ON QUADRATIC POINTS OF CLASSICAL MODULAR CURVES

FRANCESC BARS

Dedicated to the memory of F. Momose

Abstract. Classical modular curves are of deep interest in arithmetic geometry. In this survey we show how the work of Fumiyuki Momose is involved in order to list the classical modular curves which satisfy that the set of quadratic points over $\mathbb{Q}$ is infinite. In particular we recall results of Momose on hyperelliptic modular curves and on automorphisms groups of modular curves. Moreover, we fix some inaccuracies of the existing literature in few statements concerning automorphism groups of modular curves and we make available different results that are difficult to find a precise reference, for example: arithmetical results on hyperelliptic and bielliptic curves (like the arithmetical statement of the main theorem of Harris and Silverman in [12], or the case $d = 2$ of Abramovich and Harris theorem in [1]) and on the conductor of elliptic curves over $\mathbb{Q}$ parametrized by $X(N)$.

1. Introduction

The propose of this survey is to present the relation of the work of Professor Fumiyuki Momose with the determination of classical modular curves which have an infinite set of quadratic points over $\mathbb{Q}$.

Over the complex numbers, a classical modular curve $X_{\Gamma,\mathbb{C}}$ corresponds to a Riemann surface obtained by completing by the cusps the affine curve $\mathbb{H}/\Gamma$ where $\mathbb{H}$ is the upper half plane and Γ is a modular subgroup of $SL_2(\mathbb{Z})$.

For this survey let us consider the following modular subgroups Γ of $SL_2(\mathbb{Z})$ with N a positive integer and Δ a strict subgroup of $(\mathbb{Z}/N\mathbb{Z})^*$ with $-1 \in \Delta$:

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

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \,\middle|\, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod N \right\},$$

$$\Gamma_\Delta(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \mid (a \pmod N) \in \Delta \right\},$$

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \,\middle|\, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod N \right\}.$$

Let us denote the associated Riemann surfaces (or complex modular curves associated to the modular subgroups) by $X(N)_\mathbb{C}, X_1(N)_\mathbb{C}, X_\Delta(N)_\mathbb{C}$ and $X_0(N)_\mathbb{C}$ respectively. Clearly $\Gamma(N) \leq \Gamma_1(N) \leq \Gamma_\Delta(N) \leq \Gamma_0(N)$, therefore we have natural maps:

$$X(N)_\mathbb{C} \to X_1(N)_\mathbb{C} \to X_\Delta(N)_\mathbb{C} \to X_0(N)_\mathbb{C}.$$

Partially supported by grant MTM2009-10359. Revised August 2013.

All these curves are algebraic and have as field of definition $\mathbb{Q}$. They are curves associated to a modular problem with a N-level structure, the modular problem over $\mathbb{C}$ can be used to give a model of the curve over $\mathbb{Q}$ which is geometrically connected, this can be done directly for $X_1(N)_{\mathbb{C}}, X_\Delta(N)_{\mathbb{C}}$ and $X_0(N)_{\mathbb{C}}$ defining modular curves over $\mathbb{Q}$: $X_1(N), X_\Delta(N)$ and $X_0(N)$, respectively, and each of them have at least one point defined over $\mathbb{Q}$.

The usual complex modular problem associated to $X(N)_{\mathbb{C}}$ is the coarse moduli spaces of the isomorphism classes of elliptic curves E together with two N-torsion points P_1, P_2 which satisfy: the points P_1, P_2 generate $E[N]$ which is isomorphic to the group scheme $(\mathbb{Z}/N\mathbb{Z})^2$ and $e(P_1, P_2) = \zeta_N$ where e is the Weil pairing and ζ_N a fixed primitive N-root of unity. In order to define a curve over $\mathbb{Q}$ with some point over $\mathbb{Q}$ we need to modify the above modular problem by (E, ϕ) with ϕ an isomorphism between $E[N]$ to the group scheme $\mathbb{Z}/N \times \mu_N$ such that is equivariant by the Weil pairing where μ_N is the group scheme of the N-roots of unity. Denote by $X(N)$ the modular curve over $\mathbb{Q}$ by this modular problem, which is isomorphic over $\mathbb{C}$ to the Riemann surface $X(N)_{\mathbb{C}}$, (see [8, §2] for more details concerning $X(N)$).

Denote by X_N any of the above geometrically connected modular curves over $\mathbb{Q}$ with genus ≥ 2.

By a great result of Gerd Faltings we know that for any number field F the set of F-points of X_N, named $X_N(F)$, is always a finite set. Consider now the set of all quadratic points over $\mathbb{Q}$ of X_N:

$$\Gamma_2(X_N, \mathbb{Q}) := \cup_{[F:\mathbb{Q}]\leq 2} X_N(F),$$

and ask if it is a finite set or not. With the work of Abramovich, Silverman and Harris we know that $\Gamma_2(X_N, \mathbb{Q})$ is an infinite set if and only if X_N has a degree two map defined over $\mathbb{Q}$ to a projective line (hyperelliptic) or to an elliptic curve E over $\mathbb{Q}$ (bielliptic) with positive rank, see §2 for the precise general statement. In this survey we list all the N where the elements of the set $\Gamma_2(X_N, \mathbb{Q})$ is infinite.

The contents of the paper are as follows. In §2 we recall Harris and Silverman results in [12] and Abramovich and Harris results in [1], in particular the relation between that the set of quadratic points over some number field L of a not singular projective curve C is infinite with the property that C is a hyperelliptic or a bielliptic curve. We also explain this relation when one fixes the field L fixing some inaccuracies in the literature. In §3 we present and fix inaccuracies of some results concerning the automorphism group of the above modular curves X_N over the algebraic closure. In §4 we present results and main ideas needed to obtain the exact list of N where the number of elements of the set $\Gamma_2(X_0(N), \mathbb{Q})$ is infinite. Finally in §5 we deal with the question on quadratic points over $\mathbb{Q}$ for the remaining X_N, observing in particular that any elliptic curve over $\mathbb{Q}$ parametrized by $X(N)$ satisfies that its conductor divides N^2. We finish the survey with a remark on the modular curves associated to the modular subgroup $\Gamma_1(M, N)$.

This paper corresponds to a written version of a lecture given at the Boston-Barcelona-Tokyo seminar on Number Theory in honor of Professor Fumiyuki Momose held in Barcelona from 23 to 25 May 2012.

2. The set of quadratic points is infinite: Hyperelliptic and Bielliptic curves

Let k be a number field, and $\overline{k}$ a fix algebraic closure of k. We write $C = C_{|k}$ for a not singular projective curve defined over k and let $\overline{C}$ be $C \times_k \overline{k}$. We denote by g_C the genus of $\overline{C}$ and we assume once and for all that $g_C \geq 2$. We write $Aut(C)$ for the automorphism group of C over $\overline{k}$.

As usual $C(L)$ denotes the set of points of C defined over L or L-points where L is a finite field extension of k inside $\overline{k}$.

Theorem 2.1 (Faltings, 1983)**.** *The set $C(L)$ is finite.*

After Falting's result we can consider the quadratic points of C over L by:

$$\Gamma_2(C, L) := \cup_{[\ell:L]\leq 2} C(\ell),$$

where ℓ run over all the extensions of degree at most 2 of L inside $\overline{k}$ and denote by $\#\Gamma_2(C, L)$ the number of elements of this set.

And we can ask: When is $\#\Gamma_2(C, L)$ infinite?

Definition 2.2. *The curve C is called hyperelliptic if $\overline{C}$ admits a degree two morphism to the projective line over $\overline{k}$.*

We have the following well-known result.

Proposition 2.3. *C is hyperelliptic if and only if exists an involution $w \in Aut(C)$ with $2g_C + 2$ fixed points. This involution is unique if exists and is defined over k and we call it the hyperelliptic involution.*

From the definition it follows easily

Lemma 2.4. *If C is hyperelliptic then exists a number field L where $\#\Gamma_2(C, L)$ is infinite.*

Next, let us obtain an arithmetic result fixing the number field L.

