On primes dividing the denominators of the invariants of genus-3 CM curves

Pınar Kılıçer

The 21st Workshop on Elliptic Curve Cryptography
13 November 2017

Elliptic curves.

Let E be an elliptic curve over number field M.

- The endomorphism ring $\mathrm{End}_{\overline{M}}(E)$ is either
  - $\mathbb{Z}$ or
  - an *order* $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Z}_{<0}$.

  In the second case we say that E has **complex multiplication** (CM) by $\mathcal{O}$.

Motivation (Class polynomials)

Elliptic curves.

Let E be an elliptic curve over number field M.

- The endomorphism ring $\mathrm{End}_{\overline{M}}(E)$ is either
  - $\mathbb{Z}$ or
  - an *order* $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Z}_{<0}$.

  In the second case we say that E has **complex multiplication** (CM) by $\mathcal{O}$.
- CM $\Rightarrow$ everywhere potential good reduction $\iff$ $j_E \in \overline{\mathbb{Z}}$.

Elliptic curves.

Let E be an elliptic curve over number field M.

- The endomorphism ring $\mathrm{End}_{\overline{M}}(E)$ is either
  - $\mathbb{Z}$ or
  - an *order* $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Z}_{<0}$.

  In the second case we say that E has **complex multiplication** (CM) by $\mathcal{O}$.
- CM $\Rightarrow$ everywhere potential good reduction $\iff$ $j_E \in \overline{\mathbb{Z}}$.
- Then the class polynomial

$$H_{\mathcal{O}}(x) = \prod_{\mathrm{End}(E) \cong \mathcal{O}} (x - j_E)$$

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

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 analogue of j-invariant is the *Igusa invariants*, given by an invariant triplet (j_1, j_2, j_3).
- The denominators of Igusa invariants correspond to the curve having bad reduction.

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 analogue of j-invariant is the *Igusa invariants*, given by an invariant triplet (j_1, j_2, j_3).
- The denominators of Igusa invariants correspond to the curve having bad reduction.

CM.

- A curve C/k of genus g has **CM** if there is an embedding $\mathcal{O} \hookrightarrow \mathrm{End}_{\overline{k}}(\mathrm{Jac}(C))$, where $\mathcal{O}$ is an order in a CM field of degree $2g$ over $\mathbb{Q}$.
- Let $\mathcal{O}$ be an order in a quartic CM field. Then the class polynomials

$$H^i_{\mathcal{O}}(x) = \prod_{C \text{ has CM by } \mathcal{O}} (x - j_i) \quad \text{for } i \in \{1, 2, 3\}.$$

have rational coefficients.

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

Theorem [GL07].
Let C be a genus 2 curve over a number field M. Suppose that the Jacobian J of C is simple and has CM by $\mathcal{O}_K$, where $K = \mathbb{Q}(\sqrt{d})(\sqrt{\mu})$ where μ totally negative in $\mathbb{Z}[\sqrt{d}]$, and $d \in \mathbb{Z}_{>0}$.

Let $\mathfrak{p}|p$ be a prime of stable bad reduction for C, and let us assume that it is a good reduction for J. Then we have $p \leq 16d^2 \operatorname{Tr}_{K/\mathbb{Q}}(\mu)^2$.

Corollary. With the notation above, if $\operatorname{ord}_{\mathfrak{p}}(j_i(C)) < 0$, then $p \leq 16d^2 \operatorname{Tr}_{K/\mathbb{Q}}(\mu)^2$.

Proof of Theorem [GL07]

Let $\overline{J} = J \pmod{\mathfrak{p}}$. Then we have $\overline{J} \cong E_1 \times E_2$ as p.p.a.v. where E_1 and E_2 are isogenous and supersingular hence

$$\iota : \mathcal{O}_K \hookrightarrow \mathrm{End}(J) \hookrightarrow \mathrm{End}(\overline{J}) \otimes \mathbb{Q} \cong \mathrm{End}(E_1 \times E_2) \otimes \mathbb{Q} \cong M_2(B_{p,\infty}).$$

Lemma [GL07]. In the quaternion algebra $B_{p,\infty}$, if for any $x, y \in B_{p,\infty}$, we have $\mathrm{N}(x)\,\mathrm{N}(y) \leq p/4$ then $xy = yx$.

