ACTA ARITHMETICA
161.3 (2013)

Bielliptic and hyperelliptic modular curves $X(N)$ and the group $\mathrm{Aut}(X(N))$

by

Francesc Bars (Barcelona), Aristides Kontogeorgis (Athens) and Xavier Xarles (Barcelona)

Dedicated to the memory of F. Momose

1. Introduction. In this paper we discuss some basic problems on the modular curves $X(N)$. By $X(N)$ we mean a geometrically connected curve defined over $\mathbb{Q}$, which over the complex field $\mathbb{C}$ is given as a Riemann surface by the quotient of $\mathbb{H}^*$ modulo the modular subgroup

$$\Gamma(N)=\left\{\begin{pmatrix} a & b\\ c & d\end{pmatrix}\in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; \begin{pmatrix} a & b\\ c & d\end{pmatrix}\equiv\begin{pmatrix} 1 & 0\\ 0 & 1\end{pmatrix} \pmod N\right\},$$

where as usual we denote by $\mathbb{H}^*$ the union of the upper half-plane $\mathbb{H}$ together with the so-called cusps $\mathbb{Q}\cup\{\infty\}$. The modular curve $X(N)$ is defined over $\mathbb{Q}$ as the moduli space parametrizing generalized elliptic curves together with a full N-level structure. Concerning the definition of $X(N)$, we adopt the point of view of [8, Section 4] (see Section 2 for a detailed discussion).

One of the problems we solve is the determination of the integers $N\geq 7$ such that $X(N)$ is hyperelliptic or bielliptic. We show in Section 4 that none of these curves is hyperelliptic (Theorem 4.1) and they are bielliptic only for $N=7$ and 8 (Theorem 4.2).

The study of this problem for some other families of modular curves was initiated by Ogg (see [22] and [2]) with the case of the curves $X_0(N)$, and followed by the modular curves $X_1(N)$ in [20] and [14], and the curves $X_1(N,M)$ in [13] and [15].

In the last section we apply our results on hyperellipticity and biellipticity to study the finiteness of quadratic points of $X(N)$. In particular we can prove that the set of quadratic points of $X(N)$ over the cyclotomic field

2010 *Mathematics Subject Classification*: Primary 11G18; Secondary 11G30.
Key words and phrases: modular curve, automorphism, bielliptic, quadratic points.

DOI: 10.4064/aa161-3-6 © Instytut Matematyczny PAN, 2013

$\mathbb{Q}(\zeta_N)$ is always finite for $N > 6$, where ζ_N denotes, as usual, a primitive Nth root of unity.

In Section 3 we consider another important issue concerning the curve $X(N)$: the explicit determination of its automorphism group over $\mathbb{C}$, which we denote by $\mathrm{Aut}(X(N))$.

Recall that, for a modular curve X of genus greater than one and with modular group $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$, the quotient of the normalizer of Γ in $\mathrm{PSL}_2(\mathbb{R})$ by $\pm\Gamma$ always gives a subgroup of $\mathrm{Aut}(X)$. We denote this subgroup by $\mathrm{Norm}(\Gamma)/\pm\Gamma$. It is a quite difficult problem to determine when $\mathrm{Norm}(\Gamma)/\pm\Gamma$ coincides with the full group of automorphisms of the corresponding modular curve X (if it is of genus greater than one). An automorphism $v \in \mathrm{Aut}(X) \setminus (\mathrm{Norm}(\Gamma)/\pm\Gamma)$ is called *exceptional*.

Kenku and Momose [19] determined the full automorphism group for $X_0(N)$ with $N \neq 63$; Elkies [7] obtained $\mathrm{Aut}(X_0(63))$, and finally Harrison [12] corrected the Kenku–Momose statement for $\mathrm{Aut}(X_0(108))$ (1). In particular, there are exceptional automorphisms for $X_0(N)$ only for $N = 37, 63$ and 108. For the modular curve $X_1(N)$ and N square-free, Momose proved in [21] that there are no exceptional automorphisms.

Finally, let us explain briefly the history concerning $\mathrm{Aut}(X(N))$. J.-P. Serre in a letter to B. Mazur [25] computed that the automorphism groups of the modular curves $X(p)$ for p prime ≥ 7 are isomorphic to the simple groups $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$. Back in 1997, in a conference held in Sant Feliu de Guíxols, the second author met G. Cornelissen, who wanted to compute the automorphism group of the Drinfeld modular curves [6, Sec. 10] and asked if there is a generalization for composite N. After finishing the computation, the second author communicated the generalization to J.-P. Serre, who answered that he proved the theorem in the letter to Mazur, and the generalization for composite N should be known to the pioneers of modular forms; but we were not able to find a reference in the literature. Since there is new interest (see [4], [24]) in the automorphisms of the modular curves $X(N)$ and we are not aware of any reference for this computation, we believe that writing down a proof might be useful to the mathematical community.

2. Preliminary results on the curve $X(N)$. The (non-complete) Riemann surface $Y(N)(\mathbb{C})$ is constructed as the quotient of the upper half-plane $\mathbb{H}$ modulo the modular subgroup $\Gamma(N)$. The set $Y(N)(\mathbb{C})$ parametrizes the pairs $(E,(P_1,P_2))$, where E is an elliptic curve defined over $\mathbb{C}$, and P_1 and P_2 are points of order exactly N in $E(\mathbb{C})$, which generate the subgroup of N-torsion points and satisfy $e(P_1,P_2) = \exp(2\pi i/N)$, where e denotes the Weil pairing.

(1) We would like to mention that this correction does not affect the results in [2].

This interpretation can be used to give a model of the modular curve $Y(N)$ (and its completion $X(N)$) over other fields of characteristic not dividing N (or general schemes over $\mathrm{Spec}(\mathbb{Z}[1/N])$). We have two options: either we ignore the last condition on the Weil pairing, obtaining a non-geometrically connected curve, or we modify the moduli problem introducing the Weil pairing in some way. The first option is essentially the one taken by Deligne and Rappoport [3], and also by Katz and Mazur [18]. We consider here the second option, following for example Elkies [8, Section 4]. Over fields containing all the N-roots of unity μ_N the second curve is isomorphic to a connected component of the first.

