Primes of bad reduction of curves of genus 3 with CM

Elisa Lorenzo García

Université Rennes 1

Joint work with P. Kılıçer, K. Lauter, R. Newton, E. Ozman and M. Streng

19-06-2017

The result

Theorem

Let C/M be a curve of **genus** 3 *over a number field M. Suppose that the Jacobian $\mathrm{Jac}(C)$ has* **complex multiplication (CM)** *by an order $\mathcal{O}$ inside a CM field K of degree 6 and that the CM type of C is* **primitive***.*

Let $\mathfrak{p}$ be a prime of M lying over a rational prime p such that C does not have potential good reduction modulo $\mathfrak{p}$.

Then the following upper bound holds on p. For every $\mu \in \mathcal{O}$ with μ^2 totally real and $K = \mathbb{Q}(\mu)$, we have

$$p < \frac{1}{8} B^{10}$$

where $B = -\frac{1}{2} \mathrm{Tr}_{K/\mathbb{Q}}(\mu^2)$.

The motivation

Construction of CM-curves.
For constructing elliptic curves with CM by an order $\mathcal{O}$ in an imaginary quadratic field we can use the complex multiplication method. That is, by numerically computing the Hilbert class polynomial

$$H_{\mathcal{O}}(x) = \prod_{E \text{ has CM by } \mathcal{O}} (x - j(E)) \in \mathbb{Z}[x].$$

For curves of genus 2 and higher, these polynomial have rational coefficients, so in order to imitate the method, we need to bound the coefficients.
This was done for the case of genus 2 by Goren-Lauter and Lauter-Viray.

A corollary

A **hyperelliptic curve of genus** 3 is a curve defined by an equation of the form

$$C : y^2 = f(x)$$

such that f is a separable polynomial of degree 8.
Shioda gives a set of absolute invariants $j = u/\Delta^l$. The discriminant Δ has degree 56.
A **Picard curve of genus** 3 is a smooth plane curve of the form

$$C : y^3 = f(x)$$

such that f is a monic separable polynomial of degree 4.
We have the a set of absolute invariants $j = u/\Delta^l$. The discriminant Δ has degree 12.

A corollary

Theorem

Let C/M be a hyperelliptic or Picard curve of genus 3 over a number field M. Suppose that C has CM by an order $\mathcal{O}$ inside a CM field K of degree 6 and that the CM type of C is primitive. Let $l \in \mathbb{Z}_{>0}$ and let $j = u/\Delta^l$ be a quotient of invariants of hyperelliptic (respectively Picard) curves, such that the numerator u has degree 56l (respectively 12l). Let $\mathfrak{p}$ be a prime over a prime number p such that $\mathrm{ord}_{\mathfrak{p}}(j(C)) < 0$. Then

$$p < \frac{1}{8} B^{10}$$

where B is as in previous Theorem.

The proof: the idea

Let $\mathfrak{p} \mid p$ be a prime such that C does not have potential good reduction modulo $\mathfrak{p}$.
Possibly after extending the base field again, we have

$$\overline{J} \cong E \times A$$

as principally polarized abelian varieties.
Let us write $\mathrm{End}(E) = \mathcal{R}$ and $\mathcal{B} = \mathcal{R} \otimes \mathbb{Q}$.
There is an isogeny $s : E^2 \to A$ ([BCLLMNO15]).
Then, there is a natural embedding

$$\iota : \mathcal{O} \overset{\iota_0}{\hookrightarrow} \mathrm{End}(E \times A) \overset{\iota_1}{\hookrightarrow} \mathrm{End}(E^3) \otimes \mathbb{Q} \cong \mathcal{M}_3(\mathcal{B}) \subseteq \mathcal{M}_3(B_{p,\infty})$$

We will see that **if p is big enough such embedding cannot exist** and then p cannot be a prime of bad reduction.

The proof: sketch

Let us write $K = \mathbb{Q}(\mu^2)$ with $\mu \in K_+$ a totally negative element such that $K_+ = \mathbb{Q}(\mu)$.

Step 1 is to show that for sufficiently large primes p, the entries of $\iota(\mu^2)$ lie in a field $\mathcal{B}_1 \subset \mathcal{B}$ of degree ≤ 2 over $\mathbb{Q}$.

Step 2 is to show that in the situation of Step 1, the field $\mathcal{B}_1$ embeds into K and the CM type is induced from $\mathcal{B}_1$, which contradicts primitivity of the CM type.

The isogeny

Let $\iota_0 : \mathcal{O} \hookrightarrow \mathrm{End}(E \times A)$ be the injective ring homomorphism coming from reduction of J at $\mathfrak{p}$ and write

$$\iota_0(\mu) =: \begin{pmatrix} x & y \\ z & w \end{pmatrix},$$

We define a homomorphism

$$s = \begin{pmatrix} z & wz \end{pmatrix} : E \times E \longrightarrow A.$$

Lemma

The map s is an isogeny and it defines an embedding $\iota : \mathcal{O} \hookrightarrow \mathcal{M}_3(B_{p,\infty})$.

Step 1

$$\begin{cases} \iota(-\mu) = \iota(\overline{\mu}) = \iota(\mu)^{\dagger} := \lambda\iota(\mu)^{\vee}\lambda^{-1} \\ \mu^6 + B\mu^4 + B'\mu^2 + B'' = 0 \end{cases} \Longrightarrow \iota(\mu) = \begin{pmatrix} x & a & b \\ 1 & 0 & c/n \\ 0 & 1 & d/n \end{pmatrix},$$

where $x, a, b, c, d, n \in \mathcal{R}$ satisfying "some relations".

