Arithmetic properties of genus 3 curves II

Elisa Lorenzo García

Mémoire d'habilitation à diriger des recherches

École doctoral MathSTIC
Mathématics et leurs Interactions

préparé à l'IRMAR - Université de Rennes 1

présenté par

Elisa Lorenzo García

le 13 janvier 2021

Arithmetic properties of genus 3 curves II

devant le jury composé de

M Tim Dokchitser	Professeur, University of Bristol	Rapporteur
M David Kohel	Professeur, Aix-Marseille Université	Rapporteur
Mme Bianca Viray	Professeure, University of Washington	Rapportrice
Mme Irene Bouw	Professeure, Universität Ulm	Examinatrice
M Sylvain Duquesne	Professeur, Université de Rennes 1	Examinateur
M Qing Liu	Professeur, Université de Bordeaux	Examinateur

Contents

Preface

The 10th September 2014 in the afternoon, I defended my Ph.D. thesis entitled "Arithmetic properties of genus 3 curves". It contained my results on an algorithm to compute twists of non-hyperelliptic curves, the explicit computations for the case of genus 3, and the study of the Sato-Tate distribution for some families of curves and varieties, in particular for the twists of the Fermat and Klein quartics. Those results are published in [LG17, LG18, FLGS18].

One year before, in October 2013, I had attended the conference Women in Numbers Europe at CIRM. It was there, in the group led by I. Bouw and K. Lauter that my interest in the subject of controlling the primes of bad reduction of curves of genus 3 started. I will be always thankful to both, Irene and Kristin, for introducing me to the topic and all their help and support during the last years.

Since the beginning of my thesis in 2010 I have been always asked: "why genus 3? Are you talking next year about the same result for genus 4?" and I always had to explain that no, I was not planning to do the genus 4 case next year and the genus 5 one the next one. In general, genus g curves are non-hyperelliptic, but there is no non-hyperelliptic curve until genus 3, so while trying to prove a general result for curves, the first real difficulties come up for genus 3. This is why I'm interested in genus 3 curves, plus because the simple reason that I just like them. I've been called many times "the genus 3 girl". I guess I'm lucky, because in 2015 I met "the genus 3 guy", and since them we have worked on many nice genus 3 problems together.

In this report entitled "Arithmetic properties of genus 3 curves II" I summarize my results after my thesis on the study of the primes in the discriminant of genus 3 curves. This study takes two directions: bounding these primes and their exponents in the CM case, in order to be able to define class polynomials with good properties for genus 3 curves; and determining the reduction type of genus 3 curves at these primes. I present here my works: [BCL+15], [BCK+21], [IKL+20], [IKL+19], [KLS20], [KLL+20], [LLLR20], [LLR18], [Lor20] and my Ph.D. student on-going work [Fav20]. In Chapter 1 of this report, I explain the state of the art for these questions in genus 1 and 2. I show my computations on different expressions for curve invariants that are useful to deal with these questions (results in [BCK+21, Lor20]) in Chapter 2. I discuss the possibilities for the character of primes appearing in the discriminant of a genus 3 curve: results in [IKL+19, KLS20, LLLR20] in Chapter 3. I give the results concerning the bad reduction type of certain curves of genus 3 (CM, hyperelliptic, Ciani), see [BCK+21, Fav20, Lor20], in Chapter 4. The bounds for the primes, and their exponents, on the denominators of class polynomials are given in Chapter

5, they correspond to my results in [BCL+15, IKL+20, KLL+20, KLS20]. Finally, in Chapter 6, I present the conclusions after my work of these last 6 years and I briefly discuss the new projects I have in mind.

While I am skipping almost all the proofs, I am anyway trying to give the ideas behind and showing many examples. I invite the interested reader to consult the published version of my papers. I apology in advance for the sometimes lack of consistency in the notation: since this is a compendium of different papers, I am trying to keep the notation in them to facilitate the comparison with the results in the published versions of the papers and this report. For instance, I usually denote a curve by C, but in [BCK+21] and [IKL+20] the letter C is booked for one of the coefficients of a polynomial, so curves are denoted by X. Moreover, in [BCK+21] different curves play an important role, so the genus 3 curve in consideration is denoted by Y. I did my best to avoid confusion and make these changes of notation easy to follow.

Last but not least, I would like to highlight that I also worked on other subjects since I finished my thesis. If I chose to talk about my results about primes in the discriminant of genus 3 curves in this report is to show a real evolution of my research after my Ph.D.. However, I also kept working on Galois cohomology and on particular on twist computations, see [BBL19, BBL18, LL19, Lor17]; on arithmetic statistics [LMM17]; and on automorphisms of curves and isogenies of their Jacobians, see [BGL+17, BL20, LLRS20].

Chapter 1

Introduction

In this chapter we present the state of the art of the two problems we are interested in. Namely, the problem of understanding the denominators of class polynomials, so the discriminants of CM curves; and the problem of characterizing the reduction type of low genus curves, again related with the study of curves discriminants. By a curve, we understand a "nice" curve, i.e., a geometrically irreducible, connected, smooth and projective one.

1.1 Elliptic curves

Let K be a field of characteristic $\neq 2, 3$. Let E/K be an elliptic curve. It admits an integral short Weierstrass model $y^2 = f(x)$, i.e., with $f(x) = x^3 + ax + b$ and $a, b \in \mathcal{O}_K$. The polynomial f can be factor over $\overline{K}$ as follows $f(x) = (x - e_1)(x - e_2)(x - e_3)$. The discriminant of the elliptic curve can be expressed in different ways:

$$\Delta(E) = 16\Delta(f) = -16(4a^3 + 27b^2) = (e_1 - e_2)^2(e_2 - e_3)^2(e_3 - e_1)^2.$$

Since elliptic curves are smooth curves, their discriminant is not zero. Equivalently, they do not have repeated roots. This allows to introduce the well-defined quantity:

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2} = -2^8 \cdot 3^3\frac{(e_1e_2 + e_2e_3 + e_3e_1)^3}{(e_1 - e_2)^2(e_2 - e_3)^2(e_3 - e_1)^2},$$

that is known as the j-invariant of the elliptic curve. Two elliptic curves are isomorphic over $\overline{K}$ if and only if they have the same j-invariant. Indeed, two elliptic curves given in short Weierstrass form are isomorphic if and only if there is an isomorphism between them of the form $(x, y) \mapsto (u^2x, u^3y)$ for some $u \in \overline{K}^*$ (e.g. [Was08, Thm. 2.19]) which happens if and only if we have the equality of weighted projective invariants $(a : b) = (a' : b') \in \mathbb{P}^1_{(2,3)}$; this is equivalent to having the stated equality of j-invariants[1].

Let us consider now an elliptic curve $E/\mathbb{C}$ defined over the complex numbers. It can be seen as a complex torus $\mathbb{C}/\Lambda$, that is, as the quotient of $\mathbb{C}$ by a lattice $\Lambda = \langle 1, \tau \rangle$ where $\tau \in \mathbb{H}$

[1]The j-invariant is actually not an invariant in the sense of the Classical Invariant Theory but what is called an absolute invariant, i.e., a quotient of same weight invariants.

is an element in the Siegel upper half-space. Isomorphism classes of elliptic curves are given by the orbits of the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$. There exists a well-known expression for the j-invariant of the elliptic curve corresponding to Λ in terms of τ:

$$j(E) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + ... \tag{1.1.1}$$

where $q = \exp(2\pi i\tau)$. The expression in Equation 1.1.1 is a modular function for $\mathrm{SL}_2(\mathbb{Z})$: it is the quotient of 2 modular forms of weight 12.

We consider now the theta function for genus 1 (it is a modular forms of weight 1/2):

$$\theta(z,\tau) = \sum_{n=-\infty}^{\infty} \exp(\pi i n^2\tau + 2\pi i n z),$$

and the theta constants

$$\vartheta_0 = \theta(0,\tau),\ \vartheta_1 = \theta(1/2,\tau),\ \vartheta_2 = \exp(\frac{1}{4}\pi i\tau)\vartheta(\tau/2,\tau) \text{ and } \vartheta_3 = \exp(\frac{1}{4}\pi i\tau\frac{1}{2}\pi i)\theta(\tau/2+1/2,\tau),$$

satisfying the relations: $\vartheta_3 = 0$ and $\vartheta_0^4 = \vartheta_1^4 + \vartheta_2^4$. We can rewrite Equation 1.1.1 as

$$j(E) = 2^5\frac{(\vartheta_0^8 + \vartheta_1^8 + \vartheta_2^8)^3}{(\vartheta_0\vartheta_1\vartheta_2)^8}. \tag{1.1.2}$$

The advantage of this expression is that while Equation 1.1.1 is only valid over the complex numbers, Equation 1.1.2 is still valid over any field K of characteristic different from 2: Mumford [Mum06, Prop. 5.11] (see also loc. cit. Definition. 5.8) defined algebraic theta constants for any abelian variety defined over such a field K (who coincide in the case $K = \mathbb{C}$ with the ones previously defined). Even more, when working over a discrete valuation field of characteristic different from 2, the reduction of the theta constants coincides with the theta constants of the reduction, see [LLR18, Sec. 2] for a discussion about this. We call Equality 1.1.2 a modular expression for the j-invariant of an elliptic curve. In particular, we also have a modular expressions for the invariants:

$$(a:b) = (-1(\vartheta_0^8 + \vartheta_1^8 + \vartheta_2^8)/6 : (\vartheta_0^8 + \vartheta_1^8)(\vartheta_0^8 + \vartheta_2^8)(\vartheta_1^8 - \vartheta_2^8)) \in \mathbb{P}^1_{(2,3)}.$$

1.1.1 Reduction type

Let K be a discrete valuation field, $\mathcal{O}_K$ its ring of integers, π an uniformizer and we assume that $k = K/(\pi)$ is an algebraic close field of characteristic p. We also assume $\mathrm{char}(K)$ and $p \neq 2$. We normalize the valuation v such that $v(p) = 1$.