Thus, we take the full modular curve $Y(N)$ (for $N > 2$) as the (geometrically connected) curve which over any field K (of characteristic not dividing N) parametrizes pairs (E, ϕ), where E is an elliptic curve over K and ϕ is a Weil-equivariant isomorphism of group schemes between $E[N]$, the kernel of the multiplication by N on E, and $\mathbb{Z}/N\mathbb{Z}\times\mu_N$. This means that

$$\langle\ ,\ \rangle \circ (\phi \times \phi) = e$$

where $e : E[N] \times E[N] \to \mu_N$ is the Weil pairing and $\langle\ ,\ \rangle$ is the natural (symplectic) self-pairing of $\mathbb{Z}/N\mathbb{Z} \times \mu_N$ given by

$$\langle (m, \xi), (n, \eta)\rangle := \xi^n \eta^{-m}.$$

The map ϕ is called the *N-level structure*. We denote by $X(N)$ the completion of $Y(N)$; it also has a moduli interpretation like $Y(N)$ by allowing generalized elliptic curves. For the cases $N = 1$ and 2 one takes the usual coarse moduli space (in both cases isomorphic to the projective line).

There are other options one can take to get a model of the curve $X(N)$; for example, one can take a fixed elliptic curve $\tilde{E}$, and consider the N-level structures ϕ given as Weil-equivariant isomorphisms between $E[N]$ and $\tilde{E}[N]$. One gets a twisted form of $X(N)$, usually denoted by $X_{\tilde{E}}(N)$ (see for example [10]).

Recall that the curve $X(1)$ is isomorphic (via the j-function) to the projective line $\mathbb{P}^1$. The canonical cover $X(N) \to X(1)$ that forgets the N-level structure is Galois over any field containing all the N-roots of unity, and with Galois group $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$. The degree of this cover is equal to

$$\delta_N := \begin{cases} (N^3/2)\prod_{p\mid N}(1-p^{-2}) & \text{if } N > 2,\\ 6 & \text{if } N = 2.\end{cases}$$

Moreover the genus g_N of $X(N)$ is equal to [27, p. 23]

$$g_N = 1 + \delta_N \frac{N-6}{12N}. \tag{2.1}$$

We see that the curves $X(2), X(3), X(4)$ and $X(5)$ are rational, while $X(6)$ is elliptic. For all other values $N \geq 7$ the curves $X(N)$ have genus > 1.

We now want to relate the curve $X(N)$ to some other modular curves. First, observe that we have natural "forgetful" maps $f_1 : X(N) \to X_1(N)$ given, in the moduli interpretation, by sending the pair (E, ϕ) to the pair $(E, \phi^{-1}((1,1)))$, since $\phi^{-1}((1,1))$ is a point of exact order N. Thus, we have maps $f_0 : X(N) \to X_0(N)$ obtained by composing the map f_1 with the forgetful map $\varrho : X_1(N) \to X_0(N)$. There is also another independent map $f_0' : X(N) \to X_0(N)$, which can be defined in terms of the moduli interpretation, as the map sending the pair (E, ϕ) to the pair $(E, \phi^{-1}(\{0\} \times \mu_N))$. If we see the curve $X(N)$ as the compactified quotient of $\mathbb{H}$ by a discrete subgroup, then we can interpret these maps f_1 and f_0' as the quotient maps of $X(N)$ by the subgroups

$$\Gamma_1(N) = \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\} \quad \text{and} \quad \Gamma^0(N) = \left\{ \begin{pmatrix} * & 0 \\ * & * \end{pmatrix} \right\}$$

of $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$, respectively.

Over a field containing a primitive N-root of unity ζ_N, there is a map $f_1' : X(N) \to X_1(N)$, which depends on ζ_N, given by assigning to the pair (E, ϕ), in the notation above, the N-torsion point $\phi^{-1}((0, \zeta_N))$. The map f_0' can be factored as $f_0' = \varrho \circ f_1'$.

We now recall a construction of natural maps from $X_1(N^2)$ to $X(N)$ and from $X(N)$ to $X_0(N^2)$, for which we do not know a precise reference (see, however, [18, Section 11.3.5], for the second morphism in the case $N = p^n$, p a prime).

Lemma 2.1. *Let $N \geq 3$ be an integer. Then there exist morphisms of curves $\pi_1 : X_1(N^2) \to X(N)$ of degree N and $\pi_0 : X(N) \to X_0(N^2)$ of degree $\varphi(N)/2$ defined over $\mathbb{Q}$, such that the composition $\pi_0 \circ \pi_1 : X_1(N^2) \to X_0(N^2)$ is the natural forgetful map. Moreover, the maps make the following diagram commutative:*

$$\begin{tikzcd}
 & & X_1(N^2) \arrow[d, "\pi_1"] \arrow[dddll, bend right] & & \\
 & & X(N) \arrow[ddll, "f_1"'] \arrow[dl, "\pi_0"'] \arrow[dddrr, bend left, "f_0'"] & & \\
 & X_0(N^2) \arrow[rr, leftrightarrow, "\omega_{N^2}"] \arrow[dd] & & X_0(N^2) \arrow[dd] & \\
X_1(N) \arrow[d] & & & & \\
X_0(N) \arrow[r, leftrightarrow, "\omega_N"] \arrow[drr] & X_0(N) & & X_0(N) \arrow[r, leftrightarrow, "\omega_N"] & X_0(N) \arrow[dll] \\
 & & X(1) & &
\end{tikzcd}$$

where ω_N and ω_{N^2} denote the Atkin–Lehner involutions, and the maps without label are the usual projection maps given by the forgetful maps.

Proof. We will construct the maps from $X_1(N^2)$ to $X_0(N)$ and from $X(N)$ to $X_0(N^2)$ in two equivalent ways. First, over the complex numbers, the map is deduced by observing that

$$\Gamma_1(N^2) \leq U^{-1}\Gamma(N)U \leq \Gamma_0(N^2), \quad \text{where} \quad U = \begin{pmatrix} 1 & 0 \\ 0 & 1/N \end{pmatrix}.$$

These maps can be defined over $\mathbb{Q}$ (or any field with characteristic prime to N) by using the moduli interpretation. First, the map from $X(N)$ to $X_0(N^2)$ can be described on $Y(N)$ by sending the point of $Y(N)$ given by an elliptic curve E and the N-level structure $\phi : E[N] \to \mathbb{Z}/N\mathbb{Z} \times \mu_N$ to the N^2-cyclic isogeny obtained by composing the dual of the N-isogeny $E \to E/F_1$ with the N-isogeny $E \to E/F_2$, where we consider the subgroups $F_1 := \phi^{-1}(\mathbb{Z}/N\mathbb{Z} \times \{1\})$ and $F_2 := \phi^{-1}(\{0\} \times \mu_N)$.

The morphism π_0 can also be interpreted as the natural map from $X(N)$ to $X(N)/C$, where C is the full Cartan subgroup of $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$ (formed by the diagonal matrices).

