Automorphism group of split Cartan modular curves

Josep González *

Dedicated to the memory of Fumiyuki Momose

Abstract

We determine the automorphism group of the split Cartan modular curves $X_{\rm split}(p)$ for all primes p.

1 Introduction

For a rational prime p, let $X_{\rm split}(p)$ be the modular curve defined over $\mathbb{Q}$ attached to the congruence subgroup of level p

$$\Gamma_{\rm split}(p)=\left\{\left(\begin{array}{cc} a & b\\ c & d\end{array}\right)\in {\rm SL}_2(\mathbb{Z})\colon b\equiv c\equiv 0 \text{ or } a\equiv d\equiv 0 \pmod p\right\}.$$

It is well-known that $X_{\rm split}(p)$ is isomorphic over $\mathbb{Q}$ to the modular curve $X_0^+(p^2):=X_0(p^2)/w_{p^2}$, where w_{p^2} stands for the Fricke involution. The genus of this curve is positive when $p\geq 11$ and, in this case, it is at least 2.

The automorphism group of the modular curve $X_0(N)$ was determined, except for $N=63$, by Kenku and Momose in [KM88] and was completed by Elkies in [Elk90]. Later, the automorphism group of the modular curve $X_0^+(p)=X_0(p)/w_p$ was determined by Baker and Hasegawa in [BH03]. In this article, we focus our attention on the automorphism group of the split Cartan modular curves $X_{\rm split}(p)$. Our main result is the following.

Theorem 1. *Assume that the genus of $X_{\rm split}(p)$ is positive. Then,*

$$\operatorname{Aut}(X_{\rm split}(p))=\operatorname{Aut}_{\mathbb{Q}}(X_{\rm split}(p))\simeq\begin{cases}\{1\} & \text{if } p>11,\\ (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } p=11.\end{cases}$$

2 General facts

We recall that, for a normalized newform $f=\sum_{n\geq 1}a_nq^n\in S_2(\Gamma_1(N))^{\rm new}$ and a Dirichlet character χ of conductor N', the function

$$f_\chi:=\sum_{n\geq 1}\chi(n)a_nq^n$$

is a cusp form in $S_2(\Gamma_1(\operatorname{lcm}(N,N'^2))$ (cf. Proposition 3.1 of [AL78]). Here, as usual, $q=e^{2\pi i z}$. Let $f\otimes\chi$ denote the unique normalized newform with q-expansion $\sum_{n\geq 1}b_nq^n$ that satisfies

*The author is partially supported by DGI grant MTM2012-34611.
Keywords: Automorphisms of curves, Split Cartan modular curves.
2010 *Mathematics Subject Classification*: 14G35, 14H37.

$b_\ell = \chi(\ell)a_\ell$ for all primes $\ell \nmid N \cdot N'$. If $f \otimes \chi$ is a newform of level M and f_χ has level M', then $M|M'$. Moreover, if $M = M'$, then $f_\chi = f \otimes \chi$.

We restrict ourselves to the cusp forms in $S_2(\Gamma_0(N))$. Let New_N denote the set of normalized newforms in $S_2(\Gamma_0(N))^{\mathrm{new}}$. For $f \in \mathrm{New}_N$, $\varepsilon(f)$ denotes the eigenvalue of f under the action of the Fricke involution w_N and set $\mathrm{New}_N^+ = \{f \in \mathrm{New}_N \colon \varepsilon(f) = 1\}$. For a cusp form $f = \sum_n b_n q^n \in S_2(\Gamma_0(N))$ such that $\mathbb{Q}(\{b_n\})$ is a number field, $S_2(f)$ denotes the $\mathbb{C}$-vector space of cusp forms spanned by f and its Galois conjugates. In the particular case that $f \in \mathrm{New}_N$, A_f stands for the abelian variety attached to f by Shimura. It is well-known that A_f is a quotient of $J_0(N) := \mathrm{Jac}(X_0(N))$ 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. $S_2(f)dq/q \cap \mathbb{Q}[[q]]$. Moreover, the endomorphism algebra $\mathrm{End}_{\mathbb{Q}}(A_f) \otimes \mathbb{Q}$ is a totally real number field.

From now on, we assume $p \geq 11$ and 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 $p^* = (-1)^{(p-1)/2}p$.

Lemma 1. *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 $p \equiv 3 \pmod 4$.*

Proof. Since $f_\chi \in S_2(\Gamma_0(p^2))$ for $f \in \mathrm{New}_{p^2} \cup \mathrm{New}_p$ (cf. Proposition 3.1 of [AL78]), the level of $f \otimes \chi$ divides p^2 and, thus, the map is well defined. The bijectivity follows from the fact that $(f \otimes \chi) \otimes \chi = f$. The condition $f = f \otimes \chi$ amounts to saying that f has complex multiplication (CM) by the imaginary quadratic field K attached to χ, i.e. $p \equiv 3 \pmod 4$, and, moreover, f is obtained from a Hecke character ψ whose conductor is the ideal of K of norm p, which implies $f \in \mathrm{New}_{p^2}$. Since f has trivial Nebentypus, the Hecke character ψ is unique up to Galois conjugation. $\square$

Remark 1. *The above map does not preserve the eigenvalue of the corresponding Fricke involution, i.e. it may be that $\varepsilon(f)$ and $\varepsilon(f \otimes \chi)$ are different.*

Remark 2. *Let $f \in \mathrm{New}_{p^2} \cup \mathrm{New}_p$ without CM. If f has an inner twist $\chi' \neq 1$, i.e. $f \otimes \chi' = {}^\sigma f$ for some $\sigma \in G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, then $\chi' = \chi$ because χ' must be a quadratic character of conductor dividing p^2. In such a case, $\mathrm{End}(A_f) \otimes \mathbb{Q} = \mathrm{End}_K(A_f) \otimes \mathbb{Q}$ is a non commutative algebra. Otherwise, $\mathrm{End}(A_f) \otimes \mathbb{Q} = \mathrm{End}_{\mathbb{Q}}(A_f) \otimes \mathbb{Q}$ is a totally real number field.*

Remark 3. *If $f \in \mathrm{New}_{p^2}$ has CM, then the dimension of A_f is the class number of K, A_f has all its endomorphisms defined over the Hilbert class field of K and $\mathrm{End}_K(A_f) \otimes \mathbb{Q}$ is the CM field $\mathrm{End}_{\mathbb{Q}}(A_f) \otimes K$ which only contains the roots of the unity ± 1 (cf. Theorem 1.2 of of [GL11] and part (3) in Proposition 3.2 of [Yan04]). Moreover, $f \in \mathrm{New}^+_{p^2}$ if, and only if, $p \equiv 3 \pmod 8$ (cf. Corollary 6.3 of [MY00]).*

Remark 4. *For two distinct $f_1, f_2 \in (\mathrm{New}_{p^2} \cup \mathrm{New}_p)/G_{\mathbb{Q}}$, the abelian varieties A_{f_1} and A_{f_2} are nonisogenous over $\mathbb{Q}$ and are isogenous if, and only if, $f_1 \otimes \chi = {}^\sigma f_2$ for some $\sigma \in G_{\mathbb{Q}}$ (see Proposition 4.2 of [GJU12]) and, in this particular case, there is an isogeny defined over K.*

The abelian variety $J_0^+(p^2) := \mathrm{Jac}(X_0^+(p^2))$ splits over $\mathbb{Q}$ as the product $(J_0(p^2)^{\mathrm{new}})^{\langle w_{p^2}\rangle} \times J_0(p)$. More precisely,

$$J_0^+(p^2) \stackrel{\mathbb{Q}}{\sim} \prod_{f \in (\mathrm{New}^+_{p^2} \cup \mathrm{New}_p)/G_{\mathbb{Q}}} A_f\,. \tag{2.1}$$

Each $f \in \mathrm{New}_p$ provides a vector subspace of $S_2(\Gamma_0(p^2))^{\mathrm{old}}$ of dimension 2 generated by $f(q)$ and $f(q^p)$. The normalized cusp forms $f(q) + p\,\varepsilon(f) f(q^p)$ and $f(q) - p\,\varepsilon(f) f(q^p)$ are eigenforms for all Hecke operators T_m with $p \nmid m$ and the Fricke involution w_{p^2} with eigenvalues 1 and -1 respectively. The splitting of $J_0^+(p^2)$ over $\mathbb{Q}$ provides the following decomposition for its vector space of regular differentials

$$\Omega^1_{J_0^+(p^2)} = \left(\bigoplus_{f \in \mathrm{New}^+_{p^2}/G_{\mathbb{Q}}} S_2(f(q)) \frac{dq}{q} \right) \bigoplus \left(\bigoplus_{f \in \mathrm{New}_p/G_{\mathbb{Q}}} S_2(f(q) + p\,\varepsilon(f) f(q^p)) \frac{dq}{q} \right). \qquad (2.2)$$

Let g^+ and g_0 be the genus of the curves $X_0^+(p^2)$ and $X_0(p)$, respectively. From the genus formula for these curves, one obtains the following values

p	g^+	g_0
$p \equiv 1 \pmod{12}$	$\frac{(p-1)(p-7)}{24}$	$\frac{p-13}{12}$
$p \equiv 5 \pmod{12}$	$\frac{(p-3)(p-5)}{24}$	$\frac{p-5}{12}$
$p \equiv 7 \pmod{12}$	$\frac{(p-1)(p-7)}{24}$	$\frac{p-7}{12}$
$p \equiv 11 \pmod{12}$	$\frac{(p-3)(p-5)}{24}$	$\frac{p+1}{12}$

