Bielliptic modular curves

Francesc Bars*

Departament de Matemàtiques
Universitat Autònoma de Barcelona
e-mail: francesc@mat.uab.cat
08193 Bellaterra
Catalonia,Spain

1 Introduction

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 number of K-rational points of C is always finite. In order to generalize this, the natural object to consider is the set

$$\Gamma_d(C, K) = \{P \in C(L) | [L : K] \leq d\}$$

of points of degree d of C. For quadratic points, that is $d = 2$, Abramovich and Harris show that the existence of infinitely many such points is equivalent to the fact that the curve C is either hyperelliptic or bielliptic, i.e. C has a degree two map to a projective line or an elliptic curve respectively.

In this work we shall study the family of modular curves $X_0(N)$ admitting infinitely many quadratic points. It consists of all the hyperelliptic and bielliptic curves. The family of hyperelliptic modular curves is completely determined by Ogg's contribution [10]. We shall settle here the bielliptic case. Our main result is:

Theorem. *There are exactly forty one values of N, such that $X_0(N)$ is bielliptic. For each value, $X_0(N)$ has a bielliptic involution of Atkin-Lehner type, except for $X_0(72)$. 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.

Finally, we solve completely the arithmetical question of finding all the values of N such that the curve $X_0(N)$ has infinitely many quadratic points over the ground field $\mathbb{Q}$.

Acknowledgments

I am grateful to Salvador Comalada for his much help in proving the results of this paper and for his useful comments and suggestions by the writing of this work. I thank Angela Arenas and Jordi Quer who pointed out to me their results concerning the computation of the degree of a strong Weil parametrization. I also thank Karl Rubin and the referee for his useful comments and his help in improving the result and for the collaboration of the referee in proving proposition 3.5. in a more easy way.

*Partially supported by Grant PB-96-1154 from DIGYCT.

2 The main result for $N \geq 210$ or $4 \nmid N$ and $9 \nmid N$

Assume $X_0(N)$ to have genus greater than 1. In [5] we find the following:

Lemma 2.1. *If $X_0(N)$ is a bielliptic curve with genus ≥ 6 then:*

$$\#\ cusps\ in\ \mathbb{F}_4 + \frac{1}{12}\mu(N) \leq 18 \quad if\ 2 \nmid N$$

$$\#\ cusps\ in\ \mathbb{F}_9 + \frac{1}{6}\mu(N) \leq 32 \quad if\ 3 \nmid N$$

$$\#\ cusps\ in\ \mathbb{F}_{25} + \frac{1}{3}\mu(N) \leq 72 \quad if\ 5 \nmid N$$

$$\#\ cusps\ in\ \mathbb{F}_{49} + \frac{1}{2}\mu(N) \leq 128 \quad if\ 7 \nmid N$$

where $\mu(N) = (SL_2(\mathbb{Z}) : \Gamma_0(N))$.

Lemma 2.2. *Write $P = \begin{pmatrix} x \\ d \end{pmatrix}$ for a cusp of $X_0(N)$ with $d|N$. Write $t = (d, N/d)$. Suppose $X_0(N)$ is not hyperelliptic over $\mathbb{F}_p$, $p \nmid N$. If $\varphi(t) \leq 2$ then P is defined over $\mathbb{F}_{p^2}$.*

Proof. If $\varphi(t) = 1$ it is already defined over $\mathbb{Q}$ ([11]). Since $p \nmid N$ we have good reduction, so we obtain a cusp defined over $\mathbb{F}_p$. Consider now $\varphi(t) = 2$ and let P' be the conjugate of P. The divisor $P + P' - 2P''$, where P'' is a point of $X_0(N)$ defined over $\mathbb{Q}$, is a point of $Jac(X_0(N))$ defined over $\mathbb{Q}$. Because of good reduction, we obtain a divisor defined over $\mathbb{F}_p$ and, if π denotes the Frobenius in $\mathbb{F}_p$, we have $\pi(P) = P'$ or $\pi(P) = P$. Hence, in both cases, $\pi^2(P) = P$. □

