g_7$. Therefore the automorphisms of $X_0^*(275)$ and the automorphisms of $X_0(275)/w_{25}$ are defined over $\mathbb{Q}[\sqrt{5}]$. Moreover, any non-trivial automorphism of $X_0(275)/w_{25}$ which is not Atkin-Lehner type, induces a non-trivial automorphism of $X_0^*(275)$ (cf. Corollary 19). By [BaGo20], we know that $X_0^*(275)$ is bielliptic over $\mathbb{Q}$ and using Magma we see that the automorphism groups of $X_0^*(275)$ and $X_0(275)/w_{25}$ over $\mathbb{F}_2$ have exactly two elements. Thus $Aut_{\mathbb{Q}}(X_0(275)/w_{25}) = \{id, w_{11}\}$ and $Aut_{\mathbb{Q}}(X_0^*(275)) = \{id, biel\}$ where *biel* is the bielliptic involution of $X_0^*(275)$ (cf. [BaGo20, Proof of Proposition 6.1]). Again, using Magma we see that the automorphism groups over $\mathbb{Q}[\sqrt{5}]$ of the curves $X_0(275)/\langle w_{25}\rangle$ and $X_0^*(275)$ each have at most 6 elements. We prove that we do have an order three automorphism over $\mathbb{Q}[\sqrt{5}]$ for $X_0^*(275)$ and the result follows.

The Jacobian decomposition of $X_0^*(275)$ over $\mathbb{Q}[\sqrt{5}]$ is given by $J_0^*(275) \sim_{\mathbb{Q}[\sqrt{5}]} 1_{E55a,g_2}^2 + 2_{275.2.a.e,g_6}$ and a canonical model over $\mathbb{Q}$ for $X_0^*(275)$ (following notations and techniques also introduced in [BaGo20] or [BaGo21]) is given by

$$-24t^2 + 3x^2 + 5y^2 + 6tz - 2z^2 = 0,$$

$$135tx^2 + 384t^2y - 192x^2y + 225ty^2 + 102t^2z + 12x^2z - 96tyz + 20y^2z + 6tz^2 + 32yz^2 = 0.$$

Now over $\mathbb{Q}[\sqrt{5}]$, a non-trivial automorphism u acts on the decomposition $1_{g_2}^2 + 2_{g_6}$ (up to multiplication by -1) as follows: on $1_{g_2}^2$ it acts by a 2×2 matrix and on 2_{g_6} it acts as $+1$. We take $A = -\begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{5}}{2} \\ \frac{3}{2\sqrt{5}} & \frac{1}{2} \end{pmatrix}$, A acting on (x, y) corresponding to $1_{55a,g_2} + 1_{275a,g_4}$ and (z, t) invariant corresponding to 2_{g_6}. Such order three automorphism does not commute with the bielliptic involution $x \leftrightarrow -x$ (keeping y, z, t invariant), thus the automorphism group of $X_0^*(275)$ is isomorphic to the symmetric group S_3.

Now apply Corollary 19 to conclude the result (recall that w_{11} acts as $+1$ on both g_2 and g_4). □

Remark 26. *For the automorphism of $X_0^*(25 \cdot p)$ or $X_0(25 \cdot p)/w_{25}$ with $p = 7$, $p = 13$ and $p = 17$ we make the following comments:*

- *$N = 175$: The Jacobian decomposition of $X_0(25 \cdot 7)/w_{25}$ over $\mathbb{Q}$ is given by*

$$J_0^{\langle w_{25}\rangle}(175) \sim^{\mathbb{Q}} 1_{E35a,f1,(w7=)-1} + 2_{35.2.a.b,f2,1} + 1_{E175b,f3,1} + 2_{175.2.a.e,f4,-1} + 2_{175.2.a.f,f5,-1}$$

  where each f_i has no inner twists, and the only quadratic twist between them correspond to $f_1 \otimes \chi_{\mathbb{Q}[\sqrt{5}]} = f_3$ and $f_2 \otimes \chi_{\mathbb{Q}[\sqrt{5}]} = f_5$. Therefore, all automorphisms of $X_0^*(175)$ are defined over $\mathbb{Q}$ (the factors of $J_0^{\langle w_{25}\rangle}(175)$ that remains in $J_0^*(175)$ are the ones with w_7 acting as $+1$) and all automorphisms of $X_0(175)/\langle w_{25}\rangle$ are defined over $\mathbb{Q}[\sqrt{5}]$ (cf. Corollary 12). Now using Magma we see that $Aut_{\mathbb{F}_9}(X_0^*(175))$ is trivial, therefore $Aut(X_0^*(175)) = \{id\}$. Because the action of w_7 is different in the repeated factors of the isogeny decomposition over $\mathbb{Q}(\sqrt{5})$ of the curve $X_0(175)/\langle w_{25}\rangle$, if such quotient curve has an automorphism, then it may not descend to an automorphism of $X_0^*(175)$. Thus we need to deal directly with the quotient curve $X_0(175)/\langle w_{25}\rangle$. Using Magma we get $|Aut_{\mathbb{F}_3}(X_0(175)/\langle w_{25}\rangle)| = 2$, thus $Aut_{\mathbb{Q}}(X_0(175)/\langle w_{25}\rangle) = \{id, w_7\}$. Moreover, $|Aut_{\mathbb{F}_q}(X_0(175)/\langle w_{25}\rangle)| = 6$ with $q = p$ for any prime p which splits in $\mathbb{Q}[\sqrt{5}]$ and $q = p^2$ for any prime p which remains inert in $\mathbb{Q}[\sqrt{5}]$, with $p \leq 61$ and $p \nmid 35$. Thus a study of an automorphism of order 3 over $\mathbb{Q}[\sqrt{5}]$ is needed for the genus 8 quotient curve $X_0(175)/\langle w_{25}\rangle$ as we did for level $N = 275$.

- *Consider $N = 325$:*

$$J_0^{\langle w_{25}\rangle}(325) \sim^{\mathbb{Q}} 1_{65a,h1,w_{13}=1} + 2_{65.2.a.c,h2,-1} + 2_{65.2.a.b,h3,1} + 1_{325b,h4,1} + 1_{325c,h5,-1} +$$

$$1_{325e,h6,-1} + 2_{325.2.a.g,h7,1} + 2_{325.2.a.h,h8,-1} + 2_{325.2.a.i,h9,-1}$$

  where each h_i has no inner twist, and the quadratic twists correspond to $h_1 \otimes \chi_{\mathbb{Q}[\sqrt{5}]} = h_5$, $h_2 \otimes \chi_{\mathbb{Q}[\sqrt{5}]} = h_7$ and $h_3 \otimes \chi_{\mathbb{Q}[\sqrt{5}]} = h_9$. The operator w_{13} acts differently in each component, thus we obtain that $Aut_{\mathbb{Q}}(X_0^*(325)) = Aut(X_0^*(325))$ and $Aut_{\mathbb{Q}[\sqrt{5}]}(X_0(325)/w_{25}) = Aut(X_0(325)/\langle w_{25}\rangle)$. Now using Magma we see that $Aut_{\mathbb{F}_7}(X_0^*(325)) = \{id\}$ and we have $Aut_{\mathbb{Q}}(X_0^*(325)) = \{id\}$. Moreover, $Aut_{\mathbb{Q}}(X_0(325)/\langle w_{25}\rangle) = \{id, w_{13}\}$ by Corollary 19, and using Magma we see that $Aut_{\mathbb{F}_{11}}(X_0(325)/\langle w_{25}\rangle) = Aut_{\mathbb{F}_{19}}(X_0(325)/\langle w_{25}\rangle) = 6$. It remains to study whether there is an order 3 element in $Aut(X_0(325)/\langle w_{25}\rangle)$, similar to the case $N = 175$ and 275. We hope to resolve this issue in future work.

- *$N = 425$:*

$$J_0^{\langle w_{25}\rangle}(425) \sim^{\mathbb{Q}} ((1_{17a,j_1,w_{17}=-1})^2 + 1_{85a,j_2,-1} + 2_{85.2.a.b,j_3,1} + 2_{85.2.a.c,j_4,1} +$$

$$1_{425a,j_5,1} + 1_{425c,j_6,1} + 1_{425d,j_7,1} + 2_{425.2.a.e,j_8,-1} + 2_{425.2.a.f,j_9,-1} + 5_{425.2.a.i,j_{10},-1}$$

where each j_i has no inner twist and there are the quadratic twists $j_1 \otimes \chi_5 = j_5$, $j_3 \otimes \chi_5 = j_9$ and $j_4 \otimes \chi_5 = j_8$ between them. Therefore all automorphisms of $X_0^*(425)$ and $X_0(425)/\langle w_{25}\rangle$ are defined over $\mathbb{Q}[\sqrt{5}]$. Using Magma we see that $|Aut_{\mathbb{F}_4}(X_0^*(425))| = 1$, hence $Aut(X_0^*(425)) = \{id\}$.

Remark 27. *Continuing with Example 20, the $\mathbb{Q}$-decomposition of the Jacobian of $X_0(49 \cdot p)/\langle w_{49}\rangle$ for $p \in \{3, 5, 11, 13, 17\}$ has isogeny factors over $\mathbb{Q}[\sqrt{-7}]$, where w_p is not acting with the same sign in both isogeny factors. Thus all automorphisms of such quotient curves are defined over $\mathbb{Q}[\sqrt{-7}]$ (if any automorphism is defined over $\mathbb{Q}[\sqrt{-7}]$ but not over $\mathbb{Q}$, then such automorphism does not induce an automorphism for $X_0^*(49\cdot p)$), but for $p = 11$ or when we consider $X_0^*(49 \cdot p)$ with $p \in \{3, 5, 11, 13, 17\}$, the modular forms appearing in the $\mathbb{Q}$-decomposition of the Jacobian have no quadratic twists. Thus, in such cases all automorphisms are defined over $\mathbb{Q}$. Using Magma we get $|Aut_{\mathbb{F}_2}(X_0^*(49\cdot p))| = 1$ for $p \in \{11, 13, 17\}$, thus $Aut(X_0^*(49\cdot p)) = \{id\}$ for such primes. Moreover, $|Aut_{\mathbb{F}_4}(X_0(147)/\langle w_{49}\rangle)| = |Aut_{\mathbb{F}_9}(X_0(245)/\langle w_{49}\rangle)| = 2$, thus $Aut_{\mathbb{Q}[\sqrt{-7}]}(X_0(147)/\langle w_{49}\rangle) = \{id, w_3\}$ and $Aut_{\mathbb{Q}(\sqrt{-7})}(X_0(245)/\langle w_{49}\rangle) = \{id, w_5\}$. Unfortunately, for the other values of p, the genus of $X_0(49 \cdot p)/\langle w_{49}\rangle$ is big and we are not able to get any conclusion using the current version of Magma (V2.27-7).*

Lemma 28. *Consider the curves $X_0(160)/\langle w_{32}\rangle$ and $X_0^*(160)$. Then, $Aut(X_0^*(160)) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, generated by the bielliptic involution of $X_0^*(160)$ defined over $\mathbb{Q}(i)$ and an involution defined over $\mathbb{Q}$ and we have an exact sequence:*

$$1 \to \{id, w_5\} \to Aut(X_0(160)/w_{32}) \to Aut(X_0^*(160)).$$

Moreover, we have $Aut_{\mathbb{Q}}(X_0(160)/\langle w_{32}\rangle) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Proof. Observe that the genus 4 quotient curve $X_0^*(160)$ is non-hyperelliptic and it is bielliptic over $\mathbb{Q}(i)$ (but not over $\mathbb{Q}$) (cf. [BaGo20, Theorem 1.2]). The Jacobian decomposition of $X_0^*(160)$ over $\mathbb{Q}$ and $\mathbb{Q}(i)$ are given by:

$$J_0^*(160) \sim_{\mathbb{Q}} E20a^2 \times E80b \times E160a,$$

$$J_0^*(160) \sim_{\mathbb{Q}[i]} (E20a)^3 \times E160a.$$

Moreover, $E20a$ and $E160a$ have no inner twists. Thus all automorphisms of $X_0^*(160)$ are defined over $\mathbb{Q}(i)$. Observe that 7 is inert in $\mathbb{Q}(i)$, thus the order of the automorphism group of $X_0^*(160)$ is bounded by the order of $Aut_{\mathbb{F}_{49}}(X_0^*(160))$. Using Magma we get $|Aut_{\mathbb{F}_{49}}(X_0^*(160))| = 4$ and $|Aut_{\mathbb{F}_7}(X_0^*(160))| = 2$. Recall that the normalizer of $\Gamma_0(160)$ in $\mathrm{PSL}_2(\mathbb{Z})$ is strictly bigger than $\langle\Gamma_0(160), B(160)\rangle$ because $4|160$ (cf. [AtLe70, Theorem 8]). In particular, it contains $S_2 = \begin{pmatrix} 1 & 1/2 \\ 0 & 1 \end{pmatrix}$ (which does not belong to $\langle\Gamma_0(160), B(160)\rangle$), and is well-known that $V_2 = S_2 w_{32} S_2$ commutes with w_5 and w_{32} [BKS23, Proposition 4.15], thus induces a non-trivial automorphism of $X_0^*(160)$ over $\mathbb{Q}$. Therefore $Aut_{\mathbb{Q}}(X_0^*(160)) = \{id, V_2\}$ and $Aut_{\mathbb{Q}[i]}(X_0^*(160)) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ by the bound on the order of automorphism group over finite fields.