The map from $X_1(N^2)$ to $X(N)$ can be analogously described in the moduli interpretation for the points in $Y_1(N^2)$ over a field K, given as pairs (E, P) where E is an elliptic curve over K and P is a point of exact order N^2: Consider the point $Q := [N]P$, which has order N, and the elliptic curve $E' := E/\langle Q\rangle$. Then E' has two natural cyclic isogenies of degree N, the quotient $E' \to E/\langle P\rangle$ and the dual isogeny of $E \to E'$. The kernel F_1 of the first map is canonically isomorphic to $\mathbb{Z}/N\mathbb{Z}$, i.e. $F_1 \cong \mathbb{Z}/N\mathbb{Z}$, where the isomorphism is given by the point P. We denote by F_2 the kernel of the second isogeny $E' \to E$, dual of $E \to E'$. Then the two subgroups F_1 and F_2 have zero intersection and hence there must be a canonical isomorphism $F_2 \cong \mu_N$ given by the Weil pairing. Therefore we have a Weil-equivariant isomorphism $\phi : E'[N] = F_1 \oplus F_2 \cong \mathbb{Z}/N\mathbb{Z} \times \mu_N$.

The commutativity of the diagram is clear from the definition of the maps via the moduli interpretation of the curves. Recall that the natural projection map from $X_0(N^2)$ to $X_0(N)$ sends a non-cuspidal point (E, φ) of $Y_0(N^2)$ to the point (E, φ_1), where $\varphi = \varphi_2 \circ \varphi_1$ is the decomposition of the degree N^2 cyclic isogeny $\varphi : E \to E'$ as composition of two cyclic degree N isogenies, and that the Atkin–Lehner involution sends an isogeny to its dual.

Finally, the assertions on the degrees are easy over $\mathbb{C}$, taking into account that the subgroup $\Gamma_0(N^2)$ contains $-\mathrm{Id}_2$, but $\Gamma(N)$ and $\Gamma_1(N^2)$ do not. ∎

REMARK 2.2. This lemma implies that, for $N = 3$, 4 and 6, the moduli curves $X(N)$ and $X_0(N^2)$ are identical over $\mathbb{Q}(\zeta_N)$. This is analogous to the case of the curves $X_1(N)$ and $X_0(N)$ for $N = 3$, 4 and 6. Note that this does not imply that given an elliptic curve E over a field K and a cyclic subgroup scheme F of order 3 defined over K, then F contains a point of order 3; but there exists a (unique) quadratic twist E' of E such that the corresponding subgroup scheme F' of E' contains a point of order 3. Equivalently, there exists a point P in F, defined over a (quadratic) extension L, such that the pair $\{P, -P\}$ is defined over K. The same is true for $N = 4$ and 6, and, in general, for the elliptic curves whose j-invariant is in the image of the map $Y_1(N)(K) \to Y(1)(K) \xrightarrow{j} K$.

COROLLARY 2.3. *The curve $X(N)$ is isomorphic over $\mathbb{Q}$ to the fiber product of $X_1(N)$ and $X_0(N^2)$ over $X_0(N)$, with respect to the natural map $X_1(N) \to X_0(N)$ and the map $X_0(N^2) \to X_0(N) \xrightarrow{\omega_N} X_0(N)$ given by the composition of the natural map with the Atkin–Lehner involution ω_N.*

Proof. From the previous lemma and the universal property of the fiber product we have a natural map from $X(N)$ to the fiber product. In order to show it is an isomorphism we will prove they both parametrize the same moduli problem. The moduli problem parametrized by the fiber product is easily seen to be the triplets (E, P, φ) where E is an elliptic curve, P is a point of order exactly N, $\varphi : E'' \to E/\langle P\rangle$ is a degree N^2 cyclic isogeny such that $\varphi = \varphi_2 \circ \varphi_1$, where $\varphi_1 : E \to E/\langle P\rangle$ is the quotient isogeny. Now, the kernel of the dual of φ_2 is a subgroup scheme F of order N in E. From the condition $E/F \to E \to E/\langle P\rangle$ being a cyclic isogeny of degree N^2, we deduce that the subgroups F and $\langle P\rangle$ have zero intersection. Hence $E[N] \cong F \times \langle P\rangle \cong F \times \mathbb{Z}/N\mathbb{Z}$. The Weil pairing then implies that $F \cong \mu_N$ and that this isomorphism is compatible with the Weil pairing. ∎

3. The automorphism group of $X(N)$. Recall that the curves $X(N)$ have genus greater than two if $N \geq 7$, and their automorphism groups are bounded by the Hurwitz bound:

$$|\mathrm{Aut}(X(N))| \leq 84(g_N - 1). \tag{3.1}$$

It is also known that exactly three points of $X(1)$ are ramified in the cover $X(N) \to X(1)$, namely $j(i), j(\omega)$ and $j(\infty)$, with ramification indices $2, 3$ and N, respectively (j denotes the natural j-invariant isomorphism between $\mathbb{P}^1$ and $X(1)$). The main result of this section is the following:

THEOREM 3.1. *The automorphism group of $X(N)$ over $\mathbb{C}$ for values N such that $g_N \geq 2$ equals $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$.*

We will prove the theorem in several steps.

LEMMA 3.2. *Suppose* $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z}) \lhd \mathrm{Aut}(X(N))$ *then* $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z}) = \mathrm{Aut}(X(N))$.

Proof. Since $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z}) \lhd \mathrm{Aut}(X(N))$, we can restrict automorphisms in $\mathrm{Aut}(X(N))$ to automorphisms of $X(1) \cong \mathbb{P}^1$ and these automorphisms should fix the three ramification points. Therefore the restriction is the identity. ∎

Let m be the index of $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z}) = \mathrm{Gal}(X(N)/X(1))$ in $\mathrm{Aut}(X(N))$. The equation for the genus (2.1) for $N \neq 2$ can be written as

$$84(g_N - 1) = |\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})|(7 - 42/N), \tag{3.2}$$

and this combined with (3.1) gives the following bounds for the index m:

$$\begin{aligned} &m \le 2 && \text{for } 7 \le N < 11,\\ &m \le 3 && \text{for } 11 \le N < 14,\\ &m \le 4 && \text{for } 14 \le N < 21,\\ &m < 7 && \text{for } N \ge 21. \end{aligned} \tag{3.3}$$

Therefore, for $7 \le N < 11$ we have $\mathrm{Aut}(X(N)) \cong \mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$ by Lemma 3.2.

The following lemma is elementary.

