Primes dividing the invariants of CM Picard Curves

Elisa Lorenzo García

Université Rennes 1
Joint work with Pınar Kılıçer and Marco Streng

02-06-2017

Picard Curves

Definition

Let k be a field of characteristic not 2 or 3. A *Picard curve* of genus 3 is a smooth plane projective curve given by an equation of the form

$$C : y^3 = x^4 + ax^2 + bx + c,$$

where a, b, $c \in k$.

- This model for the Picard curves is unique up to the scaling $(x, y) \mapsto (u^3x, u^4y)$.(Holzapfel.)
- If k contains a primitive 3rd root of unity ζ_3, then $\mathrm{Aut}(C)$ contains $\rho : (x, y) \mapsto (x, \zeta_3 y)$.
- Let C be a Picard curve with CM by an order $\mathcal{O}$ in a sextic CM field K. Then $\zeta_3 \in \mathcal{O}$. (The converse also holds, Koike-Weng.)

Picard Curves

In 2004, Koike and Weng showed a **conjectural** list of all the Picard curves with CM by a maximal order defined over $\mathbb{Q}$. They used the Complex Multiplication method and they *numerically computed class polynomials*.

In 2016, Kılıçer proved that there are 10 Picard curves with CM over $\mathbb{Q}$.

In 2016, Lario-Somoza improves previous algorithm and (**conjecturally**) computed the other 5 Picard curves with CM defined over $\mathbb{Q}$.

Picard Curves

In 2004, Koike and Weng showed a **conjectural** list of all the Picard curves with CM by a maximal order defined over $\mathbb{Q}$. They used the Complex Multiplication method and they *numerically computed class polynomials*.

In 2016, Kılıçer proved that there are 10 Picard curves with CM over $\mathbb{Q}$.

In 2016, Lario-Somoza improves previous algorithm and (**conjecturally**) computed the other 5 Picard curves with CM defined over $\mathbb{Q}$.

For elliptic curves the class polynomials have integer coefficients. For genus 2 curves, Goren-Lauter and Lauter-Viray provided bounds for the denominators of the class polynomials.

For genus 3 curves, we only have a bound for the primes in the denominators [BCLLMNO15] + [KLLNOS16].

Picard Curves: Invariants

Let Δ be the discriminant of $y^3 = x^4 + ax^2 + bx + c$:

$$\Delta = -4a^3b^2 + 16a^4c - 27b^4 + 144ab^2c - 128a^2c^2 + 256c^3.$$

It has weight 12.

Dixmier-Ohno invariants: for plane quartics, quite complicated. The denominators are Δ^3.

Shioda invariants:

$$\frac{a^6}{\Delta}, \frac{b^4}{\Delta}, \frac{c^3}{\Delta}.$$

Koike-Weng:

$$\frac{b^2}{a^3}, \frac{c}{a^2}.$$

Our invariants:

$$j_1 = \frac{a^3}{b^2}, j_2 = \frac{ac}{b^2}.$$

Main Theorem

Theorem

Let C be a Picard curve of genus 3 over a number field M which has primitive CM by an order $\mathcal{O}$ of a sextic CM field.

Let K_+ be the real cubic subfield of K and $\mathcal{O}_+ = K_+ \cap \mathcal{O}$. Let μ be a totally real element in $\mathcal{O}_+$ such that $K = \mathbb{Q}(\mu)(\zeta_3)$.

Let $j = u/b^k$ be a normalized Picard curve invariant. Let $\mathfrak{p}$ be a prime of M lying over a rational prime p. If $\mathrm{ord}_{\mathfrak{p}}(j(C)) < 0$, then

$$p < \mathrm{Tr}_{K_+/\mathbb{Q}}(\mu^2)^3 \leq 3^3 |\Delta(\mathcal{O}_+)|^{3/2}.$$

Main Theorem: idea

In [BCLLMNO15] and [KLLNOS16] we prove that a prime of bad reduction for a genus 3 curve with CM by a sextic order $\mathcal{O}$ gives a **solution to an embedding problem:**

$$\mathcal{O} \hookrightarrow \mathcal{M}_3(B_{p,\infty}).$$

Then we proved the non-existence of such embeddings if p was big enough.