Proposition 2.3. *$X_0(N)$ is not a bielliptic curve for $N > 210$.*

Proof. We can apply lemma 2.1, since $X_0(N)$ has genus ≥ 6 for $N > 210$. We use also the facts that $\mu(N) \geq N$ and that there are at least two cusps defined over $\mathbb{F}_{p^2}$, if $p \nmid N$, to get:

$$N \leq 192 \quad if\ 2 \nmid N$$

$$N \leq 180 \quad if\ 3 \nmid N$$

$$N \leq 210 \quad if\ 5 \nmid N$$

$$N \leq 252 \quad if\ 7 \nmid N$$

Now, we know ([5]) that the statement is true for $N \geq 344$. If N is not divisible by $2, 3$ or 5 we are done. Otherwise $30|N$ and for $7 \nmid N$, $210 < N \leq 252$, the only case to consider is $N = 3D240$, which provides a non bielliptic curve $X_0(240)$ by computing the number of rational points and applying lemma 2.1. Finally, for $7|N$, $210 < N < 344$, there are no cases at all. □

Corollary 2.4. *For each N listed below, $X_0(N)$ is not a bielliptic curve:*
80, 84, 96, 99, 100, 104, 108, 112, 117, 120, 124, 126, 128, 135, 136, 144, 152, 153, 160, 162, 168, 176, 180, 184, 188, 189, 192, 196, 200, 208.

Proof. It's a straightforward computation using lemma 2.1 and lemma 2.2. □

We note that if $X_0(N)$ is a bielliptic curve there exists an involution υ, called bielliptic involution, such that $X_0(N)/\upsilon$ is an elliptic curve. It is unique if the genus of $X_0(N) \geq 6$ and it has exactly $2g-2$ fixed points, being this last property determinant of bielliptic curves. If $4 \nmid N$ and $9 \nmid N$, by [7] the only bielliptic involutions are the ones of Atkin-Lehner type (if $N \neq 37$), whose number of fixed points is computed in [8]. So, we get:

Corollary 2.5. *All the values N, with $4 \nmid N$ and $9 \nmid N$, such that $X_0(N)$ is a bielliptic curve are the following: 22, 26, 30, 33, 34, 35, 37, 38, 39, 42, 43, 50, 51, 53, 55, 61, 62, 65, 69, 75, 79, 83, 89, 94, 95, 101, 119, 131.*

3 The main result when $4|N$ or $9|N$

Using the fact that the image of a bielliptic curve under a finite morphism of curves is either bielliptic or hyperelliptic (see [5]) we obtain:

Corollary 3.1. *$X_0(N)$ is not a bielliptic curve for N: 116, 132, 140, 148, 156, 164, 171, 172, 198, 204, 208.*

Using the number of fixed points of the involutions of Atkin-Lehner type we get:

Corollary 3.2. *$X_0(N)$ is a bielliptic curve for the values: 28, 40, 44, 45, 48, 54, 56, 60, 63, 64, 81, 92.*

From proposition 2.3 and corollaries 2.4,2.5, 3.1 and 3.2 it follows that the only remaining cases to settle are:

$$N = 52, 68, 72, 76, 88, 90$$

In all the cases above, no involution of Atkin-Lehner type is seen to be bielliptic. Since $4|N$ or $9|N$ new involutions arise, which we are going to study next. It is well-known ([7]) that $Aut(X_0(N)) = 3DNorm(\Gamma_0(N))/\Gamma_0(N)$, where $Norm(\Gamma_0(N))$ is the normalizer of $\Gamma_0(N)$ in $SL_2(\mathbb{R})$ if $N \neq 37, 63$. Further, the last theorem of [2] provides the generators and relations for the group $Norm(\Gamma_0(N))/\Gamma_0(N)$. Write $S_k = 3D\begin{pmatrix} 1 & 1/k \\ 0 & 1 \end{pmatrix}$ and for $(r, N/r) = 3D1$ denote w_r the rth-Atkin-Lehner involution defined by $\frac{1}{\sqrt{r}}\begin{pmatrix} ra & b \\ Nc & dr \end{pmatrix}$, $det(w_r) = 1$ with $a, b, c, d \in \mathbb{Z}$.