Step 1

$$\begin{cases} \iota(-\mu) = \iota(\overline{\mu}) = \iota(\mu)^\dagger := \lambda \iota(\mu)^\vee \lambda^{-1} \\ \mu^6 + B\mu^4 + B'\mu^2 + B'' = 0 \end{cases} \implies \iota(\mu) = \begin{pmatrix} x & a & b \\ 1 & 0 & c/n \\ 0 & 1 & d/n \end{pmatrix},$$

where $x, a, b, c, d, n \in \mathcal{R}$ satisfying "some relations".

$$B \geq \sum \text{"positive things"}$$

Step 1

$$\begin{cases} \iota(-\mu) = \iota(\overline{\mu}) = \iota(\mu)^\dagger := \lambda\iota(\mu)^\vee\lambda^{-1} \\ \mu^6 + B\mu^4 + B'\mu^2 + B'' = 0 \end{cases} \implies \iota(\mu) = \begin{pmatrix} x & a & b \\ 1 & 0 & c/n \\ 0 & 1 & d/n \end{pmatrix},$$

where $x, a, b, c, d, n \in \mathcal{R}$ satisfying "some relations".

$$B \geq \sum \text{"positive things"}$$

Lemma (Goren, Lauter)

Let $\mathcal{R}$ be an order in the quaternion algebra $B_{p,\infty}$ and $x, y \in \mathcal{R}$. If $\mathrm{N}(x)\mathrm{N}(y) < p/4$, then x and y commute.

Step 1

$$\begin{cases} \iota(-\mu) = \iota(\overline{\mu}) = \iota(\mu)^\dagger := \lambda \iota(\mu)^\vee \lambda^{-1} \\ \mu^6 + B\mu^4 + B'\mu^2 + B'' = 0 \end{cases} \implies \iota(\mu) = \begin{pmatrix} x & a & b \\ 1 & 0 & c/n \\ 0 & 1 & d/n \end{pmatrix},$$

where $x, a, b, c, d, n \in \mathcal{R}$ satisfying "some relations".

$$B \geq \sum \text{"positive things"}$$

Lemma (Goren, Lauter)

Let $\mathcal{R}$ be an order in the quaternion algebra $B_{p,\infty}$ and $x, y \in \mathcal{R}$. If $\mathrm{N}(x)\mathrm{N}(y) < p/4$, then x and y commute.

Proposition

If $p > \frac{1}{8}B^{10}$, then the image $\iota(\mathcal{O})$ is inside the ring of 3×3 matrices over a field $\mathcal{B}_1 \subset \mathcal{B}$ of degree ≤ 2.

Step 2

Let $\sqrt{-\delta} \in \mathcal{O}$ with $\delta \in \mathbb{Z}_{>0}$ and $p \nmid 2\delta$. Let $\mathcal{O}_{\mathfrak{p}}$ be the valuation ring of $\mathfrak{p}$ and let $\mathfrak{K} = \mathcal{O}_M/\mathfrak{p}$ be the residue field. Let $\mathcal{J}/\mathcal{O}_{\mathfrak{p}}$ be a Néron model for J/M and let $\overline{J}/\mathfrak{K}$ be the special fibre of $\mathcal{J}$. Let $\tilde{e} : \mathrm{Spec}(\mathcal{O}_{\mathfrak{p}}) \to \mathcal{J}$, $e : \mathrm{Spec}(M) \to J$ and $e_0 : \mathrm{Spec}(\mathfrak{K}) \to \overline{J}$ be the identity sections of $\mathcal{J}$, J and $\overline{J}$ respectively.

Lemma

The $\mathcal{O}_{\mathfrak{p}}$-module $T^{\tilde{e}}_{\mathcal{J}/\mathcal{O}_{\mathfrak{p}}}(\mathcal{O}_{\mathfrak{p}})$ is free of rank 3. Furthermore, there are natural isomorphisms

$$T^{e}_{J/M}(M) \cong T^{\tilde{e}}_{\mathcal{J}/\mathcal{O}_{\mathfrak{p}}}(\mathcal{O}_{\mathfrak{p}}) \otimes_{\mathcal{O}_{\mathfrak{p}}} M$$

and

$$T^{e_0}_{\overline{J}/\mathfrak{K}}(\mathfrak{K}) \cong T^{\tilde{e}}_{\mathcal{J}/\mathcal{O}_{\mathfrak{p}}}(\mathcal{O}_{\mathfrak{p}}) \otimes_{\mathcal{O}_{\mathfrak{p}}} \mathfrak{K}$$

as vector spaces over M and $\mathfrak{K}$ respectively. Moreover, these isomorphisms respect the action of $T(f)$ for $f \in \mathrm{End}_M(J) = \mathrm{End}_{\mathcal{O}_{\mathfrak{p}}}(\mathcal{J})$.

Step 2

Since the CM type is primitive, there exists a matrix P such that

$$P\iota(\sqrt{-\delta})P^{-1} = \pm \begin{pmatrix} \sqrt{-\delta} & 0 & 0 \\ 0 & \sqrt{-\delta} & 0 \\ 0 & 0 & -\sqrt{-\delta} \end{pmatrix}.$$

Now since $P\iota(\mu^2)P^{-1}$ commutes with it, it can be written as

$$\begin{pmatrix} * & * & 0 \\ * & * & 0 \\ 0 & 0 & * \end{pmatrix},$$

which is a contradition with μ^2 being a root of a degree 3 irreducible polynomial.

Thank you!