Theorem 1.1.1. *([Tat75]) Let $E/K : y^2 = x^3 + ax + b$ be an elliptic curve given by an integer model, i.e., $a, b \in \mathcal{O}_K$. Then:*

- *E has good reduction if $v(\Delta(E)) = 0$.*
- *E has multiplicative (bad) reduction if $v(\Delta(E)) > 0$ and $v(a) = 0$.*

- *E has additive (bad) reduction if $v(\Delta(E)) > 0$ and $v(a) > 0$.*

After a finite field extension, additive reduction always becomes multiplicative or good. E has potentially good reduction if and only if $3v(a) \geq v(\Delta(E))$, or equivalently, if $v(j(E)) \geq 0$.

Remark 1.1.2. Te result in Theorem 1.1.1 can be seen in terms of collisions of ramification points, in others words, by looking at the cluster picture (see Definition 4.1.2).

Example 1.1.3. Let us consider the elliptic curve $E : y^2 = x^3+5x+5/\mathbb{Z}_5$. It has discriminant $\Delta(E) = -2^4 \cdot 5^2 \cdot 47$, so this model has bad reduction at $p = 5$. Since $v(\Delta) = 2$, $v(a) = v(b) = 1$ and accordingly to previous theorem, we get that it has additive bad reduction, but potentially good reduction. Indeed, consider the change of variable $x' = \sqrt[3]{5}$, $y' = \sqrt{5}$ over $\mathbb{Q}_5(\sqrt[6]{5})$ and the new model $y'^2 = x'^3 + \sqrt[3]{5}x' + 1$ that has discriminant $\Delta' = -2^4 \cdot 47$ and hence good reduction modulo $\mathfrak{p} = (\sqrt[6]{5}) \mid 5$.

1.1.2 The Complex Multiplication method

Let K be an imaginary quadratic field and $\mathcal{O}$ an order of K. The Hilbert class polynomial associated to $\mathcal{O}$ is defined as follows:

$$H_{\mathcal{O}}(T) = \prod_{E/\mathbb{C} \text{ has CM by } \mathcal{O}/\simeq} (T - j(E)).$$

Elliptic curves, and in general abelian varieties, with CM have potentially good reduction everywhere [ST68]. Then the Hilbert class polynomial has integer coefficients, i.e., $H_{\mathcal{O}}(T) \in \mathbb{Z}[T]$. So in order to compute it, it suffices to numerically approximate its coefficients, e.g., [BBEL08, Bro08, Sut11].

Example 1.1.4. Let $p = 17$, we want to construct an elliptic curve $E/\mathbb{F}_p$ with

$$\#E(\mathbb{F}_p) = p + 1 - a = 22.$$

The Complex Multiplication Method tells us to construct an elliptic curve with an endomorphism (the Frobenius) of norm $p = 17$ and trace $a = -4$.

Let us set $\mathcal{O} = \mathbb{Z}[\frac{a+\sqrt{-d}}{2}]$ with $-d = a^2 - 4p = -2^2 \cdot 13$. We want then to construct an elliptic curve with endomorphism ring isomorphic to $\mathcal{O}$.

We find with Sage [S+20] that $H_{\mathcal{O}}(T) \equiv (T + 12)(T + 13) \bmod 17$. The elliptic curve $\mathcal{E} : y^2 = x^3 - 435x - 42050$ has j-invariant -12. Let E be its reduction modulo 17, we find that

$$\#E(\mathbb{F}_{17}) = 22.$$

It may have occurred that we had obtain an elliptic curve with trace $a = 4$, so in this case we should have taken the quadratic twist in order to get trace $a = -4$.

1.2 Curves of genus 2

Let C be a curve of genus 2 defined over K. All curves of genus 2 are hyperelliptic, so if $\mathrm{char}(K) \neq 2$ it admits a model $y^2 = f(x,z)$ in $\mathbb{P}^2_{1,3,1}$ with $f \in \mathcal{O}_K[x,y]$ a homogeneous polynomial of degree 6.

Gordan computed generators for the invariant ring of binary sextics [Gor68]. Igusa computed invariants [Igu60] for genus 2 curves: $\mathrm{Ig} = (\mathrm{Ig}_2 : \mathrm{Ig}_4 : \mathrm{Ig}_6 : \mathrm{Ig}_8 : \mathrm{Ig}_{10})$. These invariants determine isomorphism classes: two genus 2 curves C, C' are isomorphic if and only if $\mathrm{Ig}(C) = \mathrm{Ig}(C') \in \mathbb{P}^3_{(1,2,3,4,5)}(\bar{K})$. The weight 8 invariant is only needed in characteristic 2 since otherwise it may be expressed in terms of the other invariants.

Igusa invariants, that are polynomials on the curve coefficients, can also be defined in terms of the differences of roots of $f(x)$ [Cle70] or as Siegel modular forms for $\mathbb{H}_2$ with respect to the modular group $\mathrm{Sp}_4(\mathbb{Z})$, see [Bol87, Igu62, Igu67]. This has applications for determining the reduction type of genus 2 curves and for implementing class polynomials which is for example useful for carrying out the CM method in genus 2.

1.2.1 Reduction types

Let K be a discrete valuation field, $\mathcal{O}_K$ its ring of integers, π an uniformizer and we assume that $k = K/(\pi)$ is an algebraic close field of characteristic p. We normalize the valuation v such that $v(p) = 1$. We also introduce the invariants

$$\mathrm{Ig}'_2 = 12^{-1}\,\mathrm{Ig}_2,\ \mathrm{Ig}'_4 = \mathrm{Ig}_2^2 - 2^3 3\,\mathrm{Ig}_4,\ \mathrm{Ig}'_6 = \mathrm{Ig}_6,\ \mathrm{Ig}'_8 = \mathrm{Ig}_8$$
$$\mathrm{Ig}'_{12} = -2^3\,\mathrm{Ig}_4^3 + 3^2\,\mathrm{Ig}_2\,\mathrm{Ig}_4\,\mathrm{Ig}_6 - 3^3\,\mathrm{Ig}_6^2 - \mathrm{Ig}_2^2\,\mathrm{Ig}_8\,.$$

We define $\epsilon = 1$ if $p \neq 2, 3$, $\epsilon = 3$ if $p = 3$ and $\epsilon = 4$ if $p = 2$.

The reduction type and the description of the special fiber of the stable model of a genus 2 curve in terms of the valuation of its invariants is a beautiful result in [Liu93, Thm. 1]. See also [Mes91, Sec. 2.3]. We rephrase this result as follows:

Theorem 1.2.1. *Let C/K be a smooth genus 2 curve with Igusa invariants Ig_{2i} and Ig'_{2i}, then the reduction of the stable model of C is:*

- *a smooth genus 2 curve if and only if $v(\mathrm{Ig}_{2i}^5 / \mathrm{Ig}_{10}^i) \geq 0$ for all $i \leq 5$.*
- *irreducible with a single (doble) singular point if and only if $v(\mathrm{Ig}_{2i}^6 / \mathrm{Ig}'^i_{12}) \geq 0$ for all $i \leq 5$ and $v(\mathrm{Ig}_{10}^6 / \mathrm{Ig}'^5_{12}) > 0$.*
- *irreducible with two (double) singular point if and only if $v(\mathrm{Ig}_{2i}^2 / \mathrm{Ig}'^i_4) \geq 0$ for all $i \leq 5$, $v(\mathrm{Ig}_{10}^2 / \mathrm{Ig}'^5_4) > 0$, $v(\mathrm{Ig}'_{12} / \mathrm{Ig}'^3_4) > 0$ and $v(\mathrm{Ig}_4 / \mathrm{Ig}'_4) = 0$ or $v(\mathrm{Ig}_6^2 / \mathrm{Ig}'^3_4) = 0$.*
- *2 projective lines intersecting each other at 3 points if and only if $v(\mathrm{Ig}_{2i}^2 / \mathrm{Ig}'^i_4) > 0$ for all $2 \leq i \leq 5$.*
- *2 elliptic curves intersecting at 1 point if $v(\mathrm{Ig}'^\epsilon_4 / \mathrm{Ig}'^2_{2\epsilon}) > 0$, $v(\mathrm{Ig}_{10}^\epsilon / \mathrm{Ig}'^5_{2\epsilon}) > 0$, $v(\mathrm{Ig}'^2_{12} / \mathrm{Ig}'^6_{2\epsilon}) > 0$, $v(\mathrm{Ig}'^{3\epsilon}_4 / (\mathrm{Ig}_{10}^\epsilon\,\mathrm{Ig}'_{2\epsilon})) = 0$ and $v(\mathrm{Ig}'^\epsilon_{12} / (\mathrm{Ig}_{10}^\epsilon\,\mathrm{Ig}'_{2\epsilon})) = 0$.*