If a prime p divides b, we do not necessarily have bad reduction, but we are able to construct a solution to an embedding problem by using that if $b = 0$ the jacobian of a Picard curve is not simple anymore and we can explicitly compute an elliptic factor.

Main Theorem: idea

In [BCLLMNO15] and [KLLNOS16] we proved that given a prime p of bad reduction of the curve, we have that the reduction of the Jacobian

$$\overline{J} \simeq E \times A.$$

This isomorphism induces the solution

$$\mathcal{O} \hookrightarrow \mathcal{M}_3(\mathcal{R}/n) \text{ with } \mathcal{R} = \mathrm{End}(E) \subseteq B_{p,\infty} \text{ and } n \text{ bounded }.$$

When $b = 0$ we have $\overline{J} \sim E \times A$. If the isogeny has degree m, we get

$$\mathcal{O} \hookrightarrow \mathcal{M}_3(\mathcal{R}/nm) \text{ with } \mathcal{R} \subseteq B_{p,\infty}.$$

So, we need to bound m.

Extra

Indeed, with Ritzenthaler-Rogmany recently result, we can compute that the jacobian of the curve

$$y^3 = x^4 + ax^2 + 1$$

is isogenous to $E \times A$, where

$$E: \ y^2 + ay = x^3 - 1,$$

and $A = J(D)$ with D the genus 2 curve

$$D: \ -ay^2 = (x^2 + 2x - 2)(x^4 + 4x^3 + (2a^2 - 8)x - a^2 + 4).$$

Main Lemma

Lemma

Let C/M be a Picard curve of genus 3 over a number field and let $\mathfrak{p} \nmid 6$ be a prime of M. Let $j = u/b^k$ be a normalized Picard curve invariant. If $\mathrm{ord}_{\mathfrak{p}}(j(C)) < 0$, then up to extension of M and isomorphism of C, we are in one of the following cases.

1. *$C : y^3 = x^4 + ax^2 + bx + 1$ with $b \equiv 0$ and $a \equiv \pm 2$ modulo $\mathfrak{p}$, and the reduction of this model is the singular curve $y^3 = (x^2 \pm 1)^2$ of geometric genus 1;*
2. *$C : y^3 = x^4 + x^2 + bx + c$ with $b \equiv c \equiv 0$ modulo $\mathfrak{p}$, and the reduction of this model is the singular curve $y^3 = (x^2 + 1)x^2$ of geometric genus 2;*
3. *$C : y^3 = x^4 + ax^2 + bx + 1$ with $b \equiv 0$ and $a \not\equiv \pm 2$ modulo $\mathfrak{p}$, and the reduction of this model is the smooth curve $y^3 = x^4 + \bar{a}x^2 + 1$ of genus 3.*

Example

Let $K = K_+(\zeta_3)$, where $K_+ = \mathbb{Q}(y)/(y^3 - y^2 - 4y - 1)$ is the totally real cubic subfield. The curve

$$C : y^3 = x^4 - 2 \cdot 7^2 \cdot 13x^2 + 2^3 \cdot 5 \cdot 13 \cdot 47x - 5^2 \cdot 13^2 \cdot 31$$

has CM by $\mathcal{O}_K$ (Koike and Weng).
We compute

$$j_1 = -\frac{7^6 \cdot 13}{2^3 \cdot 5^2 \cdot 47^2}, \quad j_2 = \frac{7^2 \cdot 13 \cdot 31}{2^5 \cdot 47^2}.$$