Now the $\mathbb{Q}$-isogeny decomposition of the Jacobian of $X_0(160)/\langle w_{32}\rangle$ is:

$$(1_{E20a,f_1})^2 + (1_{E40a,f_2})^2 + 1_{E80a,f_3} + 1_{E80b,f_4} + 1_{160a,f_5} + 2_{160.2.a.c,f_6},$$

the corresponding modular forms have only the inner twist $f_6 \otimes \chi_{\mathbb{Q}[i]} = f_6$, and the quadratic twists $f_1 \otimes \chi_{\mathbb{Q}[i]} = f_4$ and $f_2 \otimes \chi_{\mathbb{Q}[i]} = f_3$. Thus the automorphisms of $X_0(160)/\langle w_{32}\rangle$ are defined over $\mathbb{Q}[i]$. The factors $1_{E20a,f_1}$ and $1_{E80b,f_4}$ (resp., $1_{E40a,f_2}$ and $1_{E80a,f_3}$) are non-isogenous over $\mathbb{Q}$ but isogenous over $\mathbb{Q}(i)$, and w_5 acts as $+1$ (resp., -1) on both factors. By Corollary 19, any non-trivial $u \in Aut(X_0(160)/\langle w_{32}\rangle)$ with $u \neq w_5$ induces a non-trivial automorphism of $X_0^*(160)$. This proved the first part.

Using Magma we see that $|Aut_{\mathbb{F}_7}(X_0(160)/\langle w_{32}\rangle)| = 4$. Hence the automorphism group of $X_0(160)/\langle w_{32}\rangle$ over $\mathbb{Q}$ is generated by w_5 and V_2 (cf. [BKS23, Proposition 4.15]). □

Remark 29. *Using the canonical model of $X_0^*(N)$, in [BaGo20, §2] (resp., in [BaGo21, Lemma 2]), the first author and González gave a methodology to check if $X_0^*(N)$ has a bielliptic involution over $\mathbb{Q}$ (resp., any involution over $\mathbb{Q}$ when N square-free). In general, to obtain all automorphisms over $\mathbb{Q}$ we need to find all matrices of finite order in $\mathrm{PGL}_{g_N^*}(\mathbb{Q})$ which leaves the canonical model (which is obtained using the cusp forms appearing in the $\mathbb{Q}$-isogeny decomposition of the Jacobian) invariant. Since we know the $\mathbb{Q}$-isogeny decomposition of its Jacobian and each isogeny factor remains invariant under the action of any automorphism, such matrices can be obtained by blocks. For example, we know that $J_0^*(160) \sim_{\mathbb{Q}} E20a^2 \times E80b \times E160a$. In order to obtain an automorphism of $X_0^*(160)$ over $\mathbb{Q}$, it suffices to compute a matrix of the form* $\begin{pmatrix} A & & \\ & \pm1 & \\ & & \pm1 \end{pmatrix}_{4\times4}$ *with $A \in \mathrm{GL}_2(\mathbb{Q})$, which fixes the canonical model of $X_0^*(160)$ in 4 variables x_1, x_2, x_3, x_4, where x_1, x_2 correspond to $E20a^2$, x_3 corresponds to $E80b$, and x_4 corresponds to $E160a$ (we denote the corresponding automorphism by $A \times \pm1 \times \pm1$).*

5 On automorphisms group for square free $N = Mq$ by reduction modulo q

Let $N = qM$, where M is a positive integer and q is a prime such that $q \nmid M$. For any subgroup W_N of $B(N)$, if $u \in Aut(X_0(N)/W_N)$ commutes with all $w_d \in B(N) \setminus W_N$, then u induces a non-trivial automorphism on $X_0^*(N)$. By [BaGo20], we know the structure of the group $Aut(X_0^*(N))$ when N is square-free.

By Deligne-Rapaport [DeRa72], the reduction modulo q of $X_0(q \cdot M)$ consists of two copies Z and Z' of $X_0(M)$ over $\mathbb{F}_q$ which intersects transversally at the supersingular points on $X_0(M)$. The Atkin-Lehner involution w_d with $d|N$ acts on $X_0(N)$ modulo q as follows:

(i) if $q \nmid d$, then w_d fixes each component Z and Z' and it acts in characteristic q in the same way as in characteristic zero. Note that in this case, w_d still acts as an involution on $X_0(M)$ and the image $w_d(P)$ of a point P is supersingular if and only if P is supersingular on $X_0(M)$. Therefore a point on $X_0(M)/\langle w_d\rangle$ is supersingular if and only if its preimage under the quotient map is supersingular on $X_0(M)$ (recall that a point on a quotient curve $X_0(M)/W$ is supersingular if the underlying elliptic curve is supersingular).

(ii) if $q|d$, then w_d interchanges Z and Z'. In particular, if $w_d = w_q$ then w_q fixes each $\mathbb{F}_q$-rational supersingular point while it exchanges each properly $\mathbb{F}_{q^2}$-rational supersingular points to its conjugate.

Now consider a subgroup $W_N \leq B(N)$ generated by certain Atkin-Lehner involutions. If W_N is generated by w_d's with $q \nmid d$, then $X_0(N)/W_N$ mod q consists of two copies Z and Z' of $X_0(M)/W_N$ over $\mathbb{F}_q$, meeting transversally at the supersingular points on $X_0(M)/W_N$ (note that the assumption on W_N implies $W_N \leq B(N) \cap B(M)$). On the other hand, if $w_d \in W_N$ such that $q|d$, then $X_0(N)/W_N$ mod q consists of only one component Z'', where Z'' is some quotient of $X_0(M)$ (cf. [Has97] and [FuHa99] for more details).

Lemma 30. *Let $N = qM$, where M is a positive integer and q is a prime such that $q \nmid M$. For any subgroup W_N of $B(qM)$ such that $(q, d) = 1$ for all $w_d \in W_N$, the number of intersection points for the two components Z and Z' of $X_0(M)/W_N$ modulo q is equal to:*

$$1 + g(X_0(N)/W_N) - 2 \cdot g(X_0(M)/W_N).$$

Moreover, all the points in $Z \cap Z'$ are $\mathbb{F}_{q^2}$-rational.

Proof. By the specialization principle, the arithmetic genus of $Z + Z'$ is equal to $g(X_0(N)/W_N)$. Moreover, we have the following relation

$$1 + p_a(Z + Z') = p_a(Z) + p_a(Z') + Z \cdot Z' = g(X_0(M)/W_N) + g(X_0(M)/W_N) + Z \cdot Z',$$

where p_a denotes the arithmetic genus. Since Z and Z' intersect transversally, $Z \cdot Z'$ is exactly the number of intersection points of Z and Z' (which is also equal to the number of supersingular points on $X_0(M)/W_N$ mod q). Therefore

$$Z \cdot Z' = \#Z \cap Z' = 1 + g(X_0(N)/W_N) - 2 \cdot g(X_0(M)/W_N).$$

This proves the first part. Recall that the set $Z \cap Z'$ contains only the supersingular points on $X_0(M)/W_N$ in characteristic q, and a point on $X_0(M)/W_N$ is supersingular if and only if its preimage is supersingular on $X_0(M)$. Since the supersingular points on $X_0(M)$ in characteristic q are $\mathbb{F}_{q^2}$-rational, all the points in $Z \cap Z'$ are $\mathbb{F}_{q^2}$-rational. □

Lemma 31. *Let $N = qM$, where M is a square-free positive integer and q is a prime such that $q \nmid M$. Suppose W_N is a subgroup of $B(qM)$ such that $(q, d) = 1$ for all $w_d \in W_N$. For any $u \in Aut(X_0(N)/W_N) \setminus \{id\}$, consider the automorphism $v := u \circ w_q \circ u^{-1} \circ w_q^{-1} \in Aut(X_0(N)/W_N)$. If n denotes the order of v, then we have*

$$g(X_0(N)/W_N) - 1 \geq n(g(X_0(N)/W_N) - 1 - 2g(X_0(M)/W_N)). \tag{5.1}$$

Proof. Recall that $X_0(N)/W_N$ mod q is $Z + Z'$ where Z and Z' isomorphic to $X_0(M)/W_N$ mod q. Since u either fixes or swaps Z and Z', v mod q fixes both Z and Z'. Thus v mod q can be thought as an automorphism on $X_0(M)/W_N$ mod q. Since u is rational and w_q acts as Frobenius on $Z \cap Z'$, v fixes every point in $Z \cap Z'$ (recall that every point in $Z \cap Z'$ is $\mathbb{F}_{q^2}$-rational). Therefore v mod q induces an automorphism of order n on $Z = X_0(M)/W_N$ mod q which fixes every point in $Z \cap Z'$. Since $\#Z \cap Z' = 1 + g(X_0(N)/W_N) - 2 \cdot g(X_0(M)/W_N)$ (cf. Lemma 30), by Riemann Hurwitz formula we obtain

$$\begin{aligned} 2g(X_0(M)/W_N) - 2 &\geq n(2\overline{g} - 2) + (n-1)(1 + g(X_0(N)/W_N) - 2 \cdot g(X_0(M)/W_N)) && (5.2)\\ &\geq -2n + (n-1)(1 + g(X_0(N)/W_N) - 2 \cdot g(X_0(M)/W_N)), && (5.3)\end{aligned}$$

where $\overline{g}$ denotes the genus of Z/v. In particular, we have

$$g(X_0(N)/W_N) - 1 \geq n(g(X_0(N)/W_N) - 1 - 2g(X_0(M)/W_N)). \tag{5.4}$$

□

Corollary 32. *Let M, q, N, W_N, u, v and n be as in Lemma 31. If $n = 1$ for all $u \in Aut(X_0(N)/W_N)\setminus \{id\}$, then we have an exact sequence:*

$$1 \to \langle w_q \rangle \to Aut(X_0(N = qM)/W_N) \to Aut(X_0(N)/\langle W_N, w_q\rangle).$$

Proof. Suppose $n = 1$ for all $u \in Aut(X_0(N)/W_N)\setminus\{id\}$, then $u \circ w_q = w_q \circ u$ on $Aut(X_0(N)/W_N)$. Thus $u \in Aut(X_0(N)/\langle W_N, w_q\rangle)$ and there is a natural mapping

$$\varphi_q : Aut(X_0(N)/W_N) \to Aut(X_0(N)/\langle W_N, w_q\rangle).$$

Now to prove the corollary it suffices to prove that $\ker(\varphi_q) = \langle w_q\rangle$. Let $u \in Aut(X_0(N)/W_N)$ such that $u = id$ on $Aut(X_0(N)/\langle W_N, w_q\rangle)$. Consider a non-trivial element $u \in Aut(X_0(N)/W_N)$ such that $u \neq w_q$. Since automorphisms $u, w_q^{-1} \circ u \in Aut(X_0(N)/W_N)$ have finitely many fixed points on $X_0(N)/W_N$, there exists $P \in X_0(N)/W_N$ such that $u(P) \notin \{P, w_q(P)\}$. Therefore $u \neq id$ on $X_0(N)/\langle W_N, w_q\rangle$ and we conclude that $\ker(\varphi_q) = \langle w_q\rangle$. □

Lemma 33. *Suppose $M \geq 2$ is a square-free integer and q is a prime such that $(q, M) = 1$. For any $d||M$, let $\nu(M, d)$ (resp., $\nu(qM, d)$) denote the number of fixed points of the Atkin-Lehner involution w_d on $X_0(M)$ (resp., $X_0(qM)$). Then we have*

$$2\nu(M, d) - \nu(qM, d) \geq 0. \tag{5.5}$$

Proof. For any square-free positive integer N and $d||N$, we have

$$\begin{aligned}\nu(N,d) := \Big(\prod_{p|\frac{N}{d}} c_1(p)\Big)h(-4d) &+ \begin{cases}\Big(\prod_{p|\frac{N}{d}} c_2(p)\Big)h(-d) \text{ if } 4 \leq d \equiv 3 \pmod 4\\ 0, \text{ otherwise}\end{cases}\\ &+ \begin{cases}\prod_{p|\frac{N}{2}}\left(1+\left(\frac{-4}{p}\right)\right), \text{ if } d = 2\\ 0, \text{ otherwise}\end{cases}\\ &+ \begin{cases}\prod_{p|\frac{N}{3}}\left(1+\left(\frac{-3}{p}\right)\right), \text{ if } d = 3\\ 0, \text{ otherwise,}\end{cases}\end{aligned}$$

where, for $i = 1, 2$

$$\begin{aligned} c_i(p) &:= \begin{cases}1+\left(\frac{-d}{p}\right), \text{ if } p \neq 2, d \equiv 3 \pmod 4\\ 1+\left(\frac{-4d}{p}\right), \text{ if } p \neq 2, d \not\equiv 3 \pmod 4,\end{cases}\\ c_1(2) &:= \begin{cases}1, \text{ if } d \equiv 1 \pmod 4 \text{ and } 2||N\\ 2, \text{ if } d \equiv 3 \pmod 4 \text{ and } 2||N\end{cases}\\ c_2(2) &:= 1 + \left(\frac{-d}{2}\right) \text{ if } d \equiv 3 \pmod 4.\end{aligned}$$

In particular for any $d||M$, it is easy to see that

$$\begin{aligned}2\nu(M,d) - \nu(qM,d) = (2 - c_1(q))h(-4d)\prod_{p|\frac{M}{d}} c_1(p) &+ \begin{cases}(2-c_2(q))h(-d)\prod_{p|\frac{M}{d}} c_2(p),\\ \qquad\qquad \text{if } 4 \leq d \equiv 3 \pmod 4\\ 0, \text{ otherwise}\end{cases}\\ &+ \begin{cases}\left(1-\left(\frac{-4}{q}\right)\right)\prod_{p|\frac{M}{2}}\left(1+\left(\frac{-4}{p}\right)\right), \text{ if } d = 2\\ 0, \text{ otherwise}\end{cases}\\ &+ \begin{cases}\left(1-\left(\frac{-3}{q}\right)\right)\prod_{p|\frac{M}{3}}\left(1+\left(\frac{-3}{p}\right)\right), \text{ if } d = 3\\ 0, \text{ otherwise.}\end{cases}\end{aligned}$$

Since $c_i(q) \leq 2$, we always have $2\nu(M,d) - \nu(qM,d) \geq 0$. The result follows. □

We are now ready to prove the main theorem of this section.

