Momose and bielliptic modular curves

Francesc Bars

Universitat Autònoma de Barcelona

23 May 2012

k number field
$C = C_{|k}$ non-singular projective curve over k
Fix $\overline{k}$ and write $\overline{C} = C \times_k \overline{k}$
$g_C := genus(C)$ (always ≥ 2)
L/k finite field extension (all extensions of k in $\overline{k}$):
$C(L)$ point of C defined over L or L-points
$\#C(L)$ number of L-points (say $= \infty$ if is not finite)

Theorem (Faltings, 1983)

If $g_C \geq 2$ then $\#C(L)$ is finite.

After Falting's result we ask for finite number or not of quadratic points over k:

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

When $\Gamma_2(C,k)$ is a finite set?

Theorem (Abramovich,Harris, 1991)

Take C with $g_C \geq 2$. Then:
$\exists L/k\ \#\Gamma_2(C,L) = \infty \Leftrightarrow \overline{C}$ *is hyperelliptic or bielliptic curve.*

Recall: $\overline{C}$ hyperelliptic if has a degree 2 map to $\mathbb{P}^1$
(iff $\exists w \in Aut(\overline{C})$ involution with $2g_C + 2$ fixed points)
$\overline{C}$ is bielliptic if exists $\overline{C} \to^{2:1} E$; E an elliptic curve over $\overline{k}$
(iff $\exists v \in Aut(\overline{C})$ involution with $2g_C - 2$ fixed points).

An arithmetical geometry statement is:
* If $\overline{C}$ hyperelliptic and $C(k) \neq \emptyset$, exists $\varphi : C_{|k} \to^{2:1} \mathbb{P}^1_{|k}$ all defined over, thus $\#\Gamma_2(C,k) = \infty$.

Theorem (Abramovich-Harris,1991)

Take C with $g_C \geq 2$ and defined over k with $C(k) \neq \emptyset$. Then:

$$\#\Gamma_2(C,k) = \infty$$

$$\Updownarrow$$

$\overline{C}$ hyperelliptic or $\exists \varphi : C \to^{2:1} E$ all defined over k and $rank(E(k)) \geq 1$.

* If $g_C \geq 6$ and $\overline{C}$ bielliptic with $C(k) \neq \emptyset$, then exists an unique $\varphi : C \to^{2:1} E$ and all defined over k (the bielliptic involution is unique).

Take a family of modular curves X_N: for example $X_0(N)$
*: By Faltings: $X_N(L)$ is a finite set.

Question

Which N satisfies $\#\Gamma_2(X_N, L_{X_N}) = \infty$ for some number field L_{X_N}?

- Need list X_N hyperelliptic ($Aut(\overline{X_N})$ could be useful).
- Need list X_N bielliptic ($Aut(\overline{X_N})$ could be useful).

Question

Which N satisfies $\#\Gamma_2(X_N, \mathbb{Q}) = \infty$?

Consider the classical modular curves $X_0(N) = \overline{\mathbb{H}}/\Gamma_0(N)$ where

$$\Gamma_0(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) | c \equiv 0 (mod\ N)\}$$

$Norm(\Gamma_0(N))$ is the normalizer of $\Gamma_0(N)$ in $SL_2(\mathbb{R})$
*Obviously $Norm(\Gamma_0(N))/\Gamma_0(N) \leq Aut(\overline{X_0(N)})$ (inner automorphisms).
*Known all the elements of $Norm(\Gamma_0(N))$ [Newman, 1955]
*Known the group structure of $Norm(\Gamma_0(N))/\Gamma_0(N)$
Warning: last theorem of "Hecke operators of $\Gamma_0(N)$" by Atkin-Lehner is wrong.
*If $4 \nmid N$ and $9 \nmid N$ $Norm(\Gamma_0(N))/\Gamma_0(N) = \{w_d | (d, N/d) = 1\}$ where w_d are the Atkin-Lehner involutions.

First step: List N where $X_0(N)$ is hyperelliptic curve.

Theorem (Ogg, 1974)

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 reading in 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}

Second step: Reduce the N where $X_0(N)$ maybe is bielliptic to a finite list.
Take p prime $p \nmid N$, reduce the modular curve to $\mathbb{F}_p$

Theorem (Harris-Silverman,1991)

If $X_0(N)$ bielliptic (with genus ≥ 6) then:

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

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

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

It follows $2 \nmid N$ inequalities as $N \leq 192$ and we deduce

Proposition

$X_0(N)$ non-bielliptic for $N > 210$.