The prime 5 is of case 2, and the prime 47 is of case 3.
For the prime 47, we take an integer $r \equiv 15$ modulo 47 and take $k = \mathbb{Q}_{47}(\alpha)$ with $\alpha^2 = r$. Then consider the model

$$C : y^3 = x^4 - \alpha^2 \cdot 2 \cdot 7^2 \cdot 13x^2 + \alpha^3 \cdot 2^3 \cdot 5 \cdot 13 \cdot 47x - \alpha^4 \cdot 5^2 \cdot 13^2 \cdot 31,$$

which modulo 47 is

$$\overline{C} : y^3 = x^4 + \overline{19}x^2 + \overline{1}.$$

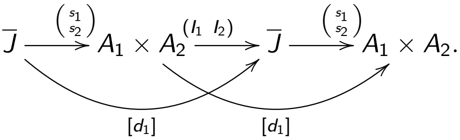
Bounding the isogeny

Theorem

Let C/M as is previous Lemma. Then there are abelian subvarieties $I_i : A_i \hookrightarrow \overline{J}$, surjective homomorphisms $s_i : \overline{J} \to A_i$ for $i \in \{1, 2\}$, endomorphisms $e_i \in \mathrm{End}(\overline{J})$ and an integer $d_1 \in \{1, 2\}$ such that the following holds for all i and $j \in \{1, 2\}$.

(a)
$$e_1 + e_2 = [d_1],\ e_i^2 = [d_1]e_i,\ e_1 e_2 = e_2 e_1 = 0,\ e_i^\dagger = e_i,$$
$$e_i = I_i s_i,\ \ s_i I_i = [d_1],\ \ \text{if } i \neq j,\ \text{then } s_i I_j = 0.$$

(b) *The abelian variety A_i has dimension i and we have a commutative diagram*



(c) *if $i \neq j$, then we have $s_i \zeta_3 I_j = 0 \in \mathrm{Hom}(A_j, A_i)$.*

Computations

Let us write $K = \mathbb{Q}(\zeta_3)K^+$ with $K^+ = \mathbb{Q}(\mu)$ with μ a totally positive element. Following the ideas in [KLLNOS16], we get

$$\iota(\mu) = \begin{pmatrix} x & a & b \\ 1 & 0 & c/n \\ 0 & 1 & d/n \end{pmatrix}, \text{ and } \iota(2\zeta_3 + 1) = \begin{pmatrix} r & 0 & 0 \\ 0 & s & t \\ 0 & u & v \end{pmatrix},$$

where $x, a, b, c, d, r, ns, nt, nu, nv \in \mathcal{R}$. These two matrices have to commute and satisfy a condition given by the Rosati involution, which implies, after some computations, that **all the entries are contained in a field**. In [KLLNOS16] we proved that this implies that $p \mid n$.

On the other hand, we get $n \leq ma^2 \operatorname{Tr} \mu^2$ and

$$\operatorname{Tr} \mu^2 = x^2 + 2a + 2(c/n) + (d/n)^2 \geq \ldots \geq x^2 + 2a.$$

Comparisons of invariants

In [KLLNOS16] we had the bound for the primes in the denominator of *Dixmier-Ohno or Shioda invariants*:

$$p < \frac{1}{8}\,\mathrm{Tr}_{K_+/\mathbb{Q}}(\mu^2)^{10}.$$

For the *Koike-Weng Invariants*:

There is **no** bounds.

For our invariants:
Main Theorem:

$$p < \mathrm{Tr}_{K_+/\mathbb{Q}}(\mu^2)^3.$$

+ we give an algorithm to compute all the solutions.

This will help to compute the exponents.

Example

Let us consider the Picard curve (computed by Koike-Weng) with CM by $K = \mathbb{Q}(\zeta_3) \cdot K^+$ with $K^+ = \mathbb{Q}(\mu)$ and $\mu^3 - \mu^2 - 14\mu - 8 = 0$:

$$y^3 = x^4 - 2 \cdot 7 \cdot 43^2 \cdot 223x^2 + 2^7 \cdot 11 \cdot 41 \cdot 43^2 \cdot 59x - 11^2 \cdot 43^3 \cdot 419 \cdot 431$$

We have

$$\Delta = 2^{30} \cdot 11^6 \cdot 47^6 \approx 2.1 \cdot 10^{25},$$

$$b = 2^7 \cdot 11 \cdot 41 \cdot 43^2 \cdot 59 \approx 3.4 \cdot 10^6.$$

Using [KLLNOS16] we get the bound $29^{10}/8 \approx 5.25 \cdot 10^{13}$ for the primes in Δ, while for the primes in b we get the bound

$$p < 29^3 = 24389.$$

Thank you!