- Commutativity of $\sqrt{d}$ and $\sqrt{\mu}$ and the fact that Rosati involution induces complex conjugation on $\mathcal{O}_K$ (gives $\iota(\overline{\eta}) = \iota(\eta)^\vee$) gives that the entries $\iota(\sqrt{d})$ and $\iota(\sqrt{\mu})$ have norm less than $\sqrt{p}/2$ if $p > 16d^2 \operatorname{Tr}_{K/\mathbb{Q}}(\mu)^2$.

$\Longrightarrow$ $\iota(K) \subset M_2(K_1)$, where K_1 is an imaginary quadratic field. This implies that $K_1 \subset K$. Contradicts the assumption on K. Hence $p \leq 16d^2 \operatorname{Tr}_{K/\mathbb{Q}}(\mu)^2$.

More complicated:

1. Not all genus-3 curves are hyperelliptic anymore. A genus-3 curve is either
   - a smooth plane quartic (Dixmier-Ohno invariants)
   - a hyperelliptic (Shioda invariants).
2. If a genus-3 curve C over a number field M has a stable bad reduction modulo prime ideal $\mathfrak{p} \subset \mathcal{O}_M$ then

$$\overline{J} \cong E_1 \times A \quad \text{or} \quad \overline{J} \cong E_1 \times E_2 \times E_3$$

   as p.p.a.v., where E_1, E_2, E_3 are elliptic curves and A is the Jacobian of a genus-2 curve.
3. Not all CM types in sextic CM fields are primitive.

Theorem [KLLNOS16].

Let C be a curve of genus 3 defined over a number field M. Suppose that the Jacobian J is simple and has CM by an order $\mathcal{O}$ inside a sextic CM field $K = \mathbb{Q}(\mu)$ with $\mu \in \mathcal{O}$.

Let $\mathfrak{p}|p$ be a prime of stable bad reduction for C, and let us assume that it is a good reduction for J. Then we have

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

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

A *hyperelliptic curve* of genus 3 is smooth projective curve given by an equation of the form

$$C : y^2 = f(x) \quad \text{with } \deg(f) = 7, \text{ or } 8.$$

- Shioda gives a set of absolute invariants $j = u/\Delta^l$, where Δ is the discriminant of $f(x)$.

A *Picard curve* of genus 3 is a smooth projective curve given by an equation of the form

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

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

- There is a set of absolute invariants $j = u/\Delta^l$, where Δ is the discriminant of $x^4 + ax^2 + bx + c$.

Corollary.

Let C/M be a hyperelliptic or Picard curve of genus 3 over a number field M whose Jacobian is simple. Suppose that C has CM by an order $\mathcal{O}$ inside a sextic CM field $K = \mathbb{Q}(\mu)$ with $\mu \in \mathcal{O}$.

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

Proof of Theorem [KLLNOS16]

Suppose that C has bad reduction modulo prime ideal $\mathfrak{p} \subset \mathcal{O}_M$ such that the Jacobian J has good reduction modulo $\mathfrak{p}$.

Bouw-Cooley-Lauter-Lorenzo-Manes-Newton-Ozman proved:

$$J \cong E \times A,$$

as principally polarized abelian varieties, where E is an elliptic curve and A is a principally polarized abelian surface such that there is an isogeny $s : E \times E \to A$.
Once we fix an isogeny $s : E \times E \to A$, there are natural embeddings

$$\iota : \mathcal{O} \hookrightarrow \mathrm{End}(J) \hookrightarrow \mathrm{End}(\overline{J}) = \mathrm{End}(E \times A) \hookrightarrow \mathrm{End}(E^3) \otimes \mathbb{Q} \cong M_3(\mathcal{B}),$$

where $\mathrm{End}(E) = \mathcal{R}$ and $\mathcal{B} = \mathcal{R} \otimes \mathbb{Q}$.
As in $g = 2$ case, we will show that when p is too large this embedding does not exist, then $\mathfrak{p} | p$ cannot be a prime of bad reduction.

Decomposition

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

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

where we have $x \in \mathcal{R}$, $y \in \mathrm{Hom}(A, E)$, $z \in \mathrm{Hom}(E, A)$ and $w \in \mathrm{End}(A)$.

- We would like to have $\mathcal{O} \hookrightarrow M_3(\mathcal{B})$.
- We need a further isogeny $E^3 \to E \times A$.
- To get the bound, we need the 'right' isogeny.