Third step: Study case by case when $X_0(N)$ bielliptic or not.
* Atkin-Lehner involutions $w_d \in Norm(\Gamma_0(N))/\Gamma_0(N)$ are classically known the # of fixed points on $X_0(N)$, thus:

Lemma

We can list N where $X_0(N)$ bielliptic with an involution of Atkin-Lehner type (in particular $N = 37, 63$ are bielliptic curves).

* Automorphism contribution.

Theorem (Kenku-Momose, 1988)

For $N \neq 37, 63$ we have

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

* For $4 \nmid N$ and $9 \nmid N$ all the involutions are Atkin-Lehner involutions, the biellipic problem is over for $X_0(N)$.

* If $4|N$ or $9|N$ more involutions than the Atkin-Lehner type appear.
We compute [B,1999] the fixed points for some of these new involutions, in order to conclude:

Theorem (B, 1999)

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, expect $X_0(2^3 3^2)$. 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

Fourth step: Quadratic points over $\mathbb{Q}$ of $X_0(N)$.

Theorem (B, 1999)

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	

Restrict N where $X_0(N)$ bielliptic and non-hyperelliptic.
Suppose $X_0(N)$ bielliptic over rationals, discard by Carayol the conductors and divisors where the rank of elliptic curves is zero.
Luckily, the remaining cases come from the study of the strong modular parametrization of Weil [Mazur,Swinnerton-Dyer, 1974].

We can consider different modular families X_N:

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

corresponding to modular groups $\Gamma(N), \Gamma_1(N) = \Gamma_{\{\pm 1\}}(N)$,

$$\Gamma_\Delta(N) := \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) | c \equiv 0 (mod\ N), (a\ mod\ N) \in \Delta\}$$

and recall that we have natural finite maps:

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

Let us try to follow what we did for $X_0(N)$ for these other families of modular curves.

First step: Find N where X_N hyperelliptic.

Theorem (Ishii-Momose, 1991)

$X_1(N)$ is hyperelliptic only for $N = 13, 16$ and 18.

[Newman (1955), Kim-Koo (2000)] *Norm*$(\Gamma_1(N))$ generated by $\Gamma_0(N)/\pm Id$ (named $[a] \equiv \begin{pmatrix} a & * \\ 0 & * \end{pmatrix}$ modulo N) and w_d .

Theorem (Ishii-Momose, 1991)

If $\{\pm 1\} \subsetneq \Delta$ the only hyperelliptic curve for the family $X_\Delta(N)$ is $X_{\{\pm 1, \pm 8\}}(21)$.

w_d not always in *Norm*$(\Gamma_\Delta(N))$.

Theorem (...,B-Xarles 2012)

There are no N where $X(N)$ is hyperelliptic.

Second step: reduce to a finite set of N where X_N bielliptic.

Proposition (Silverman-Harris, 1991)

Let be $C \to C'$ a finite morphisms with $g_{C'} \geq 2$. If C is bielliptic then C is bielliptic or hyperelliptic.

Corollary

For X_N is non-bielliptic for the N where $X_0(N)$ is not bielliptic or hyperelliptic, in particular for $N \geq 132$.

Thrid step: Study case by case remaining N.

Theorem (Jeon-Kim, 2004)

Take N with $g_{X_1(N)} \geq 2$, i.e. $N \geq 16$ or $N = 13$. $X_1(N)$ is bielliptic for exactly when $2 \leq g_{X_1(N)} \leq 6$ (which are the following values $13, 16, 17, 18, 20, 21, 22, 24$).

- $2 \leq g_{X_1(N)} \leq 6$: [Ishii-Momose] studied fixed points for $[a]w_d$, a bielliptic involution are of the above form in the normalizer.
- Other situations are non-bielliptic $g_{X_1(N)} > 6$, arguments used:
  * [Momose, preprint, available?] N square-free
  $Norm(\Gamma_1(N))/\Gamma_1(N) = Aut(\overline{X_1(N)})$
  * $X_1(N) \to X_0(N)$ induces involution on $X_0(N)$, the action on cusps on $X_1(N)$ moving rational to non-rational cusps gives a contradition (the bielliptic involution is defined over rationals if exists)

* for square values dividing N from [Kenku-Momose] deduce bielliptic involution on $Norm(\Gamma_1(N))/\Gamma_1(N)$ (from $X_1(N) \to X_0(N)$), is generated by Atkin-Lehner involutions and $\Gamma_0(N)$, and these AL-involutions are not rational on $X_1(N)$ in a lot of cases.

Theorem (B-Xarles,2012)

Take N with $g_{X(N)} \geq 2$, i.e. $N \geq 7$. Then $X(N)$ is bielliptic for $X(7)$ or $X(8)$.