Theorem 3.3 (Atkin-Lehner)**.** *For $N = 52, 68, 76,$ or 88, $Norm(\Gamma_0(N))/\Gamma_0(N)$ is the direct product of the following groups:*

1. *$< w_{q^i} >$ for every q prime, $q \geq 5$, $q^i \mid\mid N$.*
2. *(a) If $\upsilon_3(N) = 0$, $\{ 1\}$*
   (b) If $\upsilon_3(N) = 1$, $< w_3 >$
   (c) If $\upsilon_3(N) = 2$, $\{w_9, S_3 | w_9^2 = S_3^3 = (w_9 S_3)^3 = 1\}$ (order 12)
   (d) If $\upsilon_3(N) \geq 3$; $\{S_{3^{\upsilon_3(N)}}, S_3 | w_{3^{\upsilon_3(N)}}^2 = S_3^3 = 1, w_{3^{\upsilon_3(N)}} S_3 w_{3^{\upsilon_3(N)}} S_3 = S_3 w_{3^{\upsilon_3(N)}} S_3 w_{3^{\upsilon_3(N)}}\}$ (order 18)
3. *Put $\lambda = \upsilon_2(N)$, $\mu = min(3, [\frac{\lambda}{2}])$ and write $\upsilon'' = 2^\mu$ then:*

(a) *If* $\lambda = 0$ *;* $\{ 1\}$

(b) *If* $\lambda = 1$*;* $< w_2 >$

(c) *If* $\lambda = 2\mu$*;* $= \{w_{2^{\upsilon_2(N)}}, S_{\upsilon''} | w^2_{2^{\upsilon_2(N)}} = S^{\upsilon''}_{\upsilon''} = (w_{2^{\upsilon_2(N)}} S_{\upsilon''})^3 = 1\}$. *We have orders 6,24, 96 for* $\upsilon'' = 2, 4, 8$ *respectively. (Note that for* $\upsilon'' = 8$ *the relations do not define completely this group factor).*

(d) *If* $\lambda > 2\mu$*;* $\{w_{2^{\upsilon_2(N)}}, S_{\upsilon''} | w^2_{2^{\upsilon_2(N)}} = S^{\upsilon''}_{\upsilon''} = 1, S_{\upsilon''} w_{2^{\upsilon_2(N)}} S_{\upsilon''} w_{2^{\upsilon_2(N)}} = w_{2^{\upsilon_2(N)}} S_{\upsilon''} w_{2^{\upsilon_2(N)}} S_{\upsilon''}\}$ *(order* $2\upsilon''^2$*).*

Note 3.4. *We must warn the reader that the general assertion of this theorem is not always true. Take, for example,* $X_0(48)$*. By this characterization we should have:*

$$Aut(X_0(48)) \cong \mathbb{Z}/2\mathbb{Z} \times \mathcal{S}_4$$

where $\mathbb{Z}/2\mathbb{Z}$ *is generated by the involution* w_3*. Now, we know [10] that* $X_0(48)$ *is a hyperelliptic curve having a hyperelliptic involution which is not of Atkin-Lehner type. This leads to a contradiction because any hyperelliptic involution belongs to the center of the automorphism group.*
We have checked, however, that the theorem remains true for the cases $4||N$*,* $9 \nmid N$ *and* $8||N$*,* $9 \nmid N$*.*