Let

$$F = \begin{pmatrix} 1 & 0 & 0 \\ \boxed{0} & \boxed{z} & \boxed{wz} \end{pmatrix} : E^3 \longrightarrow E \times A$$

$$(P, Q, R) \longmapsto (P, z(P) + wz(Q)).$$

So we obtain a further embedding

$$\begin{aligned} \iota_1 : \mathrm{End}(E \times A) &\longrightarrow \mathrm{End}(E^3) \otimes \mathbb{Q} \cong M_3(\mathcal{B}) \\ f &\longmapsto F^{-1} f F. \end{aligned}$$

Let $\iota = \iota_1 \circ \iota_0 : \mathcal{O} \hookrightarrow M_3(\mathcal{B})$. Let $n \in \mathbb{Z}_{>0}$ be such that the kernel of the isogeny $F : E^3 \to E \times A$ is killed by n.
We get

$$\iota(\mu) = F^{-1} \left(\begin{array}{c|c} x & y \\ \hline z & w \end{array} \right) F = \begin{pmatrix} x & a & b \\ 1 & 0 & c \\ 0 & 1 & d \end{pmatrix},$$

where $x, a, b, nc, nd \in \mathcal{R}$.

- We now want to show that if $p > \frac{1}{8}B^{10}$, then $\iota(K) \subset M_3(K_1)$, where K_1 is a quadratic field over $\mathbb{Q}$.
- If E is ordinary then this holds. Suppose that E is supersingular.

Explicit computations using the polarization gives

- $c = \frac{n+bd}{a}$;
- $\mathrm{N}(x) < B$; $\mathrm{N}(a) < B^2/4$; $\mathrm{N}(b) < B^3/3$; $\mathrm{N}(d) < B^7/8$.

Hence the product of any pair of distinct elements of $\{x, a, b, nc, nd\}$ has norm less than $p/4$. By Lemma [GL07], they all commute.
$\implies \iota(K) \subset M_3(K_1) \implies K_1 \subset K$.

- This finishes the proof of Theorem [KLLNOS16] in the case where K does not contain an imaginary quadratic subfield.

Suppose that K contains $K_1 = \mathbb{Q}(\sqrt{-\delta})$ and $p \nmid n$ (recall that n is the annihilator of $\ker(F)$ where $F : E^3 \to E \times A$). If the CM type of K is primitive then $\iota(\sqrt{-\delta})$ has distinct eigenvalues. In other words, there is an invertible matrix $P \in M_3(\mathbb{Q}(\sqrt{-\delta}))$ such that

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

Suppose that $p > \frac{1}{8}B^{10}$. Then $\iota(\mu)$ has coefficients in $\mathbb{Q}(\sqrt{-\delta})$. Moreover, since μ commutes with $\sqrt{-\delta}$, we have

$$P\iota(\mu)P^{-1} = \begin{pmatrix} * & * & 0 \\ * & * & 0 \\ 0 & 0 & * \end{pmatrix}.$$

- The bottom right entry of $P\iota(\mu)P^{-1}$ is a root of the minimal (degree 6 irreducible) polynomial of μ over $\mathbb{Q}$. This gives a contradiction because the entries of the matrix $P\iota(\mu)P^{-1}$ lie in the quadratic field $\mathbb{Q}(\sqrt{-\delta})$.

This completes the proof of Theorem [KLLNOS16].

CM Picard curves

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

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

- 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

Discriminant-normalized 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:

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

Theorem [KLS17].
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 $\mathrm{ord}_{\mathfrak{p}}(j(C)) < 0$, then $p < \mathrm{Tr}_{K_+/\mathbb{Q}}(\mu^2)^3$.

We prove a stronger result:

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

Reduction of Picard curves

- If a prime $\mathfrak{p}$ divides the denominator of the invariant j_1 or j_2, we do not necessarily have bad reduction.

Let $C : y^3 = x^4 + ax^2 + bx + c$ over local field.
Extending the base field, can scale such that a, b, c are all integral and $a = 1$, $b = 1$, or $c = 1$.
If e.g., $\mathrm{ord}_{\mathfrak{p}}(j_1) < 0$, then we are in these cases

1. $C : y^3 = x^4 + ax^2 + bx + 1$ with $b \equiv 0$ modulo $\mathfrak{p}$, or
2. $C : y^3 = x^4 + x^2 + bx + c$ with $b \equiv c \equiv 0$ modulo $\mathfrak{p}$.

- This talk: restrict to case 1 with $a \not\equiv \pm 2$.

