

ON THE AUTOMORPHISMS OF THE NONSPLIT CARTAN MODULAR CURVES OF PRIME LEVEL

VALERIO DOSE

Abstract. We study the automorphisms of the nonsplit Cartan modular curves $X_{\text{ns}}(p)$ of prime level p . We prove that if $p \geq 29$ all the automorphisms preserve the cusps. Furthermore, if $p \equiv 1 \pmod{12}$ and $p \neq 13$, the automorphism group is generated by the modular involution given by the normalizer of a nonsplit Cartan subgroup of $\text{GL}_2(\mathbb{F}_p)$. We also prove that for every $p \geq 29$ the existence of an exceptional rational automorphism would give rise to an exceptional rational point on the modular curve $X_{\text{ns}}^+(p)$ associated to the normalizer of a nonsplit Cartan subgroup of $\text{GL}_2(\mathbb{F}_p)$.

Introduction

Modular curves can be constructed as compactifications of certain quotients of the upper half complex plane. When the genus exceeds 1, it is a classical question to ask if all of their automorphisms are induced by an automorphism of the upper half complex plane. Here we make some progress toward answering this question for nonsplit Cartan modular curves.

Let N be a positive integer and let H be a subgroup of $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ with the property that the determinant homomorphism from H to $\mathbb{Z}/N\mathbb{Z}^*$ is surjective. We write X_H for the modular curve over \mathbb{Q} associated to the subgroup H . Let Γ_H be the subgroup of $\text{SL}_2(\mathbb{Z})$ made up of the elements which reduce modulo N to an element in H . The complex points of X_H can be identified with the orbit space $\mathcal{H} \cup \mathbb{Q} \cup \{\infty\} / \Gamma_H$, where \mathcal{H} is the upper half complex plane on which any element of $\text{SL}_2(\mathbb{R})$ acts as a Möbius transformation $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d}$, for every $\tau \in \mathcal{H}$. Let $\text{Norm}(\Gamma_H)$ be the normalizer of Γ_H in $\text{SL}_2(\mathbb{R})$. An element of $\text{Norm}(\Gamma_H)$ induces naturally an automorphism of the curve X_H ; hence the group $B(X_H) \stackrel{\text{def}}{=} \text{Norm}(\Gamma_H) / \Gamma_H$ can be considered as a subgroup of the automorphism group

Received February 28, 2015. Revised September 18, 2015. Accepted September 18, 2015.

2010 Mathematics subject classification. 14G35, 11G05.

L'Autore ha svolto parte di questo lavoro come titolare di un Assegno "Ing. Giorgio Schirillo" dell'Istituto Nazionale di Alta Matematica.

© 2016 by The Editorial Board of the *Nagoya Mathematical Journal*

$\text{Aut}(X_H)$ of X_H . We call an element of $B(X_H)$ a *modular automorphism* of X_H . A nonmodular automorphism is also called *exceptional*.

If H is a Borel subgroup of $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$, the curve X_H is the classical modular curve $X_0(N)$ and Γ_H is the classical congruence subgroup $\Gamma_0(N)$. For every positive integer N , the automorphism group of $X_0(N)$ has been determined in [Ogg77, KM88, Elk90, Har11], and if the genus of $X_0(N)$ is at least 2 and $N \neq 37, 63, 108$, we have $\text{Aut}(X_0(N)) = B(X_0(N))$. If we take $N = p$ a prime number, the group $B(X_0(p))$ is generated by the Atkin–Lehner involution w_p . The automorphism group of $X_0^*(p) \stackrel{\text{def}}{=} X_0(p)/\langle w_p \rangle$ has been determined in [BH03] and it is trivial when the genus exceeds 2. When $X_0^*(p)$ has genus 2, the curve $X_0^*(p)$ is hyperelliptic, so it must admit an involution.

In this paper, we concentrate on the case of H being a nonsplit Cartan subgroup of $\text{GL}_2(\mathbb{F}_p)$, and we write $X_{\text{ns}}(p)$ for the modular curve associated to H . This curve always has a modular involution w , because of the fact that a nonsplit Cartan subgroup of $\text{GL}_2(\mathbb{F}_p)$ has index 2 in its normalizer. We have $B(X_{\text{ns}}(p)) = \langle w \rangle$ (see Section 3). Let $X_{\text{ns}}^+(p) \stackrel{\text{def}}{=} X_{\text{ns}}(p)/\langle w \rangle$ be the modular curve associated to the normalizer of a nonsplit Cartan subgroup of $\text{GL}_2(\mathbb{F}_p)$. The curve $X_{\text{ns}}(p)$ has genus smaller than 2 when $p \leq 7$. The same happens for $X_{\text{ns}}^+(p)$ when $p \leq 11$. It is not true that $\text{Aut}(X_{\text{ns}}(p)) = \langle w \rangle$ whenever the genus is at least 2. For example, the automorphism group of $X_{\text{ns}}(11)$, determined in [DFGS14], is the Klein four group generated by w and an exceptional involution.

Here, extending techniques of [Ogg74, KM88, BH03], we prove the following

THEOREM 1.1. *If $p \geq 11$ the modular curve $X_{\text{ns}}(p)$ is not hyperelliptic. If $p \geq 13$ the modular curve $X_{\text{ns}}^+(p)$ is not hyperelliptic.*

We remark that this result already follows directly from [Abr96, Theorem 0.1] for $X_{\text{ns}}(p)$ when $p \geq 23$ and for $X_{\text{ns}}^+(p)$ when $p \geq 29$.

THEOREM 5.2. *If $p \geq 29$, all the automorphisms of $X_{\text{ns}}(p)$ preserve the cusps. If $p \equiv 1 \pmod{12}$ and $p \neq 13$, the automorphism group of $X_{\text{ns}}(p)$ is generated by the modular involution w .*

Some of the techniques used in this paper also apply to $X_{\text{ns}}^+(p)$, but the main result does not seem to be reachable right away. In general, one can expect the automorphism group of $X_{\text{ns}}(p)$ to be generated by the modular involution w and the automorphism group of $X_{\text{ns}}^+(p)$ to be trivial for $p \geq 13$.

The interest in nonsplit Cartan modular curves comes mainly from Serre's uniformity conjecture, which is an important statement regarding Galois representations attached to elliptic curves. It is equivalent to assert that for almost all p and for every maximal subgroup H of $\mathrm{GL}_2(\mathbb{F}_p)$, the modular curve X_H has no rational points except the cusps and the points associated to elliptic curves with complex multiplication, usually called CM points. The only case left to prove, concerns modular curves associated to the normalizer of a nonsplit Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$.

We prove the following statement relating the existence of exceptional automorphisms of $X_{\mathrm{ns}}(p)$ with the existence of non-CM rational points on $X_{\mathrm{ns}}^+(p)$.

THEOREM 5.3. *Let $p \geq 29$. If there exists an exceptional automorphism of $X_{\mathrm{ns}}(p)$ defined over \mathbb{Q} , then $X_{\mathrm{ns}}^+(p)$ has a non-CM rational point.*

Therefore, Serre's uniformity conjecture implies the nonexistence of rational exceptional automorphisms of $X_{\mathrm{ns}}(p)$ for almost all p .

§1. Hyperelliptic modular curves of type $X_{\mathrm{ns}}(p)$ and $X_{\mathrm{ns}}^+(p)$

Let p be a prime number. We recall that the modular curve $X_{\mathrm{ns}}(p)$ has genus 0 for $p \leq 5$ and is elliptic only for $p = 7$. The modular curve $X_{\mathrm{ns}}^+(p)$ has genus 0 for $p \leq 7$ and is elliptic only for $p = 11$ [Bar10].