First of all, let's consider the case $4|N$ and the following involutions:

$$S_2, w_{2^{\upsilon_2(N)}} S_2 w_{2^{\upsilon_2(N)}}$$

$$w_r S_2, w_r w_{2^{\upsilon_2(N)}} S_2 w_{2^{\upsilon_2(N)}}, \ if \ (2, r) = 1$$

Proposition 3.5. $X_0(N)/w_{2^{\upsilon_2(N)}} S_2 w_{2^{\upsilon_2(N)}} = 3DX_0(N/2)$ *and the morphism induced by the involution is* $\pi : X_0(N) \to X_0(N/2)$*, the natural projection. Moreover,* $X_0(N)/S_2 = X_0(N/2)$ *and* $\varphi : X_0(N) \to X_0(N)/S_2$ *is multiplication by 2.*

Proof. For the case $w_{2^{\upsilon_2(N)}} S_2 w_{2^{\upsilon_2(N)}}$, it amounts to show that this involution belongs to $\Gamma_0(N/2) \setminus \Gamma_0(N)$.
For the case S_2, let $r = \upsilon_2(N)$, then,

$$w_{2^{r-1}} \Gamma_0(N/2) w_{2^{r-1}} =< w_{2^r} S_2 w_{2^r}, \Gamma_0(N) >= w_{2^r} < S_2, \Gamma_0(N) > w_{2^r}.$$

It follows that $w_{2^r} w_{2^{r-1}} \Gamma_0(N/2) w_{2^{r-1}} w_{2^r} =< S_2, \Gamma_0(N) >$ and $w_{2^{r-1}} w_{2^r}$ is represented by multiplication by 2. □

Proposition 3.6. *The numbers of fixed points of the involutions* $w_r S_2$ *and* $w_r w_{2^{\upsilon_2(N)}} S_2 w_{2^{\upsilon_2(N)}}$ *are equal to*

$$\kappa = 2(N/2)_r - (N)_r$$

where $(M)_r$ *is the number of fixed points of the involution* w_r *in* $X_0(M)$*.*

Proof. Observe that if τ is a fixed point of $w_r S_2$ then:

$$w_r 2\tau = \delta 2\tau$$

for some $\delta \in \Gamma_0(N/2, 2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) | b \equiv 0 (mod\ 2), c \equiv 0 (mod\ N/2) \right\}$.
If τ is not an elliptic point of $\Gamma_0(N) \cup S_2 \Gamma_0(N)$ we have finished. It τ is elliptic

we can also argue easily by considering the morphism $X_0(N) \to X_0(N/2)$, multiplication by 2.
A similar argument holds as well for the other involution by using the usual projection $X_0(N) \to X_0(N/2)$. □

In the case $4||N$ and $9 \nmid N$, the only non-Atkin-Lehner involutions are the four involutions studied before. Thus we obtain:

Corollary 3.7. *The modular curves $X_0(52)$, $X_0(68)$ and $X_0(76)$ are not bielliptic.*

Corollary 3.8. *The modular curve $X_0(72)$ is bielliptic.*

In the case $8||N$ four additional involutions come into play, namely

$$S_2 w_8 S_2 w_8, S_2 w_8 S_2$$

$$w_r S_2 w_8 S_2 w_8, w_r S_2 w_8 S_2$$

Proposition 3.9. *The numbers of fixed points of $S_2 w_8 S_2$ and $w_r S_2 w_8 S_2$ in $X_0(N)$ are equal to the numbers of fixed points of w_8 and $w_r w_8$, respectively.*

Proof. It is clear for $S_2 w_8 S_2$ and only note that S_2 and w_r commute. □

Proposition 3.10. *The number of fixed points of $S_2 w_8 S_2 w_8$ is equal to:*

$$2(N/2)_2 - (N)_2$$

where $(M)_2$ is the number of fixed points of S_2 in $X_0(M)$.
The number of fixed points of $w_r S_2 w_8 S_2 w_8$ is equal to:

$$2(N/2)_{2,r} - (N)_{2,r}$$

where $(M)_{2,r}$ is the number of fixed points of $w_r S_2$ in $X_0(M)$.

