Courbes modulaires bielliptiques

Francesc Bars
Departament de Matemtiques
Universitat Autnoma de Barcelona
e-mail: francesc@manwe.mat.uab.es
08193 Bellaterra
Catalunya, Espagne

Résumé.- Nous determinons toutes les valeurs de N telles que $X_0(N)$ est bielliptique. D'autre part, nous résolvons la question arithmétique de trouver toutes les valeurs de N pour lesquelles $X_0(N)$ a un nombre infini de points quadratiques sur le corps $\mathbb{Q}$.

Version abrégée.

Nous considérons les courbes modulaires $X_0(N)$ de genre > 1. D'aprs [1] la non finitude du nombre de points quadratiques d'une courbe non singulière sur un certain corps de nombres K, est caractérisée par le fait que la courbe est hyperelliptique ou bielliptique. Pour $X_0(N)$, le cas hyperelliptique a été étudié par Ogg [4]. Dans le cas bielliptique nous étudions les points fixes des involutions qui apparaissent dans $Aut(X_0(N))$, ce qui nous mène au résultat suivant:

Théorème. *Il y a exactement quarante et une valeurs de N, telles que la courbe modulaire $X_0(N)$ soit bielliptique. De plus, chaque $X_0(N)$ possède une involution bielliptique de type Atkin-Lehner, sauf $X_0(2^3 3^2)$. (Pour la liste complète des valeurs de N vovi le théorème 1)*

Quand on fixe le corps de nombres K, on a besoin d'imposer certaines propriétés arithmétiques. Dans le cas bielliptique, il faut que le morphisme de degré deux soit défini sur K et que la courbe elliptique ait K-rang positif pour qu'elle ait un nombre infini de points quadratiques (genre plus grand que 2). On obtient:

Théorème. *Il y a exactement vingt-huit valeurs de N, telles que*

$$\#\bigcup X_0(N)(L) = \infty$$

, o L parcourt toutes les extensions de degré deux de $\mathbb{Q}$. (Pour la liste complète des valeurs de N vovi théorème 4).

Rappelors qu'une courbe hyperelliptique a toujours un nombre infini de points quadratiques sur $\mathbb{Q}$. Si on a un revtement d'une courbe elliptique par la courbe $X_0(N)$ le conducteur de cette courbe elliptique divise N. Cette propriété fournit avec les tables des rangs de c.e. sur $\mathbb{Q}$, une première liste de valeurs possibles pour N. Nous étudierons finalement les quotients de la courbe par les involutions bielliptiques correspondantes pour conclure la démonstration du théorème.

Bielliptic modular curves

Abstract.- We find all the values of N such that $X_0(N)$ is bielliptic. Moreover, we solve the arithmetic question of finding all the values of N such that $X_0(N)$ has infinitely many quadratic points over the ground field $\mathbb{Q}$.

Assume $X_0(N)$ to have genus greater than 1. Write w_i with $(i, N/i) = 1$ for the corresponding Atkin-Lehner involution of $X_0(N)$ and $S_i = \begin{pmatrix} 1 & 1/i \\ 0 & 1 \end{pmatrix}$.

Theorem 1. *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 $X_0(72) = X_0(2^3 3^2)$. The full list of N, $N \neq 72$, is the following:*

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*

N	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	$w_{37}, \alpha w_{37}$[1]
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	$w_{11}, w_{44}, w_{11}S_2, w_{11}w_4S_2w_4$
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}

[1] α denotes the hyperelliptic involution.

N	Bielliptic involutions
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 2. *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*					

We define $\Gamma_d(X_0(N), K)$ as the union of $X_0(N)(L)$ for all extensions L of K of degree $\leq d$.

Corollary 3. *We have*

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

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*	*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.

Theorem 4. *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*

About the proofs.- If $X_0(N)$ is a bielliptic curve we have a degree two map to an elliptic curve. If genus of $X_0(N)$ is greater than six we can define everything over $\mathbb{Q}$. Then, reducing over $\overline{\mathbb{F}_p}$ for $p \nmid N$ and counting points of $X_0(N)$ defined over $\mathbb{F}_{p^2}$, we obtain that $X_0(N)$ is not a bielliptic curve for $N > 210$, and also that is not a bielliptic curve if $16|N$ or $27|N$ or $36|N$. The remaining cases are determined by finding the correponding bielliptic involutions, i.e., the involutions υ of $X_0(N)$ such that $X_0(N)/\upsilon$ has genus 1. If $4 \nmid N$ and $9 \nmid N$, the only possible involutions are the ones of Atkin-Lehner type. If $4|N$ or $9|N$ new involutions appear (see [3]) and a computation of the number of fixed points for each one leads to the result of theorem 1.
Using the fact that bielliptic curves map to bielliptic or hyperelliptic curves and [4] we obtain corollary 2. Corollary 3 follows from the following property ([1]): Let C be a non-singular curve of genus greater than 2, then C has infinitely many quadratic points if and only if it is either hyperelliptic or bielliptic. In fact, one can state ([1]) a stronger arithmetical result, namely: if C is defined over a number field K, then $\#\Gamma_2(C, K) = \infty$ if and only if C is a hyperelliptic or a bielliptic curve mapping (over K) to an elliptic curve E with $rank_K(E) \geq 1$. With this arithmetical result in mind, if we have a degree 2 parametrization over $\mathbb{Q}$, $\varphi : X_0(N) \to E$, Carayol's theorem says that the conductor of E divides N. This allows us to throw away some values of N for which $\#\Gamma_2(X_0(N), \mathbb{Q}) < \infty$. For the other values of N, it amounts to a case-by-case verification for we know, by theorem 1, the corresponding bielliptic involutions. This finish the proof of the result stated in theorem 4.

Remark 5. The problem of finding N with $\varphi : X_0(N) \to E$ with degree 2 over $\mathbb{Q}$, is essentially the problem of finding modular paremitrizations of degree 2. It is known that if the conductor of E is equal to N then there exists a minimal degree parametrization called strong modular parametrization. In general, if $\varphi : X_0(N) \to E$ is a modular parametrization defined over $\mathbb{Q}$ the conductor M of E is a divisor of N and there exists a modular parametrization

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

In this situation one can ask if there is 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 $X_0(11) = 11B$.
But, for example, a situation with positive answer is:

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.

Acknowledments

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 also grateful to Sammy Tindel for his help for the writing the french parts of this work.

References

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

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

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

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