PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 4, *Number* 1, *March* 2019, *pages* 49-59

Elisa Lorenzo García

Primes of bad reduction of CM curves of genus 3

Written by Guido Maria Lido

1 Introduction

The aim of this talk is to present some recent results bounding the primes of bad reduction for a CM curve of genus 3. Before looking at this problem we will look at the analogue for curves of genus 1 and curves of genus 2 in order to give motivation in a more familiar context.

2 Hilbert class polynomial and good reduction of CM elliptic curves

If we fix an algebraically closed field k, all elliptic curves over k up to isomorphism can be parametrized with a single invariant called j-invariant. For example if the characteristic of k is different from 2 or 3 every elliptic curve E over k has a Weierstrass model

$$y^2 = x^3 + Ax + B$$

for certain $A, B \in k$ such that $4A^3 + 27B^3 \neq 0$ and we can write the j-invariant of E as

$$j(E) = -1728\frac{(4A)^3}{\Delta(E)} = -1728\frac{(4A)^3}{16(4A^3 + 27B^2)}.$$

If we consider the endomorphism ring of an elliptic curve E we know that there are three kinds of possibilities:

1. $\mathrm{End}(E) \cong \mathbb{Z}$, if the only endomorphisms are of the form $[n] : P \to P + \cdots + P$;

2. End(E) is isomorphic to an order $\mathcal{O}$ in an quadratic imaginary number field; every such order $\mathcal{O}$ is of the form $\mathbb{Z}[\frac{\sqrt{D}+D}{2}]$ for some negative integer D not congruent to 3 (mod 4);

3. $\mathrm{End}(E)$ is an order inside a quaternion algebra $\mathcal{B}$; this can only happen in positive characteristic and if $p = char(k)$ then $\mathcal{B}$ is the only quaternion algebra over $\mathbb{Q}$ such that $\mathcal{B} \otimes \mathbb{Q}_v$ is isomorphic to $\mathrm{Mat}_{2\times 2}(\mathbb{Q}_v)$ for all rational places in v except from ∞ and p; We will denote it as $\mathcal{B}_{p,\infty}$.

In characteristic zero there are two kinds of elliptic curves: ordinary elliptic curves (case 1) and elliptic curves with *complex multiplication* (case 2). Let us now recall some "classical" facts about complex multiplication whose proof can be found in the second chapter of [10]. Since any elliptic curve with CM defined over a field k of characteristic zero is isomorphic to an elliptic curve defined over the algebraic numbers, we only need to look at curves defined over $\overline{\mathbb{Q}}$.

Proposition 1 *Let $\mathcal{O}$ be an order in a quadratic imaginary field. Then:*

1. *there exists an elliptic curve E over $\overline{\mathbb{Q}}$ such that* $\mathrm{End}(E) = \mathcal{O}$*;*

2. *if E over $\overline{\mathbb{Q}}$ is any elliptic curve such that* $\mathrm{End}(E) = \mathcal{O}$*, then the set*

$$\left\{(E)^\sigma : \ \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\right\}$$

is equal to the set of all elliptic curves E' over $\overline{\mathbb{Q}}$ such that $\mathrm{End}(E') = \mathcal{O}$*, up to isomorphism.*

3. *if E is an elliptic curve with complex multiplication defined over a number field L, then E has potential good reduction over any prime $\mathcal{P} \subset \mathcal{O}_L$; in particular $j(E)$ is an algebraic integer.*

The second point of proposition 1 implies that up to isomorphism there are only finitely many elliptic curves over $\overline{\mathbb{Q}}$ with ring of endomorphism a fixed order $\mathcal{O}$, thus we can give the following definition.

Definition 1 *Given an order $\mathcal{O}$ inside a quadratic imaginary field we define the* modular polynomial relative to $\mathcal{O}$ *to be*

$$H_{\mathcal{O}}(X) = \prod_{E:\ \mathrm{End}(E)=\mathcal{O}} \Big(X - j(E)\Big)$$

where the product is taken over the set of elliptic curves E such that $\mathrm{End}(E) = \mathcal{O}$*, up to isomorphism.*

A motivation for studying and computing modular polynomials is given by cryptography, since they can be used to construct elliptic curves over finite fields with a given number of rational points. Proposition 1 implies that $H_{\mathcal{O}}(X)$ is an irreducible polynomial with coefficients in $\mathbb{Z}$. Let us see how to exploit this, together with some tools from complex analysis, to compute modular polynomials.