Theorem 34. *Suppose $M \geq 2$ is a square-free integer and q is a prime such that $(q,M) = 1$. Let W be any subgroup of $B(qM)$ such that $(q,d) = 1$ for all $w_d \in W$ and $g(X_0(qM)/W) \geq 2$. Then there is an exact sequence*

$$1 \to \langle w_q \rangle \to Aut(X_0(qM)/W) \to Aut(X_0(qM)/\langle W, w_q \rangle).$$

Proof. We follow the approach of [Ogg77, Hilfsatz 11]. Observe that by assumption on W, we have $W \subseteq B(qM) \cap B(M)$. For simplicity of notations, we denote Z=$X_0(M)/W \pmod q$ by $\overline{X_0(M)/W}$. Let $u \in Aut(X_0(qM)/W)\backslash\{id\}$, and consider the automorphism $v := u \circ w_q \circ u^{-1} \circ w_q^{-1}$ on $\overline{X_0(qM)/W}$. From the proof of Lemma 31, we see that v induces an automorphism on $\overline{X_0(M)/W}$, and it fixes at least $1 + g(X_0(qM)/W) - 2 \cdot g(X_0(M)/W)$ points over $\mathbb{F}_{q^2}$. If n denotes the order of v, then by Lemma 31, we have

$$\begin{aligned} 2g(X_0(M)/W) - 2 &\geq n(2\overline{g} - 2) + (n-1)(1 + g(X_0(qM)/W) - 2 \cdot g(X_0(M)/W)) \qquad (5.6)\\ &\geq -2n + (n-1)(1 + g(X_0(qM)/W) - 2 \cdot g(X_0(M)/W)), \qquad (5.7)\end{aligned}$$

where $\overline{g}$ denotes the genus of Z/v. In particular we have

$$g(X_0(qM)/W) - 1 \geq n(g(X_0(qM)/W) - 1 - 2g(X_0(M)/W)). \qquad (5.8)$$

We show that $n = 1$. This implies $v = id$, i.e., w_q commutes with u and the result follows. Note that if $Aut(X_0(qM)/W)$ is commutative, then we automatically have $n = 1$.

Let $|W| = 2^s$. Recall that

$$g(X_0(qM)/W) = \frac{1}{2^{s+1}}\Big(2g(X_0(qM)) - 2 + 2^{s+1} - \sum_{w_d \in W} \nu(qM,d)\Big) \text{ and,} \qquad (5.9)$$

$$g(X_0(M)/W) = \frac{1}{2^{s+1}}\Big(2g(X_0(M)) - 2 + 2^{s+1} - \sum_{w_d \in W} \nu(M,d)\Big), \qquad (5.10)$$

where $\nu(M,d)$ (resp., $\nu(qM,d)$) denote the number of fixed points of the Atkin-Lehner involution w_d on $X_0(M)$ (resp., $X_0(qM)$).

For any square-free positive integer N, the genus of $X_0(N)$ is given by

$$g(X_0(N)) = 1 + \frac{\psi(N)}{12} - \frac{\mu_{-4}(N)}{4} - \frac{\mu_{-3}(N)}{3} - 2^{r_N - 1} \leq 1 + \frac{\psi(N)}{12} - 2^{r_N - 1}, \qquad (5.11)$$

where

$$\psi(N) = \prod_{p|N}(p+1)$$
$$\mu_{-m}(N) = \prod_{p|N}\Big(1 + \Big(\frac{-m}{p}\Big)\Big) \text{ for } m \in \{3,4\},$$

and r_N denotes the number of distinct prime divisors of N.

Recall that for any $w_d \in B(qM) \cap B(M)$, from Lemma 33 we have

$$2\nu(M,d) - \nu(qM,d) \geq 0. \qquad (5.12)$$

Combining (5.9), (5.10), (5.11) and (5.12), we get

$$\begin{aligned}
&g(X_0(qM)/W)-1-2g(X_0(M)/W)\\
=&\frac{1}{2^{s+1}}\Big(2g(X_0(qM))+2-2^{s+2}-4g(X_0(M))+\sum_{w_d\in W}(2\nu(M,d)-\nu(qM,d))\Big)\\
=&\frac{1}{2^{s+1}}\Bigg(2\cdot\Big(-2^{s+1}+(q-1)\frac{\psi(M)}{12}+\Big(1-\Big(\frac{-4}{q}\Big)\Big)\frac{\mu_{-4}(M)}{4}+\Big(1-\Big(\frac{-3}{q}\Big)\Big)\frac{\mu_{-3}(M)}{3}\Big)\\
&\qquad\qquad\qquad\qquad\qquad\qquad+\sum_{w_d\in W}(2\nu(M,d)-\nu(qM,d))\Bigg)\\
\geq&\frac{1}{2^s}\Big(-2^{s+1}+(q-1)\frac{\psi(M)}{12}\Big),
\end{aligned}$$

i.e.,

$$g(X_0(qM)/W)-1-2g(X_0(M)/W)\geq\frac{1}{2^s}\Big(-2^{s+1}+(q-1)\frac{\psi(M)}{12}\Big). \tag{5.13}$$

On the other hand, from (5.9) and (5.11) we obtain

$$g(X_0(qM)/W)-1\leq\frac{1}{2^{s+1}}\Big(2g(X_0(qM))-2\Big)\leq\frac{1}{2^s}\Big(\frac{\psi(qM)}{12}-2^{r_M}\Big). \tag{5.14}$$

We now compute the values of the triple (q,M,W) such that $g(X_0(qM)/W)-1-2g(X_0(M)/W)\leq 0$.

If $g(X_0(qM)/W)-1-2g(X_0(M)/W)\leq 0$, then from (5.13) we have

$$(q-1)\frac{\psi(M)}{12}\leq 2^{s+1}\leq 2^{r_M+1}, \tag{5.15}$$

where r_M denotes the number of distinct prime divisors of M.

If possible let $r_M\geq 4$. Since $q\geq 2$ and $M\geq 2$, from (5.15) we get

$$2^{r_M+1}<\frac{3\cdot4\cdot6\cdot8\cdot8^{r_M-4}}{12}\leq(q-1)\frac{\psi(M)}{12}\leq 2^{r_M+1},$$

which is a contradiction. Therefore, we must have $r_M\leq 3$. Using this bound, from (5.15) we obtain

$$(q-1)\psi(M)\leq 12\cdot 2^4=192. \tag{5.16}$$

Since $q\geq 2$, $M\geq 2$ and $M<\psi(M)$, from (5.16) it is easy to see that $q\leq 64$ and $M\leq 192$.

Furthermore, for $2\leq q\leq 64$ and $2\leq M\leq 192$ with $q\nmid M$, using MAGMA we get $g(X_0(qM)/W)-1-2g(X_0(M)/W)\leq 0$ if and only if

$$(q,M,W)\in S_0:=\{(2,15,\langle w_3\rangle),(2,21,\langle w_7\rangle),(2,33,\langle w_3\rangle),(2,35,\langle w_7\rangle),(3,14,\langle w_2\rangle)\}.$$

Therefore, we conclude that $g(X_0(qM)/W)-1-2g(X_0(M)/W)\leq 0$ if and only if $(q,M,W)\in S_0$.

For $(q,M,W)\in S_0$, using MAGMA, we see that $|Aut_{\mathbb{F}_p}(X_0(qM)/W)|=4$ for some prime $p\nmid qM$ (choose the primes $p=7,11,5,3,5$ respectively). Hence the group $Aut_{\mathbb{Q}}(X_0(qM)/W)$ is commutative for $(q,M,W)\in S_0$. Consequently, for such values of (q,M,W) we must have $v=id$, i.e., $n=1$.

From now on we assume that

$$(q,M,W)\notin\{(2,15,\langle w_3\rangle),(2,21,\langle w_7\rangle),(2,33,\langle w_3\rangle),(2,35,\langle w_7\rangle),(3,14,\langle w_2\rangle)\}.$$

For such values of q, M and W we have $g(X_0(qM)/W) - 1 - 2g(X_0(M)/W) > 0$.

We now study the validity of (5.8). Here, the main idea is that we show the inequality (5.8) does not hold when some parameters are too large.

Case I: $q \geq 5$.

First consider the case $q \geq 5$. If possible let $n \geq 2$ for $q \geq 5$. From (5.8), we have

$$g(X_0(qM)/W) - 1 \geq 2(g(X_0(qM)/W) - 1 - 2g(X_0(M)/W)). \tag{5.17}$$

Combining (5.17), (5.13) and (5.14), we get

$$\frac{\psi(qM)}{12} - 2^{r_M} \geq -2^{s+2} + 2(q-1)\frac{\psi(M)}{12}. \tag{5.18}$$

Simplifying we get (recall that $s \leq r_M$)

$$0 < (q-3)\frac{\psi(M)}{12} \leq 2^{s+2} - 2^{r_M} \leq 3 \cdot 2^{r_M}. \tag{5.19}$$

If possible let $r_M \geq 4$. Since $q \geq 5$, from (5.19) we obtain

$$12 \cdot 3 \cdot 2^{r_M+1} \leq 2 \cdot 3 \cdot 4 \cdot 6 \cdot 8 \cdot (12)^{r_M-4} \leq (q-3)\psi(M) \leq 12 \cdot 3 \cdot 2^{r_M}, \tag{5.20}$$

which is a contradiction. Therefore $r_M \leq 3$.

Since $q \geq 5$ and $r_M \leq 3$, from (5.19) we get

$$2M < (q-3)\psi(M) \leq 12 \cdot 3 \cdot 8, \text{ i.e., } M < 144.$$

On the other hand, since $\psi(M) \geq 3$ and $r_M \leq 3$, from (5.19) we obtain

$$(q-3) \cdot 3 \leq (q-3)\psi(M) \leq 12 \cdot 3 \cdot 8, \text{ i.e., } q \leq 99. \tag{5.21}$$

Using `MAGMA`, we conclude that for prime $5 \leq q \leq 99$, $r_M \leq 3$ and $2 \leq M \leq 144$ (recall that $g(X_0(qM)/W) \geq 2$), the inequality (5.17) is satisfied if and only if $(q, M, W) = (5, 14, \langle w_2 \rangle)$.

Therefore, for $q \geq 5$ and $(q, M, W) \neq (5, 14, \langle w_2 \rangle)$, we must have $n = 1$, i.e., w_q commutes with u.

Now consider the curve $X_0(5 \cdot 14)/\langle w_2 \rangle$. Clearly, $\langle w_5, w_7 \rangle \subseteq Aut(X_0(5 \cdot 14)/\langle w_2 \rangle)$. Using `MAGMA`, we see that $\#Aut_{\mathbb{F}_3}(X_0(5 \cdot 14)/\langle w_2 \rangle) = 4$. Hence $Aut(X_0(5 \cdot 14)/\langle w_2 \rangle) = \langle w_5, w_7 \rangle$, i.e., $Aut(X_0(5 \cdot 14)/\langle w_2 \rangle)$ is commutative. Consequently, in this case we have $n = 1$.

Therefore, in the case $q \geq 5$ and $M \geq 2$, we conclude that $n = 1$, i.e., w_q commutes with u and the result follows.

Case II: $q \in \{2, 3\}$ **and** $n \geq 4$.

Now assume that $q \in \{2, 3\}$. If possible let $n \geq 4$. Then we have

$$g(X_0(qM)/W) - 1 \geq 4(g(X_0(qM)/W) - 1 - 2g(X_0(M)/W)). \tag{5.22}$$

Combining (5.22), (5.13) and (5.14) we get

$$(3q-5)\frac{\psi(M)}{12} \leq 2^{s+3} - 2^{r_M} \leq 7 \cdot 2^{r_M}. \tag{5.23}$$

If $r_M \geq 4$, then from (5.23) we have

$$7 \cdot 2^{r_M} < \frac{3 \cdot 6 \cdot 8 \cdot 12 \cdot (14)^{r_M-4}}{12} \leq (3q-5)\frac{\psi(M)}{14} \leq 7 \cdot 2^{r_M}, \tag{5.24}$$

which is a contradiction. Hence we must have $r_M \leq 3$. Using this bound, from (5.23) we have

$$(3q-5)\psi(M) \leq 7 \cdot 12 \cdot 2^{r_M} \leq 7 \cdot 12 \cdot 2^3. \tag{5.25}$$

If $q = 2$, then from (5.25) we get $M < \psi(M) \leq 672$. On the other hand, if $q = 3$, then from (5.25) we get $M < \psi(M) \leq 168$.