- *1 elliptic curve and a singular conic intersecting at 1 point if* $v(\mathrm{Ig}_4'^{\epsilon} / \mathrm{Ig}_{2\epsilon}'^{2}) > 0$, $v(\mathrm{Ig}_{10}^{\epsilon} / \mathrm{Ig}_{2\epsilon}'^{5}) > 0$, $v(\mathrm{Ig}_{12}'^{2} / \mathrm{Ig}_{2\epsilon}'^{6}) > 0$, $v(\mathrm{Ig}_4'^{3} / \mathrm{Ig}_{12}') = 0$ *and* $v(\mathrm{Ig}_{10}^{\epsilon}\,\mathrm{Ig}_{2\epsilon}' / \mathrm{Ig}_{12}'^{\epsilon}) > 0$.
- *2 singular conics intersecting at one point otherwise.*

My on-going Ph.D. student Harold Faverau has re-proved this result [Fav20] by using different techniques that allow generalization to higher genus. The idea is to determine the cluster picture by looking at the valuations of the invariants when these are expressed in terms of the differences of the roots of the polynomial defining the genus 2 curve. The cluster picture determines the special fiber of the stable model of the curve [DDMM19, DDMM18]. I used this idea in [Lor20, Sec. 6.1] and also Mestre followed a similar approach in [Mes91, Sec. 1.4].

1.2.2 The Complex multiplication method

We consider here the absolute Igusa invariants

$$i_1 = \frac{(\mathrm{Ig}_2\,\mathrm{Ig}_4 - 3\,\mathrm{Ig}_6)\,\mathrm{Ig}_4}{\mathrm{Ig}_{10}},\ i_2 = \frac{\mathrm{Ig}_2\,\mathrm{Ig}_4^2}{\mathrm{Ig}_{10}} \text{ and } i_3 = \frac{\mathrm{Ig}_4^5}{\mathrm{Ig}_{10}^2}.$$

The computation and implementation of the Igusa class polynomials

$$\begin{aligned} H_{\mathcal{O},1} &= \prod_C (T - i_1(C)), \\ H_{\mathcal{O},2} &= \sum_C i_2(C) \prod_{C' \neq C} (T - i_2(C')), \\ H_{\mathcal{O},3} &= \sum_C i_3(C) \prod_{C' \neq C} (T - i_3(C')), \end{aligned}$$

for quartic CM-fields by using the modular expressions of Igusa invariants are discussed in Streng's paper [Str14]. Since for genus greater than 1 the coefficients of class polynomials are rational numbers and not integers any more, a bound for their denominators is needed to perform exact computations by approximating modular expressions of the invariants: [BY06, GL07, Yan13, LV15]. Denominators of class polynomials only contains primes of bad reduction of the genus 2 curves, in order to bound them we need to bound these primes and the exponents they appear with at the denominators. The question about bounding these primes is considered in Goren and Lauter's work [GL07], we formulate their result as in [Str14, Lemma 10.4]:

Theorem 1.2.2. *Let* $K = \mathbb{Q}(\sqrt{-a + b\sqrt{d}})$ *a primitive quartic CM-field, and* $\mathcal{O}$ *its maximal order. Then the primes dividing the denominators of the Igusa class polynomials* $H_{\mathcal{O},i}$ *(*$i = 1, 2, 3$*) are smaller or equal than* $4da^2$.

In [Yan13, Sec. 9] a relation between the exponents of a prime ℓ in the denominator and the arithmetic intersection number $(\mathrm{CM}(K) \cdot G_1)_\ell$ is given, this is the power of the prime ℓ in

the intersection number of the cycle of decomposable principally polarized abelian surfaces and the points of the moduli space with CM by the maximal order of the CM-field K.

A explicitly computable formula for the number $(\mathrm{CM}(K)\cdot G_1)_\ell$ is given in Lauter and Viray's paper [LV15]. For computational purposes, we show the bounds as in [Str14, Thm 10.1].

Let be h and h_0 the class numbers of K and K^+, let $h_1 = h/h_0$ and $h' = h_1$ if K is cyclic and $2h_1$ otherwise.

Theorem 1.2.3. *The denominator of each of the Igusa class polynomials of K divides $D = 2^{24h'}D_1^2$ for*

$$D_1 = \left(\prod_{p<4da^2} p^{4f(p)(1+\log(2da^2)/\log p)}\right)^{h'},$$

where $f(p)$ is equal to 8 if $p = 2, 3$ ramifies in $K/\mathbb{Q}$ and to 1 otherwise.

Example 1.2.4. Let us consider the quartic CM-field K that is the splitting field of the polynomial $t^4 + 10t^2 + 20$. Let $\mathcal{O}$ its maximal order. By using the implementation in [Str14], the corresponding Igusa class polynomials are computed in [BS15]:

$$\begin{aligned} H_{\mathcal{O},1} &= x^2 - 367416000x, \\ H_{\mathcal{O},2} &= 367416000x - 1203634148850000000/14641, \\ H_{\mathcal{O},3} &= 367416000x - 8474823196875000000000/14641. \end{aligned} \tag{1.2.1}$$

This gives us the two curves with Igusa invariants: $\mathrm{Ig}(C_1) = (630 : 8100 : 1459080 : 16)$ and $\mathrm{Ig}(C_2) = (64710 : 13176900 : 284225733000 : 50214854027536)$. With Mestre reconstruction algorithm [Mes91], we obtain the equations (see [BS15, Section 4] for a detailed discussion about how to get the "nicest" possible equations):

$$C_1 : y^2 = 4x^5 - 30x^3 + 45x - 22 \text{ and } C_2 : y^2 = 8x^6 + 52x^5 - 250x^3 + 321x - 131.$$

These two curves are the only ones with CM by the maximal order of K. By using Theorem 1.2.1, we check that they have potentially good reduction at every prime different from 2 and 11. The curve C_1 has also potentially good reduction at 11. The special fiber of the stable model of both curves at $p = 2$ and of C_2 at $p = 11$ is the union of two elliptic curves intersecting at 1 point (actually this is the only possibility for bad reduction of CM genus 2 curves since they have compact reduction).

1.3 Curves of genus 3

Curves of genus 3 may be non-hyperelliptic (plane quartics) or hyperelliptic. For both families we have generators of the invariant ring that describe the isomorphism classes:

Dixmier-Ohno invariants[2] [Dix87, Ohn05] for plane quartics and Shioda invariants [Shi67] for hyperelliptic curves of genus 3.

The questions I have been working on during the last 6 years and that I present in this thesis are the following:

1. producing different curves' invariants expressions: modular invariants, in terms of differences of roots, for particular families of curves, etc.

2. study of the different character of primes in the denominators of class polynomials and/or in curves discriminants.

3. characterization of the types of bad reduction.

4. computation of bounds for the primes of bad reduction and their exponents in the discriminant.

My results on these questions are found in my works: [BCL+15], [BCK+21], [IKL+20], [IKL+19], [KLS20], [KLL+20], [LLLR20], [LLR18], [Lor20] and my Ph.D. student on-going work [Fav20].

Remark 1.3.1. Another motivation for constructing class polynomials for genus 3 curves (which is not the possible crypto applications) is that genus 3 is the last genus for which there still exist infinitely many CM (non superelliptic) curves accordingly to (the modified) Coleman's conjecture [MO13, Conj. 4.1]. See Somoza's thesis [Som19] for algorithms related to the construction of CM superelliptic curves.

[2]Technically, DO invariants are only proved to generate the invariant ring in characteristic 0. For practical issues only an HSOP (*homogeneous sytem of parameters*, i.e., an algebraically independent set of invariants such that the full algebra of invariants is a finite module over the subalgebra generated by them) is required and those are computed for any characteristic in [LLLR20]. Shioda invariants also need to be slightly modified for small characteristics.

Chapter 2

Different expressions for genus 3 curve invariants

As we have already seen in the previous section, having different expressions for curve invariants may be useful for different reasons. The algebraic expressions in terms of the coefficients of curves equations are useful for explicit computations. Modular expressions are useful for computing class polynomials (and hence for the CM method), so for computing algebraic equations when starting from analytical information, i.e., the period matrix of the Jacobian of the curve. For hyperelliptic curves we have seen that expressions of the invariants in terms of the differences of their roots are also useful, since they describe the cluster picture (see Definition 4.1.2) which is very helpful for determining the reduction type.

In this chapter I describe my contributions to this problem in [Lor20] which mainly focuses on the hyperelliptic case. Simultaneously to this work my co-authors also found a modular expression for non-hyperelliptic genus 3 curves [LR20]. However, for this case we still do not know a useful expression of the invariants that would help to determine the reduction type of plane quartics since there is no analogous to the cluster picture.

2.1 Tsuyumine invariants

Let $f(x,z) \in K[x,z]$ be a binary octic. Let $\alpha_i, \beta_i \in \overline{K}$ such that $f(x,z) = \prod_{i=1}^{8}(\beta_i x - \alpha_i z)$. We introduce the following notations:

$$(i_1 ... i_r) = \prod_{\substack{i<j \\ i,j \in \{i_1,...,i_r\}}} (\beta_j\alpha_i - \beta_i\alpha_j),$$

$$(i_1 ... i_r, j_1 ... j_s) = \prod_{\substack{i \in \{i_1,...,i_r\} \\ j \in \{j_1,...,j_s\}}} (\beta_j\alpha_i - \beta_i\alpha_j).$$

With this notation, the discriminant of f is given by the expression $D = \prod_{i<j}(ij)^2$.