THEOREM 1.1. *If $p \geq 11$ the modular curve $X_{\mathrm{ns}}(p)$ is not hyperelliptic. If $p \geq 13$ the modular curve $X_{\mathrm{ns}}^+(p)$ is not hyperelliptic.*

Proof. (Following [Ogg74, p. 455, Theorem 3]). Let $q \neq p$ be a prime number, let \mathbb{F}_q be the finite field with q elements and let $\overline{\mathbb{F}_q}$ be an algebraic closure. The points of $X_{\mathrm{ns}}(p)(\overline{\mathbb{F}_q})$ parametrize pairs (E, φ) , where E is an elliptic curve over $\overline{\mathbb{F}_q}$ and φ is an isomorphism from the p -torsion points of E to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Moreover, two pairs (E, φ) , (E', φ') are parametrized by the same point of $X_{\mathrm{ns}}(p)(\overline{\mathbb{F}_q})$ if and only if there exist an isomorphism f from E to E' such that, on the p -torsion of E , we have $\varphi' \circ f = M \circ \varphi$, where M is a generator of a nonsplit Cartan subgroup C of $\mathrm{GL}_2(\mathbb{F}_p)$. The Frobenius automorphism σ generating $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_{q^2})$ acts on $X_{\mathrm{ns}}(p)(\overline{\mathbb{F}_q})$ as $\sigma(E, \varphi) = (E^\sigma, \varphi \circ \sigma^{-1})$, so that every elliptic curve E over \mathbb{F}_{q^2} gives a point (E, φ) in $X_{\mathrm{ns}}(p)(\mathbb{F}_{q^2})$ if and only if $\varphi \circ \sigma^{-1} \circ \varphi^{-1}$ is contained in C .

Take a supersingular elliptic curve E over $\overline{\mathbb{F}_q}$. This means that the q -torsion of E is trivial, that the endomorphism algebra $\mathrm{End}(E)$ is an order in a quaternion algebra, and implies that E can be defined over

\mathbb{F}_{q^2} [Sil09, p. 144, Theorem 3.1, (a)]. The fact that multiplication by q is purely inseparable implies that the q^2 th power Frobenius endomorphism φ_{q^2} and multiplication by q differ by an automorphism of E , which means that $\varphi_{q^2} = \zeta q$ in $\text{End}(E)$ and ζ is a root of unity. If $j \neq 0, 1728$, we have $\varphi_{q^2} = \pm q$. If $j = 0, 1728$, the elliptic curve E is isomorphic over $\overline{\mathbb{F}_q}$ to a curve E' defined over \mathbb{F}_q with equation $y^2 + y = x^3$ or $y^2 = x^3 - x$. We have $\#E'(\mathbb{F}_q) = q + 1$ ([Sil09, p. 154, Exercise 5.10, (b)] when $q \geq 5$, a direct count when $q = 2, 3$). Hence the q th power Frobenius endomorphism of E' has characteristic polynomial $x^2 + q = 0$ which implies that $\varphi_{q^2} = -q$ in $\text{End}(E)$.

This shows that every supersingular elliptic curve over $\overline{\mathbb{F}_q}$ is isomorphic to a supersingular elliptic curve E defined over \mathbb{F}_{q^2} , with the property that φ_{q^2} acts on the p -torsion points as multiplication by q or $-q$. Which says that φ_{q^2} acts on the p -torsion of E as a scalar matrix of $\text{GL}_2(\mathbb{F}_p)$ and therefore as an element contained in every conjugate of the nonsplit Cartan subgroup C in $\text{GL}_2(\mathbb{F}_p)$. Hence, E gives a point in $X_{\text{ns}}(p)(\mathbb{F}_{q^2})$ for each conjugate of C in $\text{GL}_2(\mathbb{F}_p)$, up to automorphisms of E , in the sense that a pair (E, φ) gives the same point on $X_{\text{ns}}(p)$ as $(E, \varphi \circ f)$ for any automorphism f of E . Among the automorphisms of any supersingular elliptic curve, we have multiplication by -1 , which acts on torsion points as an element contained in C . Thus, since the index of a nonsplit Cartan subgroup in $\text{GL}_2(\mathbb{F}_p)$ is equal to $p(p - 1)$, we have the following inequality

$$\#X_{\text{ns}}(p)(\mathbb{F}_{q^2}) \geq p(p - 1) \cdot 2 \cdot \sum_{\substack{E \text{ over } \overline{\mathbb{F}_q} \\ \text{supersingular}}} \frac{1}{\#\text{Aut}(E)} = \frac{p(p - 1)(q - 1)}{12},$$

where in the last equality we used the Deuring–Eichler formula [Sil09, p. 154, Exercise 5.9]

$$\sum_{\substack{E \text{ over } \overline{\mathbb{F}_q} \\ \text{supersingular}}} \frac{1}{\#\text{Aut}(E)} = \frac{q - 1}{24}.$$

Note that this lower bound on the number of supersingular points can also easily be deduced from [BGJGP05, Lemmas 3.20 and 3.21].

Suppose now that $X_{\text{ns}}(p)$ is hyperelliptic. Then we have

$$\frac{p(p - 1)(q - 1)}{12} \leq \#X_{\text{ns}}(p)(\mathbb{F}_{q^2}) \leq 2(q^2 + 1),$$

where the second inequality holds because $X_{\text{ns}}(p)$ is hyperelliptic and because the projective line over \mathbb{F}_{q^2} has exactly $q^2 + 1$ points. Now, putting $q = 2$ we have

$$\frac{p(p-1)}{12} \leq \#X_{\text{ns}}(p)(\mathbb{F}_4) \leq 10$$

and we obtain $p \leq 11$ which ends the proof for $X_{\text{ns}}(p)$ in the case $p \geq 13$. With an analogous reasoning, taking into account that the index of the normalizer of a nonsplit Cartan subgroup in $\text{GL}_2(\mathbb{F}_p)$ is equal to $\frac{p(p-1)}{2}$, we obtain the statement for $X_{\text{ns}}^+(p)$ in the case $p \geq 17$.

The case $p = 11$ for $X_{\text{ns}}(p)$ and the case $p = 13$ for $X_{\text{ns}}^+(p)$ can be worked out by explicitly counting the points over \mathbb{F}_4 of the respective curves. Recall that the Jacobian of $X_{\text{ns}}(p)$ is isogenous to the new part of the Jacobian of $X_0(p^2)$ and the Jacobian of $X_{\text{ns}}^+(p)$ is isogenous to the new part of the Jacobian of $X_0^*(p^2) \stackrel{\text{def}}{=} X_0(p^2)/\langle w_{p^2} \rangle$, where w_{p^2} is the Atkin–Lehner involution [Che98, dSE00]. Then we can count the points over \mathbb{F}_4 by looking at the roots of the characteristic polynomial of a Frobenius at 2 on the Jacobian of $X_0(p^2)$, and using the well-known formula

$$\#C(\mathbb{F}_{q^r}) = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r$$

where C is a nonsingular projective curve of genus g over the finite field \mathbb{F}_q with q prime, and the α_i 's are the roots of the characteristic polynomial of the Frobenius automorphism at q , acting on the Jacobian variety of C .

Looking at the tables in [Ste12] of weight-2 newforms for $\Gamma_0(121)$, we see that the Jacobian of $X_{\text{ns}}(11)$ is isogenous to the product of four elliptic curves for which the traces of a Frobenius automorphism at 2 are respectively $-1, 0, 1, 2$, so that the roots of the characteristic polynomial of a Frobenius at 2 acting on the Jacobian of $X_{\text{ns}}(11)$ are $\frac{-1 \pm \sqrt{-7}}{2}, \pm\sqrt{-2}, \frac{1 \pm \sqrt{-7}}{2}, 1 \pm i$. Hence $\#X_{\text{ns}}(11)(\mathbb{F}_4) = 15 > 10$.