For simplicity of notations, we denote the triple (q, M, W) by $(q, M, d_1, d_2, \ldots, d_k)$, where $W := \langle w_{d_1}, w_{d_2}, \ldots, w_{d_k} \rangle$.

Using `MAGMA`, we see that for $q \in \{2, 3\}$ the inequality (5.22) is satisfied only for the values of (q, M, W) appearing in Table 2. For the triples (q, M, W) appearing in Table 2, if we can show that either $Aut_{\mathbb{F}_q}(X_0(M)/W)$ has no element of order ≥ 4 or $Aut(X_0(qM)/W)$ is commutative, then we can conclude that for such values of (q, M, W) the only possibility is $n \leq 3$.

Now consider the triples (q, M, W) appearing in Table 2. Using `MAGMA`[4], we see that

$$|Aut_{\mathbb{F}_2}(X_0(115)/\langle w_{23} \rangle)| = 2, \text{ and } |Aut_{\mathbb{F}_2}(X_0(165)/\langle w_3, w_5 \rangle)| = 2.$$

Hence for the triples $(2, 115, 23)$ and $(2, 165, 3, 5)$, we must have $n \leq 3$ (since there is no automorphism of order ≥ 4).

For the remaining triples (q, M, W) in Table 2, using `MAGMA`, we see that $|Aut_{\mathbb{F}_p}(X_0(qM)/W)| \leq 4$ for some prime $p \nmid qM$ (cf. Table 3). Hence for the remaining values of (q, M, W) in Table 2, the group $Aut_{\mathbb{Q}}(X_0(qM)/W)$ is commutative. Consequently, for such values of (q, M, W) we must have $n = 1$.

Therefore in any case, we have $n \leq 3$. We now show that $n \neq 3$ for $q \in \{2, 3\}$.

Case III: $n = 3$ and $q = 3$

Consider the case $q = 3$ and $n = 3$. For such cases we have

$$g(X_0(qM)/W) - 1 \geq 3(g(X_0(qM)/W) - 1 - 2g(X_0(M)/W)). \tag{5.26}$$

Combining (5.26), (5.14) and (5.13) we obtain

$$(2q-4)\frac{\psi(M)}{12} = \frac{\psi(M)}{6} \leq 3 \cdot 2^{s+1} - 2^{r_M} \leq 5 \cdot 2^{r_M}. \tag{5.27}$$

If $r_M \geq 4$, then from (5.27) we get

$$27 \cdot 4 \cdot 2^{r_M} < 3 \cdot 6 \cdot 8 \cdot 12 \cdot (14)^{r_M - 4} \leq 6 \cdot 5 \cdot 2^{r_M}, \tag{5.28}$$

which is a contradiction. Hence we must have $r_M \leq 3$. Using this bound, from (5.27) we have

$$M < \psi(M) \leq 30 \cdot 2^3 = 240. \tag{5.29}$$

Using `MAGMA`, we see that for $q = 3$ and $2 \leq M \leq 240$, the inequality (5.26) is satisfied only for the triples (3,22,2), (3,35,7). But using `MAGMA`, we see that the curves $X_0(22)/\langle w_2 \rangle \pmod 3$ and $X_0(35)/\langle w_7 \rangle \pmod 3$ have no automorphism of order 3.

Therefore for $q = 3$, we must have $n \leq 2$.

Case IV: $n = 3$ and $q = 2$.

Now consider the case $q = 2$ and $n = 3$. If possible let $\bar{g} \geq 1$ (recall that $\bar{g}$ denotes the genus of $(\overline{X_0(M)/W})/v$).

From (5.6), we get

$$2g(X_0(M)/W) - 2 \geq 2(1 + g(X_0(2M)/W) - 2g(X_0(M)/W)), \tag{5.30}$$

[4] For the curves $X_0(115)/\langle w_{23} \rangle$ and $X_0(165)/\langle w_3, w_5 \rangle$, the built-in models in `MAGMA` are not good over $GF(2)$, for these curves we first construct good models over $GF(2)$ and then compute the automorphism group.

i.e.,

$$3g(X_0(M)/W) - 2 \geq g(X_0(2M)/W). \tag{5.31}$$

Note that we have the following commutative diagram over $\mathbb{Q}$:

$$\begin{tikzcd}
X_0(2M) \arrow[r, "\deg 3"] \arrow[d, "\deg 2^s"'] & X_0(M) \arrow[d, "\deg 2^s"] \\
X_0(2M)/W \arrow[r, "\deg 3"'] & X_0(M)/W
\end{tikzcd} \tag{5.32}$$

Since the natural mapping $X_0(2M)/W \to X_0(M)/W$ is not unramified (it ramifies atleast at one cusp), by Riemann Hurwitz theorem we have

$$2g(X_0(2M)/W) - 2 > 3(2g(X_0(M)/W) - 2), \tag{5.33}$$

i.e.,

$$g(X_0(2M)/W) > 3g(X_0(M)/W) - 2, \tag{5.34}$$

which contradicts (5.31). Therefore if $q = 2$ and $n = 3$, then $\bar{g} = 0$. Thus $\overline{X_0(M)/W}$ is trigonal over $\mathbb{F}_2$, i.e., there is a degree 3 mapping $\overline{X_0(M)/W} \to \mathbb{P}^1$ defined over $\mathbb{F}_2$. Consequently, we must have

$$\#\overline{X_0(M)}(\mathbb{F}_{2^\alpha}) \leq 2^s \cdot \#\overline{X_0(M)/W}(\mathbb{F}_{2^\alpha}) \leq 3 \cdot 2^s \cdot \mathbb{P}^1(\mathbb{F}_{2^\alpha}) \text{ for } \alpha \in \mathbb{N}. \tag{5.35}$$

In particular, we have (cf. [Ogg74, Page 455-456])

$$\frac{\psi(M)}{12} + 2^{r_M} \leq \#\overline{X_0(M)}(\mathbb{F}_4) \leq 3 \cdot 2^s \cdot 5. \tag{5.36}$$

From (5.36), we see that $r_M \leq 4$ and $M < \psi(M) \leq 12 \cdot 16 \cdot 14 = 2688$ (the arguments are similar as for the equation (5.28)). Moreover, since $\bar{g} = 0$, M and W should satisfy the following inequality (cf. (5.8))

$$g(X_0(2M)/W) - 1 \geq 3(g(X_0(2M)/W) - 1 - 2g(X_0(M)/W)). \tag{5.37}$$

Using `MAGMA`, we see that for $q = 2$ and $M \leq 2688$, the inequalities (5.35), (5.36), and (5.37) are satisfied only for the values of (q, M, W) appearing in Table 4. For the triples (q, M, W) appearing in Table 4, if we can show that either $\overline{X_0(M)/W}$ is not trigonal over $\mathbb{F}_2$ or $Aut_{\mathbb{F}_2}(X_0(M)/W)$ has no element of order 3 or the group $Aut(X_0(qM)/W)$ is commutative, then we can conclude that n can not take the value 3 when $q = 2$.

Now consider the values of (q, M, W) appearing in Table 4. Let $w \in B(M)\backslash W$ such that $g(X_0(M)/\langle W, w\rangle) \geq 1$. Recall that there is a degree 2 mapping $\overline{X_0(M)/W} \to \overline{X_0(M)/\langle W, w\rangle}$ defined over $\mathbb{F}_q$. By Castelnuovo-Severi's inequality, if $\overline{X_0(M)/W}$ is trigonal over $\mathbb{F}_2$, then we must have

$$g(X_0(M)/W) \leq 2g(X_0(M)/\langle W, w\rangle) + 2. \tag{5.38}$$

For example, consider the curve $X_0(105)/\langle w_3\rangle$. There is degree 2 mapping $\overline{X_0(105)/\langle w_3\rangle} \to \overline{X_0(105)/\langle w_3, w_{35}\rangle}$ defined over $\mathbb{F}_2$, where $g(X_0(105)/\langle w_3, w_{35}\rangle) = 1$. Since

$$7 = g(X_0(105)/\langle w_3\rangle) > 2g(X_0(105)/\langle w_3, w_{35}\rangle) + 2,$$

by Castelnuovo-Severi's inequality we get that $\overline{X_0(105)/\langle w_3\rangle}$ is not trigonal over $\mathbb{F}_2$. Using a similar argument we conclude that $\overline{X_0(M)/W}$ is not trigonal over $\mathbb{F}_q$ for the following values of (q, M, W):

(2,105,7), (2,105,15), (2,111,37), (2,123,3), (2,129,43), (2,143,11), (2,143,13), (2,159,3), (2,161,23), (2,177,177), (2,183,61), (2,185,5), (2,185,37), (2,187,11), (2,195,3,5), (2,195,3,13), (2,203,29), (2,209,11), (2,215,43), (2,217,7), (2,231,3,7), (2,231,3,11), (2,247,19), (2,255,3,5), (2,255,5,17), (2,285,3,5), (2,285,3,19), (2,357,3,7), (2,357,7,51).

On the other hand, for the following values of (q, M, W), the automorphism group of the curve $\overline{X_0(M)/W}$ has no element of order 3 over $\mathbb{F}_q$:

(2,115,5),(2,115,23), (2,163,163), (2,165,3,5),(2,165,3,55), (2,165,5,33), (2,165,15,33), (2,235,5,47), (2,253,11,23), (2,265,5,53), (2,273,3,7,13).

For the remaining triples (q, M, W) in Table 4, using MAGMA, we see that $|Aut_{\mathbb{F}_p}(X_0(qM)/W)| \leq 4$ for some prime $p \nmid qM$ (cf. Table 5). Hence for the remaining values of (q, M, W) in Table 4, we see that $Aut_{\mathbb{Q}}(X_0(qM)/W)$ is commutative. Consequently, for such values of (q, M, W) we must have $n = 1$.

Therefore for $q = 2$, we must have $n \leq 2$. Summarizing the discussions so far, we conclude that for $q \in \{2, 3\}$, the only possibility is $n \leq 2$. We now prove that n can not take the value 2 for $q \in \{2, 3\}$.

Cast V: $n = 2$ and $q = 3$.

Consider the case $q = 3$ and $n = 2$. Note that we have the following commutative diagram over $\mathbb{Q}$:

$$\begin{tikzcd}
X_0(3M) \arrow[r, "\deg 4"] \arrow[d, "\deg 2^s"'] & X_0(M) \arrow[d, "\deg 2^s"] \\
X_0(3M)/W \arrow[r, "\deg 4"'] & X_0(M)/W
\end{tikzcd} \tag{5.39}$$

A similar argument as in the case $q = 2$ and $n = 3$ shows that $\bar{g} = 0$, i.e., $\overline{X_0(M)/W}$ is hyperelliptic over $\mathbb{F}_3$. Consequently, we must have

$$\#\overline{X_0(M)}(\mathbb{F}_{3^\alpha}) \leq 2^s \cdot \#\overline{X_0(M)/W}(\mathbb{F}_{3^\alpha}) \leq 2^{s+1} \cdot \mathbb{P}^1(\mathbb{F}_{3^\alpha}) \text{ for } \alpha \in \mathbb{N}. \tag{5.40}$$

In particular, we have (cf. [Ogg74, Page 455-456])

$$2 \cdot \frac{\psi(M)}{12} + 2^{r_M} \leq \#\overline{X_0(M)}(\mathbb{F}_{3^2}) \leq 2^{s+1} \cdot 10. \tag{5.41}$$

Using a similar argument as in (5.28), from (5.41), we see that $r_M \leq 4$ and $M < \psi(M) \leq 6 \cdot 19 \cdot 2^4 = 1824$. Moreover, since $\bar{g} = 0$, M and W should satisfy the following inequality (cf. (5.8))

$$g(X_0(3M)/W) - 1 \geq 2(g(X_0(3M)/W) - 1 - 2g(X_0(M)/W)). \tag{5.42}$$

Using MAGMA, we see that for $q = 3$ and $M \leq 1824$, the inequalities (5.40), (5.41), and (5.42) are satisfied only for the values of (q, M, W) appearing in Table 6. For the triples (q, M, W) appearing in Table 6, if we can show that either $\overline{X_0(M)/W}$ is not hyperelliptic over $\mathbb{F}_3$ or $Aut_{\mathbb{F}_3}(X_0(M)/W)$ has no element of order 2 which fixes at least $1 + g(X_0(qM)/W) - 2 \cdot g(X_0(M)/W)$ points over $\mathbb{F}_{3^2}$ (from the proof of Lemma 31, recall that v has at least $1 + g(X_0(qM)/W) - 2 \cdot g(X_0(M)/W)$ fixed points over $\mathbb{F}_{3^2}$) or the group $Aut(X_0(qM)/W)$ is commutative, then we can conclude that n can not take the value 2 when $q = 3$. Consequently, we must have $n = 1$.