Proof. For τ a fixed point of $S_2 w_8 S_2 w_8$ we have

$$S_2 \tau = \gamma w_8 S_2 w_8 \tau$$

$\gamma \in \Gamma_0(N)$, but $w_8 S_2 w_8 \in \Gamma_0(N/2) \setminus \Gamma_0(N)$. Since $proj : X_0(N) \to X_0(N/2)$ has degree 2 the result follows. A similar argument for $w_r S_2 w_8 S_2 w_8$. □

Applying all the above computations to $N = 88$, we get:

Corollary 3.11. *$X_0(88)$ is not a bielliptic curve.*

Note 3.12. *When $9||N$ and $4 \nmid N$, it is easy to check that every element in $Norm(\Gamma_0(N))/\Gamma_0(N)$ can be written in the form $w_{q'}\beta$ with $\beta \in < S_3, w_9 >$.*

Finally, in the case $9||N$ and $4 \nmid N$ one can show that all the non-Atkin-Lehner involutions are:

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

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

$$\left. \begin{array}{ll} w_r S_3, & w_r S_3^2, \\ w_r w_9 S_3 w_9, & w_r w_9 S_3^2 w_9 \end{array} \right\} \; if \; r \equiv 2 (mod\ 3)$$

Proposition 3.13. *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.*
For $r \equiv 1(mod\ 3)$, the number of fixed points of $w_rS_3w_9S_3^2$ and $w_rS_3^2w_9S_3$ in $X_0(N)$ is equal to the number of fixed points of w_rw_9.
For $r \equiv 2(mod\ 3)$, the number of fixed points of $w_rS_3, w_rS_3^2, w_rw_9S_3w_9$ and $w_rw_9S_3^2w_9$ is bounded by 3 times the number of fixed points of w_r in $X_0(N/3)$.

Proof. First, if τ is a fixed point for $S_3w_9S_3^2$ then:

$$w_9S_3^2\tau = \gamma S_3^2\tau$$

and setting $S_3^2\tau = \tau'$ the result follows. A similar argument holds for the involutions $S_3^2w_9S_3$, $w_rS_3^2w_9S_3$ and $w_rS_3w_9S_3^2$. For the last two cases just notice that $w_rS_3 = S_3w_r$, if $r \equiv 1(mod\ 3)$.
When $r \equiv 2(mod\ 3)$, S_3 corresponds to multiplication by 3 and $w_9S_3w_9$, $w_9S_3^2w_9$ belong to $\Gamma_0(N/3) \setminus \Gamma_0(N)$. Now, write $i = S_3, S_3^2, w_9S_3w_9$ or $w_9S_3^2w_9$. From $w_ri\tau = \gamma\tau$, $\gamma \in \Gamma_0(N)$ we have $w_r3\tau = \delta3\tau$, $\delta \in \Gamma_0(N/3, 3)$ if $i = S_3$ or S_3^2, and $w_r\tau = \delta\tau$, $\delta \in \Gamma_0(N/3)$ if $i = w_9S_3w_9$ or $w_9S_3^2w_9$. Therefore, 3τ or τ is a fixed point of w_r in $X_0(N/3)$. □

Applying the above proposition to $N = 90$, it follows

Corollary 3.14. *$X_0(90)$ is not a bielliptic curve.*

Summarizing the results obtained above we can state:

Theorem 3.15. *There are exactly forty one values of N, such that the modular curve $X_0(N)$ is bielliptic. Moreover, each $X_0(N)$ has a bielliptic involution of Atkin-Lehner type, except for $X_0(72) = X_0(2^33^2)$. The full list of N, $N \neq 72$, is the following:*