Now, in the same tables, we look at the weight-2 newforms for $\Gamma_0(169)$. We see that the Jacobian of $X_{\text{ns}}^+(13)$ is isogenous to a simple abelian variety A over \mathbb{Q} of dimension 3. The eigenvalues of the Hecke operator T_2 acting on A are the roots a_i , with $i = 1, 2, 3$, of the polynomial $x^3 + 2x^2 - x - 1$. Then the characteristic polynomial of a Frobenius at 2 is the product

$$\prod_{i=1}^3 (x^2 - a_i x + 2).$$

It allows us to compute $\#X_{\text{ns}}^+(13)(\mathbb{F}_4) = 11 > 10$. □

§2. Endomorphisms of the Jacobian variety of $X_{\text{ns}}(p)$

In this section, for any abelian variety A over a field K , an endomorphism of A is an endomorphism defined over an algebraic closure \overline{K} of K , and we write $\text{End}(A)$ for the ring of endomorphisms of A defined over \overline{K} . The endomorphism algebra $\text{End}(A) \otimes \mathbb{Q}$ is an invariant of the isogeny class of A over \overline{K} . The minimal field where every endomorphism of A is defined is an invariant of the isogeny class over K of A . We say that A is of CM-type if $\text{End}(A) \otimes \mathbb{Q}$ contains a commutative semisimple \mathbb{Q} -algebra of dimension equal to $2 \cdot \dim A$.

PROPOSITION 2.1. *Let A be a semistable abelian variety over a field K , complete with respect to a discrete valuation. Then every endomorphism of A is defined over an unramified extension of K .*

Proof. [Rib75, p. 556, Theorem 1.1]. □

PROPOSITION 2.2. *Let A be an abelian variety over a field K . Let E be a subalgebra of $\text{End}_K(A) \otimes \mathbb{Q}$ such that $[E : \mathbb{Q}] = \dim A$ and suppose that E is a product $E_1 \times \cdots \times E_t$ of totally real number fields. This gives rise to a decomposition $A \sim A_1 \times \cdots \times A_t$ of abelian varieties up to isogeny over K . Suppose that no factor A_i is of CM-type. Then E is its own commutant in $\text{End}(A) \otimes \mathbb{Q}$ and every endomorphism of A is defined over a compositum of quadratic extensions of K .*

Proof. [Rib75, p. 557, Theorem 2.3] □

Let $J_0(N)$ be the Jacobian variety of the modular curve $X_0(N)$. It is an abelian variety over \mathbb{Q} .

PROPOSITION 2.3. *The abelian variety $J_0(N)$ is semistable at each prime p such that p^2 does not divide N .*

Proof. [DR73, p. 286, Theorem 6.9]. □

For every integer $N > 0$, there exists a set of representatives f_1, \dots, f_t of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -conjugacy classes of normalized weight-2 cuspforms for $\Gamma_0(N)$, such that every f_i is a newform at some level M_i dividing N , and $\{f_i(n\tau), n|N/M_i, i = 1 \dots t\}$ with their $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -conjugates form a basis of the complex vector space of weight-2 cuspforms for $\Gamma_0(N)$. There is a decomposition of abelian varieties up to isogeny over \mathbb{Q}

$$(2.1) \quad J_0(N) \sim A_1^{m_1} \times \cdots \times A_t^{m_t}$$

where $A_i \stackrel{\text{def}}{=} A_{f_i}$ is the abelian variety up to isogeny over \mathbb{Q} associated to the $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -conjugacy class of f_i , and m_i is the number of divisors of N/M_i (see [DS05, §6.6]). Every A_i is a simple abelian variety over \mathbb{Q} .

Let $J_0^C(N)$ be the abelian variety up to isogeny over \mathbb{Q} which is a product of the factors $A_i^{m_i}$ such that A_i is of CM-type and let $J_0^H(N)$ be the product of the remaining factors of the decomposition above. We recall here that if A_i is of CM-type, then it is isogenous (over $\overline{\mathbb{Q}}$) to a product of copies of an elliptic curve with complex multiplication by an imaginary quadratic field K of discriminant $-D$ and f_i is a weight-2 cuspform for $\Gamma_0(D \cdot N(\mathfrak{c}))$, where \mathfrak{c} is the conductor of a primitive Hecke character of K (see [Shi72, p. 138, Proposition 1.6], [Shi71]). Any factor A_i of $J_0^H(N)$ cannot be isogenous to any factor A_j of $J_0^C(N)$ because A_i and A_j have different endomorphism algebras. Hence, we have $J_0(N) \sim J_0^H(N) \times J_0^C(N)$ and $\text{End}(J_0(N)) \otimes \mathbb{Q} \cong (\text{End}(J_0^H(N)) \otimes \mathbb{Q}) \times (\text{End}(J_0^C(N)) \otimes \mathbb{Q})$.

Let p be an odd prime number. We call $K(p) = \mathbb{Q}(\sqrt{p})$ if $p \equiv 1 \pmod{4}$ and $K(p) = \mathbb{Q}(\sqrt{-p})$ if $p \equiv 3 \pmod{4}$.

PROPOSITION 2.4. *Every endomorphism of $J_0^H(p^2)$ is defined over $K(p)$.*

Proof. Proposition 2.2 tells us that endomorphisms of $J_0^H(p^2)$ can be defined over a field K which is a compositum of quadratic extensions of \mathbb{Q} . Furthermore, Propositions 2.1 and 2.3 imply that K can be taken unramified outside p . Thus, we can take $K = \mathbb{Q}(\sqrt{p})$ if $p \equiv 1 \pmod{4}$ and $K = \mathbb{Q}(\sqrt{-p})$ if $p \equiv 3 \pmod{4}$. □

Let $g_0(N)$, $g_0^H(N)$, $g_0^C(N)$ be respectively the dimensions of $J_0(N)$, $J_0^H(N)$, $J_0^C(N)$.

Let $J_{\text{ns}}(p)$ be the Jacobian of the modular curve $X_{\text{ns}}(p)$. The abelian variety $J_{\text{ns}}(p)$ is isogenous over \mathbb{Q} to the new part of $J_0(p^2)$ (see [Che98, dSE00]). Let $J_0^{\text{new}}(p^2)$ and $J_0^{\text{old}}(p^2)$ be respectively the new and the old part of $J_0(p^2)$ and let us fix an isomorphism φ from $\text{End}(J_{\text{ns}}(p)) \otimes \mathbb{Q}$ to $\text{End}(J_0^{\text{new}}(p^2)) \otimes \mathbb{Q}$. We say, with abuse of notation, that an automorphism v of $X_{\text{ns}}(p)$, induces the invertible element $v \stackrel{\text{def}}{=} \varphi(v)$ of

$$\begin{aligned} \text{End}(J_0^{\text{new}}(p^2)) \otimes \mathbb{Q} &\subset (\text{End}(J_0^{\text{new}}(p^2)) \otimes \mathbb{Q}) \times (\text{End}(J_0^{\text{old}}(p^2)) \otimes \mathbb{Q}) \\ &\subset \text{End}(J_0(p^2)) \otimes \mathbb{Q} \end{aligned}$$

where the first inclusion is given by sending v to the invertible element that acts like v on the new part and as the identity on the old part.

We can then define in an analogous way $J_{\text{ns}}^H(p)$, $J_{\text{ns}}^C(p)$, as factors of the new part of the decomposition (2.1). We also define the dimensions $g_{\text{ns}}(p)$, $g_{\text{ns}}^H(p)$, $g_{\text{ns}}^C(p)$. We have $J_{\text{ns}}(p) \sim J_{\text{ns}}^H(p) \times J_{\text{ns}}^C(p)$ and $\text{End}(J_{\text{ns}}(p)) \otimes \mathbb{Q} \cong (\text{End}(J_{\text{ns}}^H(p)) \otimes \mathbb{Q}) \times (\text{End}(J_{\text{ns}}^C(p)) \otimes \mathbb{Q})$.

THEOREM 2.5. *If $g_{\text{ns}}(p) > p$ every automorphism of $X_{\text{ns}}(p)$ is defined over $K(p)$.*

Proof. (Following [KM88, p. 55, Lemma 1.4]) Let u be an automorphism of $X_{\text{ns}}(p)$ and σ a element of $\text{Gal}(\overline{\mathbb{Q}}/K(p))$. We define $v = u^\sigma u^{-1}$ and let d be the order of v in the automorphism group of $X_{\text{ns}}(p)$. We call Y the quotient of $X_{\text{ns}}(p)$ by the automorphism v . Let g_Y be the genus of Y . We have that v induces an automorphism of the Jacobian $J_{\text{ns}}(p) \sim J_{\text{ns}}^H(p) \times J_{\text{ns}}^C(p)$ which acts trivially on $J_{\text{ns}}^H(p)$ by Proposition 2.4, because $J_{\text{ns}}^H(p)$ is a factor of $J_0^H(p^2)$. Thus we have the following morphisms of abelian varieties with finite kernel

$$\begin{aligned} J_{\text{ns}}^H(p) &\rightarrow J_{\text{ns}}^H(p) \times J_{\text{ns}}^C(p) \rightarrow J_{\text{ns}}(p) \\ x &\mapsto (x, 0) \end{aligned}$$

where the image of the composition is contained in $J_{\text{ns}}(p)^v \stackrel{\text{def}}{=} \{D \in J_{\text{ns}}(p) : vD = D\}$. Hence there are morphisms of group varieties

$$J_{\text{ns}}^H(p) \longrightarrow J_{\text{ns}}(p)^v \longrightarrow \text{Jac}(Y)$$

where the second map is the push-forward of divisors, and the composition is a morphism of abelian varieties. Furthermore, both maps have finite kernel, hence $g_Y \geq g_{\text{ns}}^H(p)$ and we have by the Riemann–Hurwitz formula

$$g_{\text{ns}}(p) - 1 \geq d(g_Y - 1) \geq 2g_{\text{ns}}^H(p) - 2,$$

where in the second inequality we supposed $d > 1$. Now using $g_{\text{ns}}(p) = g_{\text{ns}}^H(p) + g_{\text{ns}}^C(p)$ we obtain $g_{\text{ns}}(p) \leq 2g_{\text{ns}}^C(p) + 1$. Since $J_{\text{ns}}(p)$ is isogenous over \mathbb{Q} to the new part of $J_0(p^2)$ we have $g_{\text{ns}}^C(p) = g_0^C(p^2)$. Indeed, the old part of $J_0(p^2)$ is isogenous to the product of two copies of the Jacobian of $J_0(p)$ and these cannot have abelian subvarieties of CM-type (see [Shi72, p. 140, Remark 1.7]). Furthermore, $g_0^C(p^2) = 0$ if $p \equiv 1 \pmod{4}$ and $g_0^C(p^2) = h(-p)$ if $p \equiv 3 \pmod{4}$, where $h(-p)$ is the class number of $\mathbb{Q}(\sqrt{-p})$. Indeed, in the decomposition (2.1) with $N = p^2$, if a factor is of CM-type, then it is the product of copies of an elliptic curve with complex multiplication by an

imaginary quadratic field K of discriminant $-p$. This leaves no possibilities if $p \equiv 1 \pmod 4$ and it implies $K = \mathbb{Q}(\sqrt{-p})$ when $p \equiv 3 \pmod 4$. In the latter case the dimension is $h(-p)$ because by the theory of complex multiplication, the elliptic curves with complex multiplication by $\mathbb{Q}(\sqrt{-p})$ are all isogenous, $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -conjugate and their cardinality is $h(-p)$.

Then we can estimate $h(-p)$ using Dirichlet’s class number formula:

$$h(-p) = -\frac{1}{p} \sum_{m=1}^{p-1} m \left(\frac{m}{p}\right) \leq \frac{1}{p} \sum_{m=1}^{p-1} m = \frac{p-1}{2}$$

where the first equality is [Dav80, p. 51, (19)] (we are assuming $p \equiv 3 \pmod 4$ and $p \neq 3$), and in the inequality we used that the Legendre symbol $\left(\frac{m}{p}\right)$ takes values in $\{\pm 1\}$. This implies $g_{\text{ns}}(p) \leq p$. Contradiction. \square

COROLLARY 2.6. *If $p \geq 11$ every automorphism of $X_{\text{ns}}(p)$ is defined over $K(p)$.*

Proof. By [Bar10, Theorem 7.2], we have that $g_{\text{ns}}(p) > p$ for $p \geq 19$. Regarding $p = 13, 17$, they are both congruent to 1 modulo 4, so in these cases $g_{\text{ns}}^C(p) = g_0^C(p^2) = 0$ and we can use Proposition 2.4 together with the isogeny over \mathbb{Q} between $J_{\text{ns}}(p)$ and the new part of $J_0(p^2)$. The automorphisms of $X_{\text{ns}}(11)$ are explicitly computed in [DFGS14] and they are all defined over \mathbb{Q} . \square

The modular curve $X_{\text{ns}}(7)$ has genus 1, and it has the automorphisms defined as translation by points. Thus, in this case there are automorphisms defined over larger number fields.

PROPOSITION 2.7. *If an automorphism of $X_{\text{ns}}(p)$ is defined over \mathbb{Q} , then it induces an element of $\text{End}(J_0^H(p^2)) \otimes \mathbb{Q}$ contained in the Hecke algebra.*

Proof. Since $J_{\text{ns}}(p)$ is isogenous over \mathbb{Q} to the new part of $J_0(p^2)$, an automorphism u of $X_{\text{ns}}(p)$ defined over \mathbb{Q} induces an element of $\text{End}_{\mathbb{Q}}(J_0(p^2)) \otimes \mathbb{Q} \cong (\text{End}_{\mathbb{Q}}(J_{\text{ns}}^H(p)) \otimes \mathbb{Q}) \times (\text{End}_{\mathbb{Q}}(J_{\text{ns}}^C(p)) \otimes \mathbb{Q})$, as explained above. Since $J_0(p^2)$ has good reduction outside p , the reduction modulo l map is injective on the endomorphism ring of $J_0(p^2)$ for every prime number $l \neq p$. Hence, by the Eichler–Shimura relations, u commutes with every Hecke operator T_l with $l \neq p$, because u is defined over \mathbb{Q} . Moreover, the Hecke algebra acting on the new part is generated by the operators T_l with $l \neq p$, thus u commutes with the whole Hecke algebra. Then, to prove the Proposition, we note that

every factor of $J_0^H(p^2)$ is without complex multiplication and so the Hecke algebra is its own commutant in $\text{End}(J_0^H(p^2)) \otimes \mathbb{Q}$ (Proposition 2.2). \square

LEMMA 2.8. *If $g_{\text{ns}}(p) > p$ every automorphism of $X_{\text{ns}}(p)$ defined over \mathbb{Q} commutes with the modular involution w .*

Proof. Let u be an automorphism of $X_{\text{ns}}(p)$ defined over \mathbb{Q} . Then, by the previous Proposition, u and w induce elements in the Hecke algebra of $J_0^H(p^2)$, which is a commutative algebra. Hence, if we define $v = wuw^{-1}w^{-1}$ we have that v induces an invertible element of $\text{End}(J_0(p^2)) \otimes \mathbb{Q}$ which acts trivially on $J_0^H(p^2)$ and $J_{\text{ns}}^H(p)$. Then we can use the same proof as for Theorem 2.5 to see that v is trivial if $g_{\text{ns}}(p) > p$. \square

COROLLARY 2.9. *If $p \geq 11$ every automorphism of $X_{\text{ns}}(p)$ defined over \mathbb{Q} commutes with the modular involution w .*

Proof. As for Corollary 2.6, we have that $g_{\text{ns}}(p) > p$ for $p \geq 19$. Regarding $p = 13, 17$, in these cases $g_{\text{ns}}^C(p) = g_0^C(p^2) = 0$. Moreover, $g_{\text{ns}}(p) \geq 2$, so the natural map from the automorphism group of $X_{\text{ns}}(p)$ to the automorphism group of $J_{\text{ns}}(p)$ is injective [BH03, Lemma 2.1], and we can use Proposition 2.7 together with the fact that the Hecke algebra is commutative. The automorphism group of $X_{\text{ns}}(11)$ is the Klein four group (see [DFGS14]). \square

COROLLARY 2.10. *If $p \geq 11$ every automorphism of $X_{\text{ns}}(p)$ defined over \mathbb{Q} induces an automorphism of $X_{\text{ns}}^+(p)$ defined over \mathbb{Q} .*

§3. Automorphisms of $X_{\text{ns}}(p)$ preserving the cusps

Let X_H be a modular curve. Then the orbit space $\mathcal{H} \cup \mathbb{Q} \cup \{\infty\} / \Gamma_H$ can be identified with $X_H(\mathbb{C})$. Let $E \subset \mathcal{H}$ be the set of ramification points of the natural quotient map $\pi: \mathcal{H} \rightarrow \mathcal{H} / \Gamma_H$. This is a discrete set in \mathcal{H} and it is the counter image of the set of elliptic points in $X_H(\mathbb{C})$. For every $z \in \mathcal{H} \setminus E$ there exists a neighborhood $U \ni z$ such that $\gamma_i(U) \cap \gamma_j(U) = \emptyset$ for every $\gamma_i \neq \pm\gamma_j$ in Γ_H . This means that $\mathcal{H} \setminus E$ is a proper covering space of $X_H(\mathbb{C})$ without the cusps and the elliptic points.

PROPOSITION 3.1. *Let u be an automorphism of X_H . If u preserves the set of cusps and preserves the set of elliptic points of X_H , then u is induced by an automorphism of the Riemann surface \mathcal{H} preserving E .*

Proof. Let C be the set of cusps on X_H . Note that an automorphism u of X_H preserving the cusps and the elliptic points, defines naturally an automorphism of the open Riemann surface $X_H(\mathbb{C}) \setminus (C \cup \pi(E))$. If X_H

has no elliptic points ($E = \emptyset$), then the quotient $\mathcal{H} \rightarrow \mathcal{H}/\Gamma_H \cong X_H(\mathbb{C}) \setminus C$ is the universal cover of $X_H(\mathbb{C}) \setminus C$. Then u automatically lifts to an automorphism of \mathcal{H} . If instead $E \neq \emptyset$, to lift u to $\mathcal{H} \setminus E$, we need the push-forward by $u \circ \pi$ of the fundamental group of $\mathcal{H} \setminus E$ to be contained in its push-forward by π . But this is true because u actually extends to an automorphism of $X_H(\mathbb{C})$ preserving C and $\pi(E)$. Hence u lifts to an automorphism of $\mathcal{H} \setminus E$, which extends uniquely to \mathcal{H} . \square

Let p be a prime number.

PROPOSITION 3.2. *Suppose that the genus of $X_{\text{ns}}(p)$ is at least 2. Let $\Gamma_{\text{ns}}(p)$ be the subgroup of $\text{SL}_2(\mathbb{Z})$ made up of the elements which reduce modulo p to an element in a nonsplit Cartan subgroup of $\text{GL}_2(\mathbb{F}_p)$. Then the subgroup*

$$B(X_{\text{ns}}(p)) = \text{Norm}(\Gamma_{\text{ns}}(p))/\Gamma_{\text{ns}}(p) \subset \text{Aut}(X_{\text{ns}}(p))$$

is generated by the modular involution w .

Proof. Since the genus of $X_{\text{ns}}(p)$ is at least 2, the group $B(X_{\text{ns}}(p))$ must be finite. This means that $\text{Norm}(\Gamma_{\text{ns}}(p))$ is commensurable with $\text{SL}_2(\mathbb{Z})$ in the sense that $\text{Norm}(\Gamma_{\text{ns}}(p)) \cap \text{SL}_2(\mathbb{Z})$ has finite index in both $\text{Norm}(\Gamma_{\text{ns}}(p))$ and $\text{SL}_2(\mathbb{Z})$. Hence $\text{Norm}(\Gamma_{\text{ns}}(p))$ is a group acting on lattices of \mathbb{R}^2 that are commensurable with $\mathbb{Z} \times \mathbb{Z}$, with the action given by right multiplication of row vectors in the lattice. Lattices commensurable with $\mathbb{Z} \times \mathbb{Z}$ are the ones generated by two vectors $(a, b), (c, d)$ with $a, b, c, d \in \mathbb{Q}$, and if we consider them up to multiplication by a scalar (i.e., homothety), they all have a basis of the form $\{(M, \frac{g}{h}), (0, 1)\}$ with $M \in \mathbb{Q}^+, g, h \in \mathbb{Z}, \text{gcd}(g, h) = 1$ and $0 \leq g < h$ (see [Con96] for more details).

Since $\Gamma_{\text{ns}}(p) \subset \Gamma(p) = \{\gamma \in \text{SL}_2(\mathbb{Z}) \text{ s. t. } \gamma \equiv \text{Id} \pmod{p}\}$, the lattices fixed by $\Gamma_{\text{ns}}(p)$ are a subset of the lattices fixed by $\Gamma(p)$. The lattices fixed by $\Gamma(p)$ are those who belong to one of the following type (see [Lan02, Lemma 4.1])

- $M = \frac{1}{p}, h = p, g = 0, \dots, p - 1$, which gives a lattice homothetic to $\langle (1, g), (0, p) \rangle$;
- $M = \frac{1}{p}, h = 1, g = 0$, which gives a lattice homothetic to $\langle (1, 0), (0, p) \rangle$;
- $M = p, h = 1, g = 0$, which gives the lattice $\langle (p, 0), (0, 1) \rangle$;
- $M = 1, h = 1, g = 0$, which gives the lattice $\langle (1, 0), (0, 1) \rangle = \mathbb{Z} \times \mathbb{Z}$.

Recall that $\Gamma_{\text{ns}}(p)$ is the subgroup of $\text{SL}_2(\mathbb{Z})$ made up of the elements γ such that

$$\gamma \equiv \begin{pmatrix} x & \alpha y \\ y & x \end{pmatrix} \pmod{p}$$

for some $(x, y) \in \mathbb{F}_p^2$ and a nonsquare element $\alpha \in \mathbb{F}_p$. Then, a straightforward computation modulo p shows that γ fixes lattices of the first three types, only if $\gamma \in \Gamma(p)$, so that the only lattice up to homothety fixed by $\Gamma_{\text{ns}}(p)$ is $\mathbb{Z} \times \mathbb{Z}$.

The normalizer in $\text{SL}_2(\mathbb{R})$ of $\Gamma_{\text{ns}}(p)$ must preserve, by definition, the set of lattices that are fixed by $\Gamma_{\text{ns}}(p)$. Thus, also $\text{Norm}(\Gamma_{\text{ns}}(p))$ fixes $\mathbb{Z} \times \mathbb{Z}$. The stabilizer of $\mathbb{Z} \times \mathbb{Z}$ is $\text{SL}_2(\mathbb{Z})$, implying $\text{Norm}(\Gamma_{\text{ns}}(p)) \subset \text{SL}_2(\mathbb{Z})$. Therefore, $\text{Norm}(\Gamma_{\text{ns}}(p))$ is made up of the elements of $\text{SL}_2(\mathbb{Z})$ which reduce modulo p to an element in the normalizer of a nonsplit Cartan subgroup of $\text{GL}_2(\mathbb{F}_p)$, which proves the Proposition. \square

COROLLARY 3.3. *Suppose that the genus of $X_{\text{ns}}(p)$ is at least 2. If $p \equiv 1 \pmod{12}$, the only nontrivial automorphism of $X_{\text{ns}}(p)$ preserving the cusps is the modular involution w . If $p \not\equiv 1 \pmod{12}$, the only nontrivial automorphism of $X_{\text{ns}}(p)$ preserving the cusps and the elliptic points, is the modular involution w . The only automorphism of $X_{\text{ns}}^+(p)$ preserving the cusps and the elliptic points is the identity.*

Proof. Let $\Gamma_{\text{ns}}(p)$ be the subgroup of $\text{SL}_2(\mathbb{Z})$ made up of the elements which reduce modulo p to an element in a nonsplit Cartan subgroup of $\text{GL}_2(\mathbb{F}_p)$, so that $X_{\text{ns}}(p)(\mathbb{C}) \cong \mathcal{H} \cup \mathbb{Q} \cup \{\infty\} / \Gamma_{\text{ns}}(p)$. Thus, $X_{\text{ns}}(p)$ has elliptic points if and only if $\Gamma_{\text{ns}}(p)$ contains an element with characteristic polynomial equal to $x^2 + 1$ or $x^2 + x + 1$. Recall that the elements of a nonsplit Cartan subgroup of $\text{GL}_2(\mathbb{F}_p)$ (not belonging to the center) have irreducible characteristic polynomials. If $p \equiv 1 \pmod{4}$ and $p \equiv 1 \pmod{3}$, the two polynomials above have both roots over \mathbb{F}_p . Hence, when $p \equiv 1 \pmod{12}$ there are no elliptic points on $X_{\text{ns}}(p)$. The Corollary then follows from the two previous Propositions. \square

§4. Automorphisms of $X_{\text{ns}}(p)$ not preserving the cusps

Let p be a prime number and l be another prime number different from p . Let T_l be the l th Hecke operator for the modular curve $X_{\text{ns}}(p)$, defined as a modular correspondence (see [Shi58, §2]). Let E be an elliptic curve over \mathbb{C} and let φ be an isomorphism from the p -torsion $E[p]$ of E to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Then the pair (E, φ) gives a point on $X_{\text{ns}}(p)$. Let A be a subgroup of E of order l . Since $l \neq p$, taking the quotient by A on E induces an

isomorphism from the p -torsion of E to the p -torsion of E/A so that φ induces an isomorphism φ_A from the p -torsion of E/A to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. The operator T_l acts on a noncuspidal point of $X_{\text{ns}}(p)$ in the following way

$$T_l(E, \varphi) = \sum_{\substack{A \subset E(\mathbb{C}) \\ \#A=l}} (E/A, \varphi_A)$$

and it induces an element in the endomorphism algebra of $J_{\text{ns}}(p)$.

For every pair (E, φ) with E defined over $\overline{\mathbb{Q}}$ let \tilde{E} be the reduction of E modulo a prime ideal containing l , and $\tilde{\varphi} : \tilde{E}[p] \rightarrow \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ be the map naturally induced by φ , since $l \neq p$. Then the pair $(\tilde{E}, \tilde{\varphi})$ gives a point on $X_{\text{ns}}(p)$ over $\overline{\mathbb{F}_l}$. Let Frob_l be the generator of the Galois group $\text{Gal}(\overline{\mathbb{F}_l}/\mathbb{F}_l)$ and let $[l^{-1}]$ be the inverse of the multiplication by l map on $E[p]$. We have

$$\sum_{\substack{A \subset \tilde{E}(\mathbb{F}_l) \\ \#A=l}} (\tilde{E}/A, \tilde{\varphi}_A) = (\tilde{E}^{\text{Frob}_l}, \tilde{\varphi} \circ \text{Frob}_l^{-1}) + l \cdot (\tilde{E}^{\text{Frob}_l^{-1}}, \tilde{\varphi} \circ [l^{-1}] \circ \text{Frob}_l)$$

as divisors of $X_{\text{ns}}(p)$ reduced modulo l (see, for example, the proofs in [DS05, §8.7] regarding the modular curve $X_1(N)$). This implies the Eichler–Shimura relation:

$$T_l = \text{Frob}_l + l \cdot \text{Frob}_l^{-1}$$

where both terms of the equation are homomorphisms on the divisor group of $X_{\text{ns}}(p)$ reduced modulo l . Note that the Eichler–Shimura relation acquires this form in this case because a nonsplit Cartan subgroup of $\text{GL}_2(\mathbb{F}_p)$ always contains the scalar matrix associated to $[l^{-1}]$; hence, the pairs $(\tilde{E}^{\text{Frob}_l^{-1}}, \tilde{\varphi} \circ [l^{-1}] \circ \text{Frob}_l)$ and $(\tilde{E}^{\text{Frob}_l^{-1}}, \tilde{\varphi} \circ \text{Frob}_l)$ give the same point on $X_{\text{ns}}(p)$.

Since T_l induces an endomorphism of $J_{\text{ns}}(p)$, we will also write, with abuse of notation, the relation $T_l = \text{Frob}_l + l \cdot \text{Frob}_l^{-1}$ as endomorphisms of $J_{\text{ns}}(p)$ reduced modulo l .

LEMMA 4.1. *Let u be an automorphism of $X_{\text{ns}}(p)$ defined over the quadratic field $K(p)$ contained in the p th cyclotomic field. Let $\sigma_l \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be a Frobenius element at l . Then if $l \neq p$ we have*

$$u^{\sigma_l} T_l = T_l u$$

as endomorphisms of $J_{\text{ns}}(p)$, that is,

$$T_l u = \begin{cases} u T_l & \text{if } l \text{ is a square modulo } p \\ \bar{u} T_l & \text{if } l \text{ is not a square modulo } p \end{cases}$$

where \bar{u} is the $\text{Gal}(K(p)/\mathbb{Q})$ -conjugate of u .

Proof. (Following [KM88, p. 64, Lemma 2.6]) Since $J_{\text{ns}}(p)$ has good reduction outside p , the reduction modulo l map is injective on the endomorphism ring of $J_{\text{ns}}(p)$. Hence, the Lemma follows from the Eichler–Shimura relations and the fact that $K(p)$ is a quadratic field. \square

Let ζ_p be a primitive p th root of unity. The modular curve $X_{\text{ns}}(p)$ has exactly $p - 1$ cusps, all defined over $\mathbb{Q}(\zeta_p)$ and all conjugate under the action of $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ (see [Ser89, p. 194–195]).

PROPOSITION 4.2. *Let $\sigma_l \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be a Frobenius element at l . Then we have*

$$T_l C = C^{\sigma_l} + l \cdot C^{\sigma_l^{-1}}$$

as divisors on $X_{\text{ns}}(p)$, for every cusp C of $X_{\text{ns}}(p)$.

Proof. The equality must hold modulo any prime ideal \mathfrak{l} of $\mathbb{Q}(\zeta_p)$ over l because of the Eichler–Shimura relations. Moreover, since $l \neq p$, the modular curve $X_{\text{ns}}(p)$ and its reduction modulo l have the same number of cusps. Therefore, reduction modulo \mathfrak{l} is injective on the set of cusps of $X_{\text{ns}}(p)$, and the equality holds also over $\mathbb{Q}(\zeta_p)$. \square

LEMMA 4.3. *Let $p \geq 11$ and let u be an automorphism of $X_{\text{ns}}(p)$ defined over $K(p)$. Let $\sigma_l \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be a Frobenius element at l and let C be a cusp of $X_{\text{ns}}(p)$. If for every cusp C' of $X_{\text{ns}}(p)$ the divisor*

$$\begin{aligned} D_l &\stackrel{\text{def}}{=} (u^{\sigma_l} T_l - T_l u)(C - C') \\ &= u^{\sigma_l} T_l C + T_l u C' - T_l u C - u^{\sigma_l} T_l C' \end{aligned}$$

is the zero divisor, then $u C$ is a cusp, that is:

If $u^{\sigma_l} T_l - T_l u$ is the zero operator on the group of divisors of $X_{\text{ns}}(p)$ of degree zero and supported in the cusps, then u preserves the cusps.

