

---

This is the **submitted version** of the article:

Bars Cortina, Francesc; González Rovira, Josep. «The automorphism group of the modular curve  $X_0^*(N)$  with square-free level». Transactions of the American Mathematical Society, Vol. 374 (April 2021). DOI 10.1090/tran/8391

---

This version is available at <https://ddd.uab.cat/record/243414>

under the terms of the  license

# The automorphism group of the modular curve $X_0^*(N)$ with square-free level

Francesc Bars\*and Josep González †

## Abstract

We determine the automorphism group of the modular curve  $X_0^*(N)$ , obtained as the quotient of the modular curve  $X_0(N)$  by the group of its Atkin-Lehner involutions, for all square-free values of  $N$ .

## 1 Introduction

In [KM88], Kenku and Momose 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]. Subsequently, Harrison detected a mistake in these results concerning to the curve  $X_0(108)$ . In [Har14], it is proved that this curve has an extra involution which does not arise from the normalizer of  $\Gamma_0(108)$  in  $\mathrm{SL}_2(\mathbb{R})$ , as it happens for the curves  $X_0(37)$  and  $X_0(63)$ .

For the modular curve  $X_0^+(N) = X_0(N)/\langle w_N \rangle$ , where  $w_N$  denotes the Fricke involution, Baker and Hasegawa determined the automorphism group when  $N$  is a prime in [BH03] and, later, in [Gon16] it was determined the automorphism group when  $N$  is the square of a prime.

In this paper we focus our attention to the modular curves  $X_0^*(N) = X_0(N)/B(N)$ , where  $B(N)$  is the group of the Atkin-Lehner involutions of the modular curve  $X_0(N)$ , when  $N$  is square-free. The interest in these modular curves is due to their moduli interpretation. For a number field  $K$ , the non cuspidal  $K$ -rational points of  $X_0^*(N)$  parametrize a class of  $K$ -curves. More precisely, these points parametrize elliptic curves  $E/\overline{K}$  having the property that for every Galois conjugation  $\sigma \in \mathrm{Gal}(\overline{K}/K)$  there is an isogeny between  $E$  and  $E^\sigma$  of degree a divisor of  $N$ . When  $X_0^*(N)$  has genus  $< 3$ , these parametrizations are described in [GL98] and [BGX21].

We point out that for a square-free  $N \neq 37$ ,  $B(N)$  is the automorphism group of  $X_0(N)$  when its genus is greater than one and, thus, a non trivial automorphism of  $X_0^*(N)$  does not come from the action of an automorphism of  $X_0(N)$ . More generally, let us denote by  $A(N)$  the subgroup of  $\mathrm{SL}_2(\mathbb{R})$  generated by  $\Gamma_0(N)$  and  $B(N)$ . In [Lan01], it is proved that  $A(N)$  is its normalizer in  $\mathrm{SL}_2(\mathbb{R})$ . Hence, a non trivial automorphism of  $X_0^*(N)$  is exceptional in the sense that does not come from a linear fractional transformation on the complex upper-half plane.

In [BH03][Corollary 2.6], it is proved that for a square-free integer  $N$  such that the genus of  $X_0^*(N)$  is greater than 1, the group  $\mathrm{Aut} X_0^*(N)$  is elementary 2-abelian and every automorphism of  $X_0^*(N)$  is defined over  $\mathbb{Q}$ . If the curve  $X_0^*(N)$  has a non trivial involution and the genus of the quotient curve is zero, then it is hyperelliptic. When the genus of the quotient curve is one, then the curve  $X_0^*(N)$  is bielliptic.

---

\*First author is supported by MTM2016-75980-P

†The second author is partially supported by DGI grant MTM2015-66180-R.

In [HH96], it is proved that  $X_0^*(N)$  is hyperelliptic if, and only if, the curve has genus two and, moreover, all these values of  $N$  are determined. In [BG19], all values of  $N$  for which  $X_0^*(N)$  is bielliptic are determined and for each of these curves its automorphism group is determined.

All these results are summarized in the next theorem.

**Theorem 1.** *Let  $N > 1$  be a square-free integer. Assume that the genus of the modular curve  $X_0^*(N)$  is at least 2. Then,*

- (i) *The modular curve  $X_0^*(N)$  is hyperelliptic if, and only if, it has genus two. In this case, the automorphism group has order 2 if, and only if,  $N$  is in the following list*

67, 73, 85, 93, 103, 107, 115, 133, 134, 146, 154, 161, 165, 167, 170, 177,  
186, 191, 205, 206, 209, 213, 221, 230, 266, 285, 286, 287, 299, 357.

- (ii) *The automorphism group of a modular curve  $X_0^*(N)$  of genus 3 is non trivial if, and only if, the curve is bielliptic.*
- (iii) *The modular curve  $X_0^*(N)$  is bielliptic if, and only if,  $N$  is in the following table*

genus	$N$
2	106, 122, 129, 158, 166, 215, 390
3	178, 183, 246, 249, 258, 290, 303, 318, 430, 455, 510
4	370

*For these values of  $N$ , the automorphism group of  $X_0^*(N)$  has order 2 when the genus of the curve is greater than two, otherwise it is the Klein group.*

The goal of this article is to complete the values of  $N$  such that the group  $\text{Aut}(X_0^*(N))$  is non trivial and describe this group for all these values. Among the curves  $X_0^*(N)$  with genus  $> 1$ , there are exactly 37 that are hyperelliptic and 12 that are bielliptic and non hyperelliptic. In [BG19], it is proved that the curve  $X_0^*(366)$  of genus 4 has automorphism group of order 2 and the genus of the quotient curve by the non trivial involution is 2. Hence, it is reasonable to expect that there are a few curves  $X_0^*(N)$  of genus  $> 3$  that are not bielliptic and its automorphism group is non trivial. The main result of this paper, that is presented in the following theorem, gives a precise answer to this question.

**Theorem 2.** *Let  $N$  be a square-free integer such that the curve  $X_0^*(N)$  has genus  $> 3$  and it is not bielliptic, i.e.  $N \neq 370$ . Then, the group  $\text{Aut}(X_0^*(N))$  is not 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.*

The paper is organized as follows. In section 2, we fix the notation and recall some general facts. In Section 3, we show the main tools that we will use to determine the group  $\text{Aut}(X_0^*(N))$  for a fixed value of  $N$ . Sections 4 and 5 are devoted to prove Theorem 2 for odd and even levels respectively. The key point in these two last sections is the determination of a finite set of positive integers containing all levels  $N$  such that  $X_0^*(N)$  has a non trivial automorphism group. In section 4, for the odd levels, this result follows from Proposition 3. This proposition is based on an idea already used in [KM88][Lemma 2.7], [BH03][Lemma 3.3] and [Gon16][Lemma 6], but always proved with different arguments because the involved modular curves in these statements are different. In section 5, the determination of a finite set for the even levels is obtained from Proposition 4. This proposition presents an unknown inequality involving the genera of the curves  $X_0^*(N)$  and  $X_0^*(2N)$  for all odd square-free values of  $N$ .

## 2 Notation and general facts

Let  $N > 1$  be a square-free integer. We fix, once and for all, the following notation.

- (i) We denote by  $B(N)$  the group of the Atkin-Lehner involutions of  $X_0(N)$ . If  $N'|N$ ,  $B(N')$  can be also identified as the subgroup of  $B(N)$  formed by the Atkin-Lehner involutions  $w_d$  such that  $d|N'$ .
- (ii) The integer  $\omega(N)$  is the number of primes dividing  $N$ . In particular,  $|B(N)| = 2^{\omega(N)}$ .
- (iii) The integers  $g_N$  and  $g_N^*$  are the genus of  $X_0(N)$  and  $X_0^*(N)$  respectively.
- (iv) We denote by  $\text{New}_N$  the set of normalized newforms in  $S_2(\Gamma_0(N))$  and  $\text{New}_N^*$  is the subset of  $\text{New}_N$  formed by the newforms invariant under the action of the group of the Atkin-Lehner involutions  $B(N)$ .
- (v)  $S_2(N) = S_2(\Gamma_0(N))$ ,  $S_2^*(N)$  is the vector space  $S_2(N)^{B(N)}$ ,  $J_0(N) = \text{Jac}(X_0(N))$  and  $J_0^*(N) = \text{Jac}(X_0^*(N))$ .
- (vi) Let  $h \in S_2(\Gamma_0(N))$  be an eigenform of the form  $\sum_{d|N/M} c_d f(q^d)$  for some  $f \in \text{New}_M$  with  $M|N$  and  $c_d \in \mathbb{Z}$ . Since for every divisor  $d|N/M$  there is a morphism  $B_d$  from  $J_0(M)$  to  $J_0(N)$  defined over  $\mathbb{Q}$  sending every cusp form  $g \in S_2(M)$  to  $g(q^d) \in S_2(N)$ , the morphism  $\sum_{d|N/M} c_d B_d$  provides an abelian variety  $A_h$  defined over  $\mathbb{Q}$  attached to  $h$  and  $\mathbb{Q}$ -isogenous to the abelian variety  $A_f$  attached by Shimura to  $f$ . This abelian variety can be defined as the optimal quotient of  $J_0(N)$  such that the pullback of  $\Omega_{A_h/\mathbb{Q}}^1$  is the vector space generated by the Galois conjugates of  $h(q) dq/q$  with rational  $q$ -expansion. This definition determines the  $\mathbb{Q}$ -isomorphism class of  $A_h$ , although we are only interested in its  $\mathbb{Q}$ -isogeny class.
- (vii) Given two abelian varieties  $A$  and  $B$  defined over the number field  $K$ , the notation  $A \stackrel{K}{\sim} B$  expresses that  $A$  and  $B$  are isogenous over  $K$ .
- (viii) For an integer  $m \geq 1$  and  $f \in \text{New}_N$ ,  $a_m(f)$  is the  $m$ -th Fourier coefficient of  $f$ .
- (ix) As usual,  $\psi$  denotes the Dedekind psi function. That is,  $\psi(N) = N \prod_{p|N} (1 + p^{-1})$ , where the product is extended to all primes  $p$  dividing  $N$ .
- (x)  $G_{\mathbb{Q}}$  denotes the absolute Galois group  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  once an algebraic closure  $\overline{\mathbb{Q}}$  of  $\mathbb{Q}$  has been fixed.