Now consider the triples (q, M, W) appearing in Table 6. Let $w \in B(M)\backslash W$ such that $g(X_0(M)/\langle W, w\rangle) \geq 1$. By Castelnuovo-Severi's inequality, if $\overline{X_0(M)/W}$ is hyperelliptic over $\mathbb{F}_3$, then we must have

$$g(X_0(M)/W) \leq 2g(X_0(M)/\langle W, w\rangle) + 1. \tag{5.43}$$

Since $7 = g(X_0(190)/\langle w_5, w_{38}\rangle) > 2g(X_0(190)/\langle w_5, w_{38}, w_2\rangle) + 1 = 5$, by Castelnuovo-Severi's inequality we get that the curve $\overline{X_0(190)/\langle w_5, w_{38}\rangle}$ is not hyperelliptic over $\mathbb{F}_3$. Using a similar argument, we conclude that $\overline{X_0(M)/W}$ is not hyperelliptic over $\mathbb{F}_q$ for the following values of (q, M, W):

(3,91,7), (3,143,11), (3,154,2,11).

Furthermore using `MAGMA`[5] we see that $\overline{X_0(M)/W}$ is not hyperelliptic over $\mathbb{F}_q$ for the following values of (q, M, W):

(3,65,5), (3,65,13), (3,85,5), (3,85,17).

Now consider the curve $\overline{X_0(94)/\langle w_2\rangle}$ over $\mathbb{F}_3$. Using `MAGMA` we see that $\overline{X_0(94)/\langle w_2\rangle}$ is hyperelliptic over $\mathbb{F}_3$ and $Aut_{\mathbb{F}_3}(\overline{X_0(94)/\langle w_2\rangle}) = \langle \iota \rangle$, where ι is the hyperelliptic involution. Thus for the triple $(3, 94, 2)$, if $n = 2$, then we must have $\iota = v \pmod 3$. Since the supersingular points on $X_0(94)/\langle w_2\rangle$ in characteristic 3 are $\mathbb{F}_{3^2}$ rational and fixed by v, the equality $\iota = v$ (mod 3) implies that ι fixes at least $1 + g(X_0(3 \cdot 94)/\langle w_2\rangle) - 2g(X_0(94)/\langle w_2\rangle) = 12$ points over $\mathbb{F}_{3^2}$. Using `MAGMA`, we see that ι fixes only 4 points over $\mathbb{F}_{3^2}$, which is a contradiction. Therefore, for $(q, M, W) = (3, 94, 2)$, n can not take the value 2, hence we must have $n = 1$. A similar argument shows that, in the case $(3, 95, 5)$ we have $n = 1$.

For the remaining values of (q, M, W) in Table 6, using `MAGMA`, we see that $|Aut_{\mathbb{F}_p}(X_0(qM)/W)| \leq 4$ for some prime $p \nmid qM$ (cf. Table 7). Hence for such values of (q, M, W), the group $Aut_{\mathbb{Q}}(X_0(qM)/W)$ is commutative. Consequently, for such values of (q, M, W) we must have $n = 1$.

Therefore for $q = 3$, we must have $n = 1$.

Case VI: $n = 2$ **and** $q = 2$.

Now consider the case $q = 2$ and $n = 2$. If possible let $\bar{g} \geq 1$. Since the mapping $Z \to Z/v$ is wildly ramified (note that v has fixed points and the ramification at the fixed points is 2), by Riemann-Hurwitz-Hasse theorem we have

$$2g(X_0(M)/W) - 2 \geq 2(2\bar{g} - 2) + 2(1 + g(X_0(2M)/W) - 2g(X_0(M)/W)), \text{ i.e.,}$$

$$2g(X_0(M)/W) - 2 \geq 2(1 + g(X_0(2M)/W) - 2g(X_0(M)/W)). \tag{5.44}$$

The inequality (5.44) implies

$$3(2g(X_0(M)/W) - 2) \geq 2g(X_0(2M)/W) - 2, \tag{5.45}$$

which contradicts (5.33). Hence in the case $n = q = 2$, we must have $\bar{g} = 0$, i.e., $X_0(M)/W$ is hyperelliptic over $\mathbb{F}_2$. Consequently, we must have

$$\#\overline{X_0(M)}(\mathbb{F}_{2^\alpha}) \leq 2^s \cdot \#\overline{X_0(M)/W}(\mathbb{F}_{2^\alpha}) \leq 2^{s+1} \cdot \mathbb{P}^1(\mathbb{F}_{2^\alpha}) \text{ for } \alpha \in \mathbb{N}. \tag{5.46}$$

In particular, we have

$$\frac{\psi(M)}{12} + 2^{r_M} \leq \#\overline{X_0(M)}(\mathbb{F}_4) \leq 2^{s+1} \cdot 5. \tag{5.47}$$

Using a similar argument as in (5.28), from (5.47), we see that $r_M \leq 3$ and $M < \psi(M) \leq 9 \cdot 12 \cdot 8 = 864$. Moreover, since $\bar{g} = 0$, M and W should satisfy the following inequality (cf. 5.8)

$$g(X_0(2M)/W) - 1 \geq 2(g(X_0(2M)/W) - 1 - 2g(X_0(M)/W)). \tag{5.48}$$

Using `MAGMA`, we see that for $q = 2$ and $M \leq 864$, the inequalities (5.46), (5.47), and (5.48) are satisfied only for the values of (q, M, W) appearing in Table 8. For the triples (q, M, W) appearing in Table 8, if we can show that either $\overline{X_0(M)/W}$ is not hyperelliptic over $\mathbb{F}_2$ or the

[5] For example, in `MAGMA` use the code `"IsHyperelliptic(ChangeRing(X0NQuotient(65,[5]),GF(3)));"`

group $Aut(X_0(qM)/W)$ is commutative, then we can conclude that n can not take the value 2 when $q = 2$, consequently we must have $n = 1$.

Now consider the values of (q, M, W) appearing in Table 8.

Let $w \in B(M)\backslash W$ such that $g(X_0(M)/\langle W, w\rangle) \geq 1$. By Castelnuovo-Severi's inequality, if $\overline{X_0(M)/W}$ is hyperelliptic over $\mathbb{F}_2$, then we must have

$$g(X_0(M)/W) \leq 2g(X_0(M)/\langle W, w\rangle) + 1. \tag{5.49}$$

As an immediate consequence of (5.49), we get that $\overline{X_0(M)/W}$ is not hyperelliptic over $\mathbb{F}_q$ for the following values of (q, M, W):

(2,91,7), (2,111,3), (2,115,23), (2,123,123), (2,133,7).

For the remaining values of (q, M, W) in Table 8, using MAGMA, we see that $|Aut_{\mathbb{F}_p}(X_0(qM)/W)| \leq 4$ for some prime $p \nmid qM$ (cf. Table 9). Hence for the remaining values of (q, M, W), we see that $Aut_{\mathbb{Q}}(X_0(qM)/W)$ is commutative. Consequently, for such values of (q, M, W) we must have $n = 1$.

Hence combining the discussions so far, we conclude that for $M \geq 2$, the only possibility is $n = 1$. Now the result follows from Corollary 32. □

Corollary 35. *Let $N := M \cdot \prod_{i=1}^{k} q_i$, where $M \geq 2$ is a square-free integer and $q_i \geq 2$ are primes such that $(M, \prod_{i=1}^{k} q_i) = 1$ and $g(X_0^*(N)) \geq 2$. If $Aut(X_0^*(N))$ is trivial, then*

$$Aut(X_0(N)/B(M)) = B(N)/B(M) = \langle w_{q_1}, \ldots, w_{q_k}\rangle.$$

Proof. Observe that $\langle w_{q_{i+1}}, \ldots, w_{q_k}\rangle \cap \langle w_{q_1}, w_{q_2}, \ldots, w_{q_i}, B(M)\rangle = \{id\}$. Since $g(X_0^*(N)) \geq 2$, we have $g(X_0(N)/W) \geq 2$ for any subgroup $W \subseteq B(N)$. Now the result follows by repeated application of Theorem 34. □

By [BaGo21], we know that $Aut(X_0^*(N))$ is trivial for $N > 645$. Hence, as an immediate consequence of Corollary 35, we obtain:

Corollary 36. *Let $N > 645$ be a square-free integer. For any integer M such that $M|N$, we have $Aut(X_0(N)/B(M)) = B(N)/B(M)$.*

6 Automorphism Group of Quotient Curves of $X_0(pq)$

As an application of the discussions so far, we now compute the automorphism group of different quotient curves of $X_0(pq)$. Throughout the section, we assume that p and q are two distinct primes and $N := pq$. The possible quotient curves of $X_0(N)$ are $X_0^*(N) := X_0(pq)/\langle w_p, w_q\rangle$, $X_0^+(pq) := X_0(pq)/\langle w_{pq}\rangle$ and $X_0(pq)/\langle w_{p_i}\rangle$ where $p_i \in \{p, q\}$.

From [BaGo21], we know that $Aut(X_0^*(pq))$ is trivial when $N = pq$ not in the following table.

g_N^*	$N = pq$
0	6, 10, 14, 15, 21, 22, 26, 33, 34, 35, 38, 39, 46, 51, 55, 62, 69, 87, 94, 95, 119
1	57, 58, 65, 74, 77, 82, 86, 91, 111, 118, 123, 141, 142, 143, 145, 155, 159
2	85, 93, 106, 115, 122, 129, 133, 134, 146, 158, 161, 166, 177, 205, 206, 209, 213, 215, 221, 287, 299
3	178, 183, 249, 303

Table 1: $X_0^*(pq)$ with non trivial automorphism

We now compute the automorphism group of $X_0^+(pq)$.

6.1 Automorphism Group of $X_0^+(pq)$

Since $J_0^+(pq) := Jacobian(X_0^+(pq))$ is semisimple, all the automorphisms of $X_0^+(pq)$ are defined over $\mathbb{Q}$. Moreover we have (cf. [Mom87, Page 271])

$$J_0^+(pq) \cong_{\mathbb{Q}} \prod_{M|N} \prod_{f \in \mathrm{New}_M / G_{\mathbb{Q}}} A_f. \tag{6.1}$$

Hence $End(J_0^+(pq)) \otimes \mathbb{Q}$ is a product of totally real fields. Consequently, $Aut(X_0^+(pq))$ is an elementary abelian 2-group, i.e., $Aut(X_0^+(pq)) \cong \mathbb{Z}/2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/2\mathbb{Z}$ (cf. Corollary 9).

We know that $w_p (= w_q) \in Aut(X_0^+(pq))$. Since $Aut(X_0^+(pq))$ is an abelian group, any $u \in Aut(X_0^+(pq)) \backslash \langle w_p, w_q \rangle$ induces an automorphism on $X_0^*(pq)$. Recall that $Aut(X_0^*(pq))$ is trivial when $N = pq$ not in Table 1. Therefore $Aut(X_0^+(N)) \cong \mathbb{Z}/2\mathbb{Z}$ for $N = pq$ not in Table 1. When $X_0^+(pq)$ is hyperelliptic, using MAGMA, we get

$$Aut(X_0^+(pq)) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z}, & \text{for } pq = 46, 62, 69, 87, 94, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{for } pq = 57, 74, 77, 85, 91, 111, 143. \end{cases}$$

We now deal with the values of $N = pq$ appearing in Table 1. Recall that for a curve X defined over $\mathbb{Q}$ of genus ≥ 2 and a prime l of good reduction, we have an injection $Aut_{\mathbb{Q}}(X) \hookrightarrow Aut_{\mathbb{F}_l}(\overline{X})$. Using MAGMA[6] we see that the order of $Aut_{\mathbb{F}_l}(X_0^+(pq))$ is always 2 for the values of N, l given in the following table:

N	l	N	l	N	l	N	l	N	l	N	l	N	l	N	l
58	3	65	2	82	3	86	3	93	2	106	3	115	2	118	3
122	3	123	2	129	2	133	2	134	3	141	2	142	5	145	3
146	3	155	2	158	3	159	2	161	3	166	3	177	2	178	3
183	2	205	2	206	5	209	3	213	2	215	2	221	2	249	2
287	3	299	3	303	2										

Hence $Aut(X_0^+(pq)) = \langle w_p \rangle = \langle w_q \rangle$, when $X_0^+(pq)$ is non-hyperelliptic curve of genus ≥ 2. Therefore we conclude the following theorem:

Theorem 37. *Let $N = pq$, where p and q are two distinct primes. When $g(X_0^+(N)) \geq 2$, then*

$$Aut(X_0^+(N)) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{for } N = 57, 74, 77, 85, 91, 111, 143, \\ \mathbb{Z}/2\mathbb{Z}, & \text{otherwise.} \end{cases}$$

6.2 The Automorphism Group for $X_0(pq)/w_p$

Recall that p, q are two distinct primes and $N = pq$. Let $A := \mathrm{Aut}(X_0(N)/w_p)$. By Theorem 8, all automorphisms of $X_0(N)/w_p$ are defined over $\mathbb{Q}$. If $g(X_0(pq)/w_p) \geq 2$, then by Theorem 34 we have an exact sequence

$$1 \to \langle w_q \rangle \to Aut(X_0(pq)/\langle w_p \rangle) \to Aut(X_0^*(pq)). \tag{6.2}$$

Since $Aut(X_0^*(pq))$ is trivial when $N = pq$ not in Table 1, from the exact sequence (6.2) we conclude that $Aut(X_0^+(N)) \cong \mathbb{Z}/2\mathbb{Z}$ for $N = pq$ not in Table 1.