N	*All the bielliptic involutions*
22	w_2, w_{22}
26	w_2, w_{13}
28	$w_4, w_{28}, S_2w_4S_2, S_2, w_7S_2, w_7S_2w_4S_2$
30	w_5, w_6, w_{30}
33	w_{33}
34	w_2, w_{17}, w_{34}
35	w_5
37	$w_{37}, \alpha w_{37}$ †
38	w_{19}, w_{38}
39	w_3
40	w_{40},S_2,$w_8S_2w_8$,$S_2w_8S_2w_8$,$w_5S_2w_8S_2$
42	w_{14}
43	w_{43}
44	w_{11},w_{44},$w_{11}S_2$,$w_{11}w_4S_2w_4$

† α is the hyperelliptic involution

N	*All the bielliptic involutions*
48	$w_{48}, S_2w_{16}S_2, w_3S_2w_{16}S_2, S_2, w_{16}S_2w_{16}$ ‡
	$w_3S_4, w_3S_4^3, w_3w_{16}S_4w_{16}, w_3w_{16}S_4^3w_{16}$
50	w_2, w_{25}
51	w_{17}, w_{51}
53	w_{53}
55	w_{11}, w_{55}
56	$w_7, w_{56}, w_7S_2w_8S_2$
60	w_{15}
61	w_{61}
62	w_{31}
63	$w_{63}, w_7S_3^2w_9S_3, w_7S_3w_9S_3^2$ §
65	w_{65}
69	w_{23}
75	w_{75}
79	w_{79}
83	w_{83}
89	w_{89}
92	w_{23}
94	w_{47}
95	w_{95}
101	w_{101}
119	w_{119}
131	w_{131}
N	*Some bielliptic involutions*
45	w_5, w_9, w_{45}
54	$w_{27}, w_{54},\ S_3w_{27}S_3^2, S_3^2w_{27}S_3$
64	$w_{64}, S_2, w_{64}S_2w_{64}$
72	$S_2, w_8S_2w_8, w_9S_2w_8S_2w_8$
81	$w_{81}, S_3w_{81}S_3^2, S_3^2w_{81}S_3$

Corollary 3.16. *The modular curves $X_1(N)$, $X(N)$ are not bielliptic for $N \geq 132$ and, for all N in the table below:*
52, 57, 58, 66, 67, 68, 70, 73, 74, 76, 77, 78, 80, 82, 84, 85, 86, 87, 88, 90, 91, 93, 96, 97, 98, 99, 100, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130.

Proof. We have finite morphisms : $X_1(N) \to X_0(N)$ and $X(N) \to X_0(N)$. □

Corollary 3.17. *Assume $X_0(N)$ of genus greater than or equal to 2. Then*

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

for some number field L 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,

‡For $X_0(48)$ it is possible to show that every element of $Norm(\Gamma_0(48))$ can be written as a product $w_q\beta$, where $\beta \in \{w_{16}, S_4 | S_4^4 = w_{16}^2 = (w_{16}S_4)^3 = 1\}$

§For $X_0(63)$ we use the characteristic property for bielliptic involutions of acting as -1 on a codimension 1 subspace of the space of differentials. This action in computed in [7] using the result of $Aut(X_0(63))$ of [4].

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.
For $C = X(N)$ or $X_1(N)$ and N not in the previous list $\#\Gamma_2(C, L) < \infty$ for every number field L.

Proof. The list above consists of all the values of N such that $X_0(N)$ is a bielliptic or hyperelliptic curve. □

Remark 3.18. *As an afterthought to theorem 3.15 we formulate the following conjecture:*
Let a, b, c and d be integers satisfying $a^b - c^d = 1$ with $a, c \neq 1$ and $b, d \geq 2$. Then the modular curve $X_0(a^b c^d)$ is bielliptic.
We notice that the previous conjecture is equivalent to the Catalan conjecture.