Every elliptic curve E over $\mathbb{C}$ is isomorphic as a complex manifold to a complex torus of the form $\mathbb{C}/\langle 1, \tau\rangle$ for some τ in

$$\mathcal{H} = \{\tau \in \mathbb{C} :\ \ \mathrm{Im}(\tau) > 0\}.$$

Moreover we can write the j-invariant of E as the value in τ of an analytic function $J : \mathcal{H} \to \mathbb{C}$ (not depending on τ), i.e.

$$j(E) = J(\tau) = e^{-2\pi i\tau} + 744 + 196884e^{2\pi i\tau} + 21493760e^{4\pi i\tau} + \dots$$

Since the function J is effectively computable, in order to compute the modular polynomial relative to an order $\mathcal{O}$ we can do the following

1. Compute $\tau_1, \ldots, \tau_n \in \mathcal{H}$ with the following property: every elliptic curve E over $\mathbb{C}$ such that $\mathrm{End}(E) = \mathcal{O}$ is analytically isomorphic to $\mathbb{C}/\langle 1, \tau_i \rangle$ for a unique $i \in \{1, \ldots n\}$;

2. Compute an approximation $\tilde{j}_i$ of $J(\tau_i)$ up to sufficiently good precision (it is enough $2^{-n-1} \max_i\{|j(\tau_i)|\} \leq 2^{-n-1}$);

3. Compute the polynomial

$$\tilde{H}(X) = \prod_{i=1}^{n}(X - \tilde{j}_i)$$

and approximate it with the polynomial $H \in \mathbb{Z}[X]$ whose coefficients are as close as possible to the polynomial $\tilde{H}$.

The polynomial H computed in the third step is equal to the modular polynomial $H_{\mathcal{O}}$. Indeed if we call $\tilde{c}_k$'s and c_k's the coefficients respectively of $\tilde{H}(X)$ and $H_{\mathcal{O}}(X)$, then $|c_k - \tilde{c}_k| < \frac{1}{2}$ and since the c_k's are integral, we conclude that

$$H = H_{\mathcal{O}}$$

.

3 Igusa class polynomial and bad reduction of genus 2 CM curves

Let us now consider algebraic curves of genus 2 over a field k of characteristic different from 2 or 3. Any such curve C has an affine model of the form $y^2 = f(x)$ where $f \in k[x]$ is a separable polynomial of degree 6.

For any polynomial $f \in k[x]$ of degree 6 we denote $\alpha_1, \ldots, \alpha_6 \in \overline{k}$ the roots of f and we define the following quantities:

$$\Delta = \prod_{1 \leq i < j \leq 6} (\alpha_i - \alpha_j)^2$$

$$I_1 = \sum_{sym} (\alpha_1 - \alpha_2)^2(\alpha_3 - \alpha_4)^2(\alpha_5 - \alpha_6)^2$$

$$I_2 = \sum_{sym} (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2(\alpha_4 - \alpha_5)^2(\alpha_4 - \alpha_6)^2(\alpha_5 - \alpha_6)^2$$

$$I_3 = \sum_{sym} \frac{\Delta}{(\alpha_1 - \alpha_5)^2(\alpha_1 - \alpha_6)^2(\alpha_2 - \alpha_4)^2(\alpha_2 - \alpha_6)^2(\alpha_3 - \alpha_4)^2(\alpha_3 - \alpha_5)^2}$$

$$I_3' = 5I_1I_2 - 2^5 3^3 I_3$$

where "$\sum_{sym}$" means that we sum over all the permutations of $\alpha_1, \ldots, \alpha_6$. Given a curve $C : y^2 = f(x)$ the Igusa invariants of C are defined in [4] as

$$j_1 = \frac{I_2 I_3'}{2^{10} \cdot 3^5 \cdot 5 \cdot \Delta}, \quad j_2 = \frac{I_1 I_2^2}{2^8 \cdot 3^5 \cdot \Delta} \quad j_3 = \frac{I_2^5}{2^{15} \cdot 3^{10} \cdot \Delta^2}.$$

Analogously to what happens for elliptic curves and the j-invariant, two genus 2 curves $C_1 : y^2 = f_1(x)$ and $C_2 : y^2 = f_2(x)$ are isomorphic over $\overline{k}$ if and only if they have the same Igusa invariants. Moreover if k happens to be a number field and $\mathfrak{p}$ is a prime of k, then a curve C has potential good reduction modulo $\mathfrak{p}$ if and only if all Igusa invariants of C are $\mathfrak{p}$-integral.