Lemma 2.5. *If C is hyperelliptic, and w denotes the hyperelliptic involution, then*

1. *there exists a (unique) degree two map to a conic, all defined over k,*
2. *if $C(k) \neq \emptyset$, or, more generally, $C/ < w > (k) \neq \emptyset$, then there exists a (unique) degree two map to $\mathbb{P}^1_{|k}$, all defined over k.*

Proof. The curve $C/ < w >$ has genus zero, therefore corresponds to a conic, and because w and C is defined over k the conic is also defined over k.

Consider $\pi : C \to C/ < w >$ a degree two morphism defined over $\overline{k}$. For every $\delta \in Gal(\overline{k}/k)$ we have the degree two morphism $\pi^\delta : C \to C/ < w >$,. By the uniqueness of the hyperelliptic involution the morphisms π and π^δ differs by an element $\xi_\delta \in Aut(C/ < w >) = PGL_2(\overline{k})$ because the conic is isomorphic to the projective line in the algebraic closure. Thus we have an application:

$$\xi : Gal(\overline{k}/k) \to PGL_2(\overline{k})$$
$$\delta \mapsto \xi_\delta.$$

Observe that given $\sigma, \delta \in Gal(\overline{k}/k)$ we have $\xi_{\sigma\delta} = \xi_\sigma^\delta \circ \xi_\delta$ thus

$$\xi \in H^1(Gal(\overline{k}/k), PGL_2(\overline{k})) = 0$$

therefore exists $\varphi_1 \in Aut(C/ < w >)$ satisfying $\xi_\sigma = \varphi_1^\sigma \circ \varphi_1^{-1}$ for all $\sigma \in Gal(\overline{k}/k)$. The morphism:

$$\varphi := \varphi_1^{-1} \circ \pi : C \to C/ < w >$$

is defined over k.

For the second statement, if $\varphi(C(k)) \neq \emptyset$ or $C/ < w > (k) \neq \emptyset$ we obtain that the conic has a point in k, therefore isomorphic to projective line over k $\mathbb{P}^1_{|k}$. □

Remark 2.6. *Mestre proved in* [27, p.322-324] *that if g_C is even and C is defined over k then exists $\varphi : C \to \mathbb{P}^1_{|_k}$ all defined over k.*

From Lemma 2.5 we obtain:

Corollary 2.7. *If C is hyperelliptic and $(C/ < w >)(k) \neq \emptyset$ then $\#\Gamma_2(C,k)$ is always infinite.*

Question 2.8. *Let C be a not singular projective curve over k with $(C/ < w >)(k) = \emptyset$ and C hyperelliptic (over $\overline{k}$), in particular g_C is odd by Remark 2.6. Is it true that $\Gamma_2(C,k)$ is an infinite set?*

The answer to this question is NO in general, see Corollary 2.17 and Lemma 2.18.

Definition 2.9. *A curve C is called bielliptic if $\overline{C}$ admits a degree two morphism to an elliptic curve over $\overline{k}$.*

Proposition 2.10. *C is bielliptic if and only if exists an involution $w \in Aut(C)$ with $2g_C - 2$ fixed points. The involution is unique if $g_C \geq 6$ and then it is defined over k and belongs to the center of $Aut(C)$.*

See a proof of Proposition 2.10 in [33, p.706, Prop.1.2.a) and Lemma 1.3].

Corollary 2.11. *If C is bielliptic then exists L such that $\#\Gamma_2(C,L)$ is not finite.*

Proof. Take $\varphi : C \to E$ a degree two morphism where φ and E are defined in some finite extension of k. Then take L defined over some finite extension of k such that φ, E and $rank E(L) \geq 1$ to conclude. □

Harris and Silverman obtain in [12]:

Theorem 2.12 (Harris-Silverman)**.** *Take C with $g_C \geq 2$. Then:*
$\exists L/k$ such that the set $\Gamma_2(C,L)$ is not finite $\Leftrightarrow$ C is a hyperelliptic or a bielliptic curve.

Let us state an arithmetic statement of Theorem 2.12 fixing the number field L.
We first recall the result [12, Lemma 5] of J.Harris and J.H.Silverman.

Lemma 2.13. *Let C be a bielliptic curve with $g_C \geq 6$. Then exists a genus 1 curve E defined over k and a morphism $\varphi : C \to E$ of degree 2 all defined over k.*

It is well-known to the specialists the following result (from the arguments of Abramovich and Harris in [1], or with our situation on quadratic points from Harris and Silverman in [12]):

Theorem 2.14. *Take C with $g_C \geq 2$ then:*

$\#\Gamma_2(C,k) = \infty$ if and only if C is hyperelliptic with a degree two morphism $\varphi : C \to \mathbb{P}^1_{|k}$ defined over k to the projective line over k or C is bielliptic with a degree two morphism $\phi : C \to E$ all defined over k where E is an elliptic curve with $rank(E(k)) \geq 1$.

Remark 2.15. *Schweizer, in* [33, proof of Theorem 5.1] *gives different details of the proof of theorem 2.14. We warn that the statement of* [33, Theorem 5.1] *is weaker than Theorem 2.14.*

Proof (sketch). One implication of the statement of Theorem 2.14 is clear.

Let us suppose that $\#\Gamma_2(C,k) = \infty$.

Take $P \in \Gamma_2(C,k)$ a quadratic point and denote by P' its conjugate by the quadratic extension. Define then

$$\phi^{(2)} : S^2C \to Jac(C)$$

$$q_1 + q_2 \mapsto [q_1 + q_2 - P - P']$$

where S^2C corresponds to $(C \times C)/S_2$ with S_2 the permutation group and $Jac(C)$ is the Jacobian of C and denote by $proj$ the projection map $C \times C \to S^2C$. The map $\phi^{(2)}$ is defined over k.

Denote by $\phi^{(2)}(k) : S^2C(k) \to Jac(C)(k)$, the map on the k-points, observe $\#S^2C(k)$ is infinite because $\#\Gamma_2(C,k) = \infty$.

Lemma 2.16. *The map $\phi^{(2)}(k)$ is injective if and only if does not exist a degree two map defined over k of C to the projective line over k. In particular, if C is hyperelliptic and the genus zero curve $C/ < w >$ has no k-point (where w denotes the hyperelliptic involution of C), then $\phi^{(2)}(k)$ is injective.*

Proof. [of Lemma 2.16] Consider $(q_1, q_2), (q_1', q_2') \in S^2C(k)$ and suppose

$$q_1 + q_2 - P - P' = q_1' + q_2' - P - P' \in Jac(C)(k) = Pic^0(C)(k).$$

We have that is equivalent to $q_1 + q_2 - q_1' - q_2' = div(f)$ with $f \in k(C)$ of degree two. And this is equivalent to define a degree two map over k to the projective line over k.

In particular if C with $g_C \geq 2$ is hyperelliptic, the hyperelliptic involution is defined over k and we have a degree two morphism to C to a genus 0 curve all defined over k, and if the genus 0 curve has no points over k (this situation only happens with g_C odd by Remark 2.6) we have then that $\phi^{(2)}(k)$ is injective.

□

Now, we can suppose that C is not hyperelliptic if $C(k) \neq \emptyset$ or C is hyperelliptic but satisfies that $\phi^{(2)}(k)$ is injective. We will prove that under this assumption C is bielliptic with a degree two map φ defined over k of the shape $\varphi : C \to E$ with E an elliptic curve with $rank(E(k)) \geq 1$ proving theorem 2.14.