4 Quadratic points over $\mathbb{Q}$

Following Abramovich and Harris ([1]), we can state this well-known arithmetical version:

Proposition 4.1. *Let C be a curve of genus greater than or equal to 2, defined over a number field K. Then $\#\Gamma_2(C, K) = \infty$ if and only if C is a hyperelliptic curve or a bielliptic curve over K mapping to an elliptic curve E with $rank_K E \geq 1$.*

We consider now a modular parametrization defined over $\mathbb{Q}$

$$\varphi : X_0(N) \to E$$

Let ω be the Néron differential of E. Then $\varphi^*(\omega) = 2\pi i f(\tau) d\tau$, $f \in S_2(\Gamma_0(N))$. If $f \in S_2(\Gamma_0(N))^{new}$ we call φ a weak Weil parametrization ([9]).

Proposition 4.2. *The only values of N, modulo the Manin conjecture for $N = 40, 45, 48$ and 64 ¶, such that there exists a weak Weil parametrization of conductor N and degree 2 defined over $\mathbb{Q}$ are the following:*
26, 30, 34, 35, 37, 38, 39, 40, 43, 44, 45, 48, 50, 51, 53, 54, 55, 56, 61, 62, 64, 65, 69, 79, 83, 89, 92, 94, 101, 131.

Proof. For $N \leq 106$ it follows directly from the table 22 of [12]. For $N = 119$, there is no elliptic curve having this conductor. For $N = 131$ it comes from the fact that N is prime and the bielliptic involution w_{131} is defined over $\mathbb{Q}$. □

Finally, as a consequence of Carayol's theorem and the study of the $\mathbb{Q}$-simple factors of $Jac(X_0(N))$, if $\varphi : X_0(N) \to E$ is a modular parametrization defined over $\mathbb{Q}$ then the conductor of E must divide N. Using this fact we obtain:

Theorem 4.3. *The only values of N such that $\#\Gamma_2(X_0(N), \mathbb{Q}) = \infty$, are the following: 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.*

¶For each of these four values, the bielliptic involution of the strong modular parametrization of degree two is not of Atkin-Lehner type, following [9].

5 Modular parametrizations

Let $\varphi : X_0(N) \to E$ be a modular parametrization defined over $\mathbb{Q}$ and $\varphi^*(\omega) = f\frac{dq}{q}$, the pull-back of the Néron differential. Then f is an eigenvector of the Hecke operator T_p, $(p, N) = 1$. If f is a new form, there exists a modular paremetrization (called strong Weil parametrization), of minimal degree (see table 22 of [12]). Moreover, if f is not a new form, we have $f \in < g|_{B_d} >$, $g \in S_2(\Gamma_0(M))^{new}$, $M|N$, and $g|_{B_d}(\tau) = g(d\tau)$, where d runs over all divisors of N/M. Hence, the conductor of E is M and there is a modular parametrization

$$\varphi' : X_0(M) \to E'$$

Question 5.1. *The question is if one can find a morphism $\beta : X_0(N) \to X_0(M)$ such that $\varphi = \varphi' \circ \beta$?*

The general answer to this question is negative, an easy counterexample being $N = 33$. In this case $X_0(33)/w_{33} = 11A$, and $X_0(11) = 11B$.

Proposition 5.2. *Suppose $e^2|N$ and $M = N/e$. Every modular parametrization with differential $2\pi i h(e\tau)$ factorizes through $X_0(M)$ to the same elliptic curve.*

Proof. Let

$$\varphi : X_0(N) = \Gamma_0(N)\backslash\overline{\mathbb{H}} \to \mathbb{C}/\Lambda = E$$

satisfy $\varphi^*(\omega) = 2\pi i h(e\tau)$. Then φ is up to a constant equal to:

$$\varphi_h(\tau) = \int_{i\infty}^{\tau} 2\pi i h(e\tau')d\tau'$$

and $\Lambda = \{C_1(\gamma) = \int_{i\infty}^{\gamma i\infty} 2\pi i h(e\tau')d\tau' | \gamma \in \Gamma_0(N)\}$. Consider