Another analogy with the j-invariant of elliptic curves is that we can compute the Igusa invariants of a genus 2 curves in terms of a holomorphic function on a complex moduli space. Indeed if we define

$$\mathcal{H}_2 = \left\{ \tau \in M^{2\times 2}(\mathbb{C}) : \quad \tau = \tau^t, \ \ \mathrm{Im}(\tau) \text{ is positive definite} \right\}$$

then for each genus 2 curve C over the complex numbers, there is a $\tau = \left(\tau_1 | \tau_2\right) \in \mathcal{H}_2$ such that $\mathrm{Jac}(C) \cong \mathbb{C}^2 / \langle e_1, e_2, \tau_1, \tau_2 \rangle$ as principally polarized Abelian variety. Moreover there are holomorphic functions $J_1, J_2, J_3 : \mathcal{H}_2 \to \mathbb{C}$ such that $j_i(C) = J_i(\tau)$.

As in the case of elliptic curves we can define a class polynomial for genus 2 curves. Let us give some preliminary definition.

Definition 2 *A number field K is a* CM-field *if it is a totally imaginary quadratic extension of a totally real field K^+*

Definition 3 *A curve C of genus g defined over $\overline{\mathbb{Q}}$ is a* CM curve *if there exists a CM-field K of degree $2g$ and an order $\mathcal{O} \subset K$ such that*

$$\mathcal{O} \subset \mathrm{End}\Big(\mathrm{Jac}(C)\Big).$$

In this case we say that C has complex multiplication by $\mathcal{O}$.

Given a fixed order $\mathcal{O}$ inside a quartic CM-field K there are only finitely many curves of genus 2 over $\overline{\mathbb{Q}}$ having complex multiplication by $\mathcal{O}$ up to isomorphism. We can then define three *Class polynomials* $H^1_{\mathcal{O}}, H^2_{\mathcal{O}}, H^3_{\mathcal{O}}$ with the following formulas

$$H^i_{\mathcal{O}}(X) = \prod_{\substack{\mathrm{End}\left(\mathrm{Jac}(C)\right) \cong \mathcal{O} \\ g(C)=2}} \Big(X - j_i(C)\Big).$$

It is easy to show that Class polynomials $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant, i.e. that they have coefficients in $\mathbb{Q}$: indeed if C is a genus 2 curve with CM by $\mathcal{O}$, then for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ the curve C^σ is also a genus 2 curve with CM by $\mathcal{O}$; thus if j_i is a root of $H^i_{\mathcal{O}}$ then each Galois-conjugate of j_i is also a root of $H^i_{\mathcal{O}}$.

Unfortunately it is not true that a CM curve C has potential good reduction everywhere, i.e. that the invariants $j_i(C)$ are algebraic integers. Indeed the Class polynomials $H^i_{\mathcal{O}}$ may have non-integral coefficient. Anyway if we had a bound B for the denominators of the coefficients of $H^i_{\mathcal{O}}$ we could compute $H^i_{\mathcal{O}}$ with an algorithm similar to the one for elliptic curves, since all the other ingredients are still available. Such bounds have been given by Goren, Lauter and Viray, by bounding the denominators of the Igusa invariants of the curves involved. Indeed in [2] it is proved the following

Theorem 1 *Let C be a genus 2 curve with complex multiplication by an order $\mathcal{O}$ inside a a quartic CM-field K not containing any quadratic imaginary subfield. Then we can write*

$$K = \mathbb{Q}(\sqrt{d})(\sqrt{r})$$

for some $d \in \mathbb{Z}$ and some $r \in \mathbb{Q}(\sqrt{d}) \cap \mathcal{O}$ both totally real. If C has geometrical bad reduction for a prime lying over p, then

$$p < 16d^2(\mathrm{Tr}(r))^2.$$

To finish the work one also needs to bound the valuation of the Igusa invariants in the primes of bad reduction. This has been done for example in [3] achieving the following bounds for the denominators of the Class polynomials relative to some maximal orders $\mathcal{O}_K$.

Theorem 2 *Let K be a quartic CM-field not containing any quadratic imaginary subfield and let p ne any prime. In particular we can write*

$$K = \mathbb{Q}(\sqrt{d})(\sqrt{r})$$

for some $d \in \mathbb{Z}$ and some $r \in \mathbb{Q}(\sqrt{d}) \cap \mathcal{O}$ both totally real. Then the valuations at p of the coefficients of $H^1_{\mathcal{O}_K}, H^2_{\mathcal{O}_K}, H_{\mathcal{O}_K}$ are at least

$$-16 \deg H^1_{\mathcal{O}_K} \left(4 \log_p \left(\frac{d\,\mathrm{Tr}(r)^2}{2}\right) + 1\right)$$

Instead of explaining the strategy used to prove the last two theorems we will now look at analogous results for genus 3 curves and at the ideas used to prove those.