By Falting's Theorem [11] we have

$$Im(\phi^{(2)}(k)) = \cup P_i + B_i(k)$$

with P_i points of $Jac(C)$ and B_i abelian subvarieties of dimension lower or equal to 1 because $Im(\phi^{(2)}(k))$ is not an abelian variety. Therefore a B_i, say B_1 is an elliptic curve E where its k-points have positive rank, and E is defined over k (see for more details [33, proof Theorem 5.1]). Now Abramovich and Harris,

in [1, Lemma 2], construct a degree two map φ from C to E as follows: take $F := \phi^{(2)} \circ proj : C \times C \to S^2C \to Im(\phi^{(2)})$, F is defined over k. $F^{-1}(E)$ is an union of irreducible projective varieties with by F are of degree 2 to E. By [1, Lemma 2] exists Z_1, an irreducible component of $F^{-1}(E)$, and $j : Z_1 \to C$ a rational map which is one-to-one where j corresponds to the projection of $C \times C$ to C in the first or the second component. In particular j is defined over k. Therefore j induces an isomorphism ι over k from the normalization of Z_1, named Z, to C, and the normalization map ψ of Z to Z_1 is defined over k. Therefore the degree two map $\varphi : C \to E$ defined in the proof of [1, Lemma 2] is $\varphi := F_{|_{Z_1}} \circ \psi \circ \iota^{-1}$ and is defined over k. □

Corollary 2.17. *Any hyperelliptic curve C defined over k with $(C/ < w >)(k) = \emptyset$ and $g_C \geq 2$ which it is not bielliptic over k to an elliptic curve with positive rank satisfies that $\Gamma_2(C, k)$ is a finite set*

Proof. Because C is hyperelliptic and $C/ < w > (k) = \emptyset$ we have that does not exist a degree two morphism of C to the projective line over k by the uniqueness of the hyperelliptic involution w. By the proof of theorem 2.14 we conclude. □

Lemma 2.18 (Xarles)**.** *Consider the curve C in $\mathbb{P}^3$ given by the equations: $y^2 = -x^2 - t^2$ and $z^2t^4 = x^6 + x^4t^2 + x^2t^4 + t^6$.*

The curve C is defined over $\mathbb{Q}$, has genus 5, satisfies $C(\mathbb{Q}) = \emptyset$, is hyperelliptic with $C/ < w > (\mathbb{Q}) = \emptyset$ and it is not bielliptic over $\mathbb{Q}$ to an elliptic curve with positive rank. In particular $\Gamma_2(C, \mathbb{Q})$ is a finite set by Corollary 2.17, and the answer to question 2.8 is No.

Proof. The quotient of C by the automorphism $w : z \mapsto -z$ induces a map of C to the conic $y^2 = -x^2 - t^2$ with no points on $\mathbb{Q}$, implying that C is hyperelliptic and $C/ < w > (\mathbb{Q}) = \emptyset$.

The Jacobian of C is isogenous to the product of the Jacobian of C_1 and C_2 where $C_1 : t^2 = x^6+x^4+x^2+1$ and $C_2 : t^2 = (-x^2-1)(x^6+x^4+x^2+1)$. By use of Magma the Jacobian of C_1 and C_2 are $\mathbb{Q}$-simple of dimension 2 and 3 respectively, justifying the genus and that there is no elliptic curve defined over $\mathbb{Q}$ in S^2C and in particular in the Jacobian of C, thus by the proof of theorem 2.14 C is not bielliptic to an elliptic curve over $\mathbb{Q}$ with positive rank. □

To finish this section we state the following result of Bob Accola and Alan Landman (see the agreements in [12]) and also of Joe Harris and J.H. Silverman in [12, Prop.1], very useful for the study of bielliptic curves in a family of modular curves:

Proposition 2.19 (Accola-Landman, Harris-Silverman)**.** *If C is a bielliptic curve and if $C \to C'$ is a finite map then the curve C' is either bielliptic or hyperelliptic.*

3. Automorphism group of classical modular curves

An important facet for modular curves X_N with genus ≥ 2 is to compute the group $\mathrm{Aut}(X_N)$ over the algebraic closure. (We recall that if C is bielliptic or hyperelliptic it has a very special involution in $\mathrm{Aut}\,(C)$, we will work with this fact in the next sections).

We recall that for a modular curve $X_{\Gamma,\mathbb{C}}$ with modular group $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$, the quotient of the normalizer of Γ in $\mathrm{PSL}_2(\mathbb{R})$ by $\pm\Gamma$ gives a subgroup of $\mathrm{Aut}\,(X_{\Gamma,\mathbb{C}})$, we denote this subgroup by $Norm(\Gamma)/\pm\Gamma$.

This normalizer can be computed explicitly for different classical modular curves. For the modular curve $X_0(N)$, we have [30]:

Proposition 3.1 (Newman). *Write $N = \sigma^2 q$ with $\sigma, q \in \mathbb{N}$ and q square-free. Let ϵ be the* gcd *of all integers of the form $a - d$ where a, d are integers such that $\begin{pmatrix} a & b \\ Nc & d \end{pmatrix} \in \Gamma_0(N)$. Denote by $v := v(N) := \gcd(\sigma, \epsilon)$. Then $M \in \mathrm{Norm}(\Gamma_0(N))/\pm\Gamma_0(N)$ if and only if M is represented in $PSL_2(\mathbb{R})$ as a matrix of the form*

$$\sqrt{\delta}\begin{pmatrix} r\Delta & \frac{u}{v\delta\Delta} \\ \frac{sN}{v\delta\Delta} & l\Delta \end{pmatrix}$$

with $r, u, s, l \in \mathbb{Z}$ and $\delta | q$, $\Delta | \frac{\sigma}{v}$. Moreover $v = 2^\mu 3^w$ with $\mu = min(3, [\frac{1}{2}v_2(N)])$ and $w = min(1, [\frac{1}{2}v_3(N)])$ where $v_{p_i}(N)$ is the valuation at the prime p_i of the integer N.

For later convenience we define particular elements in Proposition 3.1 which induce elements of $Aut(X_0(N))$.

Definition 3.2. *Let N be a fix positive integer. For every positive divisor m' of N with $\gcd(m', N/m') = 1$ the Atkin-Lehner involution $w_{m'}$ is defined as follows,*

$$w_{m'} = \frac{1}{\sqrt{m'}}\begin{pmatrix} m'a & b \\ Nc & m'd \end{pmatrix} \in SL_2(\mathbb{R})$$

with $a, b, c, d \in \mathbb{Z}$.

Always w_d defines an involution of $Aut(X_0(N))$ and $w_d \cdot w_{d'} = w_{dd'} \in Aut(X_0(N))$ with $(d, d') = 1$.

Denote by $S_{v'} = \begin{pmatrix} 1 & \frac{1}{v'} \\ 0 & 1 \end{pmatrix}$ with $v' \in \mathbb{N} \setminus \{0\}$.

Atkin-Lehner claimed without proof in [4, Theorem 8] the group structure of $Norm(\Gamma_0(N))/\pm\Gamma_0(N))$, but their statement is wrong. Later Akbas and Singerman [3] (rediscovered also by the author in [7]) obtain the correct statement. Here we only present the following intermediate result:

Proposition 3.3 (Atkin-Lehner, Akbas-Singerman, Bars). *Any element w that belongs to $\mathrm{Norm}(\Gamma_0(N))/\pm\Gamma_0(N)$ has an expression of the form*

$$w = w_m \Omega,$$

where w_m is an Atkin-Lehner involution of $\Gamma_0(N)$ with $(m, 6) = 1$ and Ω belongs to the subgroup generated by $S_{v(N)}$ and the Atkin Lehner involutions $w_{2^{v_2(N)}}$, $w_{3^{v_3(N)}}$.

We have also an analog of Newman's result for the modular curves $X_1(N)$ in [22](or in [24]) which we state without mentioning the particular case $X_1(4)$:

Proposition 3.4 (Kim-Koo, Lang). *If $N \neq 4$, then $M \in Norm(\Gamma_1(N))/\pm\Gamma_1(N)$ if and only if M is represented in $PSL_2(\mathbb{R})$ as a matrix of determinant 1 of the form:*

$$M = \frac{1}{\sqrt{Q}}\begin{pmatrix} Qx & y \\ Nz & Qw \end{pmatrix}$$

where Q is a Hall divisor of N (i.e. $(Q, N/Q) = 1$) and x, y, z, w are all integers.