* $X(7)$ Klein quartic, $X(8)$ Wieman curve: both are known that are bielliptic curves.
* Use $\phi : X(N) \to C$ and if $X(N)$ bielliptic then

$$2g_{X(N)} - 2 \leq deg(\phi) n_v$$

where n_v is the number of fixed points of any involution on C.

Theorem (Jeon-Kim, preprint 2011)

The list of bielliptic intermediate curves are:

$X_{\{\pm1,\pm8\}}(21)$,$X_{\{\pm1,\pm5\}}(24)$,$X_{\{\pm1,\pm7\}}(24)$, $X_{\{\pm1,\pm5\}}(26)$, $X_{\{\pm1,\pm3,\pm9\}}(26)$, $X_{\{\pm1,\pm13\}}(28)$,$X_{\{\pm1,\pm3,\pm9\}}(28)$, $X_{\{\pm1,\pm4,\pm5,\pm6,\pm7,\pm9,\pm13\}}(29)$, $X_{\{\pm1,\pm11\}}(30)$, $X_{\{\pm1,\pm15\}}(32)$, $X_{\{\pm1,\pm2,\pm4,\pm8,\pm16\}}(33)$, $X_{\{\pm1,\pm9,\pm13,\pm15\}}(34)$,$X_{\{\pm1,\pm6,\pm8,\pm13\}}(35)$, $X_{\{\pm1,\pm4,\pm6,\pm9,\pm11,\pm16\}}(35)$,$X_{\{\pm1,\pm11,\pm13\}}(36)$, $X_{\{\pm1,\pm4,\pm10,\pm14,\pm16,\pm17\}}(39)$, $X_{\{\pm1,\pm9,\pm11,\pm19\}}(40)$, $X_{\{\pm1,\pm2,\pm4,\pm5,\pm8,\pm9,\pm10,\pm16,\pm18,\pm20\}}(41)$,$X_{\{\pm1,\pm4,\pm11,\pm14,\pm16,\pm19\}}(45)$, $X_{\{\pm1,\pm11,\pm13,\pm23\}}(48)$, $X_{\{\pm1,\pm6,\pm8,\pm13,\pm15,\pm20,\pm22\}}(49)$, $X_{\{\pm1,\pm9,\pm11,\pm19,\pm21\}}(50)$,$X_{\{\pm1,\pm4,\pm6,\pm9,\pm14,\pm16,\pm19,\pm21,\pm24,\pm26\}}(55)$, $X_{\{\pm1,\pm7,\pm9,\pm15,\pm17,\pm23,\pm25,\pm31\}}(64)$.

* Precise control to find precise elliptic elements for w_d in $Norm(\Gamma_0(N))$ and study the fixed points of these elliptic elements when they give involution in $X_\Delta(N)$.

4th step: Quadratic points over $\mathbb{Q}$ of X_N.
For $X_1(N)$ we can use the result

Theorem (Kenku-Momose, 1988)

$E_{tors}(\mathbb{Q}(\sqrt{d}))$ 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* $l \leq 2$
$\mathbb{Z}/4 \times \mathbb{Z}/4$.

Corollary (Jeon-Kim, 2004)

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:

$$13, 16, 18$$

Assume: given $\phi : X_N \to E$, then the conductor of E divides N:

Corollary (B,2012)

Take N with $g_{X_\Delta(N)} \geq 2$, with $\{\pm 1\} \subsetneq \Delta$. Then $\Gamma_2(X_\Delta(N), \mathbb{Q}) = \infty$ iff $X_\Delta(N) = X_{\{\pm 1, \pm 8\}}(21)$.

The assumption is not true for $X(N)$ for example we have a degree two map:

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

of conductor 32!!
Now: take any model $\mathcal{X}(N)_{\mathbb{Q}}$ over $\mathbb{Q}$ of $X(N)$ where $X(N)$ is the curve as moduli problem over $\mathbb{Q}(\zeta_N)$ with N-torsion is $(\mathbb{Z}/N)^2$ in $\mathbb{Q}(\zeta_N)$.

Theorem (B-Xarles,2012)

For any $N \geq 7$ we have that the set $\Gamma_2(\mathcal{X}(N)_{\mathbb{Q}}, \mathbb{Q})$ is always finite.

We prove $\Gamma_2(X(N), \mathbb{Q}(\zeta_N))$ is always a finite set.

Question

Take $\mathcal{X}(N)_{\mathbb{Q}}$ with $\mathcal{X}(N)_{\mathbb{Q}}(\mathbb{Q}) \neq \emptyset$. An assume that we have a morphism over $\mathbb{Q}$:

$$\mathcal{X}(N)_{\mathbb{Q}} \to E$$

with E an elliptic curve. Is $\mathrm{cond}(E)$ dividing N^2?