Now consider the values of $N = pq$ appearing in Table 1. Using MAGMA we see that the order of $Aut_{\mathbb{F}_l}(X_0(pq)/w_p)$ is always 2 for the values of N, p, l given in the following table:

[6] For example, in MAGMA (online) use the code `"#Automorphisms(ChangeRing(X0NQuotient(58,[58]),GF(3)));"`

(N,p)	l	(N,p)	l	(N,p)	l	(N,p)	l	(N,p)	l	(N,p)	l
(57,19)	5	(58,2)	5	(65,5)	7	(65,13)	7	(74,2)	5	(74,37)	5
(77,7)	5	(77,11)	5	(82,2)	5	(82,41)	5	(85,5)	7	(85,17)	7
(86,2)	3	(86,43)	3	(91,7)	5	(91,13)	5	(93,3)	7	(93,31)	7
(106,2)	7	(106,53)	7	(111,3)	5	(111,37)	5	(115,5)	3	(115,23)	7
(118,2)	5	(118,59)	5	(122,2)	3	(122,61)	3	(123,3)	5	(123,41)	5
(129,2)	2	(129,61)	2	(133,7)	3	(133,19)	2	(134,2)	5	(134,67)	5
(141,3)	2	(141,47)	2	(142,2)	3	(143,11)	2	(143,13)	2	(145,5)	3
(145,29)	3	(146,2)	5	(146,73)	3	(155,5)	3	(155,31)	3	(158,2)	5
(158,79)	5	(159,3)	5	(159,53)	5	(161,7)	3	(161,23)	3	(166,2)	3
(166,83)	3	(177,3)	2	(177,59)	2	(178,2)	3	(178,89)	5	(183,3)	5
(183,61)	2	(205,5)	3	(205,41)	3	(206,2)	3	(206,103)	3	(209,11)	3
(209,19)	3	(213,3)	5	(213,71)	2	(215,5)	2	(215,43)	2	(221,13)	2
(221,17)	3	(249,3)	5	(249,83)	2	(287,7)	2	(287,41)	5	(299,13)	3
(299,23)	5	(303,3)	2	(303,101)	2						

Since we have an embedding $Aut_{\mathbb{Q}}(X_0(pq)/w_p) \hookrightarrow Aut_{\mathbb{F}_l}(X_0(pq)/w_p)$ for primes l of good reduction and $g(X_0(pq)/w_p) \geq 2$, we conclude that

$$Aut_{\mathbb{Q}}(X_0(pq)/w_p) \cong \mathbb{Z}/2\mathbb{Z}, \text{ when } X_0(pq)/w_p \text{ is non} - \text{hyperelliptic and } g(X_0(pq)/w_p) \geq 2.$$

When $X_0(pq)/w_p$ is hyperelliptic, using `MAGMA`, we see that

$$Aut(X_0(N)/w_p) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \text{ for } (N,p) \in & \{(33,3),(35,7),(38,2),(39,13),(46,2),(51,3),(55,5),\\ & (62,2),(69,3),(87,3),(87,29),(94,2),(95,5),(95,19),\\ & (119,7),(119,17)\},\\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \text{ for} & (N,p) \in \{(57,3),(58,29),(142,71)\}. \end{cases}$$

Therefore we conclude that

Theorem 38. *Let $N = pq$, where p and q are two distinct primes. When $g(X_0(N)/w_p) \geq 2$, then*

$$Aut(X_0(N)/w_p) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \text{ for} & (N,p) \in \{(57,3),(58,29),(142,71)\} \\ \mathbb{Z}/2\mathbb{Z}, \text{ otherwise.} \end{cases}$$

7 On automorphism group for $X_0(N)/W_N$ with $N = pqr$

In this section we compute the automorphism group of certain quotient curves of $X_0(pqr)$, where p, q, r are distinct primes. Throughout this section we always assume that p, q, r denote three distinct primes.

7.1 Automorphism group for $X_0(pqr)/\langle w_{pq}, w_r\rangle$ if $g_0^*(r) = 0$

In this subsection, we compute automorphism group of $X_0(pqr)/\langle w_{pq}, w_r\rangle$.

Lemma 39. *The Jacobian decomposition of $X_0(pqr)/\langle w_{pq}, w_r\rangle$ over $\mathbb{Q}$ has no repeated factors if the genus of $X_0^*(r)$ is zero.*

Proof. By (2.2), if a factor A_f corresponding to a newform f is a repeated factor in the Jacobian decomposition of $X_0(pqr)/\langle w_{pq}, w_r\rangle$, then the conductor of f is a strict divisor of pqr. Now using the results of [BaGo20, Lemma 2.1, Proposition 2.2] (see also arguments in the proof of Corollary 19) we see that, under the assumption, f uniquely lifts to a modular form of level pqr. Thus the Jacobian decomposition of $X_0(pqr)/\langle w_{pq}, w_r\rangle$ has no repeated factors. □

Proposition 40. *Consider the quotient modular curve $X_0(pqr)/\langle w_{pq}, w_r\rangle$ such that $g_{pqr}^{\langle w_{pq},w_r\rangle} \geq 2$ and $g_0^*(r) = 0$. Then $Aut(X_0(pqr)/\langle w_{pq}, w_r\rangle) = \langle w_p\rangle \cong \mathbb{Z}/2\mathbb{Z}$ except for the following situations (where non Atkin-Lehner type automorphisms appear):*

pqr	*r*	*Aut*	*genus*	*Hyper*
102	2	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	2	*Yes*
114	2	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	2	*Yes*
138	2	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	2	*Yes*
165	11	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	3	*Yes*
195	3	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	3	*No*
195	5	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	3	*Yes*
238	2	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	3	*No*
154	2	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	4	*No*
231	7	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	4	*No*
285	3	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	4	*No*
286	2	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	4	*No*

There the levels 102, 114, 138, 165, 195 *correspond to curves that are bielliptic and hyperelliptic quotient curves (i.e. they have a degree two morphism to an elliptic curve or a projective line), and all levels with automorphism group bigger than $\mathbb{Z}/2\mathbb{Z}$ correspond to bielliptic curves (cf. [BaGoKa20]).*

Proof. By the Lemma 39 and Corollary 9, all automorphisms are defined over $\mathbb{Q}$ and form an abelian group, thus any non-trivial automorphism will provide a non-trivial automorphism of $X_0^*(pqr)$. The group $Aut(X_0^*(pqr))$ may not be trivial if the genus $X_0^*(pqr) \leq 2$ (such levels are listed in [BaGo20, Appendix]) or a finite list obtained in [BaGo21], see Theorem 16. Thus we are restricted to study a finite list of levels pqr (and of quotient curves). We denote the collection of such levels by $\mathcal{E}$. Applying the Magma code

“`#Automorphisms(ChangeRing(X0NQuotient(p*q*r,[p*q,r]),GF(l)))`”

we see that for some prime $l \nmid prq$, the automorphism group of $X_0(pqr)/\langle w_{pq}, w_r\rangle$ over the finite field $\mathbb{F}_l$ has at most two elements, except the 11 cases discussed bellow (cf. Appendix A). Therefore the full automorphism group over $\mathbb{Q}$ of the curves of the form $X_0(pqr)/\langle w_{pq}, w_r\rangle$ with $g_r^* = 0$ is generated by the Atkin-Lehner involution, except for the following 11 quotient curves where the automorphism group is of order at most 4. We denote the quotient curve $X_0(pqr)/\langle w_{pq}, w_r\rangle$ by (pqr, r) and its genus by $g_{pqr,r}$.

- When $g_{pqr,r} = 2$, the curves we need to study further are $(102, 2)$,$(114, 3)$ and $(138, 23)$. By [BaGoKa20] these curves are bielliptic. Applying [BaGo19, Remark 10], we see that for each such curve there are two bielliptic involutions v_1, v_2 and one hyperelliptic involution w. Hence in each case, there are 3 non-trivial involutions i.e, the full automorphism group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

- When $g_{pqr,r} = 3$, the curves we need to study further are $(165, 11)$, $(195, 5)$, $(195, 3)$ and $(238, 2)$. The first two curves are hyperelliptic curves and by [BaGoKa20] they are also bielliptic curves, thus its group is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$. For the remaining last two situations, by use of Petri's result and a model in $\mathbb{P}^2$ we have:

(pqr, r)	$Q(x, y, z)$
$(195, 3)$	$x^4 + x^2y^2 + y^4 + x^2z^2 - 3y^2z^2 - z^4$
$(238, 2)$	$2x^4 + 3x^2y^2 + y^4 - 3x^2z^2 - 5y^2z^2 + 2z^4$

  Observe that for each curve the mappings $x \leftrightarrow -x$ and $y \leftrightarrow -y$ are automorphisms. Consequently, for each curve the automorphism group contains two bielliptic involutions and an involution whose quotient has genus 2. Therefore for the curves $(195, 3)$ and $(238, 2)$ the automorphism group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

- When $g_{pqr,r} \geq 4$, the curves we need to study further are the genus 4 curves $(154, 2)$, $(231, 7)$, $(285, 3)$ and $(286, 2)$. Note that such curves are bielliptic (cf. [BaGoKa20]). Except $(231, 7)$, the other three quotient curve have an involution (bielliptic) which is not of Atkin-Lehner type (cf. [BaGoKa20]), thus its automorphism group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The Jacobian decomposition over $\mathbb{Q}$ of the curve $X_0(231)/\langle w_7, w_{33}\rangle$ is given by
$$Jac(X_0(231)/\langle w_7, w_{33}\rangle) \sim_{\mathbb{Q}} E11a \times E21a \times E77a \times E77c.$$
  Choosing the variables corresponding to the modular forms appearing in the above decomposition, a canonical model for $(231, 7)$ is given by
$$-29t^2 - 8tx + x^2 - 27y^2 + 63z^2 = 0$$
$$3tx^2 + 54x^3 - 812ty^2 + 224xy^2 + 493tz^2 + 38xz^2 = 0.$$
  The mappings $y \leftrightarrow -y$ and $z \leftrightarrow -z$ provide two bielliptic involutions with elliptic quotients $E21a$ and $E77a$ respectively and the other involution has genus 2 quotient curve.

□

7.2 The Automorphism group for $X_0(pqr)/\langle w_{pq}\rangle$ if $g_0^*(r) = 0$

Proposition 41. *Let p, q, r be distinct primes such that $g(X_0(pqr)/\langle w_{pq}\rangle) \geq 2$ and $g(X_0^*(r)) = 0$. Then $Aut(X_0(pqr)/\langle w_{pq}\rangle) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

Proof. By Theorem 34, there is an exact sequence
$$1 \to \langle w_r\rangle \to Aut(X_0(pqr)/\langle w_{pq}\rangle) \to Aut(X_0(pqr)/\langle w_{pq}, w_r\rangle). \tag{7.1}$$
Observe that if $Aut(X_0(pqr)/\langle w_{pq}, w_r\rangle) \cong \mathbb{Z}/2\mathbb{Z}$, then from the exact sequence (7.1) we see that
$$Aut(X_0(pqr)/\langle w_{pq}\rangle) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$
By Proposition 40, we only need to consider the curves $X_0(pqr)/\langle w_{pq}\rangle$ such that either
$$g(X_0(pqr)/\langle w_{pq}, w_r\rangle) \leq 1 \text{ or}$$
$$(pqr, pq) \in \Big\{(102, 51), (114, 57), (138, 69), (165, 15), (195, 65), (195, 39), (238, 119), (154, 77), (231, 33), (285, 95), (286, 143)\Big\}$$
For such curves, the automorphism groups over finite fields are given in Appendix B. Now the result follows from Appendix B. □

7.3 The automorphism groups of $X_0(pqr)/\langle w_p, w_q\rangle$ and $X_0(pqr)/\langle w_p\rangle$

Proposition 42. *Consider the quotient curves $X_0(pqr)/\langle w_p, w_q\rangle$ and $X_0(pqr)/\langle w_p\rangle$ of genus ≥ 2, then its automorphism group is generated by Atkin-Lehner involutions except for the following hyperelliptic and bielliptic curves (for simplicity we denote the curve $X_0(pqr)/\langle w_p, w_q\rangle$ by $(pqr; p, q)$):*

genus	*Curve*	*Aut*
2	$(190; 5, 19), (138; 3, 23), (102; 3, 17)$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
3	$(114; 2, 19), (130; 2, 13)$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Proof. By Proposition 7, all the automorphisms of $X_0(pqr)/\langle w_p, w_q\rangle$ or $X_0(pqr)/\langle w_p\rangle$ are defined over $\mathbb{Q}$. Naturally, we can consider $B(q_1q_2) = \langle w_{q_1}, w_{q_2}\rangle$ as a subgroup of $B(pqr)$ where q_i are different primes in the set $W = \{p, q, r\}$. Write $X = X_0(pqr)/B(q_1q_2)$ which we assume that has genus ≥ 2. By Theorem 34, we obtain the exact sequence (where $q_3 \in W \setminus \{q_1, q_2\}$):

$$1 \to \langle w_{q_3}\rangle \to Aut(X) \to Aut(X_0^*(pqr)).$$

If the automorphism group of $X_0^*(N)$ is trivial, then $Aut(X) = \langle w_{q_3}\rangle$. Consider the levels $N = pqr$ such that $Aut(X_0^*(pqr))$ is non-trivial and the genus of $X_0^*(N)$ is ≥ 2. By [BaGo20] we only need to consider the following levels N

$g(X_0^*(N)) = 2$	154, 165, 170, 186, 230, 266, 285, 286, 357
$g(X_0^*(N)) = 3$	246, 258, 290, 318, 430, 455
$g(X_0^*(N)) = 4$	366, 370
$g(X_0^*(N)) = 5$	645.