Concerning elements in $Aut(X_1(N))$ we observe the following corollaries (see also [15]):

Corollary 3.5. *Always $w_Q \in Aut(X_1(N))$ for a Hall divisor Q of N, but w_Q is not necessarily an involution of $X_1(N)$. The full Atkin-Lehner involution w_N is always an involution of $Aut(X_1(N))$.*

Corollary 3.6. *Consider $\gamma \in \Gamma_0(N)$ with $\gamma \equiv \begin{pmatrix} a & * \\ 0 & * \end{pmatrix}$ mod N, then γ represents an automorphisms of $X_1(N)$ which depends only of a and we name it by $[a]$. In particular, $Norm(\Gamma_1(N))/\pm\Gamma_1(N)$ is generated by w_Q and $[a]$; i.e. generated by $\Gamma_0(N)/\pm 1$ and w_d with $d|N$ and $(d, N/d) = 1$.*

For the classical modular curves $X(N)$ it follows easily following the proof of $X_1(N)$ in [22], (or see also [8]):

Proposition 3.7. *If $N \geq 5$ the normalizer of $\Gamma(N)$ in $PSL_2(\mathbb{R})$ is $PSL_2(\mathbb{Z})$ and therefore $Norm(\Gamma(N))/\pm\Gamma(N) \cong PSL_2(\mathbb{Z}/N\mathbb{Z})$.*

Remark 3.8. *We mention here that Mong-Lung Lang in* [25] *gave an algorithm that, given a subgroup Γ of finite index in $PSL_2(\mathbb{Z})$ allows us to determine the normalizer of Γ in $PSL_2(\mathbb{R})$.*

A very deep question is to determine when $Norm(\Gamma)/\pm\Gamma$ coincides with the full group of automorphisms of the corresponding modular curve $X_{\Gamma,\mathbb{C}}$.

Definition 3.9. *An automorphism $v \in \mathrm{Aut}(X_{\Gamma,\mathbb{C}}) \setminus (Norm(\Gamma)/\pm\Gamma)$ is called exceptional.*

It was known by A. Ogg [31]:

Proposition 3.10 (Ogg)**.** *If p is a prime $p \neq 37$, then $X_0(p)$ has no exceptional automorphisms. For $p = 37$ $Aut(X_0(37))$ has index two with $Norm(\Gamma_0(37))/\pm\Gamma_0(37) = \{id, w_{37}\}$ an one of the exceptional automorphism corresponds to the hyperelliptic involution of $X_0(37)$.*

F. Momose contributed strongly to this question, joint with K. Kenku they proved the following very strong result [20]:

Theorem 3.11 (Kenku-Momose)**.** *Suppose that genus of $X_0(N)$ is ≥ 2. For $N \neq 37, 63$ and 108 there are no exceptional automorphisms and therefore*

$$Aut(X_0(N)) = Norm(\Gamma_0(N))/\pm\Gamma_0(N).$$

Remark 3.12. *The case $N = 63$ was completed by Elkies in* [10] *and the case $N = 108$ was recently obtained by Harris in* [13]*. In both cases there are exceptional automorphisms and the index of the full group of automorphism to the normalizer is 2. We warn to the reader that Kenku and Momose in* [20] *did not discard the case $N = 108$, see* [13] *for fix the gap of the wrong argument did in* [20].

F. Momose also contributed to the question for the modular curves $X_1(N)$ and $X_\Delta(N)$, under some conditions, unfortunately [29] is not available in the literature as far as I know. A particular statement of the general result in [29] reads as follows:

Theorem 3.13 (Momose)**.** *If N is square-free then $Aut(X_1(N)) = Norm(\Gamma_1(N))/\pm\Gamma_1(N)$, i.e. no exceptional automorphisms in $X_1(N)$ with N square-free.*

In [29] it is stated the general result for $X_\Delta(N)$ with N square-free (where $\Delta = (\mathbb{Z}/N)^*$ is allowed), but A. Schweizer communicated us the following result which will appear in the work [18]:

Lemma 3.14 (Jeon-Kim-Schweizer)**.** *The modular curve $X_{\{\pm1,\pm6,\pm8,\pm10,\pm11,\pm14\}}(37)$, which we call $X_{\Delta_3}(37)$, has exceptional automorphisms, and one of the exceptional automorphisms is a bielliptic involution for this curve.*

Proof. $X_{\Delta_3}(37)$ has genus 4 and is an unramified Galois cover of the genus 2 curve $X_0(37)$. So by [2, Corollary 1, p. 346] it is bielliptic.

The not exceptional automorphisms of $X_{\Delta_3}(37)$ form a group S_3 generated by [2] (of order 3) and the involution w_{37}. The quotient by this group is the elliptic curve $X_0(37)/w_{37}$. Applying the Hurwitz formula to this S_3-covering, one sees that each of the 3 (conjugate) involutions has 2 fixed points. So the bielliptic involution must be exceptional.

□

Remark 3.15. *A good revision of Momose work in* [29] *is needed in the literature to fix the square-free N where $X_\Delta(N)$ has exceptional automorphisms.*

Remark 3.16. *The proof that $X_{\Delta_3}(37)$ is not hyperelliptic in the Tsukuba paper* [14] *relied on the nonexistence of exceptional automorphisms which is not correct. To prove that $X_{\Delta_3}(37)$ is not hyperelliptic one can use that unramified Galois covers of degree 3 of a hyperelliptic curve are never hyperelliptic* [2, Lemma 4].

One may wonder if a revision of [14] *is needed concerning the list of hyperelliptic modular curves, but the work of Jeon and Kim in* [16] [17] *already did this work. See in particular* [17] *for a more computational proof that $X_{\Delta_3}(37)$ is not hyperelliptic.*

Finally, we turn to the classical modular curves $X(N)$. It is known to the specialists that there are no exceptional automorphisms, but it was not an available proof in the literature until the recent work of [8]:

Theorem 3.17. *We have that $Aut(X(N)) = Norm(\Gamma(N))/\pm\Gamma(N))$.*

4. Which curves $X_0(N)$ have an infinite set of quadratic points?

By Theorem 2.12 it is enough to determine the modular curves $X_0(N)$ which are hyperelliptic or bielliptic if we do not wish to fix the number field L where $\Gamma_2(X_0(N), L)$ is not a finite set.

Andrew Ogg in [31] completed the list of hyperelliptic curves:

Theorem 4.1 (Ogg)**.** *There are 19 values of N, such that $X_0(N)$ is hyperelliptic. For $N = 37$, $N = 40$ and $N = 48$ the hyperelliptic involution is not of Atkin-Lehner type. The rest can be read off from the following table:*

N	υ	N	υ
22	w_{11}	35	w_{35}
23	w_{23}	39	w_{39}
26	w_{26}	41	w_{41}
28	w_7	46	w_{23}
29	w_{29}	47	w_{47}
30	w_{15}	50	w_{50}
31	w_{31}	59	w_{59}
33	w_{11}	71	w_{71}

In order to reduce to a finite list the N for which $X_0(N)$ could be a bielliptic curve: take N with $g_{X_0(N)} \geq 6$ and $X_0(N)$ bielliptic, then by Lemma 2.13 we have a degree two map $\varphi : X_0(N) \to E$ all defined over $\mathbb{Q}$ and if $p \nmid N$, p prime, we can reduce the map modulo p obtaining a degree two map of the reduction of $X_0(N)$ at p, denoted by $X_0(N)_{|\mathbb{F}_p}$, to an elliptic curve over the finite field $\mathbb{F}_p$.