Lemma 3.3. *Consider the coset decomposition*

$$\mathrm{Aut}(X(N)) = a_1\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z}) \cup \cdots \cup a_m\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z}),$$

and define the representation

$$\beta : \mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z}) \to S_m$$

by

$$\sigma \mapsto \{\sigma a_1\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z}), \ldots, \sigma a_m\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})\}.$$

Then $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z}) \lhd \mathrm{Aut}(X(N))$ *if and only if* β *is the trivial homomorphism.*

Lemma 3.4. *If $N = p$ is a prime ≥ 7 then $\beta = 1$.*

Proof. Since $\mathrm{PSL}_2(p)$ is simple, $\ker\beta$ is either $\mathrm{PSL}_2(p)$ or $\{1\}$. The last case is impossible since there are no elements of order p in S_m, for $m \le 6$. ∎

Let us now consider the curves $X(p^e)$ where p is prime ≥ 7.

Lemma 3.5. *For $X(p^e)$ with $p \ge 7$ we have* $\mathrm{Aut}(X(p^e)) = \mathrm{PSL}_2(p^e)$.

Proof. We will prove that $\beta = 1$ for the map β defined in Lemma 3.3.

We consider the following tower of covers:

$$\begin{tikzcd} X(p^e) \arrow[d, "H"] \arrow[dd, bend right, "\mathrm{PSL}_2(\mathbb{Z}/p^e\mathbb{Z})"'] \\ X(p) \arrow[d, "\mathrm{PSL}_2(p)"] \\ X(1) \end{tikzcd}$$

Consider $H := \mathrm{Gal}(X(p^e)/X(p))$; then $|H| = p^{3(e-1)}$, and, since $p \geq 7$, we have $H < \ker \beta$. Therefore, we can define the homomorphism $\tilde{\beta}$ so that the following diagram is commutative:

$$\begin{tikzcd} \mathrm{PSL}_2(\mathbb{Z}/p^e\mathbb{Z}) \arrow[r, "\beta"] \arrow[d] & S_m \\ \mathrm{PSL}_2(p) \arrow[ur, "\tilde{\beta}"'] & \end{tikzcd}$$

Again, since $\mathrm{PSL}_2(p)$ is simple, we obtain $\tilde{\beta} = 1$ and so $\beta = 1$ too. ■

Corollary 3.6. *Let N be a composite integer prime to $2, 3, 5$. Then $\mathrm{Aut}(X(N)) = \mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$.*

Proof. The homomorphism β is trivial in this case as well, since

$$\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z}) \cong \bigoplus_{i=1}^{s} \mathrm{PSL}_2(\mathbb{Z}/p_i^{a_i}\mathbb{Z}),$$

where $N = \prod_{i=1}^{s} p_i^{a_i}$ is the prime factorization of N. ■

End of proof of Theorem 3.1. In order to study the case of general N we will need better bounds for the index

$$m := [\mathrm{Aut}(X(N)) : \mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})].$$

We consider the tower of covers

$$\begin{tikzcd} X(N) \arrow[d, "\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})"] \arrow[dd, bend right, "\mathrm{Aut}(X(N))"'] & \arrow[d, dash, "2"'] & \arrow[d, dash, "3"'] & \arrow[d, dash, "N"'] \\ X(1) \arrow[d] & j(i) & j(\omega) & j(\infty) \\ X(N)^{\mathrm{Aut}(X(N))} & & & \end{tikzcd}$$

Observe that if $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$ is not a normal subgroup of $\mathrm{Aut}(X(N))$ then the cover $X(1) \cong \mathbb{P}^1 \to X(N)^{\mathrm{Aut}(X(N))}$ is not Galois. From the proof of inequality (3.1) in [9, p. 260], we see that if the number r of points of $X(1)$ ramified in the cover $X(N) \to X(N)^{\mathrm{Aut}(X(N))}$ is $r > 3$, then Hurwitz's bound is improved to

$$|\mathrm{Aut}(X(N))| \leq 12(g_N - 1).$$

This proves that $m \leq 1$, so $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z}) \lhd \mathrm{Aut}(X(N))$, a contradiction.

Therefore the number of ramified points is $r = 3$. Now Hurwitz's bound for $X(N) \to X(N)^{\mathrm{Aut}(X(N))}$ gives

$$2(g_N - 1) = |\mathrm{Aut}(X(N))| \left(1 - \frac{1}{\nu_1} + 1 - \frac{1}{\nu_2} + 1 - \frac{1}{\nu_3} - 2\right), \tag{3.4}$$

where ν_i are the ramification indices of the ramified points of the cover $X(N) \to X(N)^{\mathrm{Aut}(X(N))}$. We distinguish the following cases:

Case 1: The three points $j(i), j(\omega), j(\infty)$ restrict to different points p_1, p_2, p_3 with ramification indices $e(j(i)/p_1) = \kappa$, $e(j(\omega)/p_2) = \lambda$, $e(j(\infty)/p_3) = \mu$. Equation (3.4) in this case reads

$$\begin{aligned} 2(g_N - 1) &= |\mathrm{Aut}(X(N))| \left(1 - \frac{1}{2\kappa} + 1 - \frac{1}{3\lambda} + 1 - \frac{1}{N\mu} - 2\right) \\ &\geq |\mathrm{Aut}(X(N))| \left(1 - \frac{1}{2} + 1 - \frac{1}{3} + 1 - \frac{1}{N} - 2\right) \\ &\geq |\mathrm{Aut}(X(N))| \left(\frac{1}{6} - \frac{1}{N}\right), \end{aligned}$$

which in turn gives the desired result

$$|\mathrm{Aut}(X(N))| \leq \frac{12N}{N-6}(g_N - 1) = \delta_N.$$

Case 2: Some of the three points $j(i), j(\omega), j(\infty)$ restrict to the same point $X(N)^{\mathrm{Aut}(X(N))}$. We will consider the case $N \geq 11$. First, let us see that the points $j(i)$ and $j(\infty)$ could not restrict to the same point of $X(N)^{\mathrm{Aut}(X(N))}$. Since the cover $X(N) \to X(N)^{\mathrm{Aut}(X(N))}$ is Galois we should have $2\kappa = N\mu$ (with the notation used in Case 1). But the degree of the cover $X(1) \to X(N)^{\mathrm{Aut}(X(N))}$ is at most $m \leq 6$, so $\kappa \leq m \leq 6$ and $\mu = 1$, and this means that $j(i)$ and $j(\infty)$ could not restrict to the same point, unless $N \leq 12$. But if $N \leq 12$ then $\kappa \leq m \leq 3$, so $N \leq 6$, which contradicts $N \geq 11$. Using the same argument we can show that the points $j(\omega)$ and $j(\infty)$ restrict to different points of $X(N)^{\mathrm{Aut}(X(N))}$.