Proposition 2.1.1. *([Tsu86, Chap. 5]) The graded ring $S(2,8)$ of invariants of binary octics is generated by I_2, I_3, I_4, I_5, I_6, I_7, I_8, I_9, I_{10}, where I_k is an invariant of degree k given as follows:*

$$
\begin{aligned}
I_2 &= \sum (12,34)(56,78) \\
I_3 &= \sum (12)^2(34)^2(56)^2(78)^2(13)(24)(57)(68) \\
I_4 &= \sum (12)^4(345)^2(678)^2 \\
I_5 &= \sum (12)^4(345)^2(678)^2(15)(26)(37)(48) \\
I_6 &= \sum (1234)^2(5678)^2 \\
I_7 &= \sum (1234)^2(5678)^2(15)(26)(37)(48) \\
I_8 &= \sum (1234)^2(5678)^2(12,56)(34,78) \\
I_9 &= \sum (1234)^2(5678)^2(1,567)(2,678)(3,578)(4,568) \\
I_{10} &= \sum (1234)^2(5678)^2(15)^2(26)^2(37)^2(48)^2(14,67)(23,58)
\end{aligned}
$$

Even if having the same degrees, these invariants are not the Shioda invariants J_2, J_3, J_4, J_5, J_6, J_7, J_8, J_9 and J_{10} [Shi67]. As for the later, the first six invariants I_2, I_3, I_4, I_5, I_6, I_7 are algebraically independent but not the last three, Tsuyumine does not compute the algebraic relations between them.

We call them Tsuyumine invariants, they enjoy both nice properties we where looking for: a description in terms of differences of roots of f and a modular expression. However, they are not easily computable, since even if one factors the polynomial f to get its roots, one still needs to go through all the permutation in S_8. Their expressions in terms of the coefficients of f are huge. Theorem 2.1.3 gives them in terms of Shioda invariants which are easily computable. Another nice property about Shioda invariants is that the reconstruction of the curve from them is known and implemented [LR12, Sec. 2.3]. We believe both invariants have nice properties, we do not need to decide which ones to use, what we need is a *passage formula* between them.

Remark 2.1.2. Tsuyumine invariants are integral invariants, since they are polynomials with integer coefficients on the symmetric functions of the roots of the binary octic, that is, on their coefficients. However, Shioda invariants are not integer invariants, they have some denominators with powers of $2, 3, 5$ and 7, see [LR12, Section 1.5]. These are precisely the primes for which Shioda invariants are not an HSOP. In his thesis [Bas15], gives HSOP's for the characteristics $p = 3$ and 7 and the same techniques may be used to get an HSOP for $p = 5$.

In my work [Lor20] I proved the following result:

Theorem 2.1.3. *Tsuyumine invariants can be written in terms of Shioda invariants as follows:*

$$
\begin{aligned}
I_2 &= 2^9\cdot 3^2\cdot 5\cdot 7\cdot J_2,\\
I_3 &= 2^{10}\cdot 5^2\cdot 7^3\cdot J_3,\\
I_4 &= -2^{14}\cdot 3\cdot 5^2\cdot 7\cdot J_2^2 + 2^{15}\cdot 3^2\cdot 7^3 J_4,\\
I_5 &= 2^{14}\cdot 3^{-1}\cdot 5^3\cdot 7^3\cdot J_2J_3 - 2^{14}\cdot 3\cdot 5\cdot 7^4\cdot J_5,\\
I_6 &= 2^{15}\cdot 3^{-1}\cdot 7\cdot 17^3\cdot J_2^3 - 2^{18}\cdot 3\cdot 7^3\cdot 17\cdot J_2J_4 + 2^{16}\cdot 3^2\cdot 5\cdot 7^4\cdot J_3^2 - 2^{21}\cdot 3\cdot 7^4\cdot J_6,\\
I_7 &= 2^{16}\cdot 5^4\cdot 7^3 J_2^2J_3 - 2^{13}\cdot 3\cdot 5\cdot 7^4\cdot 17\cdot J_2J_5 - 2^{14}\cdot 5\cdot 7^5\cdot 13\cdot J_3J_4 - 2^{15}\cdot 3^2\cdot 5\cdot 7^5\cdot J_7,\\
I_8 &= 2^{15}\cdot 3^{-2}\cdot 7\cdot 17\cdot 6469\cdot J_2^4 - 2^{19}\cdot 5\cdot 7^3\cdot 43\cdot J_2^2J_4 - 2^{16}\cdot 3^{-2}\cdot 5\cdot 7^4\cdot 233\cdot J_2J_3^2\\
&\quad - 2^{21}\cdot 7^4\cdot 37\cdot J_2J_6 + 2^{18}\cdot 3^2\cdot 5\cdot 7^5\cdot J_3J_5 + 2^{21}\cdot 3\cdot 7^4\cdot J_4^2 + 2^{20}\cdot 3^2\cdot 5\cdot 7^5\cdot J_8,\\
I_9 &= -2^{15}\cdot 3^{-3}\cdot 7^3\cdot 134489\cdot J_2^3J_3 + 2^{13}\cdot 7^4\cdot 17\cdot 613\cdot J_2^2J_5 + 2^{14}\cdot 3^{-1}\cdot 5\cdot 7^5\cdot 1117\cdot J_2J_3J_4\\
&\quad - 2^{15}\cdot 3\cdot 5^2\cdot 7^5\cdot 19\cdot J_2J_7 - 2^{16}\cdot 3\cdot 5\cdot 7^6\cdot J_3^3 + 2^{21}\cdot 3^{-1}\cdot 5^2\cdot 7^6\cdot J_3J_6 + 0\cdot J_4J_5 - 2^{23}\cdot 3^2\cdot 7^6 J_9,\\
I_{10} &= 2^{16}\cdot 3^{-5}\cdot 7\cdot 17^2\cdot 223\cdot 227\cdot J_2^5 - 2^{21}\cdot 3^{-3}\cdot 7^3\cdot 17\cdot 1097\cdot J_2^3J_4 + 2^{17}\cdot 3^{-4}\cdot 5\cdot 7^4\cdot 37\cdot 991\cdot J_2^2J_3^2\\
&\quad - 2^{22}\cdot 3^{-3}\cdot 5^2\cdot 7^4\cdot 421\cdot J_2^2J_6 - 2^{15}\cdot 3\cdot 5\cdot 7^5\cdot 17\cdot 29\cdot J_2J_3J_5 + 2^{22}\cdot 3^{-1}\cdot 7^4\cdot 23\cdot 31\cdot J_2J_4^2\\
&\quad + 2^{25}\cdot 5\cdot 7^5\cdot 17\cdot J_2J_8 + 2^{16}\cdot 5\cdot 7^6\cdot 23\cdot J_3^2J_4 - 2^{17}\cdot 3^2\cdot 5\cdot 7^6\cdot 29\cdot J_3J_7 + 2^{25}\cdot 3^{-1}\cdot 7^5\cdot 61\cdot J_4J_6\\
&\quad + 0\cdot J_5^2 + 2^{26}\cdot 3\cdot 5\cdot 7^6\cdot J_{10}.
\end{aligned}
$$

Equivalently, I obtained expressions for Shioda invariants in terms of Tsuyumine invariants just by inverting the relations in the previous theorem, see [Lor20, Thm. 4.2]. The idea of the proof of the previous theorem is interpolation: we know that Shioda invariants are generators for the invariant ring of hyperelliptic curves of genus 3, since Tsuyumine invariants are invariants they may be expressed as a linear combination of products of Shioda invariants having the same weight. We evaluated both families of invariants for a big enough set of curves and we interpolated in order to find the coefficients of the linear combinations.

2.2 Modular expressions for Shioda invariants

Modular expressions for Tsuyumine invariants [Tsu86, Sec. 23,24,25,26] are known via the Igusa map, more particularly, and stated as in [Lor20, Cor. 3.5]:

Theorem 2.2.1. *Let $C : y^2 = f(x)$ be a genus 3 hyperelliptic curve with period matrix $\Omega = [\Omega_1, \Omega_2]$. Let $\tau = \Omega_2^{-1}\Omega_1$. Then*

$$
\begin{aligned}
I_2(f)D(f)^2 &= (2i\pi)^{90}\frac{\gamma_{20}(\tau)}{\det\Omega_2^{30}}\\
I_3(f)D(f)^3 &= (2i\pi)^{135}\frac{\gamma_{30}(\tau)}{\det\Omega_2^{45}}\\
I_4(f)D(f) &= 2^3 3^2 (2i\pi)^{54}\frac{\alpha_{12}(\tau)}{\det\Omega_2^{18}}
\end{aligned}
$$

$$
\begin{aligned}
I_5(f)D(f)^2 &= (2i\pi)^{99}\frac{\beta_{22}(\tau)}{\det\Omega_2^{33}}\\
I_6(f) &= 2^3(2i\pi)^{18}\frac{\alpha_4(\tau)}{\det\Omega_2^{6}}\\
I_7(f)D(f) &= (2i\pi)^{63}\frac{\beta_{14}(\tau)}{\det\Omega_2^{21}}\\
I_8(f)D(f)^2 &= (2i\pi)^{108}\frac{\gamma_{24}(\tau)}{\det\Omega_2^{36}}\\
I_9(f) &= (2i\pi)^{27}\frac{\alpha_6(\tau)}{\det\Omega_2^{9}}\\
I_{10}(f)D(f) &= (2i\pi)^{72}\frac{\beta_{16}(\tau)}{\det\Omega_2^{24}}\\
D^3(f) &= (2i\pi)^{126}\frac{\chi_{28}(\tau)}{\det\Omega_2^{42}}.
\end{aligned}
$$

The functions $\alpha_i, \beta_i\gamma_i$ and χ_{28} are the modular forms introduced in [Tsu86, Chap. 20]. In particular, we have modular expressions for the invariants I_kD^k which determine the isomorphism class of C.