A summary on modular abelian varieties can be found in [BGGP05][Section 3]. We recall some known facts that will be used. The  $\mathbb{Q}$ -vector space  $\Omega_{X_0(N)/\mathbb{Q}}^1$  is the subspace of elements in  $S_2(N) dq/q$  with rational  $q$ -expansion, *i.e.*  $S_2(N) dq/q \cap \mathbb{Q}[[q]]$ . For  $N$  square-free integer and  $g_N^* \geq 1$ , it is known that

$$J_0^*(N) \stackrel{\mathbb{Q}}{\sim} \prod_{1 < M|N} \prod_{f \in \text{New}_M^*/G_{\mathbb{Q}}} A_f.$$

These abelian varieties  $A_f$  in the decomposition are simple and pairwise non-isogenous over  $\overline{\mathbb{Q}}$  and the endomorphism algebra  $\text{End}(\text{Jac}(X_0^*(N)) \otimes \mathbb{Q})$  is isomorphic to the product of totally real numbers fields (cf. [BH03, §2]). Moreover, in [Rib75][Proposition 3.1] it is proved that all endomorphisms of  $J_0(N)$  are defined over  $\mathbb{Q}$ . In particular, all endomorphisms of  $J_0^*(N)$  are also defined over  $\mathbb{Q}$ .

By [BG20][Proposition 2.2], a basis of  $S_2^*(N)$  is formed by the eigenforms

$$\bigcup_{1 < M|N} \left\{ \sum_{1 \leq d|N/M} d f(q^d) : f \in \text{New}_M^* \right\}. \quad (2.1)$$

Every  $f_i \in \text{New}_{M_i}^*$  with  $M_i|N$  determines the normalized eigenform  $h_i = \sum_{1 \leq d|N/M_i} d f_i(q^d)$  in  $S_2^*(N)$  such that  $A_{f_i} \stackrel{\mathbb{Q}}{\sim} A_{h_i}$ . On the one hand, the basis of the Galois conjugates of the newforms  $f_i$  allows us to compute  $|X_0^*(\mathbb{F}_p^n)|$  for all primes  $p \nmid N$  and for all  $n \geq 1$ , thanks to the Eichler-Shimura congruence. Indeed, the characteristic polynomial of  $\text{Frob}_p$  acting on the Tate module of  $J_0^*(N)$  is

$$P(x) = \prod_{1 > M|N} \prod_{f \in \text{New}_M^*} (x^2 - a_f(f)x + p) = \prod_{i=1}^{2g_N^*} (x - \alpha_i),$$

and, thus,

$$|X_0^*(\mathbb{F}_{p^n})| = p^n + 1 - \sum_{i=1}^{2g_N^*} \alpha_i^n.$$

On the other hand, the basis of the regular differentials formed by all Galois conjugates of  $h_i(q) dq/q$  allows us to compute equations for  $X_0^*(N)$  when  $g_N^* > 1$ .

Similarly, if  $X$  is a curve defined over  $\mathbb{Q}$  of genus  $g > 0$  for which there is a non constant morphism  $X_0^*(N) \rightarrow X$  defined over  $\mathbb{Q}$ , then there is a subset  $\mathcal{S}$  of  $\cup_{1 < M|N} \text{New}_M^*$  stable by Galois conjugation such that

$$\text{Jac}(X) \stackrel{\mathbb{Q}}{\sim} \prod_{f \in \mathcal{S}/G_{\mathbb{Q}}} A_f.$$

Hence, for a prime  $p \nmid N$ , the characteristic polynomial of  $\text{Frob}_p$  acting on the Tate module of  $\text{Jac}(X)$  is

$$P(x) = \prod_{f \in \mathcal{S}} (x^2 - a_f(f)x + p) = \prod_{i=1}^{2g} (x - \alpha_i)$$

and  $|X(\mathbb{F}_{p^n})| = p^n + 1 - \sum_{i=1}^{2g} \alpha_i^n$ . The set of the normalized eigenforms attached to  $\mathcal{S}$  in  $S_2^*(N)$  is a basis of  $\pi^*(\Omega_X^1)q/dq$  that allows us to compute equations for  $X$  when  $g > 1$ .

### 3 Preliminary results

In this section, we present some tools that will be applied to decide whether the group  $\text{Aut}(X_0^*(N))$  is trivial or not, and to determine this group when it is non trivial.

For a curve  $X$  defined over  $\mathbb{Q}$  of genus  $\geq 2$  and of good reduction at a prime  $p$ , one has that  $\text{Aut}_{\mathbb{Q}}(X) \hookrightarrow \text{Aut}_{\mathbb{F}_p}(X \otimes \mathbb{F}_p)$  (cf. [Liu02][Proposition 3.10.38]). We can apply [Gon17][Theorem 2.1] to discard the existence of involutions defined over  $\mathbb{Q}$ . More precisely, we will use the following criterion (see [Gon17][Remark 2.2] taking  $N = 2$ ).

**Lemma 1.** *Let  $X$  be a curve defined over  $\mathbb{F}_p$  of genus  $g > 2$ . Consider the sequence*

$$P_p(n) := \text{mod} \left[ \left( \sum_{d|n} \mu(n/d) |X(\mathbb{F}_{p^d})| \right) / n, 2 \right]$$

where  $\text{mod}[r, 2]$  denotes 0 or 1 depending on whether  $r$  is even or not, and  $\mu$  is the Moebius function. If there is an integer  $k > 0$  such that  $\sum_{n \geq 0}^k (2n+1)P_p(2n+1) > 2g+2$ , then  $\text{Aut}_{\mathbb{F}_p}(X)$  contains no involution.

By Petri's Theorem, we know that, for a nonhyperelliptic curve  $X$  defined over  $\mathbb{C}$  with genus  $g > 2$ , the image of the canonical map  $X \rightarrow \mathbf{P}^{g-1}$  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  $\omega_1, \dots, \omega_g$  of  $\Omega_{X/\mathbb{Q}}^1$ . For any integer  $i \geq 2$ , let us denote by  $\mathcal{L}_i$  the  $\mathbb{Q}$ -vector space of homogeneous polynomials  $Q \in \mathbb{Q}[x_1, \dots, x_g]$  of degree  $i$  that satisfy  $Q(\omega_1, \dots, \omega_g) = 0$ . 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  $X$ . For  $g > 3$ ,  $\dim \mathcal{L}_2 = (g-2)(g-3)/2 > 0$  and a basis of  $\mathcal{L}_2 \oplus \mathcal{L}_3$  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 said in the above section,  $J_0^*(N) \stackrel{\mathbb{Q}}{\sim} A_{h_1} \times \dots \times A_{h_n}$  for some normalized eigenforms  $h_1, \dots, h_k \in S_2^*(N)$ . These abelian varieties are simple and pairwise nonisogenous over  $\mathbb{Q}$  and, any involution  $u$  of the curve leaves stable each  $A_{h_i}$  acting on  $\Omega_{A_{g_i}}^1$  as the product by  $-1$  or the identity.

Choose a basis  $\{\omega_1, \dots, \omega_{g_N}^*\}$  of  $\Omega_{X_0^*(N)/\mathbb{Q}}^1$  obtained as the ordered union of bases of all  $\Omega_{A_{h_i}}^1/\mathbb{Q}$ . An involution  $u$  of  $X_0^*(N)$  induces a linear map  $u^* : \Omega_{X_0^*(N)/\mathbb{Q}}^1 \rightarrow \Omega_{X_0^*(N)/\mathbb{Q}}^1$  sending  $(\omega_1, \dots, \omega_{g_N}^*)$  to  $(\varepsilon_1 \omega_1, \dots, \varepsilon_n \omega_{g_N}^*)$  with  $\varepsilon_i = \pm 1$  for all  $i \leq g_N^*$  and satisfying

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

The genus of the quotient curve is the cardinality of the set  $\mathcal{I} = \{i : \varepsilon_i = 1\}$  and  $\{\omega_j\}_{j \in \mathcal{I}}$  is a basis of the pullback of the regular differentials of the quotient curve. A 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 nonhyperelliptic.

We particularize this fact to our case, that will be the main tool to determine the group  $\text{Aut}(X_0^*(N))$  for a fixed level  $N$ .

**Lemma 2.** *Assume  $X_0^*(N)$  is nonhyperelliptic, i.e.  $g_N^* > 2$ . Let  $\omega_1, \dots, \omega_{g_N^*}$  be a basis of  $\Omega_{X_0^*(N)/\mathbb{Q}}^1$  as above. Then,*

- (i) *Let  $u$  be a non trivial involution of  $X_0^*(N)$ . Consider the curve  $X_u = X_0^*(N)/\langle u \rangle$ . Denote by  $g_u$  the genus of  $X_u$ . Then there exists an integer  $k < n$  and factors  $A_{h_1}, \dots, A_{h_k}$  such that  $\text{Jac}(X_u) \stackrel{\mathbb{Q}}{\sim} A_{h_1} \times \dots \times A_{h_k}$  and, thus, satisfying*

$$Q(-x_1, -x_2, \dots, -x_{g_u}, x_{g_u+1}, \dots, x_{g_N^*-1}, x_{g_N^*}) \in \mathcal{L}_i \text{ for all } Q \in \mathcal{L}_i \text{ and for all } i \geq 2. \quad (3.2)$$

- (ii) *If  $g_u := \dim A_{h_1} \times \dots \times A_{h_k} < g_N^*$  and the condition (3.2) is satisfied, then there exists an involution  $v$  of  $X_0^*(N)$  such that*

$$\text{Jac}(X/\langle v \rangle) \stackrel{\mathbb{Q}}{\sim} A_{h_1} \times \dots \times A_{h_k} \text{ or } \text{Jac}(X/\langle v \rangle) \stackrel{\mathbb{Q}}{\sim} A_{h_{k+1}} \times \dots \times A_{h_n}$$

In order to make easy the computation of the condition (3.2) for  $\mathcal{L}_2$ , we introduce the vector subspace  $\mathcal{L}_2^{ns}$  of polynomials in  $\mathcal{L}_2$  that do not contain square monomials, i.e. polynomials of the form  $\sum_{1 \leq i < j \leq g} a_{ij} x_i x_j$ . For any  $Q \in \mathcal{L}_2$  and any  $r \leq g$ , we have that

$$Q(-x_1, \dots, -x_r, x_{r+1}, \dots, x_g) \in \mathcal{L}_2 \Leftrightarrow Q - Q(-x_1, \dots, -x_r, x_{r+1}, \dots, x_g) \in \mathcal{L}_2^{ns}. \quad (3.3)$$

In general, it is expected that  $\dim \mathcal{L}_2^{ns} = \text{Max}(\dim \mathcal{L}_2 - g, 0) = \text{Max}((g-1)(g-6)/2, 0)$ . When  $\dim \mathcal{L}_2^{ns} = 0$ , condition (3.3) amounts to saying that  $Q$  is simultaneously even in the variables  $x_1, \dots, x_r$ .

