Primes dividing the invariants of CM Picard Curves

Pınar Kılıçer
Carl von Ossietzky Universität Oldenburg

Joint work with Elisa Lorenzo García and Marco Streng

AGC^{2}T: Arithmetic, Geometry, Cryptography and Coding Theory
19 June 2017

Motivation (Class Polynomials)

Genus 1 (Elliptic Curves):

- Two elliptic curves are isomorphic over $\overline{k}$ if and only if their j-invariants are equal.
- If an elliptic curve has CM then the j-invariant is an algebraic integer.
- The class polynomial for elliptic curves with CM by an order $\mathcal{O}$ in an imaginary quadratic field K is

$$H_{\mathcal{O}}(x) = \prod_{E \text{ has CM by } \mathcal{O}} (x - j_E).$$

  It has integer coefficients.
- Two main applications:
  - constructing class fields
  - constructing elliptic curves of prescribed order

Motivation (Class Polynomials)

Genus 2:

- All genus 2 curves are hyperelliptic hence given by an equation

$$C : y^2 = x^5 + ax^4 + bx^3 + cx^2 + dx + e.$$

The isomorphism classes are given by 3 invariants j_1, j_2, j_3, called the *Igusa invariants.*
The class polynomials for genus 2 curves with CM by $\mathcal{O}$ in a non-biquadratic quartic CM field K are

$$H^1_{\mathcal{O}}(x) = \prod_{C \text{ has CM by } \mathcal{O}} (x - j_1), \quad H^2_{\mathcal{O}}(x) = \prod_{C \text{ has CM by } \mathcal{O}} (x - j_2), \quad H^3_{\mathcal{O}}(x) = \prod_{C \text{ has CM by } \mathcal{O}} (x - j_3)$$

Remark: The coefficients of $H^j_{\mathcal{O}}(x)$ are in $\mathbb{Q}$.

- Goren-Lauter (2007) gave a bound on the primes dividing the denominators.
- Lauter-Viray (2012) bounded the exponents of the primes dividing the denominators.

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 $(x, y) \mapsto (\lambda^3 x, \lambda^4 y)$. (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.)

Invariants of Picard Curves

The discriminant of $C : y^3 = x^4 + ax^2 + bx + c$ is

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

which has weight 12.

Shioda invariants:

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

Koike-Weng invariants:

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

Our invariants:

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

Main theorem

Let C be a Picard curve of genus 3 over a number field M with simple Jacobian which has CM by an order $\mathcal{O}$ of a number field K of degree 6. 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 $\operatorname{ord}_{\mathfrak{p}}(j(C)) < 0$, then $p < \operatorname{tr}_{K_+/\mathbb{Q}}(\mu^2)^3 (\leq 3^3 |\Delta(\mathcal{O}_+)|^{3/2})$.

We prove a stronger result:

- We give an algorithm that computes the set of primes dividing the denominators of $j(C)$.

Reduction of Picard Curves

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 equation 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 equation 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 equation is the smooth curve* $y^3 = x^4 + \overline{a}x^2 + 1$ *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

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

The embedding problem

Let K be a sextic CM field, and let C be a Picard curve of genus 3 with simple Jacobian J that has CM by an order $\mathcal{O}$ in K.
In [BCLLMNO15] and [KLLNOS16], it is proven that if p is a prime of bad reduction, then

$$\overline{J} \sim E^3$$

and hence there exist an embedding

$$\iota : K = \mathrm{End}^0(J) \hookrightarrow \mathrm{End}^0(\overline{J}) = \mathcal{M}_3(B_{p,\infty}),$$

such that complex conjugation on the LHS corresponds to the Rosati involution on the RHS.

However, if a prime p divides the denominators of the invariants, we do not necessarily have bad reduction.

- If p is a prime of good reduction and divides the denominator of one of the invariants, then we have $\overline{C} : y^3 = x^4 + \overline{a}x^2 + 1$ which is a 2-cover of an elliptic curve. The cover is explicitly given by

$$\begin{aligned} \phi : \overline{C} &\to E \\ (x, y) &\mapsto (y, x^2), \end{aligned}$$

- We prove that $\overline{J} \sim A_1 \times A_2$ of degree 2 where A_1 is an elliptic curve and A_2 is an abelian surface.
- Moreover, there exists an isogeny $A_2 \sim A_1^2$, hence $\overline{J} \sim A_1^3$.

So there exist an embedding

$$\iota : K = \mathrm{End}^0(J) \hookrightarrow \mathrm{End}^0(\overline{J}) = \mathcal{M}_3(B_{p,\infty}),$$

such that complex conjugation on the LHS corresponds to the Rosati involution on the RHS.

Computations

Let us write $K = \mathbb{Q}(\zeta_3)K^+$ with $K^+ = \mathbb{Q}(\mu)$ with μ a totally positive element in $\mathbb{Z} + 2\mathcal{O}$. Let n be the degree of the isogeny $\overline{J} \sim A_1^3$.
Following [KLLNOS16] (+ a few observations), we get

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

where $x, a, b, nc, nd, r, ns, nt, nu, nv \in \mathcal{R}$.

Computations

Let us write $K = \mathbb{Q}(\zeta_3)K^+$ with $K^+ = \mathbb{Q}(\mu)$ with μ a totally positive element in $\mathbb{Z} + 2\mathcal{O}$. Let n be the degree of the isogeny $\overline{J} \sim A_1^3$.
Following [KLLNOS16] (+ a few observations), we get

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

where $x, a, b, nc, nd, r, ns, nt, nu, nv \in \mathcal{R}$.

- Commutativity of μ and $2\zeta_3 + 1$,
- considering the polarization on A_1^3, and the fact that complex conjugation is the Rosati involution on $\mathrm{End}^0(A_1^3)$

we prove that all the entries are contained in $\mathbb{Q}(\zeta_3)$.

- In [KLLNOS16] we proved that this implies that $p \mid n$.

On the other hand, we also proved that all the entries of $\iota(\mu)$ and n can be written in terms of x and a.

- So bound x and a!

As $\iota(\mu^2)$ satisfies the (cubic) minimal polynomial of μ over $\mathbb{Q}$, we find

$$\begin{aligned} t_2 := \mathrm{tr}_{K_+/\mathbb{Q}}(\mu^2) &= x^2 + 2a + 2c/n + d^2/n^2 \\ &= \cdots \\ &= x^2 + 2a + \frac{\gamma}{2x} + \frac{n}{(2x)^2} + (\frac{\beta}{2x} - \frac{d}{n})^2 \\ &\geq x^2 + 2a. \end{aligned}$$

So, we get

$$|x| \leq \sqrt{t_2} \quad \text{and}$$
$$0 < a \leq \frac{1}{2}(t_2 - x^2).$$

A simple calculation $\Rightarrow$ $n \leq t_2^3$.
We have shown $p \mid n$, hence we get $p \leq t_2^3$.

We have

$$\iota : \mathbb{Z} + 2\mathcal{O} \to \mathrm{M}_{3\times 3}(\mathbb{Q}[\zeta_3])$$
$$\eta \mapsto \begin{pmatrix} x & a & b \\ 1 & 0 & c/n \\ 0 & 1 & d/n \end{pmatrix}.$$

Algorithm:

1. Take any real $\eta \in \mathbb{Z} + 2\mathcal{O}$ and list all (a, x) satisfying
$$|x| \leq \sqrt{t_2} \quad \text{and}$$
$$0 < a \leq \frac{1}{2}(t_2 - x^2),$$
2. For each compute $n(\eta, x, a)$.
3. Let N_η be the least common multiple of the numbers $n(\eta, a, x)$.
4. List primes p dividing N_η.

Comparisons of invariants

Shioda invariants:
[KLLNOS16]:

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

Koike-Weng Invariants:

No bounds.

Our invariants:
Main Theorem: $p < \operatorname{tr}_{K_+/\mathbb{Q}}(\mu^2)^3$

+ we give an algorithm to compute all the solutions.

How can we bound the exponents of the primes?

How can we bound the exponents of the primes?

- An idea: For a prime p appearing in the denominator of the invariants j_1, j_2 of Picard curves, count the number of solutions to the embedding problem.
  - i.e., count the pairs (a, x) satisfying

$$|x| \leq \sqrt{t_2} \quad \text{and}$$
$$0 < a \leq \frac{1}{2}(t_2 - x^2),$$

    such that $p | n(x, a)$.

  The number of solutions bounds the exponent of p.