Thanks to the expressions for Shioda invariants in terms of Tsuyumine invariants (inverse expressions to the ones in Thm. 2.1.3) and the previous theorem we have modular expressions[1] for them. In [Lor20, Sec. 5] I suggested a particular combination of Shioda invariants producing modular absolute invariants which only contains in the denominator primes of bad reduction of the curve. These are the kind of properties we need to construct class polynomials. Indeed, following this suggestion, an implementation of an algorithm to compute class polynomials for genus 3 curves for maximal orders of sextic CM-fields containing $\mathbb{Q}(i)$ can be found in the paper [ID20] by one of my collaborators and her Ph.D. student.

The reason to ask for having $\mathbb{Q}(i) \subseteq K$ is the following: genus 3 curves may be hyperelliptic or not hyperelliptic, we have different families of invariants for each of them. For defining class polynomials we need to fix a family of invariant. Given an order $\mathcal{O}$ in a sextic CM-field, there exists the possibility of having both, hyperelliptic and non-hyperelliptic curves having CM by $\mathcal{O}$. This is actually something that may happen as I learnt from an example provided in a private correspondence with Jeroen Sijsling. However, if $i \in \mathcal{O}$, then we can assure that all curves having CM by $\mathcal{O}$ are hyperelliptic [Wen01, Lemma 4.5] and class polynomials can be defined with Shioda invariants in a similar fashion to Igusa class polynomials 1.2.2.

2.3 Ciani plane quartics

Recently I became interested in explicit computations of curves invariants. I taught a Ph.D. course on Classical Invariant Theory at Université de Rennes 1 during the Spring Semester of 2020. I have some on-going projects on this topic. Even if generators for the invariant ring of plane quartic curves are known (at least in characteristic 0), i.e., the Dixmier-Ohno invariants; while working with particular families of plane quartics it is more practical to work with special invariants describing only the family.

Let K be a field of characteristic different from 2.

[1] I give the precise definition of a modular invariant in [Lor20, Def. 2.2]; as a vague definition we can just say that the invariant can be written in terms of modular forms or theta constants.

Lemma 2.3.1. *Let $Y/\overline{K}$ be a smooth plane quartic such that there exists a subgroup $V \subseteq \mathrm{Aut}_{\overline{K}}(Y)$ isomorphic to the Klein group.*

1. *([Cia99, Section 4])Then Y may be defined by an equation*

$$Y: \ Ax^4 + By^4 + Cz^4 + ay^2z^2 + bx^2z^2 + cx^2y^2 = 0 \tag{2.3.1}$$

   and the elements of V act as $(x : y : z) \mapsto (\pm x : \pm y : z)$.

2. *The ramification points of $f : Y \to Y/V =: X$ are the points with $xyz = 0$.*

3. *([Cas85]) Each of the intermediate curves of the cover $f : Y \to X$ is a curve of genus 1.*

Plane quartics that admit an equation as as in 2.3.1 are called Ciani quartics.

I used Classical Invariant Theory techniques [DK02] to compute generators for the invariant ring of Ciani quartics:

Proposition 2.3.2. *(Prop. 3.2 and 3.4 in [BCK+21]) The elements*

$$I_3 = ABC, \qquad I_3' = A\Delta_a + B\Delta_b + C\Delta_c,$$
$$I_3'' = -4ABC + Aa^2 + Bb^2 + Cc^2 - abc, \qquad I_6 = \Delta_a\Delta_b\Delta_c,$$

with $\Delta_a = a^2 - 4BC$, $\Delta_b = b^2 - 4AC$ and $\Delta_c = c^2 - 4AB$ are invariants for the locus $\mathcal{M}_{3,V}^{\mathrm{quar}}$ and they generate its invariant ring.

Equivalently, for hyperelliptic curves of genus 3:

Lemma 2.3.3. *([Bou98, Section 4.3] or [LR12, Table 3]) Let $Y/\overline{K}$ be a genus 3 hyperelliptic curve such that $\mathrm{Aut}_{\overline{K}}(Y)$ contains a subgroup V isomorphic to the Klein group and such that for every non-trivial element $\sigma \in V$ the quotient $Y/\langle\sigma\rangle$ has genus 1. Then we can write:*

$$Y: \ y^2 = x^8 + Mx^6 + Nx^4 + Mx^2 + 1, \tag{2.3.2}$$

and we identify V with the group generated by

$$\sigma_1(x, y) = (-x, y) \text{ and } \sigma_2(x, y) = (1/x, y/x^4).$$

I proved that:

Proposition 2.3.4. *([BCK+21, Prop. 5.2]) The invariant ring of $\mathrm{M}_{3,V}^{\mathrm{hyp}}$ is generated by the following invariants of weight $1, 2$ and 3 respectively:*

$$L_1 = N + 10,\ L_2 = M^2 - 4N + 8,\ L_3 = (2M + N + 2)(2M - N - 2).$$

In Chapter 4 we will use these invariants to characterise the reduction type of genus 3 curves admitting a subgroup of their automorphism group isomorphic to the Klein quartic such that the quotient of the curve by each of the order 2 elements is a curve of genus 1.

Chapter 3

Primes in the discriminant of a genus 3 curve

Let K be a discrete valuation field, $\mathcal{O}_K$ its ring of integers, π an uniformizer and we assume that $k = K/(\pi)$ is an algebraically closed field of characteristic p. Let C/K be a genus 3 curve, it can be a plane quartic curve or a hyperelliptic curve. Fix an integral model of C. In the first case the discriminant Δ of the curve is given by the multiple of the Dixmier-Ohno (DO) invariant $2^{40}I_{27}$, and in the second case it is a degree 14 invariant denoted by D_{14}. The model has good reduction modulo π if and only if π does not divide the discriminant. In this chapter we discuss the possibilities for the reduction type of C modulo π when $v(\Delta) > 0$.

Definition 3.0.1. *Let $\mathcal{I}$ be a finite set of curve invariants, let I be an invariant, we define the normalized valuation of I with respect to $\mathcal{I}$ as follows:*

$$v_{\mathcal{I}}(I(C)) = v(I(C)) - \text{weight}(I) \cdot \min(v(I'(C))/\text{weight}(I') : I' \in \mathcal{I}).$$

When the set $\mathcal{I}$ is clear from the context we may write $v_{\mathcal{I}}(I(C))$ as $v_{norm}(I(C))$.

Example 3.0.2. Let us take $\mathcal{I} = \text{Ig} = \{\text{Ig}_2, \text{Ig}_4, \text{Ig}_6, \text{Ig}_8, \text{Ig}_{10}\}$ and the curve C_1 in example 1.2.4. It has Igusa invariants

$$\text{Ig}(C_1) = (2^3 \cdot 3^2 \cdot 5^2 \cdot 7, 2^6 \cdot 3^4 \cdot 5^4, 2^9 \cdot 3^3 \cdot 5^4 \cdot 7 \cdot 193, 2^3 \cdot 3^5 \cdot 5^2 \cdot 4391, 2^{14} \cdot 5^5).$$

Then after fixing the valuation such that $v(2) = 1$, we have that $v(\text{Ig}_{10}(C_1)) = 14$ and $v_{\text{Ig}}(\text{Ig}_{10}(C_1)) = 41/4 > 0$. This proves that the curve C_1 has geometrically bad reduction. This examples also evidences the necessity of the invariant I_8 in characteristic 2.

3.1 The hyperelliptic case

We fix the set $\text{Sh} = \{J_2, J_3, J_4, J_5, J_6, J_7\}$ of Shioda invariants for hyperelliptic curves of genus 3. With the results in [IKL+19] and in [Lor20] we can prove the following:

Proposition 3.1.1. *Let $C : y^2 = f(x)$ over K be a hyperelliptic curve of genus 3 with $f \in \mathcal{O}[x]$. Let $p \neq 2, 3, 5, 7$ and assume that $v_{\mathrm{Sh}}(\Delta) > 0$, then C has geometrically bad reduction modulo π.*

Even a stronger result is proved in [LLLR20, Cor. 3.17]:

Proposition 3.1.2. *Assume $p \neq 2, 3, 5$ and 7. Let $C : y^2 = f(x)$ over K be a hyperelliptic curve of genus 3 with $f \in \mathcal{O}[x]$. Then C has potentially good reduction if and only if $v_{\mathrm{Sh}}(D_{14}(f)) = 0$.*

Remark 3.1.3. The reason why the previous results exclude the characteristics $2, 3, 5$ and 7 is that for those characteristics Shioda invariants are not an HSOP (Definition 3.7 in [LLLR20]) for hyperelliptic curves of genus 3. For binary octics, Basson [Bas15] exhibits a HSOP of degree (3, 4, 5, 6, 10, 14) when $p = 7$ and one of degree (4, 5, 6, 7, 8, 9) when $p = 3$. Similar techniques for $p = 5$ lead to a HSOP over $\mathcal{O}$ of degree (4, 6, 6, 12, 14, 20). We can therefore extend Proposition 3.1.2 to all characteristics different from 2 by using these sets instead.