Recall now that Ogg in [31] proved that any point $(E, C) \in X_0(N)_{|\bar{\mathbb{F}}_p}$ with $p \nmid N$ and E a supersingular curve over $\mathbb{F}_p$ satisfies that $(E, C) \in X_0(N)_{|\bar{\mathbb{F}}_p}(\mathbb{F}_{p^2})$, this fact is the main item in order to prove in [12]:

Theorem 4.2 (Harris-Silverman)**.** *If $X_0(N)$ bielliptic (with genus ≥ 6) then:*

$$\#cusps \text{ in } \mathbb{F}_{p^2} + 2n(p)\mu(N) \leq \#X_0(N)_{|\bar{\mathbb{F}}_p}(\mathbb{F}_{p^2})$$

$$\leq min(2(p+1)^2, p^2 + pg_{X_0(N)} + 1)$$

where $\mu(N) = (SL_2(\mathbb{Z}) : \Gamma_0(N))$, and $n(p) = \sum_{E/F_p,\ supersingular} \frac{1}{|Aut(E)|}$.

We can control the cusps defined over $\mathbb{F}_{p^2}$ by [32, Prop.4.8] (or [6, Lemma 2.2]) and therefore we can deduce for example if $2 \nmid N$ then $N \leq 192$ ([6, Lemma 2.1]), and,

Proposition 4.3. [6, Prop.2.3] *The curve $X_0(N)$ is not bielliptic for $N > 210$.*

Now it remains a case-by-case study when $X_0(N)$ is bielliptic or not with $N \leq 210$. By Proposition 2.3 is enough to control the fixed points of all involutions on $X_0(N)$.

***** Because we know the number of fixed point on $X_0(N)$ of the Atkin-Lehner involutions $w_d \in Norm(\Gamma_0(N))/\pm\Gamma_0(N)$ (see for example the formula in [23] or a table computing these numbers up to $N \leq 210$ in [34]):

Lemma 4.4. *We can list all N where $X_0(N)$ is bielliptic with an involution of Atkin-Lehner type.*

***** Now by Theorem 3.11 of Kenku and Momose and the description of Newman in Proposition 3.1 we obtain that for $4 \nmid N$ and $9 \nmid N$ all the involutions are Atkin-Lehner involutions.

***** When $4|N$ or $9|N$ we haves more involutions in $Aut(X_0(N))$ than the Atkin-Lehner type. For example when $4|N$ appears the involution S_2.

In the paper [6] is done a detailed study of the involutions which are not of Atkin-Lehner type that appear in the remaining situations, in particular on the number of fixed points for these new involutions. We reproduce next a particular statement [6, p.159-160].

If $9||N$ and $4 \nmid N$, from Proposition 3.1, one obtains that all involutions which are not of Atkin-Lehner type are:

$$S_3 w_9 S_3^2, \quad S_3^2 w_9 S_3$$

$$w_r S_3 w_9 S_3^2, \quad w_r S_3^2 w_9 S_3\} \quad if\ r \equiv 1 (mod\ 3),$$

$$w_r S_3, \quad w_r S_3^2, \quad w_r w_9 S_3 w_9, \quad w_r w_9 S_3^2 w_9\} \quad if\ r \equiv 2 (mod\ 3),$$

Proposition 4.5. *The number of fixed points of $S_3w_9S_3^2$ and $S_3^2w_9S_3$ in the modular curve $X_0(N)$ is equal to the number of fixed points of w_9 in $X_0(N)$.*
For $r \equiv 1(mod\ 3)$ the number of fixed points of $w_rS_3w_9S_3^2, w_rS_3^2w_9S_3$ in $X_0(N)$ is equal to the number of fixed points of w_rw_9 in $X_0(N)$.
For $r \equiv 2(mod\ 3)$ the number of fixed points of $w_rS_3, w_rS_3^2, w_rw_9S_3w_9, w_rw_9S_3^2w_9$ is bounded by 3 times the number of fixed points of w_r in $X_0(N/3)$.

After all this study on involutions we obtain in [6, Theorem 3.15] all the bielliptic curves $X_0(N)$ with a list of bielliptic involutions, in particular:

Theorem 4.6 (Bars)**.** *There are 41 values of N, such that $X_0(N)$ is bielliptic. For each value, $X_0(N)$ has a bielliptic involuton of Atkin-Lehner type, except $X_0(2^33^2)$. The list of these N, $N \neq 72$, is given below:*

22	*26*	*28*	*30*	*33*	*34*	*35*	*37*	*38*	*39*
40	*42*	*43*	*44*	*45*	*48*	*50*	*51*	*53*	*54*
55	*56*	*60*	*61*	*62*	*63*	*64*	*65*	*69*	*75*
79	*81*	*83*	*89*	*92*	*94*	*95*	*101*	*119*	*131*

Remark 4.7. *Harrison noticed in 2011 that $X_0(108)$ has exceptional automorphisms. This result does not affect the argument in* [6] *from 1999 because one discard $X_0(108)$ to become bielliptic by arguments using Theorem 4.2, see for a precise proof* [5, Corol.lari 4.11]*. Harrison's result* [13] *does not affect the conclusion of the works on bielliptic curves for $X_1(N)$ or $X_\Delta(N)$ by Jeon and Kim because they use proposition 2.19 with $C' = X_0(N)$ to discard $N = 108$.*

From Theorem 4.1 and Theorem 4.6 we can list the modular curves $X_0(N)$ with where the set of quadratic points over some number field is not finite by Theorem 2.12:

Corollary 4.8. *Assume $X_0(N)$ of genus greater than or equal to 2. Then*

$$\#\Gamma_2(X_0(N), L_N) = \infty$$

for some number field L_N if and only if N is in the following list:
22, 23, 26, 28, 30, 31, 33, 34,35, 37, 38, 39, 40, 41, 42,43, 44, 45, 46, 47, 48, 50, 51, 53,54, 55,56, 59, 60,61, 62, 63, 64, 65, 69, 71,72, 75, 79, 81, 83, 89, 92, 94, 95, 101, 119, 131.

If we want to determine $X_0(N)$ for which $\Gamma_2(X_0(N), \mathbb{Q})$ is not finite, we need to use Theorem 2.14. We obtained in [6]

Theorem 4.9 (Bars)**.** *Assume $g_{X_0(N)} \geq 2$. We have that $\Gamma_2(X_0(N), \mathbb{Q})$ is finite if and only if N does not appear in the following list*

22	*23*	*26*	*28*	*29*
30	*31*	*33*	*35*	*37*
39	*40*	*41*	*43*	*46*
47	*48*	*50*	*53*	*59*
61	*65*	*71*	*79*	*83*
	89	*101*	*131*	

Proof (sketch). Assume that $X_0(N)$ is bielliptic or hyperelliptic. We know that $X_0(N)(\mathbb{Q}) \neq \emptyset$ (some cusps are defined over $\mathbb{Q}$), thus we restrict to $X_0(N)$ bielliptic and no-hyperelliptic by Lemma 2.5. By Carayol's Theorem we discard N where the elliptic curves over $\mathbb{Q}$ with the conductor N and all of its divisors have rank zero. The remaining situations come from the study of the Weil strong modular

parametrization studied in [26]. (We mention here that in the proof we use a weak form of Theorem 2.14 without worry if the degree two map from $X_0(N)$ to the elliptic curve is defined over $\mathbb{Q}$. This is so because in $X_0(N)$ Atkin-Lehner involutions are defined over $\mathbb{Q}$ and for $4|N$ or $9|N$ we obtain the result only searching when $Jac(X_0(N))$ contains an elliptic curve over $\mathbb{Q}$ with positive rank and if it contains such elliptic curve then the theory of Weil strong modular parametrization gives the morphism). □

5. Other classical modular curves

For simplify, we denote in the following X'_N, once and for all, any of the modular curves:

$$X(N),\ \ X_1(N),\ \textit{or}\ X_\Delta(N)\ (\textit{with}\ \{\pm 1\}\subset\Delta\leq(\mathbb{Z}/N)^*)$$

corresponding to modular groups $\Gamma(N), \Gamma_1(N)=\Gamma_{\{\pm1\}}(N)$, or $\Gamma_\Delta(N)$. And recall that always we assume $g_{X'_n}\geq 2$ and we have the natural finite maps:

$$X(N)_{\mathbb{C}}\to X_1(N)_{\mathbb{C}}\to X_\Delta(N)_{\mathbb{C}}\to X_0(N)_{\mathbb{C}}.$$

5.1. **Hyperelliptic modular curves.**

Consider the natural map $X'_{N,\mathbb{C}}\to X_0(N)_{\mathbb{C}}$. If X_N is hyperelliptic and $g_{X_0(N)}\geq 2$ then $X_0(N)$ is a hyperelliptic curve, therefore by Theorem 4.1 we are reduced to study when X'_N is hyperelliptic for a finite list of N.