Hence, we can suppose that only the points $j(i)$ and $j(\omega)$ restrict to the same point p_1 of $X(N)^{\mathrm{Aut}(X(N))}$. Thus, there should be another point p of $X(N)^{\mathrm{Aut}(X(N))}$ which ramifies only in the cover $X(1) \to X(N)^{\mathrm{Aut}(X(N))}$ with ramification index $2 \leq \nu \leq 6$. The point p_1 should have ramification index in $X(N) \to X(N)^{\mathrm{Aut}(X(N))}$ equal to $6\psi = 2\psi_1 = 3\psi_2$, where ψ_1 and

ψ_2 are ≤ 6 and denote the ramification indices of $j(i)$ and $j(\omega)$ in the cover $X(1) \to X(N)^{\mathrm{Aut}(X(N))}$. The Hurwitz bound implies

$$\begin{aligned}2(g_N - 1) &= |\mathrm{Aut}(X(N))|\left(1 - \frac{1}{6\psi} + 1 - \frac{1}{\phi N} + 1 - \frac{1}{\nu} - 2\right)\\ &\overset{\nu\geq 2,\psi=1\,\mathrm{or}\,2}{\geq} |\mathrm{Aut}(X(N))|\left(\frac{1}{3} - \frac{1}{N}\right) \overset{N\geq 11}{\geq} |\mathrm{Aut}(X(N))|\left(\frac{1}{3} - \frac{1}{11}\right),\end{aligned}$$

which gives

$$|\mathrm{Aut}(X(N))| \leq \tfrac{33}{4}(g_N - 1)$$

and in turn gives the desired result $m \leq 1$. ∎

Recall that $\mathrm{Aut}(\mathbb{H})$ is isomorphic to $\mathrm{PSL}_2(\mathbb{R})$, and $\Gamma(N)$ is torsion-free if $N \geq 5$, thus the automorphism group of $Y(N) = \mathbb{H}/\Gamma(N)$ is the quotient of the normalizer of $\Gamma(N)$ in $\mathrm{PSL}_2(\mathbb{R})$ by $\pm\Gamma(N)$.

Corollary 3.7. *For $N \geq 7$ we have* $\mathrm{Aut}(Y(N)) \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1$ *and the order of the group of automorphisms of $Y(N)$ is given by*

$$\tfrac{1}{2}N\varphi(N)\psi(N)$$

where $\varphi(N) := N\prod_{p|N}(1 - p^{-1})$ and $\psi(N) := N\prod_{p|N}(1 + p^{-1})$ with p prime.

In particular the normalizer of $\Gamma(N)$ in $\mathrm{PSL}_2(\mathbb{R})$ *is given by* $\mathrm{PSL}_2(\mathbb{Z})$ *and* $\mathrm{Norm}(\Gamma(N))/\pm\Gamma(N) \cong \mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$.

Proof. Clearly for $N \geq 5$, $\pm\Gamma(N) \leq \mathrm{PSL}_2(\mathbb{Z}) \leq \mathrm{Norm}(\Gamma(N)) \leq \mathrm{PSL}_2(\mathbb{R})$. It is known that for any Riemann surface Y with universal cover $\mathbb{H}$ such that $Y = \mathbb{H}/K$ with $K \leq \mathrm{PSL}_2(\mathbb{R})$, the group $\mathrm{Aut}(Y)$ is the normalizer of K in $\mathrm{PSL}_2(\mathbb{R})$ modulo K, in particular $\mathrm{Aut}(Y(N))$ is the normalizer of $\pm\Gamma(N)$ in $\mathrm{PSL}_2(\mathbb{R})$ modulo $\pm\Gamma(N)$. Recall also that if X is any compact Riemann surface and $Y = X - \{v_1, \ldots, v_n\}$ with v_i certain points of X, then any automorphism of Y lifts to an automorphism of X, in particular always $\mathrm{Aut}(Y(N)) \leq \mathrm{Aut}(X(N))$. Thus

$$\mathrm{PSL}_2(\mathbb{Z})/\pm\Gamma(N) \leq \mathrm{Norm}(\Gamma(N))/\pm\Gamma(N) = \mathrm{Aut}(Y(N)) \leq \mathrm{Aut}(X(N));$$

but $\mathrm{PSL}_2(\mathbb{Z})/\pm\Gamma(N)$ is isomorphic to $\mathrm{Aut}(X(N))$ for $N \geq 7$, giving the result. ∎

4. Hyperelliptic and bielliptic modular curves $X(N)$. Recall that a non-singular projective curve C of genus $g_C > 1$ over an algebraically closed field of characteristic zero is hyperelliptic if it has an involution $v \in \mathrm{Aut}(C)$, called a *hyperelliptic involution*, which fixes $2g_C + 2$ points (see, for example, [26, §1]). This involution v is unique if $g_C \geq 2$. Similarly, the curve C is bielliptic if it has an involution $w \in \mathrm{Aut}(C)$, named *bielliptic*, which fixes $2g_C - 2$ points. This involution is unique if $g_C \geq 6$.

In this section we want to determine for exactly which integers $N \geq 7$ the curve $X(N)$ is hyperelliptic or bielliptic over $\mathbb{C}$. Since $X(N)$ is naturally isomorphic over the cyclotomic field $\mathbb{Q}(\zeta_N)$ to the curve $X_1(N,N)$, these results can also be deduced from the results of Ishii–Momose [13] in the hyperelliptic case, and of Jeon–Kim [15] in the bielliptic case ([2]). Here we present a distinct and direct proof.

THEOREM 4.1. *For $N \geq 7$ the modular curve $X(N)$ is not hyperelliptic.*

THEOREM 4.2. *For $N \geq 7$ the modular curve $X(N)$ is bielliptic only when $N = 7$ or $N = 8$.*

Before we proceed to the proof of the theorems, we collect some results we will use. Observe first that, given a morphism of non-singular projective curves, $\phi : X \to Y$, which is a Galois cover (in the sense that it is given by a quotient map of the form $X \to X/H$, for H a subgroup of the group of automorphisms of X), and given ν an involution on X, if ν satisfies $\nu H = H\nu$, then either ν induces, via ϕ, an element of the Galois group H of the cover, or it induces an involution on Y.