Proposition 3.1.2 is a consequence of a much stronger result. It appears in [Sha80, Prop.2.1] and [Mum77, Lem.5.3] in the equal characteristics setting, in [Bur92, p.122] over the p-adics for $\mathbf{X} = \mathbb{P}(V)$ and in [Sil98] and [STW14] in a dynamical context. We proved it in a more general setting in [LLLR20, Cor. 3.5]. We invite the reader to check in *loc. cit.* the notations in the statement of the theorem. We show it here without more precision only to illustrate the nature and the flavour of the result.

Theorem 3.1.4. *Let $R = \mathcal{O}$ be a discrete valuation ring with field of fractions K and such that the categorical quotient $\mathbf{X}^{\mathrm{ss}}/\!\!/G$ is of finite type (hence projective) over $\mathcal{O}$. Let $\mathsf{x} \in \mathbf{X}^s(K)$. Then there exists an extension $\mathcal{O} \subseteq \mathcal{O}'$ of discrete valuation rings with $K' = \mathrm{Frac}(\mathcal{O}')$ finite over K, and an integral point $\mathfrak{x} \in \mathbf{X}^{\mathrm{ss}}(\mathcal{O}')$ such that $\mathfrak{x}_{K'} \in G(K') \cdot \mathsf{x}$. Moreover, we can ask the image of the closed point of $\mathfrak{x}$ to belong to a minimal orbit.*

3.2 The plane quartic case

As a corollary of Theorem 3.1.4, we prove the following:

Theorem 3.2.1. *(Theorem 3.15 in [LLLR20]) Let K be a discrete valuation field with valuation v, valuation ring $\mathcal{O}$ and residue field k of characteristic $p \geq 0$. Let $\underline{I}$ be a list of invariants which is a HSORG[1] for the ternary quartic forms under the action of $\mathrm{SL}_{3,\mathcal{O}}$. Then a smooth plane quartic $C/K : F = 0$ has potentially good quartic reduction if and only if $v_I(D_{27}(F)) = 0$.*

[1]HSORG stands for *Homogeneous System Of Radical Generators*, see Definition 3.7 in [LLLR20]. In aprticular, a HSOP is a HSORG.

In a down-to-earth language the previous theorem says that if a prime factor of the discriminant of a plane quartic curve can be removed by normalizing the invariants, then there exists an integral plane quartic model of the curve without this factor and hence with good reduction at this prime.

Now even if $v_{norm}(\Delta) > 0$ we still cannot conclude that C has bad reduction: Not all genus 3 curves are plane quartics and it may still have (potentially) good hyperelliptic reduction.

Example 3.2.2. The discriminant of the Klein quartic given by $C : x^3y + y^3z + z^3x = 0$ is equal to 7^7, hence the model $x^3y+y^3z+z^3x = 0$ over $\mathbb{Z}$ has good reduction everywhere except at $\pi = 7$. To study the reduction type of the stable model at 7, notice that C is $\bar{\mathbb{Q}}$-isomorphic to the curve [Elk99, pp.56]:

$$(x^2 + y^2 + z^2)^2 + \sqrt{-7}\alpha^2 \cdot (x^2y^2 + y^2z^2 + z^2x^2) = 0$$

with $\alpha = \frac{-1+\sqrt{-7}}{2}$. Consider now the scheme

$$\mathcal{C} : \begin{cases} t^2 = -(x^2y^2 + y^2z^2 + z^2x^2), \\ \sqrt[4]{-7}\alpha \cdot t = x^2 + y^2 + z^2 \end{cases}$$

in the weighted projective space $\mathbb{P}^{(1,1,1,2)}$ over the ring of integers $\mathcal{O}$ of $K = \mathbb{Q}_7(\sqrt[4]{-7})$. Its generic fiber is isomorphic over K to C whereas the special fiber $\mathcal{C}_k$ is isomorphic over $\bar{\mathbb{F}}_7$ to

$$\begin{cases} t^2 = -(x^2y^2 + y^2z^2 + z^2x^2), \\ 0 = x^2 + y^2 + z^2 \end{cases}$$

which turns out to be the hyperelliptic curve $y^2 = x^8 + 1$.

This example motivates the following definition:

Definition 3.2.3. *([LLLR20, Def. 1.4]) Let C/K be a smooth plane quartic. When $p \neq 2$, we say that C admits a toggle model if there exist an integer $s > 0$, a primitive quartic form $G \in \mathcal{O}[x_1, x_2, x_3]$ and a primitive quadric $Q \in \mathcal{O}[x_1, x_2, x_3]$ with $\bar{Q}$ irreducible such that $Q^2 + \pi^{2s}G = 0$ is K-isomorphic to C. If, moreover, $\bar{Q} = 0$ intersects $\bar{G} = 0$ transversely in 8 distinct $\bar{k}$-points, the model $Q^2 + \pi^{2s}G = 0$ is a good toggle model of C.*

See Theorem 2.9 in [LLLR20] for the definition of a toggle model in characteristic 2.

3.2.1 Hyperelliptic reduction

In [LLLR20] and in collaboration with Lercier, Liu and Ritzenthaler we characterize the hyperelliptic reduction of a plane quartic curve:

Theorem 3.2.4. *([LLLR20, Thm. 1.4]) Let K be a discrete valuation field with residue field of characteristic $p \geq 0$. Let C/K be a smooth plane quartic. Then C admits good hyperelliptic reduction over K if and only if C has a good toggle model over K.*

In terms of invariants, but unfortunately avoiding some characteristics, we have the following characterization:

Theorem 3.2.5. *([LLLR20, Thm. 1.10]) Let K be a discrete valuation field with valuation v, valuation ring $\mathcal{O}$ and a uniformizer π. Let $k = \mathcal{O}/\langle\pi\rangle$ be the residue field of characteristic $p \neq 2, 3, 5$ and 7. Let C/K be a smooth plane quartic defined by $F = 0$. Then C has potentially good hyperelliptic reduction if and only if*

$$v_{DO}(I_3(F)) = 0,\ v_{DO}(I_{27}(F)) > 0 \text{ and } v_\iota(I_3(F)^5 I_{27}(F)) = 0.$$

Under these conditions, one can also obtain an explicit equation for the special fiber (see Proposition 5.6 in [LLLR20]).

Again, for the limitation of the primes in the statement of Theorem 3.2.5, it is just a question about having an HSOP for the invariant ring of plane quartic curves for any characteristic.

While the computation of the invariants and the check of the conditions in Theorem 3.2.5 are straightforward, the criterion in Theorem 3.2.4 is not that easy to check. In order to compute a toggle model and hence a stable model of the curve we proceed as follows:

Theorem 3.2.6. *([LLR18, Thm. 1.6]) Let C be a smooth plane quartic over K with residue field of characteristic different from 2. The curve C has potentially good hyperelliptic reduction if and only if there is a unique integral theta constant of C with positive normalized valuation.*

Thanks to this result, the explicit determination of the bitangents of a plane quartic from a Riemann model (see Equation 3.2.1 in Theorem 3.2.7 looking a bit like a toggle model) and the relation of its coefficients with the values of the theta constants [Web76] we are able to produce an algorithm to compute a good toggle model for a plane quartic having potentially good hyperelliptic reduction, see Section 5 in [LLR18]. This algorithm works for a plane quartic defined over a p-adic field. In a computer, while working with p-adic fields, we need to fix the precision, i.e., the number of digits we consider. In practise, this implies that our algorithm only produces an approximation of the coefficients of a good toggle model.