Theorem 5.1 (Mestre, Ishii-Momose)**.** *$X_1(N)$ is hyperelliptic only for $N=13,16$ and 18.*

Theorem 5.2 (Ishii-Momose, Jeon-Kim)**.** *If $\{\pm1\}\subsetneqq\Delta\subsetneqq(\mathbb{Z}/N)^*$ the only hyperelliptic curve for the family $X_\Delta(N)$ is $X_{\{\pm1,\pm8\}}(21)$.*

Remark 5.3. *Mestre listed the hyperelliptic modular curves $X_1(N)$ in* [28]*. Ishii and Momose studied again this problem for the modular curves $X_\Delta(N)$ in* [14]*, reproving the result of Mestre because $X_{\{\pm1\}}(N)=X_1(N)$. Ishii and Momose claimed in* [14] *that always $X_\Delta(N)$ is not a hyperelliptic curve when $\Delta\neq\{\pm1\}$. Jeon and Kim proved that $X_{\{\pm1,\pm8\}}(21)$ is hyperelliptic in* [17]*, clarifying the gap in* [14]*.*

Remark 5.4. *Let us make explicit that w_d is not always in $Norm(\Gamma_\Delta(N))$, and therefore is not an automorphism of the curve $X_\Delta(N)$. This makes more difficult the work of finding explicit involutions which are not exceptional for $X_\Delta(N)$. This work began already in* [14] *and is deeper developed in* [18]*.*

By the work of Ishii and Momose in [14] (or with a more direct proof by Bars, Kontogerogis and Xarles in [8]):

Theorem 5.5. *There are no N for which $X(N)$ is hyperelliptic.*

5.2. **Bielliptic modular curves.**

By Proposition 2.19 with the natural map from X'_N to $X_0(N)$ and with Theorems 4.1 and 4.6:

Corollary 5.6. *Take N where $X_0(N)$ is not bielliptic and is not hyperelliptic. Then X'_N is not bielliptic, in particular X'_N is not a bielliptic curve for $N\geq 132$.*

For the families $X_1(N), X_\Delta(N), X(N)$ a detailed case-by-case analysis of the involutions is developed in order to obtain the exact list of N for which X'_N is a bielliptic curve, following Proposition 2.3.

Theorem 5.7 (Jeon-Kim)**.** *Take N with $g_{X_1(N)} \geq 2$, i.e. $N \geq 16$ or $N = 13$. We have that the curve $X_1(N)$ is bielliptic exactly when $2 \leq g_{X_1(N)} \leq 6$ (this corresponds to the values of N: $13, 16, 17, 18, 20, 21, 22, 24$).*

Let us present some main ideas given by Jeon and Kim in [15] to obtain the complete list of the curves $X_1(N)$ which are bielliptic.

By proposition 3.4 the not exceptional automorphisms of $X_1(N)$ are of the form $[a]w_d$, and we need to study involutions of this type. We warn again that w_d is not necessarily an involution of $X_1(N)$ but it is an automorphism.

- For $2 \leq g_{X_1(N)} \leq 6$: Jeon and Kim prove that all $X_1(N)$ are bielliptic with an involution in the normalizer of the modular group. They observe that always w_N is an involution of $X_1(N)$ and give some criteria for situations where the number of fixed points of w_N in $X_1(N)$ coincides with the number of fixed points of w_N in $X_0(N)$. Moreover they obtain some congruences between $[a]w_d$ which allow the authors, (joint with the hyperelliptic involutions obtained by Ishii and Momose in [14] for $N = 13, 16, 18$ and properties of automorphism groups with hyperelliptic involution) to give a bielliptic involution belonging to the normalizer of $\Gamma_1(N)$ for these $X_1(N)$.
- For $g_{X_1(N)} > 6$, the authors prove that all modular curves $X_1(N)$ are not bielliptic. If $X_1(N)$ is bielliptic, by proposition 2.10 the bielliptic involution is defined over $\mathbb{Q}$. The main argument is:
  Let v be the bielliptic involution of $X_1(N)$ and consider the natural map to $X_0(N)$, thus we obtain an involution $\tilde{v}$ of $X_0(N)$ and for $N \neq 37, 63$ is not an exceptional automorphism of $X_0(N)$, therefore the involution v is not an exceptional automorphism of $X_1(N)$. By Theorem 3.4 $\tilde{v}$ is necessarily of Atkin-Lehner type w_d. Restrict now from [6, Theorem 3.15] the couples (N, w_d) where $w_d = \frac{1}{\sqrt{d}} \begin{pmatrix} dx & y \\ Nz & dw \end{pmatrix}$ with $x, y, z, w \in \mathbb{Z}$ is a bielliptic involution of $X_0(N)$. The argument of Jeon and Kim if $d \neq 2$ is as follows: $\tilde{v}$ maps the cusp $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ to $\begin{pmatrix} y \\ d \end{pmatrix}$ with $(y, d) = 1$ for $d \neq N$ and to $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ for $d = N$, but the cusps over $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ are rational and the cusps over $\begin{pmatrix} y \\ d \end{pmatrix}$ or $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ are not, therefore v cannot exist.
  To conclude the remaining cases, the authors use properties of bielliptic involutions for example [33, Prop.1.2(b)]. We remark that the argument in [15] only uses Theorem 3.13 for $N = 37$.

Now we turn to the the exact list of bielliptic modular curves $X(N)$:

Theorem 5.8 (Jeon-Kim, Bars-Kontogeorgis-Xarles)**.** *Take N with $g_{X(N)} \geq 2$, i.e. $N \geq 7$. Then $X(N)$ is bielliptic for and only for $X(7)$ or $X(8)$.*

We sketch the main ideas of this Theorem following the approach given in [8], see also remark 5.16.
Main points in getting the above result are:

- $X(7)$ corresponds to the Klein quartic, $X(8)_{\mathbb{C}}$ is the Wiman curve of genus 5 and both are known to be bielliptic curves.

- we have a morphism over $\mathbb{Q}$ $X(N) \to X_0(N^2)$ and from Theorem 4.6 and Theorem 4.2 $X(N)$ is not bielliptic for $N \geq 10$. To deal with the case $N = 9$ one uses a Hurwitz formula argument for a convenient map with an explicit equation for $X(9)_{\mathbb{C}}$.