4 Bad reduction of genus 3 CM curves and the embedding problem

The definition of CM curves in genus 3 is just a particular case of definition 3, but there are some substantial differences with the case of

genus 2 curves, indicating that finding such bounds is a necessary but not sufficient step, if we want to compute class polynomials in genus 3. One of the missing ingredients is the analogue of Igusa invariants, since we do not know good coordinates for the moduli space of curves of genus 3. Indeed we can distinguish between two kinds of genus 3 curves, each one with its own invariants:

- hyperelliptic genus 3 curves: in characteristic different from 2 they all have a model $y^2 = f(x)$ for a separable polynomial f of degree 8; Shioda defined invariants in [9] for this kind of curves.
- non-hyperelliptic genus 3 curves: they are all isomorphic to a smooth projective plane quartic; invariants for this family of curves where defined by Dixmier and Ohno in [1] and [8].

Another difference is that in general integrality of the invariants of a genus 3 curve is not equivalent to potential good reduction of the curve. This is true for hyperelliptic curves, but not in general for smooth plane quartics. For example it may happen that C is a CM non-hyperelliptic curve of genus 3 that has potential good reduction of C modulo some prime $\mathfrak{p}$ but that the reduction of the curve is hyperelliptic; in this case one of the invariants is not $\mathfrak{p}$-integral.

In the rest of this section we will see some partial results that give bounds on the bad reduction of CM curves of genus 3. To state precisely our results we need to define a notion of "primitivity".

Definition 4 *Let ρ be usual conjugation on $\mathbb{C}$. A* CM-type *is a pair (K, ϕ) such that K is a CM-field and ϕ is a set of embeddings $K \hookrightarrow \mathbb{C}$ such that*

$$\mathrm{Hom}(K, \mathbb{C}) = \phi \cup \rho\phi, \quad \textit{and} \quad \phi \cap \rho\phi = \emptyset$$

Definition 5 *A CM-type (K, ϕ) is* primitive *if there is no proper subfield $E \subset K$ such that $(E, \phi|_E)$ is a CM-type.*

In [7] it is explained how one can define the CM-type associated to a CM Abelian variety $A/\mathbb{C}$. We say that a CM curve has primitive

CM-type if the CM-type associated to its Jacobian is primitive.

Let us now return to our main problem. Let C be a semistable CM curve of genus 3 with Jacobian J and let p be a prime of bad reduction for p. One of the ideas in [2] was to look at the reduction of J modulo p: by a theorem of Serre and Tate it is still an Abelian variety and the hypothesis on p implies that it is isogenous to the third power of a supersingular elliptic curve. If we reduce the endomorphisms of J modulo p, we step into the following, purely algebraic problem.

Problem 1 (Embedding problem for $\mathcal{O}$ and p) *Given an order $\mathcal{O}$ inside a CM sextic field and a prime p does there exist an embedding*

$$\iota : \mathcal{O} \hookrightarrow \mathrm{Mat}_{3\times 3}(\mathcal{B}_{p,\infty}) \qquad ?$$

The precise relation between the embedding problem and our original problem is in the following proposition proved in [5].

Proposition 2 *Let C be a curve a genus 3 with CM by an order $\mathcal{O}$ and primitive CM type. Suppose that C has geometric bad reduction over a prime lying over p. Then we can find $\alpha, \gamma \in \mathbb{Z}$, $\beta \in \mathcal{B}_{p,\infty}$ and an embedding $\iota : \mathcal{O} \hookrightarrow \mathrm{Mat}_{3\times 3}(\mathcal{B}_{p,\infty})$ such that*

$$\alpha\gamma \neq \beta\beta^{\vee} \quad \text{and}$$

$$\iota(\overline{\eta}) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha & \beta \\ 0 & \beta^{\vee} & \gamma \end{pmatrix}^{-1} \cdot \left(\iota(\eta)^{\vee}\right)^{t} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha & \beta \\ 0 & \beta^{\vee} & \gamma \end{pmatrix}$$

where $^{\vee} : \mathcal{B}_{p,\infty} \to \mathcal{B}_{p,\infty}$ is the canonical involution.