Theorem 3.2.7. *Let C be a smooth plane quartic curve over $\overline{K}$ of characteristic different from 2. After a linear change of variables, we may assume that 7 bitangents of C (forming an Aronhold system) are given by the equations:*

$$\beta_i : x_i = 0 \quad \beta_4 : x_1 + x_2 + x_3 = 0 \quad \beta_{4+i} : a'_{i1}x_1 + a'_{i2}x_2 + a'_{i3}x_3 = 0,$$

where $i \in \{1, 2, 3\}$. The coefficients a_{ij} satisfy $a'_{ij} = \eta_i a_{ij}$ for some $\eta_i \neq 0$, that are determined, up to sign, by the linear system:

$$\begin{bmatrix} \lambda_1 a'_{11} & \lambda_2 a'_{21} & \lambda_3 a'_{31} \\ \lambda_1 a'_{12} & \lambda_2 a'_{22} & \lambda_3 a'_{32} \\ \lambda_1 a'_{13} & \lambda_2 a'_{23} & \lambda_3 a'_{33} \end{bmatrix} \begin{bmatrix} 1/\eta_1^2 \\ 1/\eta_2^2 \\ 1/\eta_3^2 \end{bmatrix} = \begin{bmatrix} -1 \\ -1 \\ -1 \end{bmatrix},$$

where λ_1, λ_2, λ_3 are given by

$$\begin{bmatrix} \frac{1}{a'_{11}} & \frac{1}{a'_{21}} & \frac{1}{a'_{31}} \\ \frac{1}{a'_{12}} & \frac{1}{a'_{22}} & \frac{1}{a'_{32}} \\ \frac{1}{a'_{13}} & \frac{1}{a'_{23}} & \frac{1}{a'_{33}} \end{bmatrix} \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{bmatrix} = \begin{bmatrix} -1 \\ -1 \\ -1 \end{bmatrix}.$$

After the previous change of variables, the plane quartic C is given by a Riemann model

$$(x_1u_1 + x_2u_2 - x_3u_3)^2 - 4x_1u_1x_2u_2 = 0, \tag{3.2.1}$$

where u_1, u_2, u_3 are given by

$$\begin{cases} u_1 + u_2 + u_3 + x_1 + x_2 + x_3 = 0, \\ \frac{u_1}{a_{i1}} + \frac{u_2}{a_{i2}} + \frac{u_3}{a_{i3}} + a_{i1}x_1 + a_{i2}x_2 + a_{i3}x_3 = 0. \end{cases}$$

Moreover, we can express all the bitangents for this model as:

$$\beta_i : x_i = 0 \qquad \beta_4 : x_1 + x_2 + x_3 = 0 \qquad \beta_{ij} : u_k = 0$$
$$\beta_{4+i} : a_{i1}x_1 + a_{i2}x_2 + a_{i3}x_3 = 0 \quad \beta_{i4} : u_i + x_j + x_k = 0 \quad \beta_{i(4+l)} : \tfrac{u_i}{a_{li}} + a_{lj}x_j + a_{lk}x_k = 0$$
$$\beta_{4(4+i)} : \tfrac{u_1}{a_{i1}(1-a_{i2}a_{i3})} + \tfrac{u_2}{a_{i2}(1-a_{i3}a_{i1})} + \tfrac{u_3}{a_{i3}(1-a_{i1}a_{i2})} = 0 \quad \beta_{56} : \tfrac{u_1}{1-a_{32}a_{33}} + \tfrac{u_2}{1-a_{33}a_{31}} + \tfrac{u_3}{1-a_{31}a_{32}} = 0$$
$$\beta_{57} : \tfrac{u_1}{1-a_{22}a_{23}} + \tfrac{u_2}{1-a_{23}a_{21}} + \tfrac{u_3}{1-a_{21}a_{22}} = 0 \quad \beta_{67} : \tfrac{u_1}{1-a_{12}a_{13}} + \tfrac{u_2}{1-a_{13}a_{11}} + \tfrac{u_3}{1-a_{11}a_{12}} = 0,$$

where $i, l \in \{1,2,3\}$ and $\{i,j,k\} = \{1,2,3\}$.

3.3 Picard curves

Picard curves are plane quartics, but they cannot have hyperelliptic reduction (see for example [ACGH85, p. 13]), so primes dividing the discriminant of Picard curves are only primes of bad reduction or of potentially good quartic reduction. We introduce the following invariants associated to a binary quartic $a_0x^4 + a_1x^3y + a_2x^2y^2 + a_3xy^3 + a_4y^4$:

$$\begin{aligned} q_2 &= 12\,a_0\,a_4 - 3\,a_1\,a_3 + {a_2}^2\,, \\ q_3 &= 72\,a_0\,a_2\,a_4 - 27\,a_0\,{a_3}^2 - 27\,{a_1}^2 a_4 + 9\,a_1\,a_2\,a_3 - 2\,{a_2}^3, \end{aligned}$$

and the discriminant D_6 which satisfies the relation $3^3 \cdot D_6 = 4\,q_2^3 - q_3^2$.

Theorem 3.3.1. *([LLLR20, Thm. 4,7]) Let K be a discrete valuation field with valuation v, valuation ring $\mathcal{O}$ and a uniformizer π. Let $k = \mathcal{O}/\langle\pi\rangle$ be the residue field of characteristic $p \neq 2$ and 3. The curve $\mathcal{C}_0 : -x_2^3x_3 + G_0(x_1, x_3) = 0$ where $G_0 = x^4 + bx^2z^2 + cxz^3 + dz^4 = 0$ has potentially good quartic reduction if and only if*

$$\min(6v(b), 3v(d)) \geq v(D_6(G_0))\,.$$

A stable model $\mathcal{C}$ is given by $\mathcal{C} : -x_2^3x_3 + G(x_1, x_3) = 0$ where

$$G = x_1^4 + b/\mathfrak{p}^6\, x_1^2x_3^2 + c/\mathfrak{p}^9\, x_1x_3^3 + d/\mathfrak{p}^{12}\, x_3^4 = 0,$$

$\mathfrak{p} = \pi^{v(D_6(G_0))/36}$, and the map $\mathcal{C} \to \mathcal{C}_0 : (x_1 : x_2 : x_3) \mapsto (\mathfrak{p}^3x_1 : \mathfrak{p}^4x_2 : x_3)$.

The equivalent versions for $p = 2, 3$ are Theorem 4.8 and 4.9 in [LLLR20]. Picard curves are a special type of plane quartics. So, these results are just a reformulation of Theorem 3.2.1. But instead, they are stated in terms of much more convenient invariants for the family of Picard curves.

There is another interesting invariant associated to a Picard curve of the form $y^3 = x^4 + ax^2 + bx + c$. It is the invariant b. Primes for which $v_{norm}(b) > 0$ produce special fibers with extra automorphisms. I studied primes dividing this invariant in my work [KLS20] with Kılıçer and Streng. More precisely,

Lemma 3.3.2. *([KLS20, Lemma 3.1]) Let C be a Picard curve of genus 3 over a number field L and let $\mathfrak{p} \nmid 6$ be a prime of $\mathcal{O}_L$. Let $j = u/b^\ell$ be an absolute Picard curve invariant (i.e., $u \in \mathbb{Z}[a, b, c]$ has weight 3ℓ).*

If $\mathrm{ord}_\mathfrak{p}(j(C)) < 0$, then after replacing L with an extension and C with an isomorphic curve, we are in one of the following cases:

1. *$C : y^3 = x^4 + ax^2 + bx + 1$ with $a, b \in \mathcal{O}_L$ such that $b \equiv 0$ and $a \equiv \pm 2$ modulo $\mathfrak{p}$. The reduction of this equation (from $\mathcal{O}_L$ to $\mathcal{O}_L/\mathfrak{p}$) 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 $b, c \in \mathfrak{p}$. 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 $a, b \in \mathcal{O}_L$ such that $b \equiv 0$ and $a \not\equiv \pm 2$ modulo $\mathfrak{p}$. The reduction of this equation is the smooth curve $y^3 = x^4 + \overline{a}x^2 + 1$ of genus 3, where $\overline{a} = (a \bmod \mathfrak{p})$.*

Chapter 4

Reduction type of genus 3 curves

We have already discussed in Chapter 3 how to distinguish (potentially) good hyperelliptic reduction from (potentially) good plane quartic reduction from geometrically bad reduction for plane quartics and the last two situations for hyperelliptic curves. Now we focus on the different types of bad reduction.

It is a classical idea to study the collision of the ramification points of hyperelliptic curves modulo a prime to determine its reduction. This idea is formalized and set in motion in C. Mestrait thesis and papers with collaborators [Mai17, DDMM18, DDMM19]. They determine the reduction type of hyperelliptic curves of genus 2 and 3 in terms of the configuration of collisions in the reduction of the ramification points (known as the cluster picture of the model, see Definition 4.1.2). With ideas in my paper [Lor20, Section 6.1], my Ph.D. student is working on determining the cluster picture for hyperelliptic curves of genus 2 and 3 (and hence the reduction type) in terms of the valuations of suitable invariants in order to (re-)obtain Liu's Theorem 1.2.1 and the equivalent statement for genus 3.

The study of the (bad) reduction types for Picard curves (and in general for superelliptic curves $C : y^\ell = f(x)$) can also be done by studying the collisions of the ramification locus of the ℓ-cyclic morphism $C \to \mathbb{P}^1$, see [BW15, BBW17, BW17, BKSW20]. The hyperelliptic case may also be understood as the particular case of this setting with $\ell = 2$.

These arguments cannot be generalized to any plane quartic curve, but we still may try to use them for determining the reduction type in some particular cases where we still have "nice" morphisms to $\mathbb{P}^1$. This is the idea in [BCK+21] where we study and determine the reduction type of genus 3 curves being a Galois cover of $\mathbb{P}^1$ with Galois group isomorphic to the Kein group. We strongly make use of the concept of *admissible cover*, see [RW06, Wew99].

I leave for a future project to characterize the bad reduction type of general plane quartic curves. As mentioned before, different techniques should be used here.

4.1 Hyperelliptic curves

As mentioned before the strategy to determine the reduction type of a hyperelliptic curve C is looking at its cluster picture. There is only one type of bad reduction for elliptic curves

and 6 types for genus 2 curves, see Theorem 1.2.1. The number of possibilities for the reduction type grows fast as the genus does. For hyperelliptic curves of genus 3 there are 32 types of bad reduction [DDMM19, Table 9.1]; distinguishing all of them by inspecting several invariants valuations is a hard work. However, if for some reason (e.g. the curve C having CM) we know that the Jacobian of the curve has compact reduction (i.e., the intersection graph of the irreducible components of C is a tree), then there are only 2 cases for the type of bad reduction. In Example 1.2.4 we already showed that for genus 2 CM curves, only one type of bad reduction is possible.