Recently Jeon, Kim and Schweizer completed the list of bielliptic intermediate curves $X_\Delta(N)$ in [18]:

Theorem 5.9 (Jeon-Kim-Schweizer, [18])**.** *Except for $N \neq 37$, the list of bielliptic $X_\Delta(N)$ with $\{\pm 1\} \subsetneqq \Delta \subsetneqq (\mathbb{Z}/N)^*$ are the following:*
$X_{\{\pm1,\pm8\}}(21)$,$X_{\{\pm1,\pm5\}}(24)$,$X_{\{\pm1,\pm7\}}(24)$, $X_{\{\pm1,\pm5\}}(26)$,
$X_{\{\pm1,\pm3,\pm9\}}(26)$, $X_{\{\pm1,\pm13\}}(28)$,$X_{\{\pm1,\pm3,\pm9\}}(28)$,
$X_{\{\pm1,\pm4,\pm5,\pm6,\pm7,\pm9,\pm13\}}(29)$, $X_{\{\pm1,\pm11\}}(30)$, $X_{\{\pm1,\pm15\}}(32)$,
$X_{\{\pm1,\pm2,\pm4,\pm8,\pm16\}}(33)$, $X_{\{\pm1,\pm9,\pm13,\pm15\}}(34)$,$X_{\{\pm1,\pm6,\pm8,\pm13\}}(35)$,
$X_{\{\pm1,\pm4,\pm6,\pm9,\pm11,\pm16\}}(35)$,$X_{\{\pm1,\pm11,\pm13\}}(36)$,
$X_{\{\pm1,\pm4,\pm10,\pm14,\pm16,\pm17\}}(39)$, $X_{\{\pm1,\pm9,\pm11,\pm19\}}(40)$,
$X_{\{\pm1,\pm2,\pm4,\pm5,\pm8,\pm9,\pm10,\pm16,\pm18,\pm20\}}(41)$,$X_{\{\pm1,\pm4,\pm11,\pm14,\pm16,\pm19\}}(45)$,
$X_{\{\pm1,\pm11,\pm13,\pm23\}}(48)$, $X_{\{\pm1,\pm6,\pm8,\pm13,\pm15,\pm20,\pm22\}}(49)$,
$X_{\{\pm1,\pm9,\pm11,\pm19,\pm21\}}(50)$,$X_{\{\pm1,\pm4,\pm6,\pm9,\pm14,\pm16,\pm19,\pm21,\pm24,\pm26\}}(55)$,
$X_{\{\pm1,\pm7,\pm9,\pm15,\pm17,\pm23,\pm25,\pm31\}}(64)$.

Jeon, Kim and Schweizer, need new ideas to obtain the above Theorem. We list some of the main new items in [18]:

***** Precise criteria to decide when w_d gives an automorphism in $X_\Delta(N)$ and when it defines an involution in $X_\Delta(N)$ and in such case compute the number of fixed points. Mainly, they prove that the bielliptic $X_\Delta(N)$ curves have a bielliptic involution of type w_d or $[a]w_d$.

***** To discard and obtain few new bielliptic curves they study the natural morphism $X_\Delta(N)_{\mathbb{C}} \to X_0(N)_{\mathbb{C}}$ and how a bielliptic involution on $X_\Delta(N)$ should translate to $X_0(N)$ and compare with the known results on bielliptic involutions on $X_0(N)$. In particular they need to check for $X_\Delta(37)$ for different Δ, if these curves have exceptional automorphisms. They obtain, for example, that $X_{\Delta_3}(37)$ has exceptional automorphisms (this contradicts a result claimed in [29] see also Lemma 3.14) and obtain that this modular curve is bielliptic with an exceptional bielliptic involution. The authors also need a particular study for genus 4 curves to obtain that $X_\Delta(25)$ is not bielliptic.

5.3. **On infiniteness of quadratic points over $\mathbb{Q}$ of modular curves.**

Consider first the modular curves $X_1(N)$ that are defined over $\mathbb{Q}$ with moduli interpretation given by couples (E, C) with C a N-torsion subgroup of the elliptic curve E.

Fix N, then in order to have $X_1(N)$ a not finite set of quadratic points over the rationals, we need an infinite set of couples (E, C) defined over a quadratic field, in particular C should appear as torsion subgroup for elliptic curves over quadratic fields.

We have the following main result of Kenku and Momose [21]:

Theorem 5.10 (Kenku-Momose)**.** *For d a fix integer and E an elliptic cuver over a quadratic field $\mathbb{Q}(\sqrt{d})$. Then the torsion subgroup of $E(\mathbb{Q}(\sqrt{d}))$ is isomorphic to one of the following groups:*
$\mathbb{Z}/m\mathbb{Z}$ *with* $m \leq 16$ *or* $m = 18$
$\mathbb{Z}/2 \times \mathbb{Z}/2k$ *with* $k \leq 6$
$\mathbb{Z}/3 \times \mathbb{Z}/3l$ *with* $l \leq 2$
$\mathbb{Z}/4 \times \mathbb{Z}/4$.

Now by Theorem 2.14 and because $X_1(13)$, $X_1(16)$ and $X_1(18)$ are hyperelliptic (Theorem 5.1) we have after Theorem 5.7 the following result in [15]:

Corollary 5.11. *Take N with $g_{X_1(N)} \geq 2$, i.e. $N \geq 16$ or $N = 13$. We have that $\Gamma_2(X_1(N), \mathbb{Q})$ is finite if and only if N does not appear in the following list:*

$$13, 16, 18$$

Consider now the modular curves $X_\Delta(N)$ defined over $\mathbb{Q}$ and with natural morphisms

$$X_1(N) \to X_\Delta(N) \to X_0(N).$$

Corollary 5.12. *Take $N \neq 37$ with $g_{X_\Delta(N)} \geq 2$, and $\{\pm 1\} \subsetneqq \Delta \subsetneqq (\mathbb{Z}/N)^*$. Then the set $\Gamma_2(X_\Delta(N), \mathbb{Q})$ is not finite if and only if $X_\Delta(N) = X_{\{\pm 1, \pm 8\}}(21)$.*

Proof. By Theorem 2.14 we only need to study $X_\Delta(N)$ bielliptic and not hyperelliptic. Take the list of $X_\Delta(N)$ bielliptic in Theorem 5.9, and suppose is given $\phi : X_\Delta(N) \to E$ all defined over $\mathbb{Q}$. In particular we have a morphism over $\mathbb{Q}$: $X_1(N) \to E$. By Carayol's result we have that the conductor of E should divide N. Now for all the $N \neq 37$ for which $X_\Delta(N)$ is bielliptic, we have $rank E(\mathbb{Q}) = 0$ for all elliptic curves over $\mathbb{Q}$ with conductor dividing N by Cremona tables [9]. □

Remark 5.13. *For $X_\Delta(37)$ we can not use the above Carayol argument because we have the elliptic curve $37a$ $[0, 0, 1, -1, 0]$ which has rank 1. Jeon, Kim and Schweizer in* [18]*, with an ad-hoc proof, obtain that $\Gamma_2(X_\Delta(37), \mathbb{Q})$ is always a finite set for any Δ as above.*

Now consider the modular curves $X(N)$.

Here we could try to reproduce the proof of Corollary 5.12 for $X(N)$ but we warn that Carayol result does not apply, for example one can construct a map

$$X(8) \to \{y^2 = x(x-1)(x+1)\} = E$$

and E has conductor 32, not a divisor of 8 and the rational model of $X(8)$ is the one in [35] (see [8] to ensure that the model of $X(8)$ in [35] coincides with the one fixed in this paper).

Proposition 5.14. *Assume that we have a morphism φ over $\mathbb{Q}$:*

$$\varphi : X(N) \to E$$

with E an elliptic curve defined also over $\mathbb{Q}$. Then the conductor of E divides N^2.