In [5] it is proven that the (complicated version of the) embedding problem has no solution for large p, implying the following

Theorem 3 *with CM by an order $\mathcal{O}$ and primitive CM type. Suppose that C has bas reduction over a prime lying over p. Then for every $\mu \in \mathcal{O}$ with μ^2 totally real and $K = Q(\mu)$, we have*

$$p < \frac{1}{2^{13}}\left(\mathrm{Tr}_{K/\mathbb{Q}}(\mu)\right)^{10}.$$

Let us now turn to the problem of bounding from below the valuation $v_{\mathfrak{p}}(j)$ when j is the invariant of a curve having CM by a particular order $\mathcal{O}$ and $\mathfrak{p}$ is a prime. For curves of genus 2 this was obtained in [6] by relating this valuation to the number of solutions of the embedding problem. At the moment there are no similar formulas for genus 3 curves, while bounding the number of possible embeddings is the aim of an ongoing project by Garcia, Ionica, Kiliçer, Lauter, Massierer, Mânzăţenau and Vincent. One of the results of this work is a bound on the number of the embeddings and an algorithm that computes all of them. This has been achieved in a very explicit way: if we fix $\mu \in \mathcal{O}$ that generates the sextic CM field and that satisfies a relation $\mu^6 + A\mu^4 + B\mu^2 + C = 0$ over the integers, then finding all the embeddings is equivalent to solving the following system of equations in $\alpha, \beta, \gamma, d, x \in \mathcal{B}_{p,\infty}$ and $n \in \mathbb{Z}_{>0}$:

$$
\begin{aligned}
A =& \operatorname{N}(x) + \operatorname{Tr}(\alpha) + \operatorname{Tr}(\gamma)/\alpha + \operatorname{Tr}(\beta d)/(\alpha n) + \operatorname{N}(d/n),\\
B =& \alpha^2 + 2n/\alpha + 2n\operatorname{N}(x)/\alpha^2 + 2\alpha\operatorname{N}(d/n) + 2\operatorname{N}(b)/\alpha + \operatorname{Tr}(x\beta) +\\
& 2\operatorname{Tr}(d\beta/n) + n\operatorname{Tr}(d\beta/n)/\alpha^3 + N(x)N(d/n) + N(x)\operatorname{Tr}(d\beta/n)/\alpha +\\
& \big(\operatorname{N}(d/n) + 2\operatorname{N}(x)\big)N(\beta)/\alpha^2 + N(\beta)\operatorname{Tr}(d\beta/n)/\alpha^3 + \operatorname{N}(\gamma)/\alpha^2,\\
C =& \operatorname{N}\Big(- x\gamma/\alpha - x\beta d/(\alpha n) - \alpha d/n + \beta\Big).
\end{aligned}
$$

For example if $K = \mathbb{Q}[t]/(t^6 + 13t^4 + 50t^2 + 49)$ then there is only one curve of genus 3 and CM by $\mathcal{O}_K$ (indeed K has class number 1), i.e.

$$C: \quad y^2 = x^7 + 1786x^5 + 44441x^3 + 278179x$$

with $\Delta = 2^{18} \cdot 7^{24} \cdot 11^{12} \cdot 19^7$. Actually only 7 and 11 are primes of geometric bad reduction: for $p = 7$ there are two solutions to the embedding problem, for $p = 11$ there is only one.

References

[1] J. Dixmier, *On the projective invariants of quartic plane curves*. Adv. in Math., 64(3):279-304, 1987.

[2] E. Goren, K. Lauter, *Class invariants for quartic CM fields*. Ann. Inst. Fourier, 57(2):457-480, (2007).

[3] E. Z. Goren and K. E. Lauter., *Genus 2 curves with complex multiplication*. Inter. Math. Research Notices 5:1068-1142, 2012.

[4] J. I. Igusa., *Arithmetic variety of moduli for genus two*. Annals of Math., 72(3):612-649, 1960.

[5] P. Kiliçer, K. Lauter, E. Lorenzo García, R. Newton, E. Ozman, M. Streng, *A bound on the primes of bad reduction for CM curves of genus 3*. Preprint arXiv:1609.05826, (2018)

[6] K. Lauter, B. Viray, *An arithmetic intersection formula for denominators of Igusa class polynomials*. American Journal of Math., 137(2):497-533, 2015.

[7] J. S. Milne, *Complex multiplication*. Lectures Notes available on line: http://www.jmilne.org/math/CourseNotes/cm.html, 2006.

[8] T. Ohno, *Invariant subring of ternary quartics I generators and relations*. Preprint, https://www.win.tue.nl/ aeb/math/ohno-preprint.2007.05.15.pdf, 2007.

[9] T. Shioda., *On the graded ring of invariants of binary octavics*. American Journal of Math., 89:1022-1046, 1967.

[10] J. H. Silvermann, *Advanced topics in the arithmetic of elliptic curves*. Graduate texts in math, 151, 1994.

Guido Maria Lido
Department of Mathematics
University of Rome Tor Vergata
Via della Ricerca Scientifica 1
00133 Roma, Italy.
email: guidomaria.lido@gmail.com