Theorem 4.1.1. *([Lor20, Thm. 6.5]) Let $C : y^2 = f(x)$ be a hyperelliptic genus 3 curve defined over a discrete valuation ring $\mathcal{O}_K$ whose residue field k has characteristic different from 2 and such that the reduction of the Jacobian of its stable model is still a p.p.a.v. of dimension 3. Then,*

(i) C has potentially good reduction if and only if $v_{Sh}(D) = 0$.

(ii) C has geometrically bad reduction and the special fiber of its stable model over $\bar{k}$ is the union of one elliptic curve and a genus 2 curve intersecting at one point if and only if $v_{Sh}(D) > 0$ and $v_{Sh}(I_{20}) = 0$.

(iii) C has geometrically bad reduction and the special fiber of its stable model over $\bar{k}$ is the union of 3 elliptic curves, two of them intersecting the third one at one point, if and only if $v_{Sh}(D) > 0$ and $v_{Sh}(I_{20}) > 0$.

The strategy to prove this result is the following: to determine if the reduction is good or bad we use Proposition 3.1.2. If it is bad, there are only two options, the reduction is the union of a genus 2 curve and an elliptic curve or the union of 3 elliptic curves. We obtain the cluster pictures corresponding to these two options by looking at the theta constants of decomposable principally polarized threefolds [RF74, Thm. 1.11] and using Takase formulas [Tak96]. This gives to us the valuations of the differences of the roots of a model of the curve, so the corresponding cluster pictures. The following invariant is defined:

$$I_{20} = \sum_{S_8} \frac{\prod_{i<j}(ij)^4}{(123)^4(45678)^2} = \sum_{S_8}(45678)^2(123,45678)^4$$

It is constructed in such a way that only vanishes for one of these two configurations: for the one having 2 sets of 3 points collapsing but not for the one only having a set of 3.

4.1.1 General case

With lot of effort and extra ideas, my Ph.D. student Harold Favereau is using these combinatorial tools to described the reduction type of hyperelliptic curves of genus 3 [Fav20]. He is looking for combinations of Tusyumine invariants allowing one to distinguish between the 32 cluster pictures (up to equivalence). For the reader convenience we recall here the precise definition of the cluster pciture:

Definition 4.1.2. *Let $C : y^2 = \prod_{i=1}^{d}(x-\alpha_i)$ be an integer model of a hyperelliptic curve defined over a discret valuation field K. Let $\mathcal{R} = \{\alpha_i : i = 1...d\}$.*

- *([DDMM18, Def. 1.1]) A cluster is a nonempty subset $s \subseteq \mathcal{R}$ of the form $s = D \cap \mathcal{R}$ for some disc $D = \{x \in K \mid v(x-z) \geq d\}$, for some $z \in K$ and $d \in \mathbb{Q}$. If $|s| > 1$, then s is called proper and we associate to it a depth $d_s = \min\{r, r' \in s : v(r-r')\}$.*
- *([DDMM18, Def. 1.3]) If $s' \subsetneq s$ is a maximal subcluster, then we call s' a child of s. We further call s the parent of s' and write this as $s = P(s')$.*
- *The cluster picture of a squarefree polynomial is the collection of all clusters of its roots.*
- *The exterior aspect of a cluster picture is the collection of maximal subclusters of the cluster $s = \mathcal{R}$.*

The first step to described the reduction type of hyperelliptic curves of genus 3 is to distinguish between the 10 exterior aspects of cluster pictures in genus 3 as in Figure 4.1.

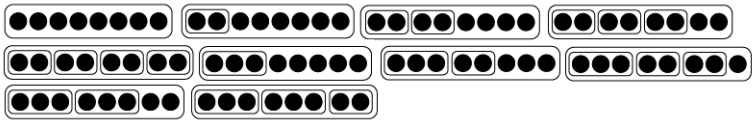


Figure 4.1: Exterior aspect of cluster pictures in genus 3

Theorem 4.1.3. *([Fav20]) The exterior aspect of the cluster picture of a genus 3 hyperelliptic curve is determined by looking at the valuations of the invariants:*

$$
\begin{aligned}
I_2 &= a_0^2 \sum (12)^2(34)^2(56)^2(78)^2 \\
I_4 &= a_0^4 \sum (12)^4(345)^2(678)^2 \\
I_6 &= a_0^6 \sum (1234)^2(5678)^2 \\
D &= a_0^{14} \prod_{i<j} (ij)^2 \\
M &= a_0^{30} \sum (12, 345678)^5(345678)^4 \\
N &= a_0^{10} \sum (1234, 5678)^1(5678)^2(12, 34)^3 \\
P &= a_0^{16} \sum (123456, 78)^2(135)^6(246)^6(78)^4 \\
Q &= a_0^{20} \sum (123, 45678)^4(45678)^2 \\
R &= a_0^{30} \sum (123, 45678)^6(45, 678)^4(678)^2 \\
S &= a_0^{10} \sum (123, 45678)^2(45)^2(67)^2(84)^2(56)^2(78)^2 \\
T &= a_0^{16} \sum (123456, 78)^2(123, 456)^4(78)^4
\end{aligned}
$$

and following the instructions in Figure 4.2.

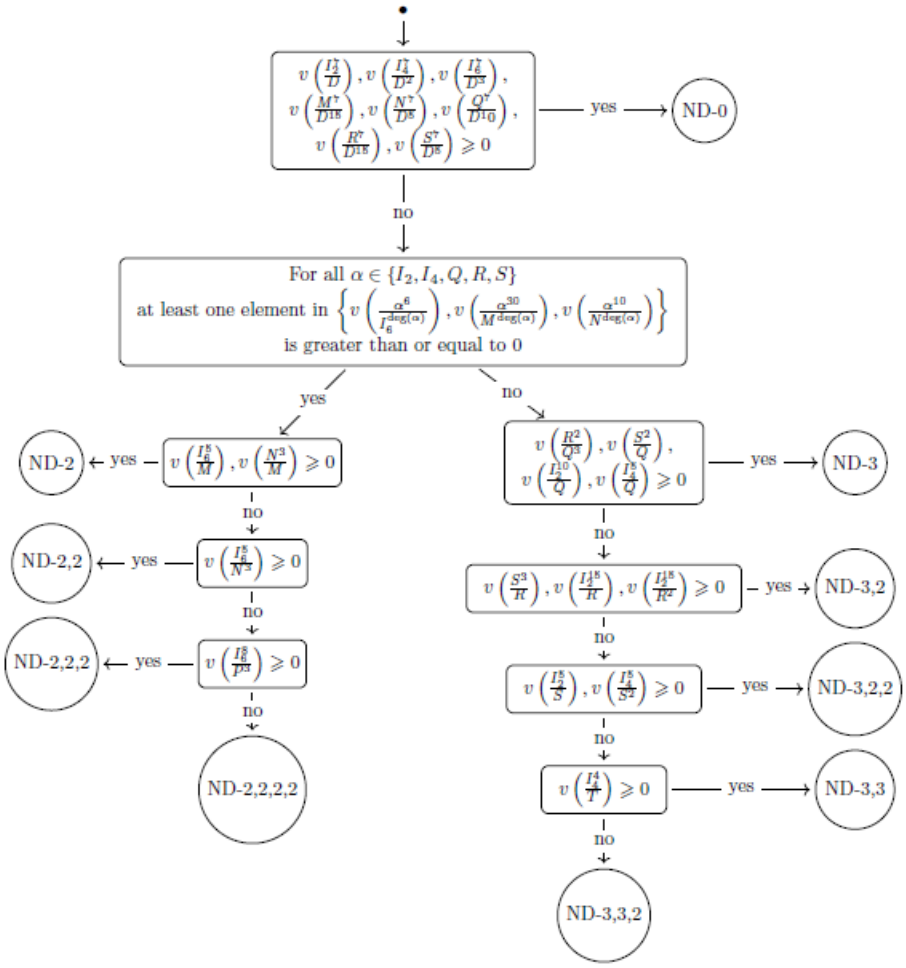


Figure 4.2: Tree to determine the exterior aspect of cluster pictures in genus 3

4.2 Ciani plane quartics

In this section I give my results with I. Bouw, N. Coppola, P. Kilicer, S. Kunzweiler and A. Somoza in [BCK+21] about the characterization of the reduction type of Ciani plane quartics in terms of the valuations of their invariants as introduced in Propositions 2.3.2 and 2.3.4.

Theorem 4.2.1. *([BCK+21, Thm. 3.7 and 3.8]) Let Y be a plane quartic curve defined by*

$$Ax^4 + By^4 + Cz^4 + ay^2z^2 + bx^2z^2 + cx^2y^2 = 0.$$

Let $\Delta(Y)$ be the normalized discriminant of the quartic Y, and let $\Delta(X)$ be the normalized discriminant of the conic X. If $\nu(I_3'') = 0$ and the valuation of $\Delta(Y)$ is positive, Y has geometric bad reduction and one of the cases in Table 4.2.1 occurs. If $\nu(I_3'') > 0$ and the valuation of $\Delