JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Josep GONZÁLEZ

Constraints on the automorphism group of a curve

Tome 29, n° 2 (2017), p. 535-548.

<http://jtnb.cedram.org/item?id=JTNB_2017__29_2_535_0>

Journal de Théorie des Nombres de Bordeaux **29** (2017), 535–548

Constraints on the automorphism group of a curve

par Josep GONZÁLEZ

Résumé. Pour une courbe de genre > 1 définie sur un corps fini, nous présentons un critère suffisant pour la non-existence d'automorphismes de l'ordre une puissance d'un nombre premier. Nous montrons comment ce critère peut être utilisé pour déterminer le groupe d'automorphismes de certaines courbes modulaires de genres supérieurs.

Abstract. For a curve of genus > 1 defined over a finite field, we present a sufficient criterion for the non-existence of automorphisms of order a power of a rational prime. We show how this criterion can be used to determine the automorphism group of some modular curves of high genus.

1. Introduction

For a curve X of genus $g > 1$ defined over a field K, the automorphism group $\mathrm{Aut}_K(X)$ is finite. In characteristic zero, it is well-known that one has the Hurwitz bound $|\mathrm{Aut}_K(X)| \leq 84(g-1)$. In [9], the inequality $|\mathrm{Aut}_K(X)| < 16g^4$ is seen to hold in positive characteristic unless X is a Hermitian curve. In particular, this provides a bound for the order of any automorphism of the curve. Nevertheless, there is not a general procedure to discard possible orders.

We are interested in the case in which K is a number field. The reduction of the curve X at a prime of K of good reduction is a curve $\widetilde{X}$ defined over a finite field $\mathbb{F}_q$. We know that $\mathrm{Aut}_K(X)$ injects into $\mathrm{Aut}_{\mathbb{F}_q}(\widetilde{X})$ (cf. [8, Proposition 10.3.38]) and although this inclusion may be strict, any information allowing to discard orders of the elements in the group $\mathrm{Aut}_{\mathbb{F}_q}(\widetilde{X})$ will be useful for our goal. Moreover, if necessary, we can change the prime of K of good reduction for X.

Manuscrit reçu le 4 septembre 2015, révisé le 29 mars 2016, accepté le 29 mars 2016.
Mathematics Subject Classification. 14G35, 14H37.
Mots-clefs. Automorphisms of curves, non-split Cartan modular curves.
I thank the referee for his or her comments, specially those that have contribute to improve the result contained in Theorem 2.1, where we have used places of the curve instead of geometric points. I also thank the referee for the example provided of a genus two curve that allows us to answer the question proposed in Remark 2.6. The author is partially supported by DGI grant MTM2015-66180-R.

The main result of this work is in Section 2. For a curve X of genus > 1 defined over a finite field $\mathbb{F}_q$, we fix an integer $s > 1$ which is a power of a rational prime. In Theorem 2.1, we present a criterion which, under a certain condition on the sequence $\{|X(\mathbb{F}_{q^n})|\}_{n\geq 1}$ depending on s, ensures the non-existence of elements in $\mathrm{Aut}_{\mathbb{F}_q}(X)$ of order s. Although this criterion is not a characterization for the non-existence of such automorphisms, it is certainly a powerful tool that can be applied in many situations.

In Section 3, in order to show the efficacy of this tool, we apply it to some modular curves. In fact, we deal with curves X defined over $\mathbb{Q}$ such that their jacobians are quotients of jacobians of modular curves $X_0(M)$ for some positive integer M. This choice is due to two reasons. On the one hand, thanks to the Eichler–Shimura congruence and using Magma or Sage, we can compute the sequence $\{|(X \otimes \mathbb{F}_\ell)(\mathbb{F}_{\ell^n})|\}_{n\geq 1}$ from the ℓ-th Fourier coefficient of certain newforms of level dividing M attached to $\mathrm{Jac}(X)$ for all primes $\ell \nmid M$. On the other hand, we can determine the algebra $\mathrm{End}(\mathrm{Jac}(X)) \otimes \mathbb{Q}$ as well as the smallest number field L where all these endomorphisms are defined; in particular, $\mathrm{Aut}(X) = \mathrm{Aut}_L(X)$ and the orders of the roots of unity in the endomorphism algebra restrict the possible orders in $\mathrm{Aut}(X)$. More precisely, in Section 3 we first test our criterion on 18 modular curves for which Baker and Hasegawa proved that their automorphism groups are trivial (cf. [1]). We also use this criterion in Proposition 3.2 to determine the automorphism group for 12 other modular curves of high genus.

2. Automorphisms of a curve defined over a finite field

Let $\mathbb{F}_q$ be the finite field with q elements and let X be a curve of genus $g > 1$ defined over $\mathbb{F}_q$. The initial strategy to find a criterion to discard orders of automorphisms in $\mathrm{Aut}_{\mathbb{F}_q}(X)$ is based on the following idea.

Assume that there exists a subgroup G of $\mathrm{Aut}_{\mathbb{F}_q}(X)$ of order > 1. Let $\mathcal{R}$ be the set of ramification points of the natural projection $\pi_G\colon X \to X/G$ and, for all integer $n > 0$, consider the sets

$$A_n := \begin{cases} X(\mathbb{F}_q) & \text{if } n = 1, \\ X(\mathbb{F}_{q^n}) \setminus \cup_{i=1}^{n-1} X(\mathbb{F}_{q^i}) & \text{if } n > 1. \end{cases}$$

The orbit of a point $S \in X(\overline{\mathbb{F}}_q)$ under the action of G has cardinality equal to $|G|$ if, and only if, $S \notin \mathcal{R}$. Since $\mathcal{R}$ is a finite set, the sequence of cardinalities $|A_n|$, $n \geq 1$, satisfies the condition $|A_n| \equiv 0 \pmod{|G|}$ for almost all n. Moreover,

$$\sum_{n\geq 1} \mathrm{mod}(|A_n|, |G|) \leq \sum_{n\geq 1} |A_n \cap \mathcal{R}| = |\mathcal{R}|\,,$$

where $\mathrm{mod}(r, |G|)$ denotes the remainder when dividing the integer r by $|G|$. In fact, this inequality when $|G| = 2$ was applied in [6] to prove the

non-existence of involutions for five modular curves and is the origin of the result presented in this article.

From the Riemann–Hurwitz formula applied to π_G, we can get an upper bound for $|\mathcal{R}|$ depending only on the genus g and $|G|$ and the corresponding inequality would provide a necessary condition for curves having a subgroup of automorphisms of order $|G|$.

For instance, assume that the order of G is equal to a prime N. In this case, it can be easily proved that $(N-1)|\mathcal{R}| \le 2g + 2(N-1)$ and, thus,

$$\sum_{n\ge 1} \operatorname{mod}(|A_n|, N) \le \left\lfloor \frac{2\,g}{N-1} \right\rfloor + 2\,. \tag{2.1}$$

Nevertheless, this condition can be improved if we take into account that the absolute Galois group $\operatorname{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ acts on $X(\overline{\mathbb{F}}_q)$ leaving the sets A_n and $\mathcal{R}$ stable. Indeed, A_n is the disjoint union of all orbits of points in $X(\overline{\mathbb{F}}_q)$ under the action of the absolute Galois group having cardinality equal to n. So, $|A_n| \equiv |A_n \cap \mathcal{R}| \equiv 0 \pmod{n}$. Hence, from the inequality $n \operatorname{mod}(|A_n|/n, N) \le |A_n \cap \mathcal{R}|$ when n is coprime to N, we obtain

$$\sum_{n\ge 1,\gcd(n,N)=1} n \operatorname{mod}(|A_n|/n, N) \le \left\lfloor \frac{2\,g}{N-1} \right\rfloor + 2\,. \tag{2.2}$$

Observe that for $N \mid n$, we have $\operatorname{mod}(|A_n|, N) = 0$, while $\operatorname{mod}(|A_n|, N) \le n \operatorname{mod}(|A_n|/n, N)$ for n coprime to N. Hence,

$$\sum_{n\ge 1} \operatorname{mod}(|A_n|, N) \le \sum_{n\ge 1,\gcd(n,N)=1} n \operatorname{mod}(|A_n|/n, N)\,,$$

and the condition (2.2) improves (2.1).

We want to generalize the inequality (2.2) to the case that G is a cyclic subgroup of order a power of a prime. In order to do that, we will consider places of the curve instead of points in $X(\overline{\mathbb{F}}_q)$. A *place* of the curve is the orbit of a point in $X(\overline{\mathbb{F}}_q)$ under the action of the absolute Galois group. In scheme language, this is simply a closed point of X. The *degree* of a place P is its cardinality. We denote by $\mathcal{P}_n$ the set of places of degree n, whose cardinality is $|A_n|/n$.

Theorem 2.1. *Assume that there exists an automorphism of X defined over $\mathbb{F}_q$ of order N^m, where N is a rational prime and m an integer > 0. Set*

$$L(n) := \frac{N^m}{\gcd(n, N^m)}\,, \quad P(n) := \operatorname{mod}(|\mathcal{P}_n|, L(n))\,,$$

and let $D(n)$ be the sum of the N-adic digits of $P(n)$. Then,

$$\sum_{n\ge 1} n(L(n)\,D(n) - P(n)) \le 2\,g + 2(N^m - 1)\,. \tag{2.3}$$

Proof. Let G be the subgroup of $\mathrm{Aut}_{\mathbb{F}_q}(X)$ generated by an automorphism of order N^m. Let $\pi_G\colon X \to X/G$ be the natural projection. By the Riemann–Hurwitz formula applied to π_G, we obtain

$$N^m(2g_G - 2) + \sum_{S \in X(\overline{\mathbb{F}}_q)} (e(S) - 1) \leq 2g - 2\,,$$

where g_G is the genus of X/G and $e(S)$ is the ramification index of the point S (the inequality can be strict only when q is a power of N). In particular, we have

$$\sum_{S \in X(\overline{\mathbb{F}}_q)} (e(S) - 1) \leq 2g + 2(N^m - 1)\,.$$

We can rewrite this inequality in terms of places of X:

$$\sum_{n \geq 1} n \sum_{P \in \mathcal{P}_n} (e(P) - 1) \leq 2g + 2(N^m - 1)\,. \tag{2.4}$$

Let Q be a place of X/G. Let $P_1, \ldots, P_r$ be the places of X that are preimages of Q by π_G. All these places have the same ramification index, say e, and the same degree, say n. We have

$$e \cdot f \cdot r = N^m\,,$$

where f is the degree of the field of definition of each P_i over the field of definition of Q. In particular, $f \mid \gcd(n, N^m)$. These r places provide in the sum in (2.4) the amount

$$n \cdot r(e - 1) = n \cdot r \left(\frac{N^m}{f \cdot r} - 1 \right) = n \left(\frac{N^m}{f} - r \right)\,.$$

Since $\frac{N^m}{f} \leq L(n)$, these r places contribute at least $n(L(n) - r)$ to (2.4). We know that there are at least $P(n)$ places of degree n. If the base-N representation of $P(n)$ is $\sum_{i=0}^{k} d_i \cdot N^i$, then the least contribution of the $P(n)$ places of degree n to the sum in (2.4) corresponds to the case where there are d_i places with $r = N^i$ for all $0 \leq i \leq k$. We have

$$\sum_{i=0}^{k} n \cdot d_i \left(P(n) - N^i\right) = n \left(D(n) \cdot L(n) - P(n)\right).$$

Observe that $n \left(D(n) \cdot L(n) - P(n)\right)$ is ≥ 0 and is equal to zero when all places of degree n are unramified. From the inequality

$$n \left(D(n) \cdot L(n) - P(n)\right) \leq n \sum_{P \in \mathcal{P}_n} (e(P) - 1)\,,$$

the statement follows. □

Remark 2.2. For $m = 1$, Theorem 2.1 states

$$\sum_{n\geq 1,\gcd(n,N)=1} n(N-1)P(n) \leq 2g + 2(N-1)\,,$$

which is the same condition as (2.2).

Remark 2.3. To apply Theorem 2.1, we only need to know the characteristic polynomial $Q(x)$ of Frob_q acting on the Tate module of $\mathrm{Jac}(X)$. Indeed, if $\alpha_1, \cdots, \alpha_{2g}$ are the roots of $Q(x)$, then

$$|X(\mathbb{F}_{q^n})| = 1 + q^n - \sum_{i=1}^{2g} \alpha_i^n\,.$$

For $n > 1$, the integer $|\mathcal{P}(n)| = |A_n|/n$ can be computed from the sequence $\{|X(\mathbb{F}_{q^i})|\}_{1\leq i\leq n}$ as follows

$$|A_n| = \sum_{d|n} \mu(n/d)|X(\mathbb{F}_{q^d})|\,, \tag{2.5}$$

where μ is the Möbius function. We note that if $\ell_1 = 2 < \cdots < \ell_r$ are the first r rational primes, for $n < \prod_{i=1}^{r} \ell_i$, the sum given in (2.5) contains at most 2^{r-1} terms.

To be more precise, to apply Criterion 2.1 we only need to know $Q(x) \pmod{N^m}$. In other words, we can change the polynomial $Q(X)$ to a polynomial $T(x) \in \mathbb{Z}[x]$ such that $Q(x) \equiv T(x) \pmod{N^m}$. We can determine $\mathrm{mod}(|A_n|, N^m)$ from the roots of $T(x)$ by applying the procedure described for the roots of $Q(x)$.

Remark 2.4. If we can prove that, for an automorphism $u \in \mathrm{Aut}_{\mathbb{F}_q}(X)$ of order a prime N, there exists an integer r such that $|\mathcal{R}| \leq r < \left\lfloor \frac{2g}{N-1} \right\rfloor + 2$, then the condition (2.3) in Theorem 2.1 can be replaced with the condition

$$\sum_{n\geq 1,\gcd(n,N)=1} n\,P(n) \leq r\,.$$

Remark 2.5. The condition (2.3) is not a sufficient condition for the existence of an automorphism in $\mathrm{Aut}_{\mathbb{F}_q}(X)$ of order N^m. For instance, it may be that two non-isomorphic curves X and Y defined over $\mathbb{F}_q$ have jacobians which are isogenous over $\mathbb{F}_q$. If Y has an automorphism of order N^m, then condition (2.3) is satisfied, even if X does not have an automorphism of order N^m. Also, if the group $G = \mathrm{Aut}_{\mathbb{F}_q}(X)$ is nontrivial, then one has $|A_n| \equiv 0 \pmod{|G|}$ for almost all n. It may be that condition (2.3) is satisfied when we take N^m dividing $|G|$ and G does not contain any N^m-cyclic subgroups.

Remark 2.6. For a prime N, the condition $|A_n| \equiv 0 \pmod{N^m}$ for almost all n seems to be strong and amounts to saying that

$$\sum_{n\geq 1} \operatorname{mod}(A_n|, N^m) < \infty\,.$$

If there exists a curve Y defined over $\overline{\mathbb{F}}_q$ such that $\operatorname{Jac}(Y)$ and $\operatorname{Jac}(X)$ are isogenous and the order of the group $\operatorname{Aut}(Y)$ is a multiple of N^m, then this condition is satisfied. One can wonder if the converse is true. I thank the referee for providing the following example, that gives a negative answer. Consider the genus two curve $X/\mathbb{F}_{13}$ defined by

$$y^2 = x^5 + x^3 + 7\,x^2 + x + 7\,.$$

The characteristic polynomial of Frob_{13} is

$$Q(t) = t^4 - 7\,t^3 + 33\,t^2 - 91\,t + 169 \equiv (t+1)^2(t-1)^2 \pmod{7}\,.$$

Therefore,

$$|X(\mathbb{F}_{13^i})| \equiv 1 + (-1)^i - 2(1+(-1)^i) \equiv \begin{cases} 0 \pmod 7 & \text{if } i \text{ is odd,} \\ 5 \pmod 7 & \text{if } i \text{ is even.} \end{cases}$$

It follows that $|A_n| \equiv 0 \pmod 7$ for all $n \neq 2$ and it is known that there is not any genus two curves with an automorphism of degree 7.

Several consequences can be obtained from Theorem 2.1. Next, we present two of them.

Corollary 2.7. *Assume that there is an integer n such that*

$$1 + \frac{2}{n} < |A_n| < \frac{2g}{n} + 1\,.$$

If there is $u \in \operatorname{Aut}_{\mathbb{F}_q}(X)$ of order a prime $N \nmid n$, then $N < \frac{2g}{n} + 1$, which improves the result obtained through the Hurwitz bound.

Corollary 2.8. *If $u \in \operatorname{Aut}_{\mathbb{F}_q}(X)$ has order a prime N, then the integer $\sum_{n\geq 1, \gcd(n,N)=1} n\,P(n)$ is a lower bound for the number of fixed points by u.*

3. Application to some modular curves

We summarize some well-known facts on modular curves and fix notation. Let New_M denote the set of normalized newforms in $S_2(\Gamma_0(M))^{\text{new}}$ and let New_M^+ be the set $\{f \in \operatorname{New}_M : w_M(f) = f\}$, where w_M is the Fricke involution. For $f \in \operatorname{New}_M$, let $S_2(f)$ be the $\mathbb{C}$-vector space of cusp forms spanned by f and its Galois conjugates. Let us denote by A_f the abelian variety attached to f by Shimura. It is a quotient of $J_0(M) := \operatorname{Jac}(X_0(M))$ defined over $\mathbb{Q}$ and the pull-back of $\Omega^1_{A_f/\mathbb{Q}}$ is the $\mathbb{Q}$-vector subspace of elements in $S_2(f)dq/q$ with rational q-expansion, i.e. $S_2(f)dq/q \cap \mathbb{Q}[[q]]$, where

$q = e^{2\pi i z}$ for z in the complex upper half-plane. Moreover, the endomorphism algebra $\mathrm{End}^0_{\mathbb{Q}}(A_f) := \mathrm{End}_{\mathbb{Q}}(A_f) \otimes \mathbb{Q}$ is isomorphic to a totally real number field E_f whose degree is equal to $\dim A_f$.

Let $G_{\mathbb{Q}}$ denote the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Let X be a curve of genus $g > 0$ defined over $\mathbb{Q}$ such that $\mathrm{Jac}(X)$ is a quotient of $J_0(M)$ defined over $\mathbb{Q}$. There exists a subset $\mathcal{S}$ of the set $\cup_{M'|M} \mathrm{New}_{M'}$, which is stable under Galois conjugation, such that $\mathrm{Jac}(X)$ is isogenous over $\mathbb{Q}$ to the abelian variety $\prod_{f \in \mathcal{S}/G_{\mathbb{Q}}} A_f^{n_f}$ for some integers $n_f > 0$. If ℓ is a prime of good reduction for X not dividing M, by the Eichler–Shimura congruence, we can compute the characteristic polynomial $Q(x)$ of Frob_ℓ acting on the Tate module of $\mathrm{Jac}(X \otimes \mathbb{F}_\ell)$ through the ℓ-Fourier coefficients $a_\ell(f)$ of the newforms f in $\mathcal{S}$:

$$Q(x) = \prod_{f \in \mathcal{S}} (x^2 - a_\ell(f)x + \ell)^{n_f} .$$

3.1. The modular curves $X_0^+(p)$. In [1], the automorphism group of the modular curves $X_0^+(p) := X_0(p)/\langle w_p \rangle$ is determined for all primes p. After applying some theoretical results and to conclude the article, the authors need to prove that the modular curve $X_0^+(p)$ does not have any involutions defined over $\mathbb{Q}$ for $p = 163, 193, 197, 211, 223, 227, 229, 269, 331, 347, 359, 383, 389, 431, 461, 563, 571, 607$. In order to do that, they apply two different arguments. The first one is used to discard 11 cases and the second one allows to discard the remaining 7 cases. Although in [1] it is proved that the number of fixed points of an involution is ≤ 12, next we show the table obtained by applying Theorem 2.1 (without using Remark 2.4) to the curve $X = X_0^+(p) \otimes \mathbb{F}_2$ and $N^m = 2$. Set $Q(n) = \sum_{i \geq 1, i \text{ odd}}^{n} iP(i)$, where $P(i)$ is as in Theorem 2.1, i.e. $P_i = \mathrm{mod}(|A_i|/i, 2)$. We get

p	g	$Q(n)$	p	g	$Q(n)$	p	g	$Q(n)$
163	6	$Q(11) = 25$	229	7	$Q(11) = 25$	389	11	$Q(11) = 27$
193	7	$Q(17) = 33$	269	6	$Q(9) = 19$	431	8	$Q(13) = 25$
197	6	$Q(9) = 20$	331	11	$Q(15) = 39$	461	12	$Q(21) = 38$
211	6	$Q(9) = 22$	347	10	$Q(21) = 63$	563	15	$Q(17) = 39$
223	6	$Q(11) = 22$	359	6	$Q(9) = 18$	571	19	$Q(17) = 49$
227	5	$\mathbb{Q}(7) = 16$	383	8	$Q(13) = 19$	607	19	$Q(17) = 42$

In all cases $\sum_{n \geq 1, n \text{ odd}} nP(n) > 2g + 2$ and, thus, all these curves do not have any involutions defined over $\mathbb{Q}$.

3.2. The non-split Cartan modular curves $X_{ns}(p)$. Here, in order to determine some automorphism groups, we deal with an example to apply Theorem 2.1. This argument is more elaborated than the one presented in the preceding subsection.

Let p be a rational prime and let $X_{ns}(p)$ be the modular curve attached to a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. This curve is a quotient of the modular curve $X(p)$ defined over $\mathbb{Q}$, which has a canonical involution w defined over $\mathbb{Q}$, the so-called modular involution. The genus g of $X_{ns}(p)$ is greater than 1 for $p \geq 11$. In [5], the following is proved

$$\mathrm{Aut}(X_{ns}(11)) = \mathrm{Aut}_{\mathbb{Q}}(X_{ns}(11)) \simeq (\mathbb{Z}/2\mathbb{Z})^2 .$$

In [4], it is proved that for $p \geq 37$ all automorphisms of $X_{ns}(p)$ preserve cusps and, moreover, if $p \equiv 1 \pmod{12}$ then $\mathrm{Aut}(X_{ns}(p)) = \{1, w\}$.

It is expected that $\mathrm{Aut}(X_{ns}(p)) = \{1, w\}$ for $p > 11$. The goal of this subsection is to prove this fact for $13 \leq p \leq 31$. We point out that the genera of these six curves are $8, 15, 20, 35, 54$ and 63.

Set $X_{ns}^+(p) = X_{ns}(p)/\langle w \rangle$ and let us denote by g^+ its genus. For $p \geq 11$, the splitting over $\mathbb{Q}$ of the jacobians of these curves is as follows (cf. [3]):

$$\begin{aligned} J_{ns}(p) := \mathrm{Jac}(X_{ns}(p)) &\overset{\mathbb{Q}}{\sim} \prod_{f \in \mathrm{New}_{p^2}/G_{\mathbb{Q}}} A_f , \\ J_{ns}^+(p) := \mathrm{Jac}(X_{ns}^+(p)) &\overset{\mathbb{Q}}{\sim} \prod_{f \in \mathrm{New}_{p^2}^+/G_{\mathbb{Q}}} A_f . \end{aligned}$$

From now on, χ denotes the quadratic Dirichlet character of conductor p, i.e. the Dirichlet character attached to the quadratic number field $K = \mathbb{Q}(\sqrt{p^*})$, where $p^* = (-1)^{(p-1)/2}p$. Next, we summarize some facts concerning the modular abelian varieties A_f attached to newforms $f \in \mathrm{New}_{p^2}$ (see [6, Section 2] for detailed references).

The map $f \mapsto f \otimes \chi$ is a permutation of the set $\mathrm{New}_{p^2} \cup \mathrm{New}_p$. Under this bijection, there is a unique newform f, up to Galois conjugation, such that $f = f \otimes \chi$ when $p \equiv 3 \pmod 4$ and, moreover, in this case $f \in \mathrm{New}_{p^2}$.

If $f \in \mathrm{New}_{p^2}$ has complex multiplication (CM), i.e. $f = f \otimes \chi$, then the dimension of A_f is the class number of K and A_f has all its endomorphisms defined over the Hilbert class field of K. The endomorphism algebra $\mathrm{End}_K^0(A_f)$ is isomorphic to the CM field $E_f \otimes K$ which only contains the roots of unity ± 1. Moreover, $f \in \mathrm{New}_{p^2}^+$ if, and only if, $p \equiv 3 \pmod 8$.

Let $f = \sum a_n q^n \in \mathrm{New}_{p^2}$ be without CM. If f has an inner twist $\chi' \neq 1$, i.e. $f \otimes \chi' = {}^{\sigma}f$ for some $\sigma \in G_{\mathbb{Q}}$, then $\chi' = \chi$ because χ' must be a quadratic character of conductor dividing p^2. In such a case, $\mathrm{End}^0(A_f) = \mathrm{End}_K^0(A_f)$ is a noncommutative algebra. More precisely, set $F_f := \mathbb{Q}(\{a_\ell^2\})$, with ℓ running over the set of all rational primes. If A_f is simple, then $\mathrm{End}_K^0(A_f)$ is a quaternion algebra $\mathcal{Q}_f$ over F_f (QM case), otherwise A_f is isogenous over K to the square of an abelian variety B_f and $\mathrm{End}_K^0(A_f)$ is isomorphic to the matrix algebra $M_2(F_f)$ (RM case).

If χ is not an inner twist for $f \in \mathrm{New}_{p^2}$, then A_f is simple and $\mathrm{End}^0(A_f)$ is isomorphic to E_f (RM case).

For two distinct $f_1, f_2 \in \mathrm{New}_{p^2}/G_{\mathbb{Q}}$, the abelian varieties A_{f_1} and A_{f_2} are not isogenous over $\mathbb{Q}$ and are isogenous if, and only if, $f_1 \otimes \chi = {}^{\sigma}f_2$ for some $\sigma \in G_{\mathbb{Q}}$. In this particular case, there is an isogeny defined over K.

In the sequel, we restrict our attention to the values $13 \leq p \leq 31$. The next lemma can be obtained through the instruction `BrauerClass` in the program MAGMA.

Lemma 3.1. *For all* $13 \leq p \leq 31$*, there is no* $f \in \mathrm{New}_{p^2}$ *with quaternionic multiplication.*

Let us fix a set $\{f_1, \cdots, f_r\}$ of representative cusp forms for the set $\mathrm{New}_{p^2}/G_{\mathbb{Q}}$. We introduce the subsets $\mathcal{S}_{cm}$, $\mathcal{S}_{rm}$, $\mathcal{S}_s$ and $\mathcal{S}_t$ of $\mathrm{New}_{p^2}/G_{\mathbb{Q}}$ as follows. The subsets $\mathcal{S}_{cm}$ and $\mathcal{S}_{rm}$ are the sets of newforms in $\mathrm{New}_{p^2}/G_{\mathbb{Q}}$ having χ as an inner twist and corresponding to the CM and RM cases respectively. The subsets $\mathcal{S}_s$ and $\mathcal{S}_t$ are defined as follows:

$$\mathcal{S}_s = \{f \in \mathrm{New}_{p^2}/G_{\mathbb{Q}} \colon f \otimes \chi \in \mathrm{New}_p/G_{\mathbb{Q}}\},$$
$$\mathcal{S}_t = \{f_i \in \mathrm{New}_{p^2}/G_{\mathbb{Q}} \colon f_j = f_i \otimes \chi, i < j\}.$$

For $\mathrm{New}^+_{p^2}/G_{\mathbb{Q}}$, we introduce the following four sets

$$\mathcal{S}^+_{cm} = \mathcal{S}_{cm} \cap \mathrm{New}^+_{p^2}, \qquad \mathcal{S}^+_{rm} = \mathcal{S}_{rm} \cap \mathrm{New}^+_{p^2}, \qquad \mathcal{S}^+_s = \mathcal{S}_s \cap \mathrm{New}^+_{p^2},$$

and $\mathcal{S}^+_t = \{f_i \in \mathcal{S}_t \cap \mathrm{New}^+_{p^2} \colon f_i \otimes \chi \in \mathrm{New}^+_{p^2}\}$. Hence, the splitting over K of $J_{ns}(p)$ and $J^+_{ns}(p)$ are

$$J_{ns}(p) \overset{K}{\sim} \prod_{f \in \mathcal{S}_{cm}} A_f \prod_{f \in \mathcal{S}_s} A_f \prod_{f \in \mathcal{S}_{rm}} B_f^2 \prod_{f \in \mathcal{S}_t} A_f^2$$

and

$$J^+_{ns}(p) \overset{K}{\sim} \prod_{f \in \mathcal{S}^+_{cm}} A_f \prod_{f \in \mathcal{S}^+_s} A_f \prod_{f \in \mathcal{S}^+_{rm}} B_f^2 \prod_{f \in \mathcal{S}^+_t} A_f^2.$$

The corresponding decomposition of their endomorphism algebras over K are

$$\mathrm{End}^0_K(J_{ns}(p)) \simeq \prod_{f \in \mathcal{S}_{cm}} E_f \otimes K \prod_{f \in \mathcal{S}_s} E_f \prod_{f \in \mathcal{S}_{rm}} M_2(F_f) \prod_{f \in \mathcal{S}_t} M_2(E_f) \tag{3.1}$$

and

$$\mathrm{End}^0_K(J^+_{ns}(p)) \simeq \prod_{f \in \mathcal{S}^+_{cm}} E_f \otimes K \prod_{f \in \mathcal{S}^+_s} E_f \prod_{f \in \mathcal{S}^+_{rm}} M_2(F_f) \prod_{f \in \mathcal{S}^+_t} M_2(E_f). \tag{3.2}$$

For $13 \leq p \leq 31$, Table 3.1 shows the description of the sets $\mathrm{New}_{p^2}/G_{\mathbb{Q}}$ and $\mathrm{New}^+_{p^2}/G_{\mathbb{Q}}$ as well as the action of the map $f \mapsto f \otimes \chi$ on the set $(\mathrm{New}_{p^2} \cup \mathrm{New}_p)/G_{\mathbb{Q}}$.

The label of the newforms in New_{p^2} is the one given by MAGMA. For a prime p, the set $\mathcal{S}_s$ is the set of newforms f which do not appear in the columns corresponding to $\mathcal{S}_{rm}$, $\mathcal{S}_{cm}$ and $\mathcal{S}_t$ (twists).

p	$\mathrm{New}_{p^2}/G_{\mathbb{Q}}$	$\dim A_{f_i}$	$\mathcal{S}_{rm}$	$\mathcal{S}_{cm}$	$\mathcal{S}_t$ (twists)	$\mathrm{New}^+_{p^2}/G_{\mathbb{Q}}$
13	f_1, f_2, f_3	$2,\ i=1$ $3,\ 2\le i\le 3$	f_1	$\emptyset$	f_2 $f_3 = f_2\otimes\chi$	f_2
17	$f_1,\cdots,f_6$	$1,\ i=1$ $2,\ 2\le i\le 3$ $3,\ 4\le i\le 5$ $4,\ i=6$	f_6	$\emptyset$	f_2, f_4 $f_3 = f_2\otimes\chi$ $f_5 = f_4\otimes\chi$	f_1, f_2, f_4
19	$f_1,\cdots,f_9$	$1,\ 1\le i\le 2$ $2,\ 3\le i\le 6$ $3,\ 7\le i\le 8$ $4,\ i=9$	f_9	f_1	f_3, f_5, f_7 $f_4 = f_3\otimes\chi$ $f_6 = f_5\otimes\chi$ $f_8 = f_7\otimes\chi$	f_1, f_7, f_9
23	$f_1,\cdots,f_{10}$	$2,\ 1\le i\le 5$ $3,\ i=6$ $4,\ 7\le i\le 8$ $5,\ 9\le i\le 10$	f_7, f_8	f_6	f_1, f_4, f_9 $f_2 = f_1\otimes\chi$ $f_5 = f_4\otimes\chi$ $f_{10} = f_9\otimes\chi$	f_7, f_8, f_9
29	$f_1,\cdots,f_{11}$	$2,\ 1\le i\le 4$ $3,\ 5\le i\le 6$ $6,\ 7\le i\le 8$ $8,\ 9\le i\le 10$ $12,\ i=11$	f_3, f_{11}	$\emptyset$	f_1, f_5, f_7, f_9 $f_4 = f_1\otimes\chi$ $f_6 = f_5\otimes\chi$ $f_8 = f_7\otimes\chi$ $f_{10} = f_9\otimes\chi$	$f_1, f_2, f_5,$ f_6, f_7, f_9
31	$f_1,\cdots,f_{12}$	$2,\ 1\le i\le 6$ $3,\ i=7$ $4,\ i=8$ $8,\ 9\le i\le 10$ $12,\ i=11$ $16,\ i=12$	f_5, f_8, f_{11}, f_{12}	f_7	f_1, f_2, f_9 $f_4 = f_1\otimes\chi$ $f_6 = f_2\otimes\chi$ $f_{10} = f_9\otimes\chi$	$f_1, f_2,$ f_9, f_{12}

Table 3.1.

Proposition 3.2. *Let p be a prime such that $13 \le p \le 31$. Then*

(1) *The group $\mathrm{Aut}(X^+_{ns}(p))$ is trivial.*
(2) *The modular involution w is the only nontrivial automorphism of $X_{ns}(p)$.*

Proof. For $p = 13$, we already know that $\mathrm{Aut}(X^+_{ns}(13))$ is trivial because the curve $X^+_{ns}(13)$ is not hyperelliptic (cf. [2]) and the endomorphism algebra $\mathrm{End}^0(J^+_{ns}(13))$ is a totally real number field which only contains the roots of unity ± 1.

We split the proof into the following steps.

Step 1: All automorphisms of $X_{ns}(p)$ and $X^+_{ns}(p)$ are defined over the quadratic field K. On the one hand, for two distinct f_1, f_2 lying in $\mathrm{New}_{p^2}/G_{\mathbb{Q}}$, without CM, A_{f_1} and A_{f_2} are isogenous if, and only if, f_2 is a Galois conjugate of $f_1\otimes\chi$ and, in this case, the isogeny is defined over K. On the other hand, if $f \in \mathrm{New}_{p^2}/G_{\mathbb{Q}}$ does not have CM, all endomorphisms of A_f are

defined over K. Hence, if $\mathrm{New}_{p^2}/G_{\mathbb{Q}}$, resp. $\mathrm{New}^+_{p^2}/G_{\mathbb{Q}}$, does not contain a newform with CM, all endomorphisms of $J_{ns}(p)$, resp. $J^+_{ns}(p)$, are defined over K and, in particular, so are all automorphisms of the corresponding curve.

Assume that $\mathrm{New}_{p^2}/G_{\mathbb{Q}}$, resp $\mathrm{New}^+_{p^2}/G_{\mathbb{Q}}$, contains a newform f with CM. Then all endomorphisms of A_f are defined over the Hilbert class field of K and A_f is unique. Let g_c be the dimension of the abelian variety A_f. Due to the fact that $g > 1 + 2g_c$ ($p \equiv 3 \pmod 4$), resp. $g^+ > 1 + 2g_c$ ($p \equiv 3 \pmod 8$), the non-existence of an automorphism not defined over K is obtained by applying the same argument used in the proof of Lemma 1.4 in [7]. □

Step 2: The only primes N which can divide the order of a nontrivial automorphism of $X_{ns}(p)$ or $X^+_{ns}(p)$ are the displayed in the following tables

(3.3)

$X_{ns}(p)$:

p	N
13	$2, 3, 7$
17	$2, 3$
19	$2, 3, 5$
23	$2, 3, 11$
29	$2, 3, 5, 7$
31	$2, 3, 5$

,

$X^+_{ns}(p)$:

p	N
13	2
17	2
19	$2, 3, 5$
23	$2, 3$
29	$2, 3, 7$
31	$2, 3$

The number fields which appear in the decomposition of $\mathrm{End}^0_K(J_{ns}(p))$ (see (3.1)), resp. $\mathrm{End}^0_K(J^+_{ns}(p))$ (see (3.2)), only contain the roots of unity ± 1. The only matrix algebras in this decomposition are of the form $M_2(F)$ for $f \in \mathcal{S}_{rm}$ and $f \in \mathcal{S}_t$ for $J_{ns}(p)$, resp. $f \in \mathcal{S}^+_{rm}$ and $f \in \mathcal{S}^+_t$ for $J^+_{ns}(p)$. In the first case, $F = F_f$ and, in the second case, $F = E_f$. In any case, F is a totally real number field. If there exists a nontrivial automorphism of order an odd prime N, then the maximal real subfield K_N of the N-th cyclotomic field must be contained in some of these number fields F. In particular, $N - 1$ must divide $2[F : \mathbb{Q}]$. By looking at the following tables, obtained from Table 3.1,

$X_{ns}(p)$:

p	$[F : \mathbb{Q}]$
13	$1, 3$
17	$2, 3$
19	$2, 3$
23	$2, 5$
29	$1, 2, 3, 6, 8$
31	$1, 2, 6, 8$

,

$X^+_{ns}(p)$:

p	$[F : \mathbb{Q}]$
13	$-$
17	$-$
19	2
23	2
29	3
31	8

,

we obtain a few possibilities for N. After checking all of them, we obtain that the only cases in which K_N is contained in some F are the displayed in (3.3). □

Step 3: There are no automorphisms of $X_{ns}(p)$ and $X_{ns}^+(p)$ of odd order. The claim is obtained applying Theorem 2.1 to the curves $X_{ns}(p)\otimes\mathbb{F}_\ell$ and $X_{ns}^+(p)\otimes\mathbb{F}_\ell$, where ℓ is a prime splitting in K, and for all $N^m=N$ as in (3.3). We only show the case $N=3$:

p	ℓ	$X_{ns}(p)\otimes\mathbb{F}_\ell : \sum_{3\nmid n} n\,P(n)$	B	$X_{ns}^+(p)\otimes\mathbb{F}_\ell : \sum_{3\nmid n} n\,P(n)$	B
13	3	$\sum_{3\nmid n,n\le 4} n\,P(n)=13$	10	$-$	
17	2	$\sum_{3\nmid n,n\le 11} n\,P(n)=27$	17	$-$	
19	5	$\sum_{3\nmid n,n\le 8} n\,P(n)=29$	22	$\sum_{3\nmid n,n\le 7} n\,P(n)=13$	10
23	2	$\sum_{3\nmid n,n\le 10} n\,P(n)=51$	33	$\sum_{3\nmid n,n\le 7} n\,P(n)=28$	15
29	5	$\sum_{3\nmid n,n\le 11} n\,P(n)=59$	56	$\sum_{3\nmid n,n\le 11} n\,P(n)=30$	26
31	2	$\sum_{3\nmid n,n\le 14} n\,P(n)=67$	65	$\sum_{3\nmid n,n\le 13} n\,P(n)=69$	30

where B denotes the upper bound for $\sum_{3\nmid n} n\,P(n)$ provided by Theorem 2.1. □

Step 4: The group $\mathrm{Aut}(X_{ns}^+(p))$ *is trivial.* We only need to prove that $X_{ns}^+(p)$ does not have any involutions defined over K. Again, the claim is obtained applying Theorem 2.1 to the curves $X=X_{ns}^+(p)\otimes\mathbb{F}_\ell$ for $p\neq 19$ and $X=X_{ns}^+(p)\otimes\mathbb{F}_{\ell^2}$ for $p=19$, and $N^m=2$:

p	ℓ	$\sum_{2\nmid,n} n\,P(n)$	$B=2\,g^+ +2$
17	2	$\sum_{2\nmid,n\le 9} n\,P(n)=22$	14
19	2	$\sum_{2\nmid,n\le 9} n\,P(n)=17$	16
23	2	$\sum_{2\nmid,n\le 17} n\,P(n)=37$	28
29	5	$\sum_{2\nmid,n\le 21} n\,P(n)=58$	50
31	2	$\sum_{2\nmid,n\le 27} n\,P(n)=68$	58

For $p=19$, we have changed the prime $\ell=5$ by $\ell=2$ (2 is inert in K), because for $\ell=5$ the sequence $n\,P(n)$ turns out to be equal to 0 for $8\le n\le 200$. □

Step 5: The modular involution w is the only nontrivial automorphism of $X_{ns}(p)$. A nontrivial automorphism different from w does not commute with w because the group $\mathrm{Aut}(X_{ns}^+(p))$ is trivial. Assume that there is a nontrivial automorphism u of $X_{ns}(p)$ different from w. Since the order of $\mathrm{Aut}_K(X_{ns}(p))$ is a power of 2, we can suppose that u is an involution different from w. The automorphism $v=u\cdot w$ cannot be an involution, otherwise u and w would commute. Therefore, either v or a power of v has order 4.

Now, applying Theorem 2.1 to $X = X_{ns}(p) \otimes \mathbb{F}_\ell$ for $N^m = 4$ and $p \neq 13, 19$, we obtain

p	ℓ	$\sum_n n(L(n)D(n) - Pn)$	$B = 2g + 6$
17	2	$\sum_{n\leq 9} n(L(n)D(n) - Pn) = 44$	36
23	2	$\sum_{n\leq 17} n(L(n)D(n) - Pn) = 76$	68
29	5	$\sum_{n\leq 21} n(L(n)D(n) - Pn) = 130$	114
31	2	$\sum_{n\leq 27} n(L(n)D(n) - Pn) = 136$	132

Hence, for these four values of p the statement is proved. For $p = 13$ or 19, the sequence $n(L(n)D(n) - Pn)$ turns out to be equal to 0 for $9 < n \leq 250$, even changing the prime ℓ. Nevertheless, applying Theorem 2.1 for $N^m = 8$, we prove that $X_{ns}(13)$ an $X_{ns}(19)$ do not have any automorphisms of order 8:

p	ℓ	$\sum_n n(L(n)D(n) - Pn)$	$B = 2g + 14$
13	3	$\sum_{n\leq 7} n(L(n)D(n) - Pn) = 56$	40
19	5	$\sum_{n\leq 5} n(L(n)D(n) - Pn) = 80$	54

Therefore, the order of any automorphism of $X_{ns}(p)$ must divide 4. Assume that there is $v \in \mathrm{Aut}(X_{ns}(p))$ of order 4. Then, the automorphism $u := v^2 \cdot w$ can only have order 2 or 4. On the one hand, u cannot be an involution since v^2 and w do not commute. On the other hand, if u has order 4, then u^2 is an involution different from w and, thus, $u^2 \cdot w = v^2 \cdot w \cdot v^2$ must have order 4, but $(u^2 \cdot w)^2 = 1$. Therefore, neither of these two curves has automorphisms of order 4. □

References

[1] M. Baker & Y. Hasegawa, "Automorphisms of $X_0^*(p)$", *J. Number Theory* **100** (2003), no. 1, p. 72-87.

[2] B. Baran, "Normalizers of non-split Cartan subgroups, modular curves, and the class number one problem", *J. Number Theory* **130** (2010), no. 12, p. 2753-5772.

[3] I. Chen, "The Jacobians of non-split Cartan modular curves", *Proc. Lond. Math. Soc.* **77** (1998), no. 1, p. 1-38.

[4] V. Dose, "On the automorphisms of the non-split Cartan modular curves of prime level", *Nagoya Math. J.* **224** (2016), no. 1, p. 74-92.

[5] V. Dose, J. Fernández, J. González & R. Schoof, "The automorphism group of the non-split Cartan modular curve of level 11", *J. Algebra* **417** (2014), p. 95-102.

[6] J. González, "Automorphism group of split Cartan modular curves", *Bull. Lond. Math. Soc.* **48** (2016), no. 4, p. 628-636.

[7] M. Kenku & F. Momose, "Automorphism groups of the modular curves $X_0(N)$", *Compos. Math.* **65** (1988), no. 1, p. 51-80.

[8] Q. Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, 2002, xv+576 pages.

[9] H. Stichtenoth, "Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. I. Eine Abschätzung der Ordnung der Automorphismengruppe", *Arch. Math.* **24** (1973), p. 527-544.

Josep González
Departament de Matemàtiques
Universitat Politècnica de Catalunya
EPSEVG, Avinguda Víctor Balaguer 1
E-08800 Vilanova i la Geltrú, Catalonia, Spain
E-mail: josep.gonzalez@upc.edu