**Remark 1.** Assume that for a high genus  $g_N^*$  we cannot prove that the automorphism group of  $X_0^*(N)$  is trivial by means of Lemma 1. In this case, the application of Lemma 2 is computationally laborious. If we want to discard that a basis  $\{\omega_1, \dots, \omega_g\}$  of the vector space  $\Omega_{\prod_{i=1}^k A_{h_i}/\mathbb{Q}}^1$  with  $k < n$  is a basis of the pullback of the regular differentials of a possible quotient curve  $X_u = X_0^*(N)/\langle u \rangle$  without applying Lemma 2 to the curve  $X_0^*(N)$ , we can proceed in two different ways. If for a prime  $\ell \nmid N$  we have the inequality  $|X_0^*(N)(\mathbb{F}_{\ell^m})| > 2|X_u(\mathbb{F}_{\ell^m})|$  for some integer  $m \geq 1$ , then we can discard this possibility. Another way is the following. If  $g > 2$  and we know that  $X_u$  is not hyperelliptic, we check if the regular differentials  $\omega_1, \dots, \omega_g$  satisfy Petri's Theorem. That is, if  $g > 3$  and the dimension of the corresponding vector space  $\mathcal{L}_2$  is not  $(g-3)(g-2)/2$  or  $g = 3$  and  $\dim \mathcal{L}_4 \neq 1$ , then we can discard this possibility.

The result in the next proposition allows us to use the knowledge of the group of automorphisms of lower levels, that can be a source for getting bounds for the even levels  $N$  such that the curves  $X_0^*(N)$  may have non trivial automorphisms. Previously, we will present the following lemma.

**Lemma 3.** Let  $X$  be a curve defined over  $\mathbb{Q}$  of genus greater than 1 and let  $p$  be a prime of good reduction of  $X$ . Assume that there is a non trivial automorphism  $\tilde{w} \in \text{Aut}_{\mathbb{F}_p} X/\mathbb{F}_p$  that is not a hyperelliptic involution. If there exists an automorphism  $v \in \text{End}_{\mathbb{Q}}(\text{Jac } X)$  such that its reduction modulo  $p$  coincides with the induced automorphism  $\tilde{w}^* \in \text{End}_{\mathbb{F}_p} \text{Jac}(X/\mathbb{F}_p)$ , then there exists an automorphism  $w \in \text{Aut}_{\mathbb{Q}} X$  such that the induced automorphism  $w^* \in \text{End}_{\mathbb{Q}}(\text{Jac } X)$  satisfies  $w^* = \pm v$ .

**Proof.** If  $\tilde{w}$  is not a hyperelliptic involution, then  $v \neq -\text{Id}$ . The automorphism  $\tilde{w}$  respects the canonical polarization of the curve  $X/\mathbb{F}_p$ . Since the reduction of the endomorphism ring is injective,  $v$  also respects the canonical polarization of the curve  $X/\mathbb{Q}$ . Therefore, by Torelli's Theorem, there exists an automorphism  $w \in \text{Aut}_{\mathbb{Q}} X$  such that the induced morphism  $w^* \in \text{End}_{\mathbb{Q}}(\text{Jac } X)$  is  $v$  or  $-v$ .  $\square$

**Proposition 1.** Let  $N > 1$  be a square-free integer and let  $p$  be a prime dividing  $N$  such that  $g_{N/p}^* > 1$ . If there exists a non trivial involution  $u$  of  $X_0^*(N)$  such that the action of  $u$  on  $J_0^*(N/p)$  is non trivial, then the group  $\text{Aut}(X_0^*(N/p))$  is non trivial or the curve  $X_0^*(N/p)/\mathbb{F}_p$  is hyperelliptic.

**Proof.** Let  $\phi$  and  $\phi_p$  be the morphisms from  $X_0(N)$  to  $X_0(N/p)$  induced by the automorphisms of the complex upper half-plane given by  $z \mapsto z$  and  $z \mapsto pz$  respectively. Consider the morphism  $\nu = \phi^* + p\phi_p^*: J_0(N/p) \rightarrow J_0(N)$ , that is defined over  $\mathbb{Q}$ . For every cusp form  $h \in S_2^*(N/p)$  one has that  $\nu(h) \in S_2^*(N)$  and, moreover,  $\nu$  is an injective linear map from  $S_2^*(N/p)$  into  $S_2^*(N)$  because  $\nu$  sends a basis of  $S_2^*(N/p)$  to a set of linearly independents cusp forms (cf. (2.1)). Let  $\pi$  and  $\pi'$  be the following natural projections  $\pi: X_0(N/p) \rightarrow X_0^*(N/p)$ ,  $\pi': X_0(N) \rightarrow X_0^*(N)$ . The kernel of the morphism

$$\nu' := \pi'_* \circ \nu \circ \pi^*: J_0^*(N/p) \longrightarrow J_0^*(N)$$

is finite since  $J_0^*(N/p)$  and the abelian variety  $A := \nu'(J_0^*(N/p))$  have the same dimension. Moreover, for any Hecke operator  $T_M$  with  $\gcd(M, N) = 1$ , one has  $\nu \cdot T_M = T_M \cdot \nu$  (cf. [Li75]) and  $\nu'$  has the same property as  $\nu$ . Since  $(\text{End } J_0^*(N)) \otimes \mathbb{Q}$  is isomorphic to the product of totally real number fields, by applying the arguments used in [Rib75][Proposition 3.2], we obtain that for any abelian subvariety  $B$  of  $J_0^*(N)$  the algebra  $(\text{End } B) \otimes \mathbb{Q}$  is generated by the Hecke operators  $T_M$  with  $\gcd(M, N) = 1$ .

Let  $u$  be a non trivial involution of  $X_0^*(N)$ . This involution induces an involution  $u^*$  of  $J_0^*(N)$  which leaves stable  $A$  because  $A$  and  $J_0^*(N)/A$  are defined over  $\mathbb{Q}$  and have no isogenous quotients. Hence,  $u^*$  induces an involution of  $A$ , that we still denominate by  $u^*$ . The dual isogeny  $\widehat{\nu}' : A \rightarrow J_0^*(N/p)$  also satisfies the condition  $\widehat{\nu}' \circ T_M = T_M \circ \widehat{\nu}'$  for all Hecke operators  $T_M$  with  $\gcd(M, N) = 1$ . Since  $u^* \in \text{End}(A)$  lies in the algebra generated by the Hecke operators  $T_M$  with  $\gcd(M, N) = 1$ , the involution  $u^*$  leaves stable  $\ker \nu'$  and, thus, provides an involution  $v$  of the quotient  $A/\ker \widehat{\nu}' = J_0^*(N/p)$ .

Now, assume that  $u^* \in \text{End } A$  is non trivial. By using Hecke operators, we get that  $v$  is non trivial and satisfies  $u^* \cdot \nu' = \nu' \circ v$ . On the one hand, the normalization of  $X_0^*(N)/\mathbb{F}_p$  is the curve  $X_0^*(N/p)/\mathbb{F}_p$  (cf. [Has97][Section 5]) and  $u$  induces an involution  $\tilde{u}$  of  $X_0^*(N/p)/\mathbb{F}_p$ . On the other hand, the reduction of  $v$  modulo  $p$  coincides with the endomorphism of  $\text{Jac}(X_0^*(N/p)/\mathbb{F}_p)$  induced by the involution  $\tilde{u}$ . Now, the statement follows from Lemma 3.  $\square$

**Corollary 1.** *Assume that there exist a non trivial involution  $u$  of  $X_0^*(N)$  and a prime  $p|N$  with  $g_{N/p}^* > 2$ . If the group  $\text{Aut}(X_0^*(N/p))$  is trivial and  $X_0^*(N/p)/\mathbb{F}_p$  is not hyperelliptic, then  $g_u \geq g_{N/p}^*$  and  $\nu(S_2^*(N/p))dq/q$  is contained in the pullback of  $\Omega_{\text{Jac}(X_u)}^1$ . In particular,  $g_{N/p}^* \leq (g_N^* + 1)/2$  since by Hurwitz theorem one has  $g_u \leq (g_N^* + 1)/2$ .*

Note that a necessary condition for  $X_0^*(N/p)/\mathbb{F}_p$  being hyperelliptic is that the following inequalities are satisfied

$$|X_0^*(N/p)(\mathbb{F}_{p^n})| \leq 2p^n + 2 \text{ for all integers } n > 0.$$

The hyperelliptic curves have a different behaviour depending on whether they are defined over fields of characteristic 2 or not. Since [BGGP05][Lemma 2.5] can be applied to hyperelliptic curves defined over fields of characteristic different from 2 and  $X_0(N)$  admits a regular model defined over  $\mathbb{Z}[1/N]$ , we have a similar result to [BGGP05][Lemma 6] for modular curves over  $\mathbb{F}_p$  with  $p \neq 2$ . More precisely, in our case:

**Lemma 4.** *Assume  $p$  is an odd prime not dividing  $M$ . Let  $X/\mathbb{Q}$  be a curve of genus  $g > 2$  for which there is a no constant morphism  $\pi : X_0^*(M) \rightarrow X$  and let  $\mathcal{S}$  be the  $\mathbb{Z}$ -module  $S_2^*(M) \cap \mathbb{Z}[1/N][[q]]$ . The curve  $X/\mathbb{F}_p$  is hyperelliptic if, and only if, there is a basis  $f_1, \dots, f_g$  of  $\mathcal{S}$  whose reductions mod  $p$  satisfy*

$$f_i(q)/q \pmod{p} = \begin{cases} q^i + O(q^i) & \text{if the cusp } \infty \text{ is not a Weierstrass point of } X/\mathbb{F}_p, \\ q^{2i-1} + O(q^{2i-1}) & \text{otherwise,} \end{cases} \quad (3.4)$$

and for any such a basis, the functions on  $X/\mathbb{F}_p$  defined by

$$x = \frac{f_{g-1}}{f_g} \pmod{p}, \quad y = \frac{qdx/dq}{f_g} \pmod{p},$$

satisfy  $y^2 = P(x)$  for an unique square-free polynomial  $P(X) \in \mathbb{F}_p[X]$  which has degree  $2g + 1$  or  $2g + 2$  depending on whether the cusp  $\infty$  is a Weierstrass point or not of  $X/\mathbb{F}_p$ .