Moreover, we know $|Aut(X_0^*(N))| = 2$, thus $|Aut(X)|$ is either 4 or 2, or the genus of $X_0^*(N)$ is ≤ 1, i.e.

$$N \in \{30, 42, 66, 70, 78, 105, 110\} \text{ for } g_N^* = 0,$$

$$\text{or } N \in \{102, 114, 130, 138, 174, 182, 190, 195, 222, 231, 238\} \text{ for } g_N^* = 1.$$

Using Magma V2.27-7 we obtain:

$(N;q_1,q_2)$	l	$\#Aut_{\mathbb{F}_l}(X)$	$(N;q_1,q_2)$	l	$\#Aut_{\mathbb{F}_l}(X)$
$(30;2,q_2)$ $q_2\in\{3,5\}$	7	2	$(42;q_1,q_2)$ $q_1,q_2\in\{2,3,7\}$	11	2
$(66;q_1,q_2)$ $q_1,q_2\in\{2,3,11\}$	5	2	$(70;q_1,q_2)$ $(q_1,q_2\in\{2,5,7\})$	3	2
$(78;q_1,q_2)$ $q_1,q_2\in\{2,3,13\}$	5	2	$(102;2,q_2)$ $q_2\in\{3,17\}$	5	2
$(102;3,17)$	5	4^*	$(105;q_1,q_2)$ $q_1,q_2\in\{3,5,7\}$	11	2
$(110;q_1,q_2)$ $q_1,q_2\in\{2,5,11\}$	3	2	$(114;3,q_2)$ $q_2\in\{2,19\}$	7	2
$(114;2,19)$	5	4^*	$(130;5,q_2)$ $q_2\in\{2,13\}$	3	2
$(130;2,13)$	3	4^*	$(138;2,q_2)$ $q_2\in\{3,23\}$	5	2
$(138;3,23)$	5	4*	$(154;q_1,q_2)$ $q_1,q_2\in\{2,7,11\}$	3	2
$(165;q_1,q_2)$ $q_1,q_2\in\{3,5,11\}$	13	2	$(170;q_1,q_2)$ $q_1,q_2\in\{2,5,17\}$	7	2
$(174;q_1,q_2)$ $q_1,q_2\in\{2,3,29\}$	5	2	$(182;q_1,q_2)$ $q_1,q_2\in\{2,7,13\}$	3	2
$(186,q_1,q_2)$ $q_1,q_2\in\{2,3,31\}$	5	2	$(190;2,q_2)$ $q_2\in\{5,19\}$	3	2
$(190;5,19)$	7	4^*	$(195;q_1,q_2)$ $q_1,q_2\in\{3,5,13\}$	7	2
$(222,q_1,q_2)$ $q_1,q_2\in\{2,3,37\}$	5	2	$(230;q_1,q_2)$ $q_1,q_2\in\{2,5,23\}$	7	2
$(231;q_1,q_2)$ $q_1,q_2\in\{3,7,11\}$	2	2	$(238;q_1,q_2)$ $q_1,q_2\in\{2,7,17\}$	3	2
$(246;q_1,q_2)$ $q_1,q_2\in\{2,3,41\}$	5	2	$(258;q_1,q_2)$ $q_1,q_2\in\{2,3,43\}$	5	2
$(266;q_1,q_2)$ $q_1,q_2\in\{2,7,19\}$	3	2	$(285;q_1,q_2)$ $q_1,q_2\in\{3,5,19\}$	2	2
$(286;q_1,q_2)$ $q_1,q_2\in\{2,11,13\}$	3	2	$(290;q_1,q_2)$ $q_1,q_2\in\{2,5,29\}$	3	2
$(318;q_1,q_2)$ $q_1,q_2\in\{2,3,53\}$	5	2	$(357;q_1,q_2)$ $q_1,q_2\in\{3,7,17\}$	5	2
$(366;61,q_2)$ $q_2\in\{2,3\}$	5	2	$(370;q_1,q_2)$ $q_1,q_2\in\{2,5,37\}$	3	2
$(430;5,43)$	3	2	$(430;5,2)$	3	2
$(430;2,43)$	7	2	$(455;q_1,q_2)$ $q_1,q_2\in\{5,7,13\}$	3	2
$(645;3,43)$	2	2	$(645;5,43)$	7	2

The genus 2 curves $(190;5,19)$,$(138;3,23)$ and $(102;3,17)$ are both hyperelliptic and bielliptic (cf. [BaGoKa20, Page 399-400]). Hence for such curves the automorphism group is isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

The genus 3 quotient curves $(114;2,19)$ and $(130;2,13)$ both are hyperelliptic and bielliptic (loc. cit.), thus in each case the automorphism group is isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

By Corollary 24, we know that $Aut(X_0(645)/\langle w_3, w_5\rangle) = \langle w_{43}\rangle$.

The only remaining case corresponds to the genus 15 curve $(366; 2, 3)$ of even level [7]. Fortunately, its Jacobian has no repeated factors and thus the all automorphisms are involutions defined over $\mathbb{Q}$, and are acting as ±1 in each $\mathbb{Q}$-isogeny factor in the Jacobian decomposition:

$$Jac(X_0(366)/\langle w_2, w_3\rangle) \sim_{\mathbb{Q}} 1_{E61a}+3_{61.2.a.b}+1_{E122a}+2_{122.2.a.b}+2_{183.2.a.a}+3_{183.2.a.b}+1_{E366e}+2_{366.2.a.h}$$

by computing its canonical model, it is easy to check that the non-trivial involution of $X_0^*(366)$ (recall that $J_0^*(366) \sim 1_{E61a} + 1_{E122a} + 2_{183.2.a.a}$, and the only non-trivial involution of $X_0^*(366)$ acts on $J_0^*(366)$ by $\pm(-1 \times -1 \times 1)$, giving a genus 2 quotient curve [BaGo21, Proposition 5], [BaGo19, Proposition 24]) does not lift to an involution of $X_0(366)/\langle w_2, w_3\rangle$ (see all details in the github folder https://github.com/FrancescBars/Files-on-Automorphism-Quotient-Curves), and therefore $Aut(X_0(366)/\langle w_2, w_3\rangle) = \langle w_{61}\rangle$.

Consider now the curves of the form $X_0(pqr)/\langle w_p\rangle$, with genus ≥ 2. The automorphism groups of all such quotient curves have an order 4 subgroup $\langle w_q, w_r\rangle$. and this will be the exact group of automorphisms if $Aut(X_0(pqr)/\langle w_p, w_q\rangle)$ has exact order 2 (or genus ≤ 1). Thus we are reduced to a finite list of levels $N = pqr$. Computing by Magma the automorphism group over a finite field of order ℓ with $\ell \nmid pqr$ for this finite list, we conclude that for each case the full automorphism group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

□

Acknowledgments

The authors are very grateful to the anonymous referee for providing many valuable comments and suggestions, which improved the article considerably. The first author's work is supported by the Spanish State Research Agency through the Severo Ochoa and María de Maeztu Program for Centers and Units of Excellence in R&D (CEX2020- 001084-M), alongside PID2020-116542GB-I00, Ministerio de Ciencia y Universidades of Spanish government.

A List of results $\#Aut_{\mathbb{F}_\ell}(X_0(pqr)/\langle w_r, w_{pq}\rangle)$

We denote the quotient curve $X_0(pqr)/\langle w_{pq}, w_r\rangle$ by (pqr, r), and we consider the finite field $\mathbb{F}_\ell$ and compute $\#Aut_{\mathbb{F}_\ell}((pqr, r))$ by Magma (online version V2.28-4 if is not marked with *) for all (pqr, r) such that has genus ≥ 2 and $g_0^*(r) = 0$ with p,q and r are three diferent primes. We denote by Aut the number $\#Aut_{\mathbb{F}_\ell}((pqr, r))$, and by Field the number ℓ in the next table.

[7] The computation by Magma of the automorphism group of $(318; 2, 3)$ over $\mathbb{F}_5$ took more than 18 hours, and for $(366; 2, 3)$ took two days to conclude that over $\mathbb{F}_5$ the automorphism group has order 2, thus we prefer to present how we deal with last curve using canonical model result on a genus 15 curve.

Curve	Field	Aut	Curve	Field	Aut	Curve	Field	Aut
(66,3)	5	2	(70,7)	3	2	(78,13)	5	2
(102,2)	5	4	(102,3)	5	2	(102,17)	5	2
(105,7)	11	2	(110,5)	3	2	(114,2)	5	2
(114,3)	5	4	(114,19)	5	2	(130,2)	3	2
(130,5)	3	2	(130,13)	3	2	(138,2)	5	2
(138,3)	5	2	(138,23)	5	4	(154,2)	3	4
(154,7)	3	2	(154,11)	3	2	(165,3)	2	2
(165,5)	2	2	(165,11)	7	4	(170,5)	3	2
(170,2)	3	2	(170,17)	3	2	(174,2)	5	2
(174,3)	5	2	(174,29)	5	2	(182,2)	3	2
(182,7)	3	2	(182,13)	3	2	(186,2)	5	2
(186,3)	5	2	(186,31)	5	2	(190,2)	3	2
(190,5)	3	2	(190,19)	3	2	(195,3)	7	4
(195,5)	11	4	(195,13)	7	2	(222,2)	5	2
(222,3)	5	2	(230,2)	3	2	(230,5)	3	2
(230,23)	7	2	(231,3)	2	2	(231,7)	2	4
(231,11)	2	2	(238,2)	3	4	(238,7)	3	2
(238,17)	3	2	(246,2)	5	2	(246,3)	5	2
(246,41)	5	2	(255,3)	2	2	(255,5)	2	2
(255,17)	2	2	(258,2)	5	2	(258,3)	5	2
(266,2)	3	2	(266,7)	3	2	(266,19)	3	2
(285,3)	2	4	(285,5)	2	2	(285,19)	2	2
(286,2)	5	4	(286,11)	5	2	(286,13)	5	2
(290,2)	3	2	(290,5)	3	2	(290,29)	3	2
(318,2)	5	2	(318,3)	5	2	(357,3)	5	2
(357,7)	2	2	(357,17)	2	2	(366,2)	5	2
(366,3)	5	2	(370,2)	3	2	(370,5)	3	2
(430,2)	3	2	(430,5)	3	2	(455,5)	2	2
(455,7)	2	2	(455,13)	2	2	(645,3)	2	2
(645,5)	2	2*						

B List of results $\#Aut_{\mathbb{F}_l}(X_0(pqr)/\langle w_{pq}\rangle)$

pqr	pq	Field	Aut	pqr	pq	Field	Aut	pqr	pq	Field	Aut
30	10	7	4	42	6	11	4	42	21	11	4
66	6	13	4	66	33	13	4	70	14	13	4
70	35	13	4	78	26	19	4	78	39	19	4
102	51	19	4	105	21	19	4	105	35	19	4
110	10	3	4	110	55	7	4	114	57	7	4
138	69	7	4	165	15	7	4	195	65	7	4
195	39	7	4	238	119	5	4	154	77	5	4
231	33	5	4	285	95	7	4	286	143	3	4

C Inequality in Theorem 34 for $n \geq 4, q = 2$

(2,39,13), (2,51,3), (2,55,5), (2,57,19), (2,65,5), (2,65,13), (2,69,3), (2,77,7), (2,77,11), (2,85,5,17), (2,87,3), (2,95,5), (2,115,23), (2,119,7), (2,165,3,5), (2,165,15,33)

Table 2: Values of (q, M, W) that satisfy the inequality (5.22)

Curve	Field	Aut	Curve	Field	Aut	Curve	Field	Aut
(2,35,7)	3	4	(2,39,13)	5	4	(2,51,3)	7	4
(2,55,5)	3	4	(2,57,19)	5	4	(2,65,5)	3	4
(2,65,13)	3	4	(2,69,3)	5	4	(2,77,7)	3	4
(2,77,11)	3	4	(2,85,5,17)	3	2	(2,87,3)	5	4
(2,95,5)	3	4	(2,119,7)	3	4	(2,165,15,33)	7	4