3 Hyperelliptic case for $X_{\mathbf{split}}(p)$

Proposition 1. *Assume $p \geq 11$. Then, $X_{\mathrm{split}}(p)$ is hyperelliptic if, and only if, $p = 11$. Moreover, one has*

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

Proof. Assume $X_0^+(p^2)$ is hyperelliptic. By applying Lemma 3.25 of [BGGP05], we obtain $g^+ \leq 10$, which implies $p \leq 19$. We have $g^+ = 2$ if, and only if, $p = 11$ and, thus, the curve $X_0^+(11^2)$ is hyperelliptic. For $p > 11$, one has $g^+ > 2$ and, moreover, $p > 13$ because $X_0^+(13^2)$ is a smooth plane quartic (cf. [Bar10]). Lemma 2.5 of [BGGP05] states that there is a basis $f_1, \cdots, f_{g^+}$ of $S_2(\Gamma_0(p^2))^{\langle w_{p^2}\rangle}$ with rational q-expansions satisfying

$$f_i(q) = \begin{cases} q^i + O(q^i) & \text{if the cusp } \infty \text{ is not a Weierstrass point of } X_0^+(p^2), \\ q^{2i-1} + O(q^{2i-1}) & \text{otherwise.} \end{cases} \qquad (3.1)$$

Moreover, for any such a basis, the functions on $X_0^+(p^2)$ defined by

$$x = \frac{f_{g^+}}{f_{g^+-1}}\,, \quad y = \frac{q dx/dq}{f_{g^+-1}}\,,$$

satisfy $y^2 = P(x)$ for a unique squarefree polynomial $P(X) \in \mathbb{Q}[X]$ which has degree $2g^+ + 1$ or $2g^+ + 2$ depending on whether ∞ is a Weierstrass point or not. The first part of the statement follows from the fact that, for $p = 17$ and $p = 19$, the vector space $S_2(\Gamma_0(p^2))^{\langle w_{p^2}\rangle}$ does not have any bases as in (3.1).

Now, we consider $p = 11$. In this case, $|\,\mathrm{New}^+_{11^2}\,| = |\,\mathrm{New}_{11}\,| = 1$. Let $f_1 \in \mathrm{New}^+_{11^2}$ and let $f_2 \in \mathrm{New}_{11}$. The newform f_1 is the one attached to the elliptic curve $E_1/\mathbb{Q}$ of conductor 11^2 with CM by $\mathbb{Z}[(1+\sqrt{-11})/2]$, and f_2 is the newform attached to an elliptic curve $E_2/\mathbb{Q}$ of conductor 11 without CM. Since $\varepsilon(f_2) = -1$, the cusp forms $f_1(q)$ and $h(q) = f_2(q) - 11 f_2(q^{11})$ are a basis of $S_2(\Gamma_0(11^2))^{\langle w_{11^2}\rangle}$. Take the following functions on $X_0^+(11^2)$

$$x = \frac{h}{f_1} = 1 - 2q + 2q^3 - 2q^5 + O(q^5)\,, \quad y = -2\frac{q\,dx/q}{f_1} = 4 - 8q^2 + 8q^3 + 24q^4 - 32q^5 + O(q^5)\,.$$

Using q-expansions, we get the following equation for $X_0^+(11^2)$:

$$y^2 = x^6 - 7x^4 + 11x^2 + 11\,. \tag{3.2}$$

The maps $(x, y) \mapsto (\pm x, \pm y)$ provide a subgroup of $\mathrm{Aut}_{\mathbb{Q}}(X_0^+(11^2))$ isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. Since $\mathrm{Aut}_{\overline{\mathbb{Q}}}(X_0^+(11^2))$ is a finite subgroup of $\mathrm{End}(E_1) \times \mathrm{End}(E_2) \simeq \mathbb{Z}[(1 + \sqrt{-11})/2] \times \mathbb{Z}$, we have that it must be a subgroup of $(\mathbb{Z}/2\mathbb{Z})^2$, which proves the second part of the statement. □

4 Preliminary lemmas

For an abelian variety A defined over a number field, we say that a number field L is the splitting field of A if it is the smallest number field where A has all its endomorphisms defined. We recall that K is the quadratic field $\mathbb{Q}(\sqrt{p^*})$, where $p^* = (-1)^{(p-1)/2}p$, and χ is the quadratic Dirichlet character attached to K .

Lemma 2. *Let L be the splitting field of $J_0^+(p^2)$. If $p \equiv 3 \pmod 8$, then L is the Hilbert class field de K. For $p \not\equiv 3 \pmod 8$, $L = K$ if there exists $f \in \mathrm{New}_{p^2}^+ \cup \mathrm{New}_p$ such that $f \otimes \chi \in \mathrm{New}_{p^2}^+ \cup \mathrm{New}_p$, otherwise $L = \mathbb{Q}$.*

Proof. On the one hand, for two distinct $f_1, f_2 \in (\mathrm{New}_{p^2}^+ \cup \mathrm{New}_p)/G_{\mathbb{Q}}$ without CM, A_{f_1} and A_{f_2} are isogenous if, and only if, f_2 is the Galois conjugate of $f_1 \otimes \chi$ and, in this case, the isogeny is defined over K.

On the other hand, if $f \in \mathrm{New}_{p^2}^+ \cup \mathrm{New}_p$ does not have CM, then f has at most χ as an inner twist. In this case, the splitting field of A_f is K or $\mathbb{Q}$ depending on whether χ is an inner twist of f or not. If f has CM, then the splitting field of A_f is the Hilbert class field of K and A_f is the unique CM factor of $J_0^+(p^2)$. □

Lemma 3. *All automorphisms of $X_0^+(p^2)$ are defined over K.*

Proof. By Lemma 2, we only have to consider the case $p \equiv 3 \pmod 8$ and, by Proposition 1, we can assume $p \geq 19$. Let g_c be the dimension of the abelian variety A_f with $f \in \mathrm{New}_{p^2}$ having CM. We know that g_c is the class number of K and, thus, $g_c = (2V - (p-1)/2)/3$, where V is the number of quadratic residues modulo p in the interval $[1, (p-1)/2]$ (see Théorème 4 in p. 388 of [BC67]). Hence, $g_c \leq (p-1)/6$. Since $g^+ > 1 + (p-1)/3$ for $p \geq 17$, we obtain $g^+ > 1 + 2g_c$. Now, the statement is obtained by applying the same argument used in the proof of Lemma 1.4 of [KM88]. Indeed, assume there is a nontrivial automorphism $u \in \mathrm{Aut}(X_0^+(p^2))$ and put $v = u^\sigma \cdot u^{-1}$ for some nontrivial $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$. Let g_v denote the genus of the curve $X_v := X_0^+(p^2))/\langle v \rangle$. On the one hand,

$$g_v \geq g^+ - g_c\,, \tag{4.1}$$

because v acts as the identity on the factors of $J_0^+(p^2)$ without CM. On the other hand, if v is not the identity, then its order is ≥ 2 and, applying the Riemann-Hurwitz formula to the natural projection $X_0^+(p^2) \to X_v$, we get

$$g^+ - 1 \geq 2(g_v - 1)\,. \tag{4.2}$$

Combining (4.1) with (4.2), we obtain $g^+ \leq 1 + 2g_c$. □

Lemma 4. *The group $\mathrm{Aut}_{\mathbb{Q}}(X_0^+(p^2))$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^s$ for some integer $s \geq 0$.*

Proof. Since $\mathrm{End}_{\mathbb{Q}}(J_0^+(p^2)) \otimes \mathbb{Q}$ is a product of totally real fields, any $u \in \mathrm{Aut}_{\mathbb{Q}}(X_0^+(p^2))$ acts as the identity or the product by -1 on $S_2(f)$ for $f \in \mathrm{New}_{p^2}^+$ and on $S_2(f(q) + p\varepsilon(f) f(q^p))$ for $f \in \mathrm{New}_p$. Hence, $\mathrm{Aut}_{\mathbb{Q}}(X_0^+(p^2))$ is isomorphic to a subgroup of $(\mathbb{Z}/2\mathbb{Z})^r$ for r equal to $|\mathrm{New}_{p^2}^+ / G_{\mathbb{Q}}| + |\mathrm{New}_p / G_{\mathbb{Q}}|$. $\square$

Lemma 5. *If u is a nontrivial automorphism of $X_0^+(p^2)$, then $u(\infty)$ is not a cusp.*

Proof. The modular curve $X_0(p^2)$ has $p+1$ cusps. Only the cusps ∞ and 0 are defined over $\mathbb{Q}$. The remaining cusps $1/p, \cdots, (p-1)/p$ are defined over the p-th cyclotomic field $\mathbb{Q}(\zeta_p)$. The Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ acts transitively on this set, and the cusp $w_{p^2}(i/p) = (p-i)/p$ is the complex conjugate of the cusp i/p (cf. [Ogg74]). Hence, among the $(p+1)/2$ cusps of $X_0^+(p^2)$ the cusp ∞ is the only one defined over the quadratic field K.

Let u be an automorphism of $X_0^+(p^2)$ such that $u(\infty)$ is a cusp. By Lemma 3, $u(\infty)$ is defined over K and, thus, $u(\infty) = \infty$. Let G_∞ denote the subgroup of $\mathrm{Aut}(X_0^+(p^2))$ consisting of the automorphisms which fix ∞ and let T_∞ be the tangent space of $X_0^+(p^2)$ at ∞ over $\overline{\mathbb{Q}}$. Since the cusp ∞ is defined over $\mathbb{Q}$, the group monomorphism $\iota : G_\infty \hookrightarrow \mathrm{Aut}_{\overline{\mathbb{Q}}}(T_\infty) \simeq \overline{\mathbb{Q}}^*$ is $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-equivariant. Hence, if $\iota(u)$ is a primitive m-th root of unity ζ_m, then u is defined over $\mathbb{Q}(\zeta_m)$. Since the unique roots of unity in K are ± 1, it follows that u is defined over $\mathbb{Q}$.

Now, we will prove that, if $u \in \mathrm{Aut}_{\mathbb{Q}}(X_0^+(p^2))$ is nontrivial, then $u(\infty) \neq \infty$. For the hyperelliptic case $p = 11$, the cusp ∞ has $(1,4)$ as (x,y) coordinates in the equation given in (3.2). Hence, ∞ is not a fixed point for any of the three nontrivial involutions of $X_0^+(11^2)$. Let $p > 11$. Since $X_0^+(p^2)$ is nonhyperelliptic and, by Lemma 5, u is an involution, we can exclude the case where all eigenvalues of u acting on $\Omega^1_{J_0^+(p^2)}$ are equal to -1 and, thus, u must have eigenvalues 1 and -1 acting on this vector space. The vector space of cusp forms $\Omega^1_{J_0^+(p^2)} q/dq$ has a basis of normalized eigenforms (see (2.2)). Since u is defined over $\mathbb{Q}$, u commutes with the Hecke operators and, thus, there are two normalized eigenforms such that their corresponding regular differentials $\omega_1 = (1 + \sum_{n>1} a_n q^n) dq$ and $\omega_2 = (1 + \sum_{n>1} b_n q^n) dq$ satisfy $u^*(\omega_1) = \omega_1$ and $u^*(\omega_2) = -\omega_2$. Hence, u sends $\omega_1 + \omega_2$, which does not vanish at ∞, to $\omega_1 - \omega_2$, which vanishes at ∞. $\square$

Let $\nu \in \mathrm{Gal}(K/\mathbb{Q})$ be the conjugation corresponding to the Frobenius element of the prime 2. The following lemma is an adapted version of Lemma 3.3 of [BH03] to our context, restricted to the prime 2.

Lemma 6. *Assume that $u \in \mathrm{Aut}(X_0^+(p^2))$ is nontrivial. For any noncuspidal point $S \in X_0^+(p^2)(\mathbb{C})$, the divisor*

$$D_S := (uT_2 - T_2 u^\nu)(\infty - S) ,$$

where T_2 denotes the Hecke operator viewed as a correspondence of the curve $X_0^+(p^2)$, is nonzero but linearly equivalent to zero. In particular, the K-gonality of $X_0^+(p^2)$ is at most 6 and u has at most 12 fixed points.

Proof. Following the arguments used in Lemma 2.6 of [KM88], we claim that $u\,T_2 = T_2\,u^\nu$. Indeed, by the Eichler Shimura congruence we know that T_2 acting on $J_0^+(p^2) \otimes \mathbb{F}_2$ is equal to $\mathrm{Frob}_2 + 2/\mathrm{Frob}_2$. On $X_0^+(p^2) \otimes \mathbb{F}_2$, one has $u^\nu = u^{\mathrm{Frob}_2}$. The claim is obtained from the equality $u \cdot \mathrm{Frob}_2 = \mathrm{Frob}_2 \cdot u^{\mathrm{Frob}\,2}$ and the injection $\mathrm{End}(J_0^+(p^2)) \hookrightarrow \mathrm{End}(J_0^+(p^2) \otimes \mathbb{F}_2)$. Hence, D_S is a principal divisor.

Set $Q = u(\infty)$ and let $P \in X_0(p^2)(\overline{\mathbb{Q}})$ be such that $\pi^+(P) = Q$, where $\pi^+\colon X_0(p^2) \to X_0^+(p^2)$ is the natural projection. Since Q is not a cusp, there is an elliptic curve E defined over $\overline{\mathbb{Q}}$ and a p^2-cyclic subgroup C of $E(\overline{\mathbb{Q}})$ such that $P = (E, C)$. The other preimage of Q under π^+ is the point $w_{p^2}(P) = (E/C, E[p^2]/C)$. Observe that if $P \notin X_0(p^2)(K)$, then P is defined over a quadratic extension L of K and $w_{p^2}(P) = P^\sigma$ for the nontrivial Galois conjugation $\sigma \in \mathrm{Gal}(L/K)$ and, in particular, $E/C = E^\sigma$.

If D_S is a zero divisor, then $uT_2(\infty)$ must be equal to $T_2 u^\nu(\infty)$ because $T_2(\infty) = 3\infty$ and ∞ 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 $3(Q) = T_2(Q^\nu)$ cannot occur for a noncuspidal point $Q \in X_0^+(p^2)(K)$.

Let C_i, $1 \le i \le 3$, be the three 2-cyclic subgroups of $E^\nu[2]$. Since

$$T_2(Q^\nu) = \sum_{i=1}^{3} \pi^+((E^\nu/C_i, (C^\nu + C_i)/C_i)\,,$$

the condition $3(Q) = T_2(Q^\nu)$ implies that each elliptic curve E^ν/C_i is isomorphic to E or E/C. So, at least two quotients E^ν/C_i are isomorphic. By using the modular polynomial $\Phi_2(X, Y)$, one can check that there are exactly five j-invariants of elliptic curves for which the polynomial $\Phi_2(j, Y)$ has at least a double root. More precisely, E^ν must be an elliptic curve with CM by the order $\mathcal{O}$, where $\mathcal{O}$ is the ring of integers $\mathbb{Z}[\sqrt{-1}]$, $\mathbb{Z}[(1+\sqrt{-3})/2]$, $\mathbb{Z}[(1+\sqrt{-7})/2]$ or $\mathbb{Z}[(1+\sqrt{-15})/2]$. For the first three cases, E^ν is defined over $\mathbb{Q}$. For the last case, there are two possible curves E^ν defined over $\mathbb{Q}(\sqrt{5})$ which are Galois conjugated. Since $K = \mathbb{Q}(\sqrt{p*}) \neq \mathbb{Q}(\sqrt{5})$, in all cases we have $E^\nu = E$.

First, assume that E is defined over $\mathbb{Q}$, i.e. $j(E) \in \{0, 12^3, -15^3\}$. Let E' be the elliptic curve E/C_i isomorphic to another quotient E/C_j. In all cases, E' has CM by the order $\mathbb{Z} + 2\,\mathcal{O}$. Since E' is not isomorphic to E, it must be isomorphic to E/C. The composition of the cyclic isogenies $E' \to E$ and $E \to E/C = E'$ of degrees 2 and p^2 respectively is a $2p^2$-cyclic isogeny of E' to itself. This fact is not possible due to the fact that the order $\mathbb{Z} + 2\,\mathcal{O}$ does not have any elements of norm $2p^2$ because $2p^2 \equiv 2 \pmod 4$.

Now, assume that E is defined over $\mathbb{Q}(\sqrt{5})$ and not over $\mathbb{Q}$. Let F be the elliptic curve which is the nontrivial Galois conjugated of E. Since P is not defined over K, E/C must be F. In this case, it turns out that there are two 2-subgroups C_1 and C_2 of $E[2]$ such that E/C_1 and E/C_2 are isomorphic to F and none of the curves E and F are isomorphic to E/C_3. Hence, it is proved that D_S is a nonzero divisor.

By taking $S = u(\infty)$, D_S is defined over K and, thus, the K-gonality is at most 6. Finally, since $u^*(D_S) \neq D_S$ for some noncuspidal point $S \in X_0^+(p^2)(\mathbb{C})$, any nontrivial automorphism of $X_0^+(p^2)$ has at most 12 fixed points (cf. Lemma 3.5 of [BH03]). □

Lemma 7. *If $X_0^+(p^2)$ has a nontrivial automorphism and $p > 11$, then $p \in \{17, 19, 23, 29, 31\}$.*

Proof. By applying Lemma 3.25 of [BGGP05] for the prime 2, we obtain that

$$g^+ < |X_0^+(p^2)(\mathbb{F}_4)| + 1\,.$$

By Lemma 6, the $\mathbb{F}_4$-gonality of $X_0^+(p^2) \otimes \mathbb{F}_4$ is ≤ 6 and, thus, $|X_0^+(p^2)(\mathbb{F}_4)| \le 30$. Hence, $g^+ \le 30$, which implies $p \le 31$. The algebra $\mathrm{End}(J_0^+(13^2)) \otimes \mathbb{Q}$ is a totally real number field and, thus, it only contains the roots of unity ± 1. Since $X_0^+(13^2)$ is nonhyperelliptic, $\mathrm{Aut}(X_0^+(13^2))$ is trivial and we can discard the case $p = 13$. □

Lemma 8. *Every nontrivial automorphism of $X_0^+(p^2)$ has even order.*

Proof. Assume that there is a nontrivial automorphism u of $X_0^+(p^2)$ whose order m is odd. Let X_u be the quotient curve $X_0^+(p^2)/u$ and denote by g_u its genus. Next, we find a positive lower bound t for g_u.