For the case  $p = 2$ , we use the following result.

**Lemma 5.** *Let  $N > 1$  be an odd square-free integer such that  $g_N^* > 2$ . If  $X_0^*(N)/\mathbb{F}_2$  is hyperelliptic, then  $N$  is in the set  $\{183, 185, 187, 203, 335, 345, 385\}$ .*

**Proof.** Put  $n = \omega(N)$ . By Ogg ([Ogg74][Theorem 3]), if  $X_0^*(N)/\mathbb{F}_2$  is hyperelliptic, then

$$\frac{\psi(N)}{12} + 2^n \leq 2^{n+1} |\mathbf{P}^1(\mathbb{F}_4)| = 5 \cdot 2^{n+1}.$$



Hence,  $\psi(N) \leq 2^n 108$  and, after discarding the values  $N$  such that  $g_N^* \leq 2$ , we obtain the following 59 values of  $N$ :

97, 109, 113, 127, 137, 139, 149, 151, 157, 163, 173, 179, 181, 183, 185, 187, 193, 197, 199, 201, 203, 211, 217, 219, 235, 237, 247, 249, 253, 259, 265, 267, 273, 291, 295, 301, 303, 305, 309, 319, 321, 323, 329, 335, 341, 345, 355, 371, 377, 385, 391, 399, 429, 435, 455, 465, 483, 561, 595.

We can discard the levels  $N$  such that  $A_{N,m} := |X_0^*(N)(\mathbb{F}_{2^m})| - 2(2^m + 1) > 0$ . Since

$(N, m)$	$A_{N,m}$	$(N, m)$	$A_{N,m}$	$(N, m)$	$A_{N,m}$	$(N, m)$	$A_{N,m}$
(97, 1)	1	(193, 1)	2	(267, 2)	4	(341, 2)	5
(109, 2)	1	(197, 2)	5	(273, 1)	1	(355, 2)	3
(113, 2)	1	(199, 2)	2	(291, 1)	3	(371, 2)	5
(137, 2)	2	(201, 1)	1	(295, 2)	2	(377, 2)	4
(139, 2)	1	(211, 2)	5	(301, 2)	3	(391, 1)	1
(149, 2)	2	(219, 1)	1	(303, 2)	3	(399, 1)	1
(151, 2)	1	(235, 1)	1	(305, 2)	4	(429, 2)	1
(157, 1)	2	(237, 1)	1	(309, 1)	2	(435, 1)	1
(163, 1)	2	(249, 2)	4	(319, 2)	1	(465, 2)	2
(173, 2)	4	(253, 1)	1	(321, 2)	5	(483, 2)	5
(179, 2)	2	(259, 2)	2	(323, 2)	2	(561, 1)	1
(181, 2)	4	(265, 1)	2	(329, 2)	2	(592, 2)	3

By Lemma 1, we also can discard the values  $N$  for which we know that  $X_0^*(N)/\mathbb{F}_2$  does not have any involution: 127, 217, 247.  $\square$

Note that for a prime  $p$  we know that the automorphism group is trivial when  $g_p^* > 2$  (cf. [BH03][Theorem 1.1]). For  $g_N^* = 3$ , the group  $\text{Aut}(X_0^*(N))$  is non trivial if, and only if,  $X_0^*(N)$  is bielliptic (cf. [BG19]Lemma 13]). For this reason in the next sections, we exclude the cases  $g_N^* \leq 3$  that can be found in Table 4 in [BG20][ Appendix].

## 4 Odd levels

We know that when  $g_N^* > 1$ , if there is a non trivial involution  $u$  of  $X_0^*(N)$ , then the cusp  $\infty$  is not a fixed point of  $u$  (cf. [BH03][Lemma 3.2]). The following result, similar to Lemma 6 in [Gon16], is the key result that allow us to determine a finite set of odd square-free integers containing all odd square-free integers  $N$  such that the group  $\text{Aut}(X_0^*(N))$  is non trivial.

**Proposition 2.** *Assume that the square-free integer  $N$  is odd,  $g_N^* > 1$  and there is a non trivial involution  $u$  of  $X_0^*(N)$ . Then, the  $\mathbb{Q}$ -gonality of  $X_0^*(N)$  is  $\leq 6$  and  $u$  has at most 12 fixed points.*

**Proof.** Take  $Q = u(\infty)$  and let  $P \in X_0(N)$  be such that  $\pi(P) = u(\infty)$ , where  $\pi$  is the natural projection of  $X_0(N)$  onto  $X_0^*(N)$ . Since  $Q$  is not a cusp, there is an elliptic curve  $E$  defined over  $\overline{\mathbb{Q}}$  and a  $N$ -cyclic subgroup  $C_N$  of  $E(\overline{\mathbb{Q}})$  such that  $P = (E, C_N)$ . The other pre-images of  $Q$  under  $\pi$  are the points

$$w_d(P) = (E/C_d, (E[d] + C_{N/d})/C_d) \quad \forall d|N,$$

where  $C_d$  denotes the  $d$ -cyclic subgroup of  $C$ , that is  $C_d = C_N \cap E[d]$ .

For any noncuspidal  $S \in X_0^*(N)$ , we consider the divisor

$$D_S := (uT_2 - T_2u)(\infty - S),$$

where  $T_2$  denotes the Hecke operator viewed as a correspondence of the curve  $X_0^*(N)$ . We claim that  $D_S$  is nonzero but linearly equivalent to zero.

The endomorphism algebra  $\text{End}(J_0^*(N)) \otimes \mathbb{Q}$  is commutative. Hence,  $uT_2 = T_2u$  and  $D_S$  is a principal divisor.

Next, we will prove that  $D_S$  is nonzero. If  $D_S$  is a zero divisor, then  $uT_2(\infty)$  must be equal to  $T_2u(\infty)$  because  $T_2(\infty) = 3\infty$  and  $\infty$  is not in the support of  $T_2(S)$ . To prove that  $D_S$  is a nonzero divisor, we only need to prove that the condition  $3(Q) = T_2(Q)$  cannot occur for a noncuspidal point  $Q \in X_0^*(N)$ .

Let  $G_i$ ,  $1 \leq i \leq 3$ , be the three 2-cyclic subgroups of  $E[2]$ . Since

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

the condition  $3(Q) = T_2(Q)$  implies that each elliptic curve  $E/G_i$  is isomorphic to  $E/C_d$  for some  $d|N$ . Therefore,  $E$  has an endomorphism whose kernel is a  $2d$ -cyclic subgroup and, thus,  $E$  has CM by a quadratic order  $\mathcal{O}$  of discriminant  $D$ . The conductor of the discriminant  $D$  cannot be even because  $2d$  is a norm of  $\mathcal{O}$  and  $2d \not\equiv 0 \pmod{4}$ . Since  $\pi(P) = \pi(w_d(P))$ , this property holds for all elliptic curves  $E/C_d$  and, thus, also for all elliptic curves  $E/G_i$ .

Now, we claim 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  $\text{End}(E/G)$  has even conductor. This fact implies that  $T_2(Q) \neq 3Q$  and, thus,  $D_S$  is nonzero. Indeed, let  $[a, b, c] := ax^2 + bxy + cy^2 \in \mathbb{Z}[x, y]$  be a primitive quadratic form of discriminant  $D$  (with odd conductor). The primitive quadratic forms attached to the three elliptic curves  $E/G_i$  are

$$Q_1 = [4a, 2b, c]/\gcd(c, 2), \quad Q_2 = [a, 2b, 4c]/\gcd(a, 2), \quad Q_3 = [4a, 2b-4a, a-b+c]/\gcd(2, a-b+c).$$

If the discriminants of  $Q_1$  and  $Q_2$  are equal to  $D$ , then  $a$  and  $c$  must be even. Since  $[a, b, c]$  is primitive,  $b$  must be odd and this fact leads to the contradiction that the discriminant of  $Q_3$  is  $4D$ , with even conductor.

By taking  $S = u(\infty)$ ,  $D_S$  is defined over  $\mathbb{Q}$  and, thus, the  $\mathbb{Q}$ -gonality is at most 6. Finally, since  $u^*(D_S) \neq D_S$  for some noncuspidal point  $S \in X_0^*(N)(\mathbb{C})$ , any non trivial automorphism of  $X_0^*(N)$  has at most 12 fixed points (cf. Lemma 3.5 of [BH03]).  $\square$

**Corollary 2.** *When  $N$  is odd, if  $g_u$  is the genus of the curve  $X_0^*(N)/\langle u \rangle$  for a non trivial involution  $u$  of  $X_0^*(N)$ , then*

$$\frac{g_N^* - 5}{2} \leq g_u \leq \frac{g_N^* + 1}{2}.$$

*Moreover, if  $J_0^*(N)$  has a simple factor of dimension larger than  $(g_N^* + 5)/2$ , then  $\text{Aut}(X_0^*(N))$  is trivial.*

**Proof.** The inequalities follows from the Riemann-Hurwitz formula applied to the projection  $X_0^*(N) \rightarrow X_0^*(N)/\langle u \rangle$ . For the last assertion see [BH03][Corollary 3.9]  $\square$

**Lemma 6.** *Assume that the  $\mathbb{Q}$ -gonality of  $X_0^*(N)$  is at most 6. If  $N$  is odd, then*

$$\psi(N) \leq 2^{\omega(N)} 348. \tag{4.1}$$

**Proof.** redAgain by Ogg, we know that  $2^{\omega(N)} + \frac{\psi(N)}{12} \leq |X_0(N)(\mathbb{F}_4)|$ . The statement follows from the fact that  $|X_0(N)(\mathbb{F}_4)| \leq 2^{\omega(N)} \cdot 6 \cdot |\mathbf{P}^1(\mathbb{F}_4)|$ .  $\square$

There are 471 values of  $N$  (square-free and odd,  $N \geq 3$ ) satisfying the condition (4.1), whose maximum value is 3003. Excluding all values that are prime or  $g_N^* \leq 3$ , we obtain 293 values.

By applying Lemma 1 to  $X_0^*(N)/\mathbb{F}_p$ , we can discard 248 values of  $N$ . More precisely, with  $p = 2$  the values

247, 253, 259, 267, 291, 301, 305, 319, 323, 327, 339, 355, 365, 377, 381, 391, 393, 395, 403, 407, 411, 413, 417, 427, 451, 453, 469, 471, 473, 481, 485, 489, 493, 501, 505, 511, 519, 527, 533, 535, 537, 543, 545, 553, 559, 565, 573, 579, 581, 589, 591, 595, 597, 611, 627, 629, 633, 635, 651, 655, 667, 669, 671, 679, 681, 685, 687, 695, 697, 699, 703, 707, 713, 717, 721, 723, 731, 737, 741, 745, 749, 755, 759, 763, 771, 777, 779, 781, 785, 789, 791, 793, 795, 799, 803, 805, 807, 813, 815, 817, 831, 835, 843, 849, 851, 865, 869, 871, 879, 885, 889, 893, 895, 897, 899, 901, 903, 905, 913, 915, 917, 921, 923, 933, 935, 939, 943, 949, 951, 955, 959, 965, 969, 973, 979, 985, 993, 995, 1001, 1003, 1005, 1007, 1011, 1015, 1023, 1027, 1037, 1041, 1043, 1045, 1057, 1065, 1067, 1073, 1081, 1085, 1095, 1099, 1105, 1111, 1113, 1115, 1121, 1131, 1133, 1135, 1139, 1141, 1145, 1147, 1157, 1159, 1169, 1173, 1177, 1185, 1189, 1199, 1207, 1209, 1211, 1219, 1221, 1235, 1239, 1241, 1243, 1245, 1247, 1261, 1265, 1271, 1273, 1281, 1295, 1311, 1353, 1407, 1419, 1435, 1443, 1455, 1463, 1479, 1491, 1505, 1515, 1533, 1545, 1547, 1581, 1595, 1599, 1605, 1635, 1645, 1653, 1659, 1677, 1695, 1705, 1729, 1743, 1749, 1767, 1771, 1785, 1833, 1855, 1885, 1887, 1955, 1995, 2015, 2035, 2093, 2145, 2415, 2805, 3003,

with  $p = 3$  the values 445, 1495, 1615, with  $p = 5$  the values 623, with  $p = 7$  the values 583, 753, 1551 and for  $p = 11$  the value 1335. Corollary 2 allows us to exclude the values

235, 237, 273, 341, 385, 415, 435, 497, 515, 517, 649, 767, 715, 989, 1079, 1309.

So, we only have to consider 29 values for  $N$ , which we present together with the splitting of the corresponding jacobians collected by the genus  $g_N^*$ . From now on, the splitting

$$J_0^*(N) \stackrel{\mathbb{Q}}{\sim} \prod_{i=1}^r A_{f_i}, \text{ with } f_i \in \text{New}_{M_i}^* \text{ and } \dim A_{f_i} = n_i$$

will be presented as  $n_{1M_1} + \cdots + n_{rM_r}$ . Obviously,  $g_N^* = \sum_{i=1}^r n_i$  and, for a divisor  $M$  of  $N$ , one has  $g_M^* = \sum_{M_i|N} n_i$ .

$N$	$J_0^*(N)$	$N$	$J_0^*(N)$
201	$2_{67} + 1_{201} + 1_{201}$	265	$1_{53} + 1_{265} + 2_{265} + 2_{265}$
219	$2_{73} + 1_{219} + 1_{219}$	447	$3_{149} + 3_{447}$
321	$2_{107} + 2_{321}$	561	$3_{187} + 3_{561}$
335	$2_{67} + 2_{335}$	609	$3_{203} + 3_{609}$
345	$2_{115} + 2_{345}$	615	$1_{123} + 2_{205} + 1_{615} + 2_{615}$
399	$1_{57} + 2_{133} + 1_{399}$	309	$2_{103} + 5_{309}$
483	$2_{161} + 2_{483}$	437	$2_{437} + 5_{437}$
		861	$1_{123} + 2_{287} + 4_{861}$
371	$1_{53} + 1_{371} + 3_{371}$	665	$2_{133} + 6_{665}$
465	$2_{93} + 1_{155} + 2_{465}$	1155	$1_{77} + 2_{165} + 3_{385} + 1_{1155} + 1_{1155}$
551	$2_{551} + 3_{551}$	689	$1_{53} + 1_{689} + 2_{689} + 2_{689} + 3_{689}$
555	$1_{37} + 1_{185} + 1_{185} + 2_{555}$	705	$1_{141} + 5_{235} + 1_{705} + 2_{705}$
645	$1_{43} + 1_{129} + 1_{215} + 2_{645}$	987	$1_{141} + 3_{329} + 2_{987} + 3_{987}$
663	$2_{221} + 3_{663}$	1365	$1_{65} + 1_{91} + 3_{273} + 1_{455} + 3_{1365}$
		957	$4_{319} + 7_{957}$
		1055	$3_{211} + 3_{211} + 3_{1055} + 6_{1055}$

**Proposition 3.** *Let  $N > 1$  be an odd square-free integer such that  $g_N^* > 3$ . The group  $\text{Aut}(X_0^*(N))$  is non trivial if, and only if,  $N = 645$ . In this case, the order of this group is 2 and an equation for the quotient curve by the non trivial involution is given by*

$$Y^2 = X^6 + 8X^4 + 20X^2 + 12X + 4.$$

**Proof.** In order to apply Petri's theorem to the curve  $X_0^*(N)$ , we will take a basis of  $\Omega_{X_0^*(N)/\mathbb{Q}}^1$  as in Lemma 2, following the order showed in the splitting tables.

For  $g_N^* = 4$ ,  $\dim \mathcal{L}_2 = 1$ . In all cases in the above table,  $\dim \mathcal{L}_2^{ns} = 0$ . The genus of a quotient curve by an involution must be 2. We have to check the condition (3.2) for all pairs  $x_i$ , and  $x_j$  such that  $\omega_i$  and  $\omega_j$  are a basis of the regular differentials corresponding to an abelian quotient of  $J_0^*(N)$  of dimension 2. A nonzero polynomial  $Q \in \mathcal{L}_2$  neither satisfies  $Q(-x_1, -x_2, x_3, x_4) = Q$  for  $N \neq 399$  nor  $Q(x_1, -x_2, -x_3, x_4) = Q$  for  $N = 399$ . Therefore, for all these cases the curves  $X_0^*(N)$  have trivial automorphism group.

For  $g_N^* = 5$ ,  $\dim \mathcal{L}_2 = 3$ . The genus of a quotient curve by an involution must be 2 or 3. It suffices to check the condition (3.2) for all pairs  $x_i$ , and  $x_j$  such that  $\omega_i$  and  $\omega_j$  is a basis of the regular differentials corresponding to an abelian quotient of  $J_0^*(N)$  of dimension 2. For the values in the above table  $N \neq 645$ , one has  $\dim \mathcal{L}_2^{ns} = 0$  and the polynomials of  $\mathcal{L}_2$  are not simultaneously even in the variables  $x_i, x_j$ . Hence, for all these cases the curves  $X_0^*(N)$  have trivial automorphism group. For  $N = 645$ , we know that  $X_0^*(645)$  is not trigonal (cf. [HS00]) and, thus,  $\mathcal{L}_2$  defines the curve. The set  $\cup_{M|645} \text{New}_M^*$  is

$$\text{New}_{43}^* = \{f_1\}, \quad \text{New}_{129}^* = \{f_2\}, \quad \text{New}_{215}^* = \{f_3\},$$

$$\text{New}_{645}^* = \{f_4 = q + \sqrt{2}q^2 + \dots, f_5 = q - \sqrt{2}q^2 + \dots\}.$$

Taking the following basis of  $\Omega_{X_0^*(645)/\mathbb{Q}}^1$ :

$$\omega_1 = \left(\sum_{d|15} d f_1(q^d)\right) dq/q, \quad \omega_2 = \left(\sum_{d|5} d f_2(q^d)\right) dq/q, \quad \omega_3 = \left(\sum_{d|3} d f_3(q^d)\right) dq/q,$$

$$\omega_4 = \frac{f_4 + f_5}{2} dq/q \text{ and } \omega_5 = \frac{f_5 - f_4}{2\sqrt{2}} dq/q,$$

we get that  $\mathcal{L}_2 = \{Q = aQ_1 + bQ_2 + cQ_3 : a, b, c \in \mathbb{Q}\}$ , where

$$\begin{aligned} Q_1 &= 6x_1^2 + 5x_1x_2 + 7x_1x_3 - 11x_2x_3 - 9x_3^2 + 2x_4^2 + 48x_4x_5 + 16x_5^2, \\ Q_2 &= 2x_1x_2 + 3x_2^2 - 2x_1x_3 + 4x_2x_3 - 3x_3^2 - 4x_4^2 + 16x_5^2, \\ Q_3 &= x_2x_4 - x_3x_4 - 2x_1x_5 + x_2x_5 + x_3x_5. \end{aligned}$$

Now,  $\mathcal{L}_2^{ns} = \langle Q_3 \rangle$ . For all possible choices  $(i, j) \in \{(1, 2), (1, 3), (2, 3), (4, 5)\}$ , we only have the possibility  $(i, j) = (4, 5)$  satisfying condition (3.3), i.e.  $Q - Q(x_1, x_2, x_3, -x_4, -x_5) \in \mathcal{L}_2^{ns}$  for all  $Q \in \mathcal{L}_2$ . Therefore, there is a unique non trivial involution  $u$  sending  $(\omega_1, \omega_2, \omega_3, \omega_4, \omega_5)$  to  $\pm(\omega_1, \omega_2, \omega_3, -\omega_4, -\omega_5)$ . The number of eigenvalues equal to 1 is the genus of  $X_u = X_0^*(N)/\langle u \rangle$  and the corresponding eigenvectors among the differentials  $\{\omega_i, i \leq 5\}$  is a basis of the pullback of  $\Omega_{X_u}^1$ . To decide the precise sign, we compute the number of fixed points of  $u$ . The set of such points in  $\mathbf{P}^4(\overline{\mathbb{Q}})$  is the set of points of the form  $(0, 0, 0, x_4, x_5)$  and of the form  $(x_1, x_2, x_3, 0, 0)$  satisfying  $Q_i(x_1, \dots, x_5) = 0$  for  $1 \leq i \leq 3$ . Since this set has 4 points, all of them of the form  $x_4 = x_5 = 0$ , the genus of  $X_u$  is 2 and  $\{\omega_4, \omega_5\}$  form a basis of the pullback of  $\Omega_{X_u}^1$ . Take  $X = \omega_4/\omega_5$  and  $Y = dx/\omega_5$  and we obtain

$$Y^2 = X^6 + 8X^4 + 20X^2 + 12X + 4.$$

For  $g_N^* = 6$ , we get  $\dim \mathcal{L}_2^{ns} = 0$ . The genus of a quotient curve by an involution must be 2 or 3. For the possible choices of pairs  $(i, j)$  or triples  $(i, j, k)$ , there are polynomials in  $\mathcal{L}_2$  that are not simultaneously even in the corresponding variables. Hence, all curves  $X_0^*(N)$  of genus 6 have trivial automorphism group.

For  $g_N^* \geq 6$ , in all cases  $\dim \mathcal{L}_2^{ns} = (g - 1)(g - 6)/2$ . We have to consider all choices  $(i_1, \dots, i_r)$  such that  $(g_N^* - 5)/2 \leq r \leq (g_N^* + 1)/2$  and  $\omega_{i_1}, \dots, \omega_{i_r}$  is a basis of the pullback of regular differentials of a quotient of  $J_0^*(N)$  of dimension  $r$ . After computing the vector space  $\mathcal{L}_2$ , we can claim that in all these cases there are polynomials in  $\mathcal{L}_2$  not satisfying the condition (3.3).

Nevertheless, we note that some of these computations can be simplified by using Proposition and Remark 1. Indeed, for the pairs  $(N, p)$  in the set

$$\{(1155, 3), (705, 3), (987, 3), (1365, 3), (1365, 5), (957, 3), (1055, 5)\},$$

the curve  $X_0^*(N/p)$  has trivial automorphism group and  $X_0^*(N/p)/\mathbb{F}_p$  is not hyperelliptic. Hence, the choice  $(i_1, \dots, i_r)$  should contain the variables corresponding to the basis of the pullback of  $\Omega_{J_0^*(N/p)}^1$ . Next, in the four following examples, we show how we use these results.

For instance, if  $X_0^*(1365)$  of genus 9 has a nontrivial involution  $u$ , by Proposition 1, the jacobian of the quotient curve  $X_u$  has  $J_0^*(273)$  and  $J_0^*(455)$  as factors. This fact leads to the contradiction that  $\text{Jac}(X_u)$  has a factor of dimension 6 when the genus of  $X_u$  is at most 5.

For  $N = 957$ , take a basis  $\{g_i\}_{1 \leq i \leq 4}$  of  $S_2^*(319) \cap \mathbb{Q}[[q]]$  and consider the set of the cusp forms  $h_i(q) = g_i(q) + 3g_i(q^3) \in S_2^*(957)$ . By observing the splitting of  $J_0^*(957)$ , the vector space spanned by  $h_i(q) dq/q$  would be the pullback of the regular differential of the unique possible quotient curve and the vector space of the homogenous polynomial in  $\mathbb{Q}[x_1, \dots, x_4]$  of degree 2 vanishing at these differentials would have dimension 1. After a computation, the dimension obtained is 0. So, we can exclude the level 957. Note that for  $X_0^*(957)$ ,  $\dim \mathcal{L}_2 = 36$ .

For  $N = 705$ , take a basis  $\{g_i\}_{1 \leq i \leq 5}$  of  $S_2^*(235) \cap \mathbb{Q}[[q]]$  and consider the set of the cusp forms  $h_i(q) = g_i(q) + 3g_i(q^3) \in S_2^*(957)$ . The vector space spanned by  $h_i(q) dq/q$  should be the pullback of the regular differential of the unique possible quotient curve and the vector space of

the homogenous polynomial in  $\mathbb{Q}[x_1, \dots, x_5]$  of degree 2 vanishing at these differentials should have dimension 3. After a computation, the dimension obtained is 0. So, we can exclude the level 705.

If  $X_0^*(1551)$  has a non trivial involution, then the jacobian of the genus six curve  $X_0^*(211)$  is isogenous to the jacobian of the quotient curve. Since  $|X_0^*(1555)(\mathbb{F}_2)| - 2|X_0^*(211)(\mathbb{F}_2)| = 4 > 0$ , we can discard  $N = 1551$ .  $\square$

## 5 Even levels

The next proposition is the key result to determine the even levels.

**Proposition 4.** *Let  $N > 1$  be an odd square-free integer. Then,*

$$g_{2N}^* - 2g_N^* \leq 2.$$

Moreover,  $g_{2N}^* - 2g_N^* < -1$  for all  $N > 1239$  and, for the particular case  $g_N^* > 2$ , one has that

(i)  $g_{2N}^* = 2g_N^* - 1$  if, and only if,  $N$  is in the set

$$\{109, 113, 139, 151, 203, 227, 259, 263, 319, 355, 411, 445, 451, 455, 461, 491, 505, 521, 555, 573, 581, 591, 695, 699, 779, 1001, 1131, 1239\}.$$

(ii)  $g_{2N}^* = 2g_N^*$  if, and only if,  $N$  is in the set

$$\{173, 267, 281, 295, 339, 341, 359, 371, 377, 413, 419, 429, 431, 447, 479, 483, 501, 551, 623, 627, 645, 663, 671, 755, 789, 987\}.$$

(iii)  $g_{2N}^* = 2g_N^* + 1$  if, and only if,  $N$  is in the set

$$\{149, 179, 239, 249, 251, 269, 305, 311, 321, 329, 393, 395, 519, 545, 689, 861, 897\}.$$

(iv)  $g_{2N}^* = 2g_N^* + 2$  if, and only if,  $N = 303$ .

**Proof.** Let us denote by  $\mathcal{P}$  the set of integer primes dividing  $N$  and set  $n := |\mathcal{P}|$ . We have that the genera of  $X_0(N)$  and  $X_0(2N)$  are

$$g_N = 1 + \frac{\psi(N)}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - 2^{n-1}, \quad g_{2N} = 1 + \frac{\psi(N)}{4} - \frac{\nu_2}{4} - 2^n, \quad (5.1)$$

where

$$\nu_2 = \begin{cases} 0 & \text{if } \exists p \in \mathcal{P}, p \equiv -1 \pmod{4}, \\ 2^n & \text{otherwise.} \end{cases}, \quad \nu_3 = \begin{cases} 0 & \text{if } \exists p \in \mathcal{P}, p \equiv -1 \pmod{3}, \\ 2^{n-\nu_3(N)} & \text{otherwise.} \end{cases},$$

where  $\nu_3$  denotes the 3-adic valuation. The genera of  $X_0^*(N)$  and  $X_0^*(2N)$  are

$$g_N^* = 1 + \frac{1}{2^n}(g_N - 1) - \frac{1}{2^{n+1}} \sum_{1 < d|N} \nu(N, d), \quad g_{2N}^* = 1 + \frac{1}{2^{n+1}}(g_{2N} - 1) - \frac{1}{2^{n+2}} \sum_{1 < d|2N} \nu(2N, d), \quad (5.2)$$

where  $\nu(M, d)$  denotes the number of fixed points of  $X_0(M)$  by the Atkin-Lehner involution  $w_d$ . Hence  $g_{2N}^* - 2g_N^* + 1$  is equal to

$$\frac{1}{2^{n+1}} \left( -\frac{\psi(N)}{12} + \frac{3\nu_2}{4} + \frac{4\nu_3}{3} - \frac{1}{2}\nu(2N, 2) + \sum_{1 < d|N} 2\nu(N, d) - \frac{1}{2}\nu(2N, d) - \frac{1}{2}\nu(2N, 2d) + 2^n \right).$$

Let  $s = 0, 1$ . By [Klu77], we know when  $d \geq 5$ :

$$\begin{aligned}\nu(d, d) &= \begin{cases} h(-4d), & \text{if } d \not\equiv -1 \pmod{4}, \\ h(-4d) + h(-d), & \text{if } d \equiv -1 \pmod{4}, \end{cases} \\ \nu(2d, d) &= \begin{cases} h(-4d), & \text{if } d \not\equiv -1 \pmod{4}, \\ h(-4d) + 3h(-d), & \text{if } d \equiv -1 \pmod{4}, \end{cases}\end{aligned}$$

where  $h(D)$  is the class number of the order of discriminant  $D$  of a quadratic field, and for  $d|N$ :

$$\nu(2^s N, d) = \prod_{p|N/d} \left(1 + \left(\frac{-d}{p}\right)\right) \nu(2^s d, d), \quad \nu(2N, 2d) = \prod_{p|N/d} \left(1 + \left(\frac{-d}{p}\right)\right) \nu(2d, 2d).$$

For  $d < 5$ :

$$\nu(2N, 2) = \prod_{p|N} \left(1 + \left(\frac{-1}{p}\right)\right) + \prod_{p|N} \left(1 + \left(\frac{-2}{p}\right)\right), \quad \nu(2^s 3N, 3) = 2 \prod_{p|N} \left(1 + \left(\frac{-3}{p}\right)\right).$$

We also know that for  $d \equiv -1 \pmod{4}$ ,  $h(-4d)$  is  $h(-d)$  or  $3h(-d)$  depending on whether  $d \equiv -1 \pmod{8}$  or not (see [Cox13][Theorem 7.24]).

Since  $\nu_2 \leq \nu(2N, 2)$  and  $\nu_2, \nu_3 \leq 2^n$ , we have

$$g_{2N}^* - 2g_N^* + 1 \leq \frac{1}{2^{n+1}} \left( -\frac{\psi(N)}{12} + \sum_{1 < d|N} (2\nu(N, d) - \frac{1}{2}\nu(2N, d)) + \frac{31}{12}2^n \right).$$

If  $D$  is the discriminant of an order of an imaginary quadratic field, we know  $h(D) \leq \frac{1}{\pi}|D|^{1/2} \log(|D|)$  (see Appendix in [Ser89]). On the one hand,

$$2\nu(d, d) - \frac{1}{2}\nu(2, d) = \begin{cases} \frac{3}{2}h(-4d) & \text{if } d \not\equiv 1 \pmod{4}, \\ 2h(-d) & \text{if } d \equiv 7 \pmod{8}, \\ \frac{5}{3}h(-4d) & \text{if } d \equiv 3 \pmod{8}, \end{cases},$$

and, on the other hand,  $\log(4d) \leq d^{1/4} + 3$ . Hence, we get

$$2\nu(d, d) - \frac{1}{2}\nu(2, d) \leq \frac{10}{3\pi}(d^{1/2} + 3d^{1/4}).$$

Since  $\frac{31}{12} < \frac{10}{3\pi}(1^{3/4} + 3 \cdot 1^{1/2})$ , we have

$$g_{2N}^* - 2g_N^* + 1 < \frac{1}{2^{n+1}} \left( -\frac{\psi(N)}{12} + \frac{10}{3\pi} \sum_{d|N} 2^{\omega(N/d)} (d^{3/4} + 3d^{1/2}) \right).$$