Table 3: Remaining cases for $n \geq 4, q = 2$

D Inequality in Theorem 34 for $n = 3, q = 2$

(2,33,33), (2,35,5), (2,37,37), (2,39,13), (2,43,43), (2,51,3), (2,55,5), (2,55,55), (2,57,19), (2,57,3,19),
(2,65,5), (2,65,13), (2,65,5,13), (2,67,67), (2,69,3), (2,77,7), (2,77,11), (2,77,7,11) (2,85,5),
(2,85,17), (2,85,5,17), (2,87,3), (2,91,7), (2,93,31), (2,93,3,31), (2,95,5) (2,105,3), (2,105,7),
(2,105,15), (2,105,3,5), (2,105,3,7), (2,105,7,15), (2,111,37), (2,115,5), (2,115,23), (2,115,5,23),
(2,119,7) (2,123,3), (2,129,43), (2,133,7), (2,143,11), (2,143,13) (2,159,3), (2,161,23), (2,163,163),
(2,165,3,5), (2,165,3,55), (2,165,5,33), (2,165,15,33), (2,165,3,5,11) (2,177,177), (2,183,61),
(2,185,5), (2,185,37), (2,187,11) (2,195,3,5), (2,195,3,13), (2,203,29), (2,209,11), (2,215,43),
(2,217,7), (2,231,3,7), (2,231,3,11), (2,235,5,47), (2,247,19) (2,253,11,23), (2,255,3,5), (2,255,5,17),
(2,265,5,53) (2,273,21,39), (2,273,3,7,13) (2,285,3,5), (2,285,3,19) (2,357,3,7), (2,357,7,51)

Table 4: Values of (q, M, W) that satisfy the inequalities (5.35), (5.36) and (5.37)

Curve	Field	Aut	Curve	Field	Aut	Curve	Field	Aut
(2,33,33)	5	4	(2,35,5)	3	4	(2,37,37)	3	2
(2,39,13)	5	4	(2,43,43)	5	2	(2,51,3)	7	4
(2,55,5)	3	4	(2,55,55)	7	4	(2,57,19)	5	4
(2,57,3,19)	5	2	(2,65,5)	3	4	(2,65,13)	3	4
(2,65,5,13)	3	2	(2,67,67)	3	2	(2,69,3)	5	4
(2,77,7)	3	4	(2,77,11)	3	4	(2,77,7,11)	3	2
(2,85,5)	11	4	(2,85,17)	3	4	(2,85,5,17)	3	2
(2,87,3)	5	4	(2,91,7)	3	4	(2,93,31)	5	4
(2,93,3,31)	5	2	(2,95,5)	3	4	(2,105,3,5)	11	4
(2,105,3,7)	11	4	(2,105,7,15)	11	4	(2,115,5,23)	3	2
(2,119,7)	3	4	(2,165,3,5,11)	7	2			

Table 5: Remaining cases for $n = 3$, $q = 2$

E Inequality in Theorem 34 for $n = 2, q = 3$

(3,22,2), (3,22,22), (3,35,5), (3,35,7), (3,38,2), (3,46,2), (3,55,5), (3,62,2), (3,65,5),
(3,65,13), (3,65,5,13), (3,70,2,7), (3,77,11), (3,85,5), (3,85,17), (3,85,5,17), (3,91,7), (3,94,2),
(3,95,5), (3,110,2,5), (3,119,7), (3,143,11), (3,154,2,11), (3,190,5,38)

Table 6: Values of (q, M, W) that satisfy the inequalities (5.40), (5.41) and (5.42)

Curve	Field	Aut	Curve	Field	Aut	Curve	Field	Aut
(3,22,2)	5	4	(3,22,22)	5	4	(3,35,5)	11	4
(3,35,7)	11	4	(3,38,2)	5	4	(3,46,2)	7	4
(3,55,5)	2	4	(3,62,2)	5	4	(3,65,5,13)	2	2
(3,70,2,7)	11	4	(3,77,11)	5	4	(3,85,5,17)	2	2
(3,110,2,5)	7	4	(3,119,7)	2	4			

Table 7: Remaining cases for $n = 2$, $q = 3$

F Inequality in Theorem 34 for $n = 2, q = 2$

(2,15,3), (2,21,7), (2,33,3), (2,33,33), (2,35,5), (2,35,7), (2,37,37), (2,39,3), (2,39,13),
(2,43,43) (2,51,3), (2,51,51), (2,53,53), (2,55,5), (2,55,11), (2,55,55), (2,57,3), (2,57,19),
(2,57,57), (2,57,3,19) (2,65,5), (2,65,13), (2,65,5,13), (2,67,67), (2,69,3), (2,69,23), (2,69,69),
(2,73,73) (2,77,77), (2,77,7,11), (2,79,79), (2,85,17), (2,85,85), (2,85,5,17), (2,87,3),
(2,87,87), (2,91,7), (2,91,13), (2,91,7,13), (2,93,31), (2,93,3,31), (2,95,5), (2,95,19),
(2,103,103), (2,105,3,5), (2,105,3,7), (2,105,7,15), (2,107,107) (2,111,3), (2,111,3,37),
(2,115,23), (2,115,5,23), (2,119,7), (2,119,17) (2,123,123), (2,127,127), (2,129,3,43),
(2,133,7), (2,133,7,19), (2,143,11,13) (2,161,7,23), (2,165,5,11), (2,165,5,33), (2,165,11,15),
(2,165,3,5,11), (2,183,3,61), (2,185,5,37) (2,187,11,17), (2,195,5,39) (2,203,7,29), (2,215,5,43),
(2,217,7,31), (2,247,13,19) (2,255,3,5,17) (2,285,3,5,19) (2,335,5,67) (2,345,3,5,23) (2,385,5,7,11)

Table 8: Values of (q, M, W) that satisfy the inequalities (5.46), (5.47) and (5.48)

Curve	Field	Aut	Curve	Field	Aut	Curve	Field	Aut
(2,33,33)	5	4	(2,35,5)	3	4	(2,37,37)	3	2
(2,39,3)	5	4	(2,39,13)	5	4	(2,43,43)	5	2
(2,51,3)	7	4	(2,51,51)	5	4	(2,53,53)	3	2
(2,55,5)	3	4	(2,55,11)	3	4	(2,55,55)	7	4
(2,57,3)	5	4	(2,57,19)	5	4	(2,57,57)	5	4
(2,57,3,19)	5	2	(2,65,5)	3	4	(2,65,13)	3	4
(2,65,5,13)	3	2	(2,67,67)	3	2	(2,69,3)	5	4
(2,69,23)	5	4	(2,69,69)	5	4	(2,73,73)	3	2
(2,77,77)	3	4	(2,77,7,11)	3	2	(2,79,79)	5	2
(2,85,17)	3	4	(2,85,85)	3	4	(2,85,5,17)	3	2
(2,87,3)	5	4	(2,87,87)	5	4	(2,91,7)	3	4

(2,91,13)	5	4	(2,91,7,13)	3	2	(2,93,31)	5	4
(2,93,3,31)	5	3	(2,95,5)	3	4	(2,95,19)	3	4
(2,103,103)	3	2	(2,105,3,5)	11	4	(2,105,3,7)	11	4
(2,105,7,15)	11	4	(2,107,107)	3	2			
(2,111,3,37)	5	2				(2,115,5,23)	3	2
(2,119,7)	3	4	(2,119,17)	3	4	(2,123,123)	5	4
(2,129,3,43)	5	2				(2,133,7,19)	3	2
(2,143,11,13)	3	2	(2,161,7,23)	3	2	(2,165,5,11)	7	4
(2,165,5,33)	7	4	(2,165,11,15)	7	4	(2,165,3,5,11)	7	2
(2,183,3,61)	5	2	(2,185,5,37)	7	2	(2,195,5,39)	7	4
(2,215,5,43)	3	2	(2,255,3,5,17)	7	2	(2,285,3,5,19)	7	2

Table 9: Remaining cases for $n = 2$, $q = 2$

References

[AtLe70] Atkin, A. O. L.; Lehner, J. Hecke operators on $\Gamma_0(m)$. Math. Ann. 185 (1970), 134–160.

[BGGP05] Baker, Matthew H.; González-Jiménez, Enrique; González, Josep; Poonen, Bjorn. Finiteness results for modular curves of genus at least 2. Amer. J. Math. 127 (2005), no. 6, 1325–1387.

[BaHa03] Baker, Matthew; Hasegawa, Yuji. Automorphisms of $X_0^*(p)$. J. Number Theory 100 (2003), no. 1, 72–87.

[BaGo19] Bars, Francesc; González Rovira, Josep. Bielliptic modular curves $X_0^*(N)$ with square-free levels. Math. Comp. 88 (2019), no. 320, 2939–2957.

[BaGo20] Bars, Francesc; González, Josep. Bielliptic modular curves $X_0^*(N)$. J. Algebra 559 (2020), 726–759.

[BaGo21] Bars, Francesc; González, Josep. The automorphism group of the modular curve $X_0^*(N)$ with square-free level. Trans. Amer. Math. Soc. 374 (2021), no. 8, 5783–5803.

[BaGoKa20] Bars, Francesc; González, Josep; Kamel, Mohamed. Bielliptic quotient modular curves with N square-free. J. Number Theory 216 (2020), 380–402.

[BKS23] Bars, Francesc; Kamel, Mohamed; Schweizer, Andreas. Bielliptic quotient modular curves of $X_0(N)$. Math. Comp. 92 (2023), no. 340, 895–929.

[Cre] Cremona, John. Elliptic Curve Data: `https://johncremona.github.io/ecdata/`

[DeRa72] Deligne, P.; Rapoport, M. Les schémas de modules de courbes elliptiques. (French) Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), pp. 143–316, Lecture Notes in Math., Vol. 349, Springer, Berlin-New York, 1973.

[DLM22] Dose, Valerio; Lido, Guido; Mercuri, Pietro. Automorphisms of Cartan modular curves of prime and composite level. Algebra Number Theory 16 (2022), no. 6, 1423–1461.

[Elk90] Elkies, Noam D. The automorphism group of the modular curve $X_0(63)$. Compositio Math. 74 (1990), no. 2, 203–208.

[FuHa99] Furumoto, Masahiro; Hasegawa, Yuji. Hyperelliptic quotients of modular curves $X_0(N)$. Tokyo J. Math. 22 (1999), no. 1, 105–125.

[Gon16] González, Josep. Automorphism group of split Cartan modular curves. Bull. Lond. Math. Soc. 48 (2016), no. 4, 628–636.

[Har14] Harrison, M. A new automorphism of $X_0(108)$. *https//arxiv.org/abs/1108.5595.*, 2014.

[HaHa96] Hasegawa, Yuji; Hashimoto, Ki-ichiro. Hyperelliptic modular curves $X_0^*(N)$ with square-free levels. Acta Arith. 77 (1996), no. 2, 179–193.

[Has97] Hasegawa, Yuji. Hyperelliptic modular curves $X_0^*(N)$. Acta Arith. 81 (1997), no. 4, 369–385.

[HaSh00] Hasegawa, Yuji; Shimura, Mahoro. Trigonal modular curves $X_0^*(N)$. Proc. Japan Acad. Ser. A Math. Sci. 76 (2000), no. 6, 83–86.

[KM88] Kenku, M. A.; Momose, Fumiyuki. Automorphism groups of the modular curves $X_0(N)$. Compositio Math. 65 (1988), no. 1, 51–80.

[Lan01] Lang, Mong-Lung. Normalizers of the congruence subgroups of the Hecke groups G_4 and G_6. J. Number Theory 90 (2001), no. 1, 31–43.

[LMFDB] LMFDB Collaboration, The L-functions and modular forms database, https://www.lmfdb.org, 2024, [Online; accessed 16 September 2024].

[Mom87] Momose, Fumiyuki. Rational points on the modular curves $X_0^+(N)$. J. Math. Soc. Japan 39 (1987), no. 2, 269–286.

[MuPa08] Murty, V. Kumar; Patankar, Vijay M. Splitting of abelian varieties. Int. Math. Res. Not. IMRN 2008, no. 12, Art. ID rnn033, 27 pp.

[Ogg74] Ogg, Andrew P. Hyperelliptic modular curves. Bull. Soc. Math. France 102 (1974), 449–462.

[Ogg77] Ogg, A. P. Über die Automorphismengruppe von $X_0(N)$. (German) Math. Ann. 228 (1977), no. 3, 279–292.

[Ogg78] Ogg, A. P. On the Weierstrass points of $X_0(N)$. Illinois J. Math. 22 (1978), no. 1, 31–35.

[Pyl04] Pyle, Elisabeth E. Abelian varieties over $\mathbb{Q}$ with large endomorphism algebras and their simple components over $\overline{\mathbb{Q}}$. Modular curves and abelian varieties, 189–239, Progr. Math., 224, Birkhäuser, Basel, 2004.

[Rib75] Ribet, Kenneth A. Endomorphisms of semi-stable abelian varieties over number fields. Ann. of Math. (2) 101 (1975), 555–562.

[Rib80] Ribet, Kenneth A. Twists of modular forms and endomorphisms of abelian varieties. Math. Ann. 253 (1980), no. 1, 43–62.

Francesc Bars Cortina
Departament Matemàtiques, Edif. C, Universitat Autònoma de Barcelona
08193 Bellaterra, Catalonia
Centre de Recerca Matemàtica (CRM), C. dels Til.lers
08193 Bellaterra, Catalonia
Francesc.Bars@uab.cat

Tarun Dalal
Institute of Mathematical Sciences, ShanghaiTech University
393 Middle Huaxia Road, Pudong, Shanghai 201210, China
tarun.dalal80@gmail.com