The endomorphism algebra $\mathrm{End}_K(J_0^+(p^2)) \otimes \mathbb{Q}$ is the product of some noncommutative algebras and some number fields $E_f = \mathrm{End}_K(A_f) \otimes \mathbb{Q}$ attached to the newforms f lying in a certain subset $\mathcal{S}$ of $(\mathrm{New}_{p^2}^+ \cup \mathrm{New}_p)/G_{\mathbb{Q}}$. The set $\mathcal{S}$ is formed by newforms f without CM such that $f\otimes\chi\notin \mathrm{New}_{p^2}^+\cup\mathrm{New}_p$ ($E_f=\mathrm{End}_{\mathbb{Q}}(A_f)$ is a totally real number field) and by a newform f with CM by K if $p\equiv 3 \pmod 8$ ($E_f=\mathrm{End}_{\mathbb{Q}}(A_f)\otimes K$ is a CM field). For $f\in\mathcal{S}$, the unique root of unities contained in E_f are ± 1. Since m is odd, the automorphism u must act on each E_f as the identity and, thus, we have

$$t:=\sum_{f\in\mathcal{S}}\dim A_f\leq g_u\,.$$

An easy computation provides the following values for t:

p	17	19	23	29	31
g^+	7	9	15	26	30
t	5	5	7	15	12

Applying Riemann-Hurwitz formula,

$$m\leq\frac{g^+-1}{g_u-1}\leq\frac{g^+-1}{t-1}<3\,,$$

which yields a contradiction. □

5 Proof of Theorem 1

Assume that, for $p\in\{17,19,23,29,31\}$, there is a nontrivial automorphism $u\in\mathrm{Aut}_K(X_0^+(p^2))$. By Lemma 8, we can suppose that u is an involution. Let g_u be the genus of the quotient curve $X_0^+(p^2)/u$. We know that u has at most 12 fixed points. By Riemann-Hurwitz formula, we get that the number of fixed points by u must be even, say $2r$, and, moreover,

$$g_u=\frac{g^++1-r}{2}\,,\quad 0\leq r\leq 6\,.$$

If g^+ is even, then u can have 2, 6 or 10 ramification points, while for the case g^+ odd, u can have 0, 4, 8 or 12 such points.

For a prime $\ell\neq p$, the curve $X=X_0^+(p^2)$ has good reduction at ℓ. Let $\widetilde{X}$ be the reduction of X modulo ℓ. We write

$$N_\ell(n):=1+\ell^n-\sum_{i=1}^{2g^+}\alpha_i^n\,,$$

where $\alpha_1,\cdots,\alpha_{2g^+}$ are the roots of polynomial

$$\prod_{f\in\mathrm{New}_{p^2}^+\cup\mathrm{New}_p}(x^2-a_\ell(f)x+\ell)$$

and $a_\ell(f)$ is the ℓ-th Fourier coefficient of f. By Eichler-Shimura congruence, $N_\ell(n)=|\widetilde{X}(\mathbb{F}_{\ell^n})|$.

Let $\mathfrak{l}$ be a prime of K over ℓ with residue degree s. The reduction of $X\otimes K$ modulo $\mathfrak{l}$ is $\widetilde{X}\otimes\mathbb{F}_{\ell^s}$ which has an involution, say $\widetilde{u}$, with at most $2r$ fixed points. The automorphism $\widetilde{u}$ acts on the set $\widetilde{X}(\mathbb{F}_{\ell^{s\,n}})$ as a permutation. If $Q\in\cup_{i=1}^n\widetilde{X}(\mathbb{F}_{\ell^{s\,i}})$, then the set $\mathcal{S}_Q=\{\widetilde{u}^i(Q)\colon 1\leq i\leq 2\}$ is contained in $\cup_{i=1}^n\widetilde{X}(\mathbb{F}_{\ell^{s\,i}})$ and its cardinality is equal to 1 or 2 according to Q is a fixed point of $\widetilde{u}$ or not. Hence, almost all integers $R_\ell(n):=|\cup_{i=1}^n\widetilde{X}(\mathbb{F}_{\ell^{s\,i}})|$, $n\geq 1$, are equivalent to the number of fixed points of $\widetilde{u}$ mod 2 and, moreover, the sequence $\{R_\ell(n)\}_{n\geq 1}$ can only contain at most $2r$ or $2r-1$ changes of parity depending on whether $N_\ell(s)$ is even or odd. In other words, the sequence of integers $\{P_\ell(n)\}_{n\geq 1}$ defined by

$$0 \leq P_\ell(n) \leq 1 \quad \text{and} \quad P_\ell(n) = R_\ell(n+1) - R_\ell(n) \pmod 2\,,$$

can only contain at most $2r$ or $2r-1$ ones according to N_{ℓ^s} being even or odd.