Since

$$\sum_{d|N} 2^{\omega(N/d)} d^{3/4} = \prod_{p \in \mathcal{P}} (2 + p^{3/4}), \quad \sum_{d|N} 2^{\omega(N/d)} d^{1/2} = \prod_{p \in \mathcal{P}} (2 + p^{1/2}),$$

the following inequality

$$\frac{10}{3\pi} \left( \prod_{p \in \mathcal{P}} \frac{2 + p^{3/4}}{1 + p} + 3 \prod_{p \in \mathcal{P}} \frac{2 + p^{1/2}}{1 + p} \right) - \frac{1}{12} < 0 \quad (5.3)$$

implies  $g_{2N}^* - 2g_N^* + 1 < 0$ . Write  $\mathcal{P} = \{p_1 < \dots < p_n\}$ . For two odd square-free integers  $N = \prod_{i=1}^n p_i$  and  $N' = \prod_{i=1}^{n'} p'_i$ , we define the order  $N \preceq N'$  if, and only if,  $n \leq n'$  and  $p_i \leq p'_i$  for all  $i \leq n$ . The real function  $f(x) = \frac{2+x^\alpha}{1+x}$  with  $\frac{1}{2} \leq \alpha \leq \frac{3}{4}$  is decreasing for  $x \geq 3$  and  $f(x) < 1$  for  $x \geq 5$ . Hence, if the inequality (5.3) is satisfied for  $N$ , then it holds for all integers  $N' \succeq N$ . Therefore, the inequality (5.3) is right for the values  $N$  that satisfy some of the following conditions

- (i)  $\omega(N) \geq 8$ .
- (ii) For  $\omega(N) = 7$  when  $p_1 \geq 5$  or  $p_7 > 73$ .
- (iii) For  $\omega(N) = 6$  when  $p_1 \geq 7$  or  $p_6 > 569$ .
- (iv) For  $\omega(N) = 5$  when  $p_1 \geq 13$  or  $p_5 > 3373$ .
- (v) For  $\omega(N) = 4$  when  $p_1 \geq 23$  or  $p_4 > 16573$ .
- (vi) For  $\omega(N) = 3$  when  $p_1 \geq 53$  or  $p_3 > 37993$ .
- (vii) For  $\omega(N) = 2$ , when  $p_1 \geq 269$  or  $p_2 > 63737$ .
- (viii) For  $\omega(N) = 1$  when  $p_1 > 54277$ .

The statement is obtained after computing  $g_{2N}^* - 2g_N^*$  for the remaining values of  $N$ .  $\square$

**Remark 2.** *The proof presented in the above proposition needs a laborious computation because it involves a lot of possibilities and, thus, many class numbers. In opinion of the authors, there has to exist a deeper explanation to justify the inequality stated for  $g_{2N}^* - 2g_N^*$ .*

## 5.1 Candidates $X_0^*(2N)$ with non trivial automorphism group

Combining Propositions 1 and 4, the cases  $g_{2N}^* - 2g_N^* < -1$  can be discarded, because of the inequality  $g_N^* > (g_{2N}^* + 1)/2$  (see Corollary 1). Now, we only have to study the automorphism group of  $X_0^*(2N)$  for the odd values  $N$  contained in the following five lists:

- (i) The list of values of  $N$  with  $g_N^* \leq 2$  such that  $g_{2N}^* > 3$ :

$$\ell_1 = \{101, 107, 131, 161, 167, 177, 191, 205, 209, 213, 221, 285, 287, 299, 357\}$$

By Lemma 1 we discard  $N = 191$  at  $p = 5$ . For the remaining  $N$ , the splitting of the jacobian of  $X_0^*(2N)$  is

$N$	$J_0^*(2N)$	$N$	$J_0^*(2N)$
101	$1_{101} + 3_{202}$	167	$2_{167} + 2_{314}$
131	$1_{131} + 1_{262} + 2_{262}$	177	$1_{118} + 2_{177} + 1_{354}$
107	$2_{107} + 1_{214} + 1_{214}$	213	$1_{142} + 2_{213} + 1_{426}$
161	$2_{161} + 2_{322}$	285	$1_{57} + 1_{190} + 1_{285} + 1_{570}$
$N$	$J_0^*(2N)$	$N$	$J_0^*(2N)$
205	$1_{82} + 2_{205} + 2_{410}$	287	$1_{82} + 2_{287} + 1_{574} + 1_{574}$
209	$2_{209} + 3_{418}$	357	$1_{102} + 1_{238} + 2_{357} + 1_{714}$
221	$2_{221} + 3_{442}$	299	$2_{299} + 4_{598}$



The genus of a quotient curve of any of these curves  $X_0^*(2N)$  by an involution non bielliptic must be equal to 2 when  $g_{2N}^* = 4$  and equal to 2 or 3 when  $5 \leq g_{2N}^* \leq 6$ . Hence, we can discard  $N = 101$  and for the remaining cases we apply Lemma 2. Finally, we get that all curves  $X_0^*(2N)$  with  $N \in \ell_1$  have trivial automorphism group.

- (ii) The list containing the values of  $N$  with  $g_N^* > 2$  such that  $X_0^*(N)/\mathbb{F}_2$  could be hyperelliptic:

$$\ell_2 = \{183, 185, 187, 203, 335, 345, 385\}.$$

The splitting of the jacobian of  $X_0^*(2N)$

$N$	$J_0^*(2N)$	$N$	$J_0^*(2N)$
183	$1_{61} + 1_{126} + 2_{183}$	203	$1_{58} + 3_{203} + 1_{406}$
185	$1_{37} + 1_{185} + 1_{185} + 1_{370}$	385	$1_{77} + 1_{154} + 3_{385}$
187	$3_{187} + 1_{374}$	335	$2_{67} + 2_{335} + 2_{670}$
		345	$2_{115} + 1_{138} + 2_{345} + 1_{690}$

The curves  $X_0^*(2N)$  with  $N \in \ell_2 \setminus \{183\}$  have trivial automorphism group. Indeed, we can discard  $N = 187$  because  $J_0^*(374)$  has no two dimensional quotients and the remaining values of  $N$  can be excluded by applying Lemma 2. For  $X_0^*(366)$  the automorphism group has order 2 (cf. [BG19]).

- (iii) The list containing the values of  $N$  with  $g_N^* > 2$  such that  $\text{Aut}(X_0^*(N))$  is not trivial (except to 183 because it is in the list  $\ell_2$ ) is:

$$\ell_3 = \{249, 303, 455\},$$

with

$N$	249	303	455
$J_0^*(2N)$	$1_{83} + 1_{166} + 1_{249} + 1_{249} + 3_{498}$	$1_{101} + 3_{202} + 2_{303} + 2_{606}$	$1_{65} + 1_{91} + 1_{455} + 2_{910}$

By applying Lemma 2, we get that all these three curves  $X_0^*(2N)$  have trivial automorphism group. We point out that  $X_0^*(202)/\mathbb{F}_3$  is not hyperelliptic (see Lemma 4) and the automorphism group of  $X_0^*(202)$  is trivial. Hence, by Proposition 1, for  $X_0^*(606)$  we only have to consider as possible quotient the curve whose jacobian is isogenous to  $J_0^*(202)$ .

- (iv) The list  $\ell_4$  contains the values of  $N$  with  $g_N^* > 2$  and  $-1 \leq g_{2N}^* - 2g_N^* \leq 0$ , except to  $N = 203$  that is in the list  $\ell_2$ . So, the list  $\ell_4$  is the union of the sets

$$\{109, 113, 139, 151, 227, 259, 263, 319, 355, 411, 445, 451, 455, 461, 491, 505, 521, 555, 573, 581, 591, 695, 699, 779, 1001, 1131, 1239\},$$

for which  $g_{2N}^* - 2g_N^* = -1$ , and

$$\{173, 267, 281, 295, 339, 341, 359, 371, 377, 413, 419, 429, 431, 447, 479, 483, 501, 551, 623, 627, 645, 663, 671, 755, 789, 987\}.$$

For all these values,  $X_0^*(N)$  has trivial automorphism group and its reduction modulo 2 is not hyperelliptic (see Lemma 5). By Proposition 1, if  $X_0^*(2N)$  has a non trivial involution, then the jacobian of the quotient curve is isogenous to  $J_0^*(N)$  because  $g_N^*$  is the greatest genus of a quotient curve of  $X_0^*(2N)$ .

When  $g_{2N}^* - 2g_N^* = -1$ , if  $X_0^*(2N)$  has a non trivial involution, by Hurwitz, this cannot have fixed points. Hence, for all odd primes  $p \nmid N$  and all integers  $k > 0$ , the number  $R(2N, p^k) := |X_0^*(2N)(\mathbb{F}_{p^k})|$  must be even. Since

$N$	$p^k$	$R(2N, p^k)$	$N$	$p^k$	$R(2N, p^k)$	$N$	$p^k$	$R(2N, p^k)$	$N$	$p^k$	$R(2N, p^k)$
109	$3^3$	21	319	3	9	491	$3^5$	75	695	3	9
113	3	9	355	3	7	505	$3^5$	147	699	5	23
139	$3^3$	21	411	$5^5$	3323	521	$3^3$	29	779	$3^3$	21
151	3	17	445	$3^3$	29	555	11	17	1001	$3^5$	305
227	3	9	451	$3^3$	11	573	$5^3$	89	1131	$5^7$	75993
259	5	17	455	3	7	581	$3^3$	27	1239	5	15
263	$3^3$	17	461	3	15	591	5	17			

we can discard all these values.