LEMMA 4.3. *Consider a Galois cover $\phi : X \to Y$ of degree d between two non-singular projective curves of genus $g_X \geq 2$ and g_Y, respectively. Suppose that $g_Y \geq 2$ or d is odd.*

(1) *Suppose that $2g_X + 2 > d(2g_Y + 2)$. Then X is not hyperelliptic.*
(2) *Denote by n_ι the number of fixed points of an involution ι of Y. Suppose $2g_X - 2 > dn_\iota$ for any involution ι on Y. Then, if $g_X \geq 6$, X is not bielliptic.*
(3) *Suppose $2g_X - 2 > d(2g_Y + 2)$. Then, if $g_X \geq 6$, X is not bielliptic.*

Proof. If v, a hyperelliptic or bielliptic involution, is in the group of the Galois cover ϕ, then we have the following factorization of ϕ:

$$X \to X/\langle v\rangle \to Y,$$

which is impossible if d is odd, since $X \to X/\langle v\rangle$ has degree 2, and also if $g_Y \geq 2$, since $X/\langle v\rangle$ has genus ≤ 1.

Suppose now that X has a hyperelliptic or bielliptic involution v, which induces an involution $\tilde{v}$ on Y. Then the involution v can have fixed points only among the points lying above the fixed points of $\tilde{v}$ on Y, and hence the map v has at most $dn_{\tilde{v}}$ fixed points, where $n_{\tilde{v}}$ denotes the number of fixed points of $\tilde{v}$ on Y. By Hurwitz's formula, the involution v must have $2g_X + 2$

([2]) The proofs of some results in [13] use the claim that there do not exist exceptional automorphisms for intermediate modular curves [21], but Andreas Schweizer informed us that this claim is false (see the forthcoming work [16]). This correction does not affect the result on $X_1(N,N)$ in [13] and [15], but here we present a proof without using any of the statements in [21].

fixed points in the hyperelliptic case, or $2g_X - 2$ fixed points in the bielliptic case. We get the result under our hypothesis, since hyperelliptic involutions and bielliptic involutions on X are (unique and) in the center of $\mathrm{Aut}(X)$ (see [26, Proposition 1.2]). ∎

The following lemmas can be easily proved over $\mathbb{C}$ by observing that both curves attain the maximal order of the group of automorphisms for their genus. Recall that from the main result in Section 3 we have $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1 \cong \mathrm{Aut}(X(N))$. Now, the maximal order of the automorphism group for a genus 3 curve is 164 (given by the Hurwitz bound), and $|\mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z})/\pm 1| = 164$; moreover, the maximal order of this group for genus 5 is 192 and $|\mathrm{SL}_2(\mathbb{Z}/8\mathbb{Z})/\pm 1| = 192$. The first lemma is proved by Elkies [8].

Lemma 4.4. *The curve $X(7)$ is a genus 3 curve isomorphic over $\mathbb{Q}$ to the Klein quartic which is a bielliptic curve and is not hyperelliptic.*

Recall that the Klein curve is the curve over $\mathbb{Q}$ defined by the quartic equation

$$x^3y + y^3z + z^3x = 0.$$

Similarly, we take the model W defined over $\mathbb{Q}$ of the Wiman curve (which has the maximal order of the automorphism group for a genus 5 curve over $\mathbb{C}$) given as the intersection of the following three quadrics in $\mathbb{P}^4$:

$$x_0^2 = x_3x_4, \quad x_3^2 = 4x_1^2 + x_2^2, \quad x_4^2 = x_1x_2.$$

Lemma 4.5. *The curve $X(8)$ is a genus 5 curve isomorphic over $\mathbb{Q}$ to the Wiman curve W, which is a bielliptic curve and is not hyperelliptic.*

Proof. One can easily see that W is a curve with the same group of automorphisms as $X(8)$ over $\mathbb{C}$. Since there is only one such curve over $\mathbb{C}$, we infer that they are isomorphic over $\mathbb{C}$.

Consider the involution of W over $\mathbb{Q}$ given by

$$\iota_1(x_0, x_1, x_2, x_3, x_4) = (x_0, x_1, x_2, -x_3, -x_4).$$

The quotient curve W/ι_1 has equation

$$x_0^4 = x_1x_2(4x_1^2 + x_2^2)$$

and is isomorphic to the curve $X_0(64)$ over $\mathbb{Q}$ (e.g. by a computation via [5]).

Hence $X(8)$ and W are curves over $\mathbb{Q}$, isomorphic over $\mathbb{C}$, and both unramified degree two covers of the same curve over $\mathbb{Q}$. Moreover, one can see that there is only one involution of W defined over $\mathbb{C}$ whose quotient is $X_0(64)$: in fact, there are four involutions without fixed points; three of them give quotients of genus three that are hyperelliptic and one gives $X_0(64)$ (see also [17, Subsection 3.2]). We deduce that the cover $f : W \to X_0(64)$ must be a twisted form (over $\mathbb{Q}$) of the cover $X(8) \to X_0(64)$.

The twisted forms of a fixed (degree 2) unramified covering are well-known. In our case they can be described as the curves W_d given by

$$x_0^2 = x_3x_4, \quad dx_3^2 = 4x_1^2 + x_2^2, \quad x_4^2 = dx_1x_2,$$

where d is a squarefree integer, together with the natural map f to $X_0(64)$ given by $f_d(x_0, x_1, x_2, x_3, x_4) = (x_0, x_1, x_2)$. Now, since the covering f is unramified, the subsets $f_d(W_d(\mathbb{Q}))$ do not intersect for distinct covers and they give a partition of the set $X_0(64)(\mathbb{Q})$. This implies that only a finite number of covers do have rational points. In our case, since $X_0(64)$ has four $\mathbb{Q}$-rational points corresponding to the cusps, a simple computation shows that only $W = W_1$ and W_2 have $\mathbb{Q}$-rational points; both have four $\mathbb{Q}$-rational points, each one covering two points of $X_0(64)(\mathbb{Q})$.

Since $X(8)$ does have rational points (some cusps), the curve $X(8)$ is isomorphic to either W or W_2 over $\mathbb{Q}$. But, although W and W_2 produce distinct coverings of $X_0(64)$ over $\mathbb{Q}$, they are isomorphic as curves over $\mathbb{Q}$. An explicit isomorphism $\psi : W_2 \to W$ is given by

$$\psi(x_0, x_1, x_2, x_3, x_4) = (2x_0 - 2x_4, 2x_3 - 4x_2, 2x_1 + x_3 + 2x_2, -4x_1 + 2x_3 + 4x_2). \ \blacksquare$$

REMARK 4.6. A computation with MAGMA reveals that the curve W is also isomorphic over $\mathbb{Q}$ to the model of $X(8)$ over $\mathbb{Q}$ given by Yang in [29, Table, p. 507]. Moreover, it has a degree 2 map to an elliptic curve isogenous to $X_0(32)$. In fact, $X(8)$ has three different bielliptic involutions (see [17] or the next section).

Finally, we recall that the curve $X_0(N^2)$ has genus > 1 if and only if $N \geq 8$. For them we have the following special case of a result cited in the Introduction.

PROPOSITION 4.7 (Ogg–Bars, [22], [2]). *The curve $X_0(N^2)$ with $g_{X_0(N^2)} \geq 2$ is never hyperelliptic, and it is bielliptic exactly for $N = 8$ and 9.*

Now we can proceed to the proof of the main theorems of the section.

Proof of Theorem 4.1. First of all, recall that, if $f : C \to C'$ is a non-constant morphism between non-singular projective curves such that the genus of C' is ≥ 2, and C is hyperelliptic, then C' is hyperelliptic.

Since $X_0(N^2)$ is never hyperelliptic if the genus is larger than 1 by Proposition 4.7, i.e. if $N > 7$, we see that $X(N)$ cannot be hyperelliptic unless $N = 7$. But this case was already considered in Lemma 4.4. $\blacksquare$

Proof of Theorem 4.2. Recall the following result by Harris and Silverman [11]: Let $\phi : C \to C'$ be a non-constant morphism between non-singular projective curves such that the genus of C' is ≥ 2. If C is bielliptic then C' is bielliptic or hyperelliptic.

Now, the result follows for $N > 9$ by using the map to $X_0(N^2)$ given in Lemma 2.1 and the result in Proposition 4.7. The cases $N = 7$ and 8 were already considered in Lemmas 4.4 and 4.5. It only remains to show that $X(9)$ is not bielliptic.

Recall that the genus of $X(9)$ is $10 > 6$. We will construct a map ρ, which is a Galois cover (over $\mathbb{C}$) and satisfies the conditions of Lemma 4.3(3). Consider the (singular) model of $X(9)$ given by $y^6 - x(x^3+1)y^3 = x^5(x^3+1)^2$ [29, p. 507] (although this model is defined over $\mathbb{Q}$, we do not know if it is isomorphic to $X(9)$ over $\mathbb{Q}$). Now let E' be the curve given by the equation

$$z^2 - x(x^3+1)z = x^5(x^3+1)^2.$$

We get a map ρ from $X(9)$ to E' by taking $z = y^3$, which has degree 3 (hence odd) and is Galois. The curve E' is an elliptic curve isomorphic to $E : t^2 - t = x^3$ by writing $t := z/(x(x^3+1))$. By applying Lemma 4.3(3), and since

$$2g(X(9)) - 2 = 2\cdot 10 - 2 = 18 > \deg(\rho)(2g(E)+2) = 3\cdot(2\cdot 1+2) = 12,$$

we conclude that $X(9)$ is not bielliptic. ∎

Remark 4.8. It is possible to describe theoretically the construction in the last proof for the case $X(9)$. First, consider the map $f_0 : X(9) \to X_0(81)$ given by Lemma 2.1; it is a degree 3 map to a curve of genus 4. Then, consider the degree 3 map $\pi : X_0(81) \to X_0(27)$, where the target is an elliptic curve. Finally, let E be the elliptic curve, given by the simple equation $y^2 - y = x^3$. The curve E is 3-isogenous (over $\mathbb{Q}$) to the curve $X_0(27)$. The map ρ makes the following diagram commutative:

$$\begin{tikzcd} X(9) \arrow[r, "f_1"] \arrow[d, "\rho"'] & X_0(81) \arrow[d, "\pi"] \\ E \arrow[r] & X_0(27) \end{tikzcd}$$

An analogous construction (but with degree 2 maps) can also be done for the curve $X(8)$.

5. On quadratic points for $X(N)$. Let C be a non-singular curve of genus greater than one, defined over a number field K. Mordell's conjecture, proved by Faltings, states that the set of K-rational points $C(K)$ of C is always finite. In order to generalize this, it is natural to consider the set

$$\Gamma_d(C,K) = \bigcup_{[L:K]\le d} C(L)$$

of points of degree d of C over K. For quadratic points, that is, $d = 2$, Harris and Silverman [11] showed that $\Gamma_2(C,F)$ is not finite for some finite extension F of K if and only if the curve C is either hyperelliptic or bielliptic. Hence, the following result is a direct consequence of Theorems 4.1 and 4.2.

Corollary 5.1. *The only modular curves $X(N)$ of genus ≥ 2 such that there exists a number field L where the set $\Gamma_2(X(N), L)$ is not finite are $X(7)$ and $X(8)$.*

Now, we can ask if, for $N = 7$ or $N = 8$, there are infinitely many quadratic points over the cyclotomic field $\mathbb{Q}(\zeta_N)$ (which is the smallest field where they can have non-cuspidal rational points).

Theorem 5.2. *For all $N \geq 7$, the number of quadratic points of $X(N)$ over $F := \mathbb{Q}(\zeta_N)$ is always finite.*

Proof. By the corollary above, we only need to study $N = 7$ or $N = 8$.

If $C(F) \neq \emptyset$, then by [1] we have: $\#\Gamma_2(C, F) = \infty$ with C a non-singular curve over F if and only if C is hyperelliptic or has a degree 2 morphism $\varphi : C \to E$ all defined over F, with E an elliptic curve of $\operatorname{rank}_{\mathbb{Z}} E(F) \geq 1$.

It is known (see for example [23]) that $\operatorname{Jac}(X(7))$ over $\mathbb{Q}(\zeta_7)$ is isomorphic to E^3, where E is the elliptic curve $y^2 + 3xy + y = x^3 - 2x - 3$, which is isomorphic to $X_0(7^2)$. Therefore, since $X(7)$ is non-hyperelliptic, we have an infinite number of quadratic points over $\mathbb{Q}(\zeta_7)$ only if there is a degree 2 map $X(7) \to E'$ defined over $\mathbb{Q}(\zeta_7)$, where E' is an elliptic curve of positive rank over $\mathbb{Q}(\zeta_7)$. But then, necessarily, E' is isogenous to E and, in particular, $\operatorname{rank}_{\mathbb{Z}} E'(\mathbb{Q}(\zeta_7)) = \operatorname{rank}_{\mathbb{Z}} E(\mathbb{Q}(\zeta_7))$. But the last rank is zero, as a (2-Selmer) computation with `MAGMA` [5] or `SAGE` [28] reveals.