Note that the integer $R_\ell(n+1) - R_\ell(n)$ can be obtained from the sequence $\{N_\ell(s\,n)\}$ by using

$$\widetilde{X}(\mathbb{F}_{\ell^{s\,d_1}}) \cap \widetilde{X}(\mathbb{F}_{\ell^{s\,d_2}}) = \widetilde{X}(\mathbb{F}_{\ell^{s\,\gcd(d_1,d_2)}})\,, \qquad \text{and if } d_1|d_2 \text{ then } \widetilde{X}(\mathbb{F}_{\ell^{s\,d_1}}) \cup \widetilde{X}(\mathbb{F}_{\ell^{s\,d_2}}) = \widetilde{X}(\mathbb{F}_{\ell^{s\,d_2}})\,.$$

More precisely, if $\{p_1, \cdots, p_k\}$ is the set of primes dividing $n+1$ and we put $d_i = (n+1)/p_i$ for $1 \leq i \leq k$, then

$$R_\ell(n+1) - R_\ell(n) = N_\ell(s(n+1)) - \sum_{j=1}^{k} (-1)^{j+1} \sum_{1\leq i_1<\cdots<i_j\leq k} N_\ell(s\gcd(d_{i_1}, \cdots, d_{i_j}))\,.$$

For the five possibilities for p, we have:

$p = 31$: $g^+ = 30$, $2r \leq 10$ and $\ell = 2$ splits in $K = \mathbb{Q}(\sqrt{-31})$. One has

$$N_2(1) = 9\,, \qquad \sum_{n\leq 36} P_2(n) = 10\,.$$

$p = 29$: $g^+ = 26$, $2r \leq 10$ and $\ell = 2$ is inert in $K = \mathbb{Q}(\sqrt{29})$. One has

$$N_2(2) = 42\,, \qquad \sum_{n\leq 42} P_2(n) = 11\,.$$

$p = 23$: $g^+ = 15$, $2r \leq 12$ and $\ell = 2$ splits in $K = \mathbb{Q}(\sqrt{-23})$. One has

$$N_2(1) = 8\,, \qquad \sum_{n\leq 38} P_2(n) = 13\,.$$

$p = 19$: $g^+ = 9$, $2r \leq 12$ and $\ell = 2$ is inert in $K = \mathbb{Q}(\sqrt{-19})$. One has

$$N_2(2) = 22\,, \qquad \sum_{n\leq 46} P_2(n) = 13\,.$$

$p = 17$: $g^+ = 7$, $2r \leq 12$ and $\ell = 2$ splits in $K = \mathbb{Q}(\sqrt{17})$. One has

$$N_2(1) = 6\,, \qquad \sum_{n\leq 46} P_2(n) = 13\,.$$

So, we can discard the five cases considered and the statement is proved.

References

[AL78] A. O. L. Atkin and Wen Ch'ing Winnie Li. Twists of newforms and pseudo-eigenvalues of W-operators. *Invent. Math.*, 48(3):221–243, 1978.

[Bar10] B. Baran. Normalizers of non-split Cartan subgroups, modular curves, and the class number one problem. *J. Number Theory*, 130(12):2753–2772, 2010.

[BC67] Z. I. Borevitch and I. R. Chafarevitch. *Théorie des nombres.* Traduit par Myriam et Jean-Luc Verley. Traduction faite d'après l'édition originale russe. Monographies Internationales de Mathématiques Modernes, No. 8. Gauthier-Villars, Paris, 1967.

[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. Baker and Y. Hasegawa. Automorphisms of $X_0^*(p)$. *J. Number Theory*, 100(1):72–87, 2003.

[Elk90] N. D. Elkies. The automorphism group of the modular curve $X_0(63)$. *Compositio Math.*, 74(2):203–208, 1990.

[GJU12] J. González and J. Jiménez-Urroz. The Sato-Tate distribution and the values of Fourier coefficients of modular newforms. *Experiment. Math.*, 21(1):84–102, 2012.

[GL11] J. González and J.-C. Lario. Modular elliptic directions with complex multiplication (with an application to Gross's elliptic curves). *Comment. Math. Helv.*, 86(2):317–351, 2011.

[KM88] M. A. Kenku and F. Momose. Automorphism groups of the modular curves $X_0(N)$. *Compositio Math.*, 65(1):51–80, 1988.

[MY00] S. D. Miller and T. Yang. Non-vanishing of the central derivative of canonical Hecke L-functions. *Math. Res. Lett.*, 7(2-3):263–277, 2000.

[Ogg74] A. P. Ogg. Hyperelliptic modular curves. *Bull. Soc. Math. France*, 102:449–462, 1974.

[Yan04] T. Yang. On CM abelian varieties over imaginary quadratic fields. *Math. Ann.*, 329(1):87–117, 2004.

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