$$\varphi'_h(\tau) = \frac{1}{e}\int_{i\infty}^{\tau} 2\pi i h(\tau')d\tau'.$$

Using the canonical isomorphism of $X_0(N)$ to $X_0(M, e)$ represented by multiplication by e, and the natural morphism of $X_0(M, e)$ to $X_0(M)$ we have the following commutative diagram:

$$\begin{tikzcd}
X_0(N) \arrow[r, "\varphi_h"] \arrow[d, "e"'] & \mathbb{C}/\Lambda \arrow[dd, "proj"] \\
X_0(M,e) \arrow[ur, "\varphi'_h"'] \arrow[d] & \\
X_0(M) \arrow[r, "\varphi'_h"'] & \mathbb{C}/\Lambda_2
\end{tikzcd}$$

where $\Lambda_2 = \{C_2(\gamma) = \frac{1}{e}\int_{i\infty}^{\gamma i\infty} 2\pi i h(\tau')d\tau' | \gamma \in \Gamma_0(M)\}$. We have

$$\Lambda_2 = \cup_{i=0}^{e-1} C_2(\alpha_i)\Lambda$$

with $\alpha_j = \begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix}$, for $j = 0, \ldots, e-1$, where $\{\alpha_j\}_{j=0}^{e-1}$ is a right cosset full system for $\Gamma_0(M)/\Gamma_0(M, e)$. We obtain that $C_2(\alpha_j) \in \Lambda$, and thus $\Lambda_2 = \Lambda$. $\square$

Corollary 5.3. *Suppose that $X_0(N)$ is a bielliptic curve with $p^2|N$, p an odd prime. If φ is a modular parametrization of degree 2, then its differential does not have the form $\varphi^*(\omega) = f\frac{dq}{q}$, $f = h(p^n\tau)$, $h \in S_2(N/p^n)$, $n \geq 1$.*

Corollary 5.4. *Let $4|N$. If $X_0(N)$ is a bielliptic curve and φ is a modular parametrization of degree 2 with differential $f = h(2^n\tau)$, $n \geq 1$,($h \in S_2(\Gamma_0(N/2^n))$ then φ is the natural map: $X_0(N) \to X_0(N/2)$.*

References

[1] *D. Abramovich and J. Harris*, Abelian varieties and curves in $W_d(C)$; Compositio Mathematica 78, 227-238 (1991).

[2] *A.O.L. Atkin and J.Lehner*, Hecke operators on $\Gamma_0(N)$; Math. Ann.185 (1970), 134-160.

[3] *J.E. Cremona*, Algorithms for modular elliptic curves; Cambridge Univ. Press, 1992.

[4] *N. Elkies*, The automorphism group $X_0(63)$; Compos. Mathm. 74, 203-208 (1990).

[5] *J. Harris and J.H. Silvermann*, Bielliptic curves and symmetric products; Proc. of Amer. Math. Soc.,112,2 June 1991.

[6] *M. Hindry*, Points quadratiques sur les courbes; C.R.Acad.Sci.Paris t.305, p.219-221,1987.

[7] *M.A. Kenku and F. Momose*, Automorphism groups of the modular curves $X_0(N)$; Compositio Mathem. 65 (1988) 51-80.

[8] *Kluit*, On the normalizer of $\Gamma_0(N)$. In Modular forms of one variable IV, LNM 601, Springer, 239-246.

[9] *B.Mazur and P.Swinnerton-Dyer*, Arithmetic of Weil Curves; Inventiones math. 25, 1-61, (1974).

[10] *A.P. Ogg*, Hyperelliptic modular curves; Bull. Soc. math. France 102 (1974) 449-462.

[11] *A.P. Ogg*, Rational points on certain elliptic modular curves. In Analityc Number Theory, Proceedings of Symposia in Pure Mathematics XXIV, 221-232.

[12] Corbes modulars: Taules. Notes del seminari de Teoria de Nombres UB-UAB-UPC, Barcelona 1992.