For $N = 8$, consider the equations over $\mathbb{Q}$ given above. Some computations with `MAGMA` show that the group of automorphisms over $\mathbb{Q}$ is abelian and isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$, and the quotient $X(N)/\langle\sigma\rangle$ with respect to two of the elements σ of $\operatorname{Aut}(X(8))$ gives the elliptic curve E with equation $y^2 = x^3 - x$ of conductor 32, and by a third element gives the elliptic curve E' with equation $y^2 = x^3 + x$ of conductor 64. By [17] there are exactly three bielliptic involutions for $X(8)$, so these are all of them. The elliptic curves E and E' become isomorphic over $\mathbb{Q}(\zeta_8)$. Hence, they have the same rank. Finally, a (2-Selmer) computation with `MAGMA` or `SAGE` reveals that $\operatorname{rank}_{\mathbb{Z}} E(\mathbb{Q}(\zeta_8)) = 0$, proving the result. ∎

Remark 5.3. A computation with `MAGMA` shows that

$$\#\Gamma_2(X(8), \mathbb{Q}(\zeta_8)) = 24,$$

corresponding to the cusps. This result is obtained by computing all the quadratic points of $X_0(8^2)$ over $\mathbb{Q}(\zeta_8)$. The curve $X_0(8^2)$ is a genus 3 curve, with Jacobian isogenous to the cube of the elliptic curve $X_0(32)$ over $\mathbb{Q}(\zeta_8)$, which has only a finite number of points over $\mathbb{Q}(\zeta_8)$. Then we compute the inverse image with respect to the the degree 2 map $X(8) \to X_0(32)$. We find that although there are points in $\Gamma_2(X_0(32), \mathbb{Q}(\zeta_8))$ which do not come from cusps (there are more than one hundred points), none of them lift to a quadratic point of $X(8)$.

Acknowledgements. The second author wishes to thank G. Cornelissen for pointing out the problem of automorphisms of $X(N)$. The first and third authors would like to thank J. González for warning us about some results by Carayol and for his useful remarks on the writing of this note; they also thank E. González-Jiménez for his comments. We are pleased to thank A. Schweizer for his suggestions and comments. We thank our colleague H. D. Stainsby for proof-reading our English. Finally, we thank the referee for all the remarks and suggestions in order to improve the paper.

F. Bars and X. Xarles are partially supported by grant MTM2009-10359.

References

[1] D. Abramovich and J. Harris, *Abelian varieties and curves in* $W_d(C)$, Compos. Math. 78 (1991), 227–238.

[2] F. Bars, *Bielliptic modular curves*, J. Number Theory 76 (1999), 154–165.

[3] P. Deligne et M. Rapoport, *Les schémas de modules des courbes elliptiques*, in: Modular Functions of One Variable II, Lecture Notes in Math. 349, Springer, 1973, 143–316.

[4] P. Bending, A. Camina and R. Guralnick, *Automorphisms of the modular curve*, in: Progress in Galois Theory, Dev. Math. 12, Springer, 2005, 25–37.

[5] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. 24 (1997), 235–265.

[6] G. Cornelissen, F. Kato and A. Kontogeorgis, *Discontinuous groups in positive characteristic and automorphisms of Mumford curves*, Math. Ann. 320 (2001), 55–85.

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

[8] N. D. Elkies, *The Klein quartic in number theory*, in: The Eightfold Way: The Beauty of Klein's Quartic Curve, S. Levy (ed.), Cambridge Univ. Press, 1999, 51–102.

[9] H. M. Farkas and I. Kra, *Riemann Surfaces*, 2nd ed., Grad. Texts in Math. 71, Springer, 1992.

[10] E. Halberstadt and A. Kraus, *Sur la courbe modulaire* $X_E(7)$, Experiment. Math. 12 (2003), 27–40.

[11] J. Harris and J. H. Silverman, *Bielliptic curves and symmetric products*, Proc. Amer. Math. Soc. 112 (1991), 347–356.

[12] M. Harrison, *A new automorphism of* $X_0(108)$, arXiv:1108.55952011 (2011).

[13] N. Ishii and F. Momose, *Hyperelliptic modular curves*, Tsukuba J. Math. 15 (1991), 413–423.

[14] D. Jeon and C. H. Kim, *Bielliptic modular curves* $X_1(N)$, Acta Arith. 112 (2004), 75–86.

[15] D. Jeon and C. H. Kim, *Bielliptic modular curves* $X_1(M,N)$, Manuscripta Math. 118 (2005), 455–466.

[16] D. Jeon, C. H. Kim and A. Schweizer, *Bielliptic intermediate modular curve*, work in progress.

[17] T. Kato, M. Magaard and H. Völklein, *Bi-elliptic Weierstrass points on curves of genus 5*, Indag. Math. (N.S.) 22 (2011), 116–130.

[18] N. M. Katz and B. Mazur, *Arithmetic Moduli of Elliptic Curves*, Ann. of Math. Stud. 108, Princeton Univ. Press, 1985.

[19] M. A. Kenku and F. Momose, *Automorphism groups of modular curves $X_0(N)$*, Compos. Math. 65 (1988), 51–80.

[20] J.-F. Mestre, *Corps euclidiens, unités exceptionnelles et courbes elliptiques*, J. Number Theory 13 (1981), 123–137.

[21] F. Momose, *Automorphism groups of the modular curves $X_1(N)$*, preprint.

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

[23] D. T. Prapavessi, *On the Jacobian of the Klein curve*, Proc. Amer. Math. Soc. 122 (1994), 971–978.

[24] C. Ritzenthaler, *Automorphismes des courbes modulaires $X(n)$ en caractéristique p*, Manuscripta Math. 109 (2002), 49–62.

[25] J.-P. Serre, *The automorphism group of X(p)*, appendix to: B. Mazur, Open problems regarding rational points on curves and varieties, in: Galois Representations in Arithmetic Algebraic Geometry, A. J. Scholl and R. L. Taylor (eds.), London Math. Soc. Lecture Note Ser. 254, Cambridge Univ. Press, 1988.

[26] A. Schweizer, *Bielliptic Drinfeld modular curves*, Asian J. Math. 5 (2001), 705–720.

[27] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Publ. Math. Soc. Japan 11, Princeton Univ. Press, 1971.

[28] W. Stein et al., *Sage: Open Source Mathematical Software (Version 4.3)*, The Sage Group, http://www.sagemath.org, 2009.

[29] Y. Yang, *Defining equations of modular curves*, Adv. Math. 204 (2006), 481–508.

Francesc Bars, Xavier Xarles
Departament de Matemàtiques
Universitat Autònoma de Barcelona
08193 Bellaterra, Barcelona
Catalonia, Spain
E-mail: francesc@mat.uab.cat
xarles@mat.uab.cat

Aristides Kontogeorgis
K. Vesri 10 Papagou
GR-15669, Athens, Greece
E-mail: aristides.kontogeorgis@gmail.com

Received on 22.3.2013
and in revised form on 22.5.2013 (7381)