When  $g_{2N}^* = 2g_N^*$ , by applying Lemma 1, we can discard some values of  $N$ . With the prime  $p = 3$ , the values of  $N$  in the set

$$\{173, 281, 359, 377, 419, 431, 479, 671, 755\},$$

and with the prime  $p = 5$ , the following values

$$\{413, 501, 623, 789\}.$$

We only have to consider

$N$	$J_0^*(2N)$	$N$	$J_0^*(2N)$
295	$1_{118} + 3_{295} + 2_{590}$	551	$1_{58} + 2_{551} + 3_{551} + 2_{1102} + 2_{1102}$
429	$1_{143} + 1_{286} + 2_{429} + 2_{858}$	645	$1_{43} + 1_{129} + 1_{215} + 1_{258}$ $+ 1_{430} + 2_{645} + 3_{1290}$
267	$1_{89} + 2_{178} + 3_{267} + 2_{534}$	663	$1_{102} + 2_{221} + 3_{442} + 3_{663} + 1_{1326}$
341	$4_{341} + 4_{682}$	447	$3_{149} + 1_{298} + 3_{298} + 3_{447} + 1_{894} + 1_{894}$
483	$2_{161} + 2_{322} + 2_{483} + 1_{966} + 1_{966}$	627	$1_{57} + 2_{209} + 3_{418} + 3_{627} + 3_{1254}$
339	$3_{113} + 2_{226} + 2_{339} + 1_{678} + 2_{678}$	987	$1_{141} + 2_{282} + 3_{329} + 4_{658} + 2_{987}$ $+ 3_{987} + 3_{1974}$
371	$1_{53} + 1_{106} + 1_{371} + 3_{371}$ $+ 1_{742} + 3_{742}$		

It can be checked that the curves  $X_0^*(322)/\mathbb{F}_3$ ,  $X_0^*(226)/\mathbb{F}_3$ ,  $X_0^*(430)/\mathbb{F}_3$ ,  $X_0^*(442)/\mathbb{F}_3$ ,  $X_0^*(298)/\mathbb{F}_3$ ,  $X_0^*(418)/\mathbb{F}_3$ , and  $X_0^*(658)/\mathbb{F}_3$  are not hyperelliptic. By Proposition 1, the jacobian of a quotient curve de  $X_0^*(2N)$  is isogenous to  $J_0^*(N)$ . Thus, we can discard the values

$$N \in \{483, 339, 645, 663, 447, 627, 987\}.$$

Although  $X_0^*(178)$  has a unique non trivial involution, whose quotient curve is isogenous to an elliptic curve of conductor 89, the curve  $X_0^*(534)$  can also be discarded. Indeed, a non trivial involution of  $X_0^*(534)$  should induce the identity on the elliptic curve of conductor 89 and, thus on the curve  $X_0^*(178)$ . But this fact leads to the contradiction that the jacobian of the quotient curve would have as a factor an abelian surface attached to a newform of level 178. For the remaining values, i.e.

$$N \in \{295, 429, 341, 371, 551\},$$

we apply Lemma 2 and we get that the five curves  $X_0^*(2N)$  have trivial automorphism group.

- (v) The list of values  $N$  with  $g_N^* > 2$  and  $g_{2N}^* > 2g_N^*$ , except to  $N = 249$  and  $N = 303$  because they are in the lists  $\ell_3$ , are the following:

$$\ell_5 = \{149, 179, 239, 251, 269, 303, 305, 311, 321, 329, 393, 395, 519, 545, 689, 861, 897\}.$$

For all these cases,  $g_{2N}^* - 2g_N^* = 1$ . By Proposition 1, if  $X_0^*(2N)$  has a non trivial involution, then the pullback of the regular differentials of the quotient curve is the pullback of  $\Omega_{J_0^*(N)}^1$  or  $\Omega_{J_0^*(N) \times E}^1$  for some elliptic curve  $E$  in the decomposition of  $J_0^*(2N)$ , whose conductor does not divide  $N$ .

By applying Lemma 1 to  $X_0^*(2N)$ , we can discard the values of  $N$  in the set

$$\{149, 179, 239, 251, 269, 311, 393, 519, 545\},$$

taking  $p = 5$  for  $2N = 2 \cdot 393, 2 \cdot 519, 2 \cdot 179$ ,  $p = 7$  for  $2N = 2 \cdot 545$  and  $p = 3$  for the remaining cases. The splitting of  $J_0^*(2N)$  for the non discarded cases is as follows

$N$	$J_0^*(2N)$	$N$	$J_0^*(2N)$
329	$3_{329} + 4_{658}$	861	$1_{82} + 1_{123} + 1_{246} + 2_{287} + 1_{574} + 1_{574}$
305	$1_{61} + 1_{122} + 3_{305} + 4_{610}$		$+ 4_{861} + 1_{1722} + 1_{1722} + 2_{1722}$
321	$2_{107} + 1_{214} + 1_{214} + 2_{321} + 3_{642}$	897	$1_{138} + 2_{299} + 4_{598} + 5_{897} + 3_{1794}$
395	$1_{79} + 1_{158} + 3_{395} + 4_{790}$	689	$1_{53} + 1_{106} + 1_{689} + 2_{689} + 3_{689}$
			$+ 3_{689} + 3_{1378} + 6_{1378}$

It can be checked that the curves  $X_0^*(214)/\mathbb{F}_3$ ,  $X_0^*(574)/\mathbb{F}_3$ , and  $X_0^*(598)/\mathbb{F}_3$  are not hyperelliptic. By Proposition 1, the values  $N \in \{321, 861, 897\}$  can be discarded.

For the remaining values, i.e.  $N = 329, 305, 395, 689$ , we apply Lemma 2 and we get that the five curves  $X_0^*(2N)$  have trivial automorphism group.

For instance, for  $N = 689$  we can proceed in a easier way. If  $X_0^*(1378)$  has a non trivial involution  $u$ , then the jacobian of the quotient curve  $X_u$  is isogenous to  $J_0^*(689)$  or  $J_0^*(689) \times A_g$ , where  $g$  is the only newform in  $\text{New}_{106}^*$ . None of these curves could be hyperelliptic because  $|X_u(\mathbb{F}_3)| > 8$ . Take a basis  $g_1, \dots, g_9$  of  $S_2^*(689) \cap \mathbb{Q}[[q]]$ . Put  $h_i(q) := g_i(q) + 2g_i(q^2)$  and  $h_{10}(q) := g(q) + 13g(q^{13})$ . It can be checked that the dimension of the vector space of homogenous polynomials in 9 variables (resp. 10 variables) vanishing at  $h_1, \dots, h_9$  (resp.  $h_1, \dots, h_{10}$ ) has dimension 1. Hence,  $N = 689$  can be excluded. Note that for  $X_0^*(1378)$ ,  $\dim \mathcal{L}_2 = 153$ .

As a consequence of this analysis and taking into account [BG19][Proposition 24], we get the following result.

**Proposition 5.** *Let  $N > 1$  be an even square-free integer such that  $g_N^* > 3$  and  $X_0^*(N)$  is not bielliptic. The group  $\text{Aut}(X_0^*(N))$  is non trivial if, and only if,  $N = 366$ . In this case, the order of this group is 2 and an equation for the quotient curve by the non trivial involution is given by*

$$Y^2 = X^6 - 6X^5 + 23X^4 - 42X^3 + 53X^2 - 24X + 4.$$

This proposition together Proposition 3 concludes the proof of Theorem 2.

## Acknowledgements

We thank C. Ritzenthaler for his valuable comments and B. Poonen, whose contribution was decisive to prove Proposition 4.

## References

- [BGGP05] M. H. Baker, E. González-Jiménez, J. González, and B. Poonen. Finiteness results for modular curves of genus at least 2. *Amer. J. Math.*, 127(6):1325–1387, 2005.
- [BH03] M. H. Baker and Y. Hasegawa. Automorphisms of  $X_0^*(p)$ . *J. Number Theory*, 100(1):72–87, 2003.
- [BG19] F. Bars and J. González. Bielliptic modular curves  $X_0^*(N)$  with square-free levels. *Math. Comp.*, 88(320):2939–2957, 2019.
- [BG20] Francesc Bars and Josep González. Bielliptic modular curves  $X_0^*(N)$ . *J. Algebra*, 559:726–759, 2020.
- [BGX21] F. Bars, J. González, and X. Xarles. Hyperelliptic parametrizations of  $\mathbf{Q}$ -curves. *To be published in Ramanujan Journal.*, 2021.
- [Cox13] D. A. Cox. *Primes of the form  $x^2 + ny^2$* . Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013. Fermat, class field theory, and complex multiplication.
- [Elk90] N. D. Elkies. The automorphism group of the modular curve  $X_0(63)$ . *Compositio Math.*, 74(2):203–208, 1990.
- [GL98] Josep González and Joan-C. Lario. Rational and elliptic parametrizations of  $\mathbf{Q}$ -curves. *J. Number Theory*, 72(1):13–31, 1998.
- [Gon16] Josep González. Automorphism group of split Cartan modular curves. *Bull. Lond. Math. Soc.*, 48(4):628–636, 2016.
- [Gon17] J. González. Constraints on the automorphism group of a curve. *J. Théor. Nombres Bordeaux*, 29(2):535–548, 2017.
- [Har14] M. Harrison. A new automorphism of  $X_0(108)$ . <https://arxiv.org/abs/1108.5595>., 2014.
- [Has97] Y. Hasegawa. Hyperelliptic modular curves  $X_0^*(N)$ . *Acta Arith.*, 81(4):369–385, 1997.
- [HH96] Y. Hasegawa and K. Hashimoto. Hyperelliptic modular curves  $X_0^*(N)$  with square-free levels. *Acta Arith.*, 77(2):179–193, 1996.
- [HS00] Y. Hasegawa and M. Shimura. Trigonal modular curves  $X_0^*(N)$ . *Proc. Japan Acad. Ser. A Math. Sci.*, 76(6):83–86, 2000.
- [Klu77] P. G. Kluitt. On the normalizer of  $\Gamma_0(N)$ . In *Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, pages 239–246. Lecture Notes in Math., Vol. 601, 1977.
- [KM88] M. A. Kenku and F. Momose. Automorphism groups of the modular curves  $X_0(N)$ . *Compositio Math.*, 65(1):51–80, 1988.
- [Lan01] M.L. Lang. Normalizers of the congruence subgroups of the Hecke groups  $G_4$  and  $G_6$ . *J. Number Theory*, 90(1):31–43, 2001.

- [Li75] W. C. W. Li. Newforms and functional equations. *Math. Ann.*, 212:285–315, 1975.
- [Liu02] Q. Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Ern , Oxford Science Publications.
- [Ogg74] A. P. Ogg. Hyperelliptic modular curves. *Bull. Soc. Math. France*, 102:449–462, 1974.
- [Rib75] K. A. Ribet. Endomorphisms of semi-stable abelian varieties over number fields. *Ann. Math. (2)*, 101:555–562, 1975.
- [Ser89] J.-P. Serre. *Lectures on the Mordell-Weil theorem*. Aspects of Mathematics, E15. Friedr. Vieweg & Sohn, Braunschweig, 1989. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt.

Francesc Bars Cortina  
 Departament Matem tiques, Edif. C, Universitat Aut noma de Barcelona  
 08193 Bellaterra, Catalonia  
 francesc@mat.uab.cat

Josep Gonz lez Rovira  
 Departament de Matem tiques, Universitat Polit cnica de Catalunya EPSEVG,  
 Avinguda V ctor Balaguer 1, 08800 Vilanova i la Geltr , Catalonia  
 josep.gonzalez@upc.edu