Proof. By the previous Proposition, for every cusp C , we have $T_l C = C^{\sigma_l} + l \cdot C^{\sigma_l^{-1}}$. Thus, we can choose a cusp C' such that the supports of $T_l C$ and $T_l C'$ are completely disjoint. For D_l to be the zero divisor, we must have

$$u^{\sigma_l} C^{\sigma_l} + l \cdot u^{\sigma_l} C^{\sigma_l^{-1}} + T_l u C' = T_l u C + u^{\sigma_l} C'^{\sigma_l} + l \cdot u^{\sigma_l} C'^{\sigma_l^{-1}}.$$

Since we chose C' such that the supports of $T_l C$ and $T_l C'$ are completely disjoint, we have

$$(4.2) \quad T_l u C = u^{\sigma_l} C^{\sigma_l} + l \cdot u^{\sigma_l} C^{\sigma_l^{-1}}.$$

If uC is not a cusp, it corresponds to an elliptic curve E defined over $\mathbb{Q}(uC) \subset \mathbb{Q}(\zeta_p)$.

Let A and B be two different cyclic groups of order l in E . Then the natural map $E/A \rightarrow E \rightarrow E/B$ has a cyclic kernel of order l^2 . Therefore, recalling the interpretation of the action of T_l on noncuspidal points, we have that equation (4.2) can hold only if E admits an endomorphism of degree l^2 with cyclic kernel. An elliptic curve without complex multiplication cannot have such an endomorphism, hence we obtain the Lemma as a consequence of the following Proposition. □

PROPOSITION 4.4. *Let $p \geq 11$ and let E be an elliptic curve over \mathbb{C} with complex multiplication by an imaginary quadratic field K . No point of $X_{\text{ns}}(p)$ associated to E is defined over $\mathbb{Q}(\zeta_p)$.*

Proof. Let P be a point of $X_{\text{ns}}(p)$ associated to E and defined over $\mathbb{Q}(\zeta_p)$. There are three cases: p is inert, p splits or p ramifies in K .

If p is inert in K , we consider the point Q of $X_{\text{ns}}^+(p)$ given by $\{P, wP\}$. This point Q is defined over $L \subset \mathbb{Q}(\zeta_p)$ and lifts to points of $X_{\text{ns}}(p)$ defined over LK (and no smaller fields) as explained in [Ser89, p. 194–195]. But this is impossible since P, wP are defined over $\mathbb{Q}(\zeta_p)$ where p ramifies completely.

If p splits or ramifies in K , this means that the image of the $\text{Gal}(\overline{\mathbb{Q}}/K(\zeta_p))$ -representation modulo p attached to E is contained in respectively a split Cartan or a Borel subgroup of $\text{GL}_2(\mathbb{F}_p)$ (see loc. cit.). But since P is defined over $\mathbb{Q}(\zeta_p)$, the image of such representation is also contained in a nonsplit Cartan subgroup. Therefore, in both cases, it is contained in the subgroup of scalar matrixes. Then, the properties of the Weil pairing imply that $\text{Gal}(\overline{\mathbb{Q}}/K(\zeta_p))$ acts on the p -torsion of E as a subgroup of $\{\pm 1\}$. After choosing a suitable Weierstrass equation for E , this means that the x -coordinates of the p -torsion points of E are in $K(\zeta_p)$. The theory of complex multiplication tells us that the ray class field $K_{(p)}$ modulo (p) of K is generated over K by the j -invariant of E and by some rational function of the x -coordinates of the p -torsion points of E [Sil94, p. 135, Theorem 5.6]. Thus we obtain $K_{(p)} \subset K(\zeta_p)$. It is always true that $K(\zeta_p) \subset K_{(p)}$, so the opposite inclusion holds if and only if $[K_{(p)} : K] \leq [K(\zeta_p) : K]$. We have

$$[K_{(p)} : K] = h_K \frac{\#(O_K/pO_K)^*}{w_K}$$

where h_K is the class number of K , O_K is the ring of integers of K and w_K is the number of roots of unity in K taken modulo (p) . The group $(O_K/pO_K)^*$

is isomorphic to $\mathbb{F}_{p^2}^*$, $\mathbb{F}_p^* \times \mathbb{F}_p^*$ or $\mathbb{F}_p^* \times \langle a \rangle$ with a an element of order p . Thus to have the inequality $[K_{(p)} : K] \leq [K(\zeta_p) : K]$ we must have

$$\frac{(p-1)^2}{w_K} \leq (p-1)$$

and hence $p \leq w_K + 1$. Since the roots of unity in an imaginary quadratic field are at most 6, we get $p \leq 7$. □

COROLLARY 4.5. *Let $p \geq 11$ and let u be an automorphism of $X_{\text{ns}}(p)$ defined over $K(p)$. If u does not preserve the cusps, then there exists a nonconstant morphism f from $X_{\text{ns}}(p)$ to \mathbb{P}^1 , defined over the field $\mathbb{Q}(\zeta_p)$ and with degree less or equal to 6, such that $f \circ w \neq f$.*

Proof. Since u is defined over $K(p)$ and does not preserve the cusps, we can apply Lemma 4.3 to obtain, for every prime $l \neq p$, a nonzero divisor D_l on $X_{\text{ns}}(p)$, of degree zero, defined over $\mathbb{Q}(\zeta_p)$, which is the difference of two effective divisors of degree at most $2(l+1)$. Moreover, we have $D_l = (u^{\sigma_l} T_l - T_l u)(C - C')$ for two cusps C, C' of $X_{\text{ns}}(p)$. Hence, by Lemma 4.1 we deduce that D_l must be zero in $J_{\text{ns}}(p)$ when $p \geq 11$, which is to say that D_l is a principal divisor. This gives us the existence of a nonconstant morphism f from $X_{\text{ns}}(p)$ to \mathbb{P}^1 , defined over $\mathbb{Q}(\zeta_p)$ and with degree at most $2(l+1)$.

Now we apply w to D_l . If D_l were invariant under the action of w , we would have

$$(4.3) \quad wT_l uC + wu^{\sigma_l} C'^{\sigma_l} + l \cdot wu^{\sigma_l} C'^{\sigma_l^{-1}} = T_l uC + u^{\sigma_l} C'^{\sigma_l} + l \cdot u^{\sigma_l} C'^{\sigma_l^{-1}},$$

where we used the computation in the proof of Lemma 4.3. In that proof, we also showed that the divisor $T_l uC$ is the sum of $l+1$ different points. Hence since $l \geq 2$, to satisfy equation (4.3), the supports of $T_l uC$ and $wT_l uC$ must have a nonempty intersection. This means that the support of $T_l uC$ has either two different points exchanged by w or a point fixed by w . The first case is impossible because the modular automorphism w preserves the isomorphism class over \mathbb{C} of the elliptic curve associated to noncuspidal points, and we can apply the same argument at the end of the proof of Lemma 4.3. The second case is also impossible by the previous Proposition, because the points fixed by w are all associated with the elliptic curve with j -invariant equal to 1728 (see [Bar10, Proposition 7.10]), which is an elliptic curve with complex multiplication.

Thus, for $l \geq 2$, we have $wD_l \neq D_l$ which implies $f \circ w \neq f$. The degree of f is $2(l+1)$, so by choosing $l=2$ we get the Corollary. □

§5. Proof of main results

We first introduce a general Lemma.

LEMMA 5.1. *Let X be a smooth projective curve over an algebraically closed field, and let w be a nontrivial automorphism of X having r fixed points. If there exists a morphism f from X to \mathbb{P}^1 of degree k such that $f \circ w \neq f$, then $r \leq 2k$.*

Proof. [BH03, Lemma 3.5] Consider the rational function $g = f \circ w - f$ on X . If g is constant, then the fixed points of w must be poles of f , implying $r \leq k$. If g is not constant then the degree of g is at most $2k - h$, where h is the number of poles that are also points fixed by w . On the other hand, the other $r - h$ points fixed by w are zeros of g , hence there are at most $\deg g$ of them. So we have $r - h \leq 2k - h$ which implies $r \leq 2k$. \square

Let p be an odd prime number.