This is the case of smooth reduction.
The other cases have very explicit bad reduction and are very similar with minor technical changes.

- If $\mathfrak{p}$ 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 obtain an isogeny $F_0 : E \times A \to \overline{J}$ with kernel killed by [2], where E is an elliptic curve and A is a principally polarized abelian surface.
- So we have $\iota_0 : \mathcal{O} \hookrightarrow \mathrm{End}(E \times A) \otimes \mathbb{Q}$

$$\alpha \mapsto F_0^{-1} \alpha F_0$$

As in the previous case by fixing the isogeny $F : E^3 \to E \times A$, we obtain an embedding

$$\iota : \mathcal{O} \hookrightarrow \mathrm{End}(J) \hookrightarrow \mathrm{End}(\overline{J}) \otimes \mathbb{Q} \hookrightarrow \mathrm{End}(E^3) \otimes \mathbb{Q} = \mathcal{M}_3(\mathcal{B}).$$

Let $n \in \mathbb{Z}_{>0}$ such that $[n]\ker(F) = 0$. Then

$$\iota(\mu) = \begin{pmatrix} x & a & b \\ 1 & 0 & c \\ 0 & 1 & d \end{pmatrix}, \text{ and } \iota(\sqrt{-3}) = \begin{pmatrix} \sqrt{-3} & 0 & 0 \\ 0 & s & t \\ 0 & u & v \end{pmatrix},$$

where $x, a, b, nc, nd, ns, nt, nu, nv \in \mathcal{R} := \mathrm{End}(E)$.

- By the commutativity of μ and $\sqrt{-3}$, we get

$$\iota(\sqrt{-3}) = \begin{pmatrix} \sqrt{-3} & 0 & 0 \\ 0 & \sqrt{-3} & 0 \\ 0 & 0 & \sqrt{-3} \end{pmatrix}.$$

  – Recall that this implies $p|n$.

It now suffices to bound n.

Calculations

Explicit computations using the polarization, the minimal polynomial of μ give:

- $x \in \mathbb{Z}$, $a \in \mathbb{Z}_{>0}$,
- $t_2 := \mathrm{Tr}_{K_+/\mathbb{Q}}(\mu^2) \geq \ x^2 + 2a$,
- $n = n(\mu, x, a) \leq t_2^3$.

  - This bound depends on the choice of the isogeny F.

Algorithm:

1. Take one real $\eta \in \mathcal{O} \cap K_+$ such that $K = K_+(\eta)$ and list all (a, x) satisfying $t_2 \geq x^2 + 2a$.
2. Let N_η be the least common multiple of the numbers $n(\eta, a, x)$.
3. List primes p dividing N_η.

Comparisons of invariants

Discriminant-normalized invariants:
[KLLNOS16]:

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

Koike-Weng Invariants:

No bounds.

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

+ we give an algorithm to compute all the solutions.

An example

The Picard curve (computed by Koike-Weng and Lario-Somoza)

$$y^3 = x^4 - 73 \cdot 7 \cdot 2 \cdot 31x^2 + 211 \cdot 47 \cdot 31x - 7 \cdot 312 \cdot 11593$$

has CM by $\mathcal{O}_K$, where $K = K_+(\zeta_3)$ and $K_+ = \mathbb{Q}[x]/(x^3 + x^2 - 10x - 8)$. Its invariants are given by

- Discriminant-normalized:

$$i_1 = \frac{(7^3 \cdot 31 \cdot 73^3)^2}{(2^3 \cdot 23)^6}, \quad i_2 = \frac{-2 \cdot 7^3 \cdot 31 \cdot 47^2 \cdot 73^3}{23^6}, \quad i_3 = \frac{-7^5 \cdot 31^2 \cdot 73^4 \cdot 11593}{(2^{10} \cdot 23^3)^2}$$

- $\frac{1}{8}B^{10} \approx 1.2 \cdot 10^{17}$
- Koike-Weng: $j_1' = \frac{-2^{19} \cdot 47^2}{7^3 \cdot 31 \cdot 73^3}$, $j_2' = \frac{-11593}{2^2 \cdot 7 \cdot 73^2}$
- Our invariants: $j_1 = \frac{-7^3 \cdot 31 \cdot 73^3}{2^{19} \cdot 47^2}$, $j_2 = \frac{7^2 \cdot 31 \cdot 73 \cdot 11593}{2^{21} \cdot 47^2}$