Proof. By [8, Lemma1] we have natural morphisms defined over $\mathbb{Q}$: $X_1(N^2) \to X(N)$ and $X(N) \to X_0(N^2)$, therefore we have a morphism over $\mathbb{Q}$ $X_1(N^2) \to E$ and by Carayol we obtain that the conductor of E divides N^2. □

We can proof by an ad-hoc method the following result in [8] (without use of Proposition 5.14):

Theorem 5.15 (Bars-Kontogeorgis-Xarles)**.** *For any $N \geq 7$ we have that the set $\Gamma_2(X(N) \times_{\mathbb{Q}} \mathbb{Q}(\zeta_N), \mathbb{Q}(\zeta_N))$ is always a finite set, and in particular $\Gamma_2(X(N), \mathbb{Q})$ is always finite.*

Remark 5.16 (The family of modular curves $X_1(N, M)$)**.** *For positive integers $M|N$ consider the congruence subgroup $\Gamma_1(M, N)$ of $SL_2(\mathbb{Z})$ defined by:*

$$\Gamma_1(M,N) := \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) | A \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \ mod\ N,\ M|b \right\}.$$

Let $X_1(M,N)_{\mathbb{C}}$ be the Riemann surface associated to $\Gamma_1(M,N)$. It is the coarse moduli space of the isomorphism classes of elliptic curves E with a pair (P_M, P_N) of points P_M and P_N of E which generate a subgroup isomorphic to $\mathbb{Z}/M \oplus \mathbb{Z}/N$ and satisfy $e_E(P_M, \frac{N}{M}P_N) = \zeta_M$ where e_E is the Weil pairing and ζ_M a fixed M-th root of unity, is known that the field of definition of the Riemann surface $X_1(M,N)_{\mathbb{C}}$ is $\mathbb{Q}$ and the above coarse moduli problem gives a model over $\mathbb{Q}(\zeta_M)$ and denote by $X(M,N)$ this model corresponding to a curve defined over $\mathbb{Q}(\zeta_M)$.

Observe that $X_1(M,N)$ is birational, over some number field, to $X_\Delta(MN)$ with $\Delta = \{\pm 1, \pm(N+1), \pm(2N+1), \ldots, \pm((M-1)N+1)\}$.

Jeon and Kim in [16] *listed all $X_1(M,N)$ which are bielliptic (obtaining a lot of the results by working in $X_\Delta(MN)$ with arguments already exposed in the survey), and they determine in* [16, Theorem 4.5] *a list of $X_1(M,N)$ with an infinite set of quartic points over $\mathbb{Q}$, i.e. points of degree 4 over $\mathbb{Q}$ (because the model of $X(M,N)$ is over $\mathbb{Q}(\zeta_M)$ in* [16]*, the result on quartic points* [16, Theorem 4.5] *assume that the number fields of degree at most 4 over $\mathbb{Q}$ contain $\mathbb{Q}(\zeta_M)$). Because $X_1(N,N) = X(N) \times_{\mathbb{Q}} \mathbb{Q}(\zeta_N)$ and $X_1(1,N) = X_1(N)$ their results cover results in* [15] *and* [8] *explained in the survey.*

Acknowledgements

I am very happy to thank Andreas Schweizer for all his comments and suggestions, in particular for letting me know Lemma 3.14 with its proof and also the Remark 3.16 that I reproduced here. I am pleased to thank Xavier Xarles for several discussions about the related theory, in particular discussions concerning the proof of Theorem 2.14 and noticing me the example in Lemma 2.18 that I also reproduced here.

References

[1] D. Abramovich and J. Harris, Abelian varieties and curves in $W_d(C)$, Compositio Math. 78 (1991), 227-238.
[2] R. Accola, On lifting the hyperelliptic involution, Proc. AMS 122 (1994), 341-347.
[3] M. Akbas and D. Singerman, The normalizer of $\Gamma_0(N)$ in $\mathrm{PSL}_2(\mathbb{R})$, Glassgow Math. J. 32 (1990), 317-327.
[4] Atkin, A.O.L., Lehner, J.: Hecke operator on $\Gamma_0(N)$. Math.Ann.185, 134-160 (1970).
[5] F. Bars, Determinació de les corbes $X_0(N)$ biel.líptiques (1997). You find a copy in http://ddd.uab.es/record/75137?ln=es
[6] F.Bars, Bielliptic modular curves. Journal of Number Theory 76, (1999), 154-165.
[7] F. Bars, The group structure of the normalizer of $\Gamma_0(N)$ after Atkin-Lehner. Communications in Algebra 36, No. 6, 2160-2170 (2008).
[8] F. Bars, A. Kontogeorgis and X. Xarles, Bielliptic and Hyperelliptic modular curves $X(N)$ and the group $Aut(X(N))$. To appear in Acta Arithmetica.
[9] Cremona tables. See http://homepages.warwick.ac.uk/ masgaj/ftp/data/count.00000-09999.gz

[10] N.D. Elkies, The automorphism group of the modular curve $X_0(63)$, Compositio Math. 74 (1990), 203-208.
[11] G. Faltings, Diophantine aproximation on abelian varieties. Annals of Math. 133 (1991), 549-576.
[12] J.Harris and J.H.Silverman, Bielliptic curves and symmetric products. Proc. Am.Math.Soc. 112, 347-356 (1991).
[13] M. Harrison, A new automorphism of $X_0(108)$, http://arxiv.org/abs/1108.5595, (2011).
[14] N.Ishii and F. Momose, Hyperelliptic modular curves, Tsukuba J. Math. 15 (1991), 413-423.
[15] D. Jeon and C.H.Kim, Bielliptic modular curves $X_1(N)$, Acta Arith (2004), 112.1, 75–86.
[16] D. Jeon and C.H.Kim, Bielliptic modular curves $X_1(M, N)$. Manuscripta Math. 118, 455-466 (2005).
[17] D. Jeon and C.H.Kim, On the arithmetic of certain modular curves. Acta Arith. 130, 181-193 (2007).
[18] D. Jeon, C.H. Kim and A. Schweizer, Bielliptic intermediate modular curves. Work in progress (2013).
[19] N. M. Katz B. and Mazur, Arithmetic Moduli of Elliptic Curves. Annals of Mathematics Studies 108, Princeton University Press (1985).
[20] M.A. Kenku and F. Momose, Automorphsism groups of modular curves $X_0(N)$. Compositio Math. 65, 51-80 (1988).
[21] M.A. Kenku and F. Momose, Torsion points on elliptic curves defined over quadratic fields, Nagoya Math. J. 109 (1988), 125-149.
[22] C.H. Kim and J.K. Koo, The normalizer of $\Gamma_1(N)$ in $\mathrm{PSL}_2(\mathbb{R})$, Comm. Algebra 28 (2000), 5303-5310.
[23] Kluit, On the normalizer of $\Gamma_0(N)$. In the book: Modular forms of one variable IV, LNM 601, Springer, 239-246.
[24] M-L. Lang, Normalizer of $\Gamma_1(m)$, J. Number Theory 86 (2001), no. 1, 5060.
[25] M-L. Lang, Normalizers of subgroups of the modular group. J. Algebra 248 (2002), no. 1, 202218.
[26] B. Mazur and H.P.F. Swinnerton-Dyer, Arithmetic of Weil curves; Inventiones Math. 25 (1974), 1-64.
[27] J-F. Mestre, Construction de courbes de genre 2 à partir de leurs modules, In: Effective methods in algebraic geometry (Castiglioncello, 1990), 313334, Progr. Math., 94, Birkhäuser Boston, Boston, MA, 1991.
[28] J-F. Mestre, Corps euclidiens, unités exceptionnelles et courbes élliptiques. J.Number Theory 13, 123-137 (1981).
[29] F. Momose, Automorphism groups of the modular curves $X_1(N)$. Preprint.
[30] M. Newman, Structure Theorem for modular subgroups. Duke Math. J. 22, 25-32 (1955).
[31] A.P. Ogg, Hyperelliptic modular curves. Bull.Soc.Math. France 102, 449-462 (1974).
[32] A.P. Ogg, Rational points on certain elliptic modular curves. Analytic Number Theory XXIV, Proceedings of Symposia in Pure Mathematics, 221-232.
[33] A. Schweizer, Bielliptic Drinfeld modular curves. Asian J. Math. 5, 705-720 (2001).
[34] STNB 1992, Corbes modulars: Taules. Notes del seminari de Teoria de Nombres, UB-UAB-UPC, Barcelona 1992.
[35] Y.Yang, Defining equation of modular curves. Advances in Mathematics 204 (2006), 481-508.

Francesc Bars Cortina,
Depart. Matemàtiques,
Universitat Autònoma de Barcelona,
08193 Bellaterra. Catalonia.
E-mail: francesc@mat.uab.cat