THEOREM 5.2. *If $p \geq 29$, all the automorphisms of $X_{\text{ns}}(p)$ preserve the cusps. If $p \equiv 1 \pmod{12}$ and $p \neq 13$, the automorphism group of $X_{\text{ns}}(p)$ is generated by the modular involution w .*

Proof. Let u be an automorphism of $X_{\text{ns}}(p)$ not preserving the cusps. By Corollary 2.6 we have that u is defined over $K(p)$. Then Corollary 4.5 tells us that there exists a nonconstant morphism from $X_{\text{ns}}(p)$ to \mathbb{P}^1 , defined over $\mathbb{Q}(\zeta_p)$, with degree less or equal to 6 and such that $f \circ w \neq f$. Then by the previous Lemma we have

$$\#\{\text{fixed points of } w\} \leq 12.$$

Recall that the number of fixed points of w is $\frac{p-1}{2}$ if $p \equiv 1 \pmod{4}$ and it is $\frac{p+1}{2}$ if $p \equiv 3 \pmod{4}$ (see [Bar10, Proposition 7.10]). This implies $p \leq 23$ and proves the first part of the Theorem. The second part is now a consequence of Corollary 3.3. \square

We remark that the first part of the Theorem above can also be achieved avoiding the discussion about the invariance of f under the action of w , by using [Abr96, Theorem 0.1].

Now we prove that Serre's uniformity conjecture, implies the absence of rational exceptional automorphisms of $X_{\text{ns}}(p)$ for almost all p .

THEOREM 5.3. *Let $p \geq 29$. If there exists an exceptional automorphism of $X_{\text{ns}}(p)$ defined over \mathbb{Q} , then $X_{\text{ns}}^+(p)$ has a non-CM rational point.*

Proof. Let u be an automorphism of $X_{\text{ns}}(p)$ defined over \mathbb{Q} . By Corollary 2.9 we have that u commutes with w and it induces an automorphism of $X_{\text{ns}}^+(p)$ defined over \mathbb{Q} . Then it is enough to prove that u preserves the rational CM points of $X_{\text{ns}}^+(p)$ only if u is modular. Let $\pi : X_{\text{ns}}(p) \rightarrow X_{\text{ns}}^+(p)$ be the degree-2 modular morphism given by the inclusion of a nonsplit Cartan subgroup in its normalizer, and let Q be a rational CM point of $X_{\text{ns}}^+(p)$. Note that the two points in $\pi^{-1}(Q)$ are defined over the CM field of the elliptic curve associated to Q (see [Ser89, p. 194–195]). Hence uQ cannot be a rational CM point different from Q because the two points in $\pi^{-1}(uQ)$ are defined over the same field as the points in $\pi^{-1}(Q)$. Now we observe that the elliptic points of $X_{\text{ns}}(p)$ are the inverse images by π of the rational CM points associated to the elliptic curves with j -invariant equal to 0 or 1728 (see [Bar10, Proposition 7.10]). Thus, if u preserves the rational CM points of $X_{\text{ns}}^+(p)$, then it preserves the elliptic points of $X_{\text{ns}}(p)$. Furthermore, u also preserves the cusps by Theorem 5.2, hence it is modular by Corollary 3.3. \square

Acknowledgments. The author would like to thank Prof. René Schoof and the Anonymous Referee for useful remarks on earlier versions of this paper.

REFERENCES

- [Abr96] D. Abramovich, *A linear lower bound on the gonality of modular curves*, Int. Math. Res. Not. IMRN **20** (1996), 1005–1011; MR 1422373 (98b:11063).
- [Bar10] B. Baran, *Normalizers of non-split Cartan subgroups, modular curves, and the class number one problem*, J. Number Theory **130**(12) (2010), 2753–2772; MR 2684496 (2011i:11083).
- [BGJGP05] 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) (2005), 1325–1387; MR 2183527 (2006i:11065).
- [BH03] M. Baker and Y. Hasegawa, *Automorphisms of $X_0^*(p)$* , J. Number Theory **100**(1) (2003), 72–87; MR 1971247 (2004c:11100).
- [Che98] I. Chen, *The Jacobians of non-split Cartan modular curves*, Proc. Lond. Math. Soc. (3) **77**(1) (1998), 1–38; MR 1625491 (99m:11068).
- [Con96] J. H. Conway, “*Understanding groups like $\Gamma_0(N)$ ”*, in *Groups, Difference Sets, and the Monster (Columbus, OH, 1993)*, Ohio State Univ. Math. Res. Inst. Publ. **4**, de Gruyter, Berlin, 1996, 327–343. MR 1400424 (98b:11041).
- [Dav80] H. Davenport, *Multiplicative Number Theory*, second ed., Graduate Texts in Mathematics **74**, Springer, New York–Berlin, 1980, Revised by Hugh L. Montgomery. MR 606931 (82m:10001).
- [DFGS14] V. Dose, J. Fernández, J. González and R. Schoof, *The automorphism group of the non-split Cartan modular curve of level 11*, J. Algebra **417** (2014), 95–102; MR 3244639.

- [DR73] P. Deligne and M. Rapoport, “*Les schémas de modules de courbes elliptiques*”, in *Modular Functions of One Variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, Lecture Notes in Math. **349**, Springer, Berlin, 1973, 143–316. MR 0337993 (49 #2762).
- [DS05] F. Diamond and J. Shurman, *A First Course in Modular Forms*, Graduate Texts in Mathematics **228**, Springer, New York, 2005, MR 2112196 (2006f:11045).
- [dSE00] B. de Smit and B. Edixhoven, *Sur un résultat d’Imin Chen*, Math. Res. Lett. **7**(2–3) (2000), 147–153; MR 1764312 (2001j:11043).
- [Elk90] N. D. Elkies, *The automorphism group of the modular curve $X_0(63)$* , Compos. Math. **74**(2) (1990), 203–208; MR 1047740 (91e:11064).
- [Har11] M. C. Harrison, *A new automorphism of $X_0(108)$* , preprint, 2011, arXiv:1108.5595.
- [KM88] M. A. Kenku and F. Momose, *Automorphism groups of the modular curves $X_0(N)$* , Compos. Math. **65**(1) (1988), 51–80; MR 930147 (88m:14015).
- [Lan02] M. L. Lang, *Normalisers of subgroups of the modular group*, J. Algebra **248**(1) (2002), 202–218; MR 1879013 (2002m:20075).
- [Ogg74] A. P. Ogg, *Hyperelliptic modular curves*, Bull. Soc. Math. France **102** (1974), 449–462; MR 0364259 (51 #514).
- [Ogg77] A. P. Ogg, *Über die Automorphismengruppe von $X_0(N)$* , Math. Ann. **228**(3) (1977), 279–292; MR 0562500 (58 #27775).
- [Rib75] K. A. Ribet, *Endomorphisms of semi-stable abelian varieties over number fields*, Ann. of Math. (2) **101** (1975), 555–562; MR 0371903 (51 #8120).
- [Ser89] J.-P. Serre, *Lectures on the Mordell–Weil Theorem*, Aspects Math. **E15**, Springer Vieweg, Braunschweig/Wiesbaden, 1989.
- [Shi58] G. Shimura, *Correspondances modulaires et les fonctions ζ de courbes algébriques*, J. Math. Soc. Japan **10** (1958), 1–28; MR 0095173 (20 #1679).
- [Shi71] G. Shimura, *On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields*, Nagoya Math. J. **43** (1971), 199–208; MR 0296050 (45 #5111).
- [Shi72] G. Shimura, *Class fields over real quadratic fields and Hecke operators*, Ann. of Math. (2) **95** (1972), 130–190; MR 0314801 (47 #3351).
- [Sil94] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **151**, Springer, New York, 1994, MR 1312368 (96b:11074).
- [Sil09] J. H. Silverman, *The Arithmetic of Elliptic Curves*, second ed., Graduate Texts in Mathematics **106**, Springer, Dordrecht, 2009, MR 2514094 (2010i:11005).
- [Ste12] W. Stein, The Modular Forms Database, <http://wstein.org/Tables>.

Dipartimento di Matematica
Università di Roma “Tor Vergata”
Via della Ricerca Scientifica 1
00133 Roma
Italy
 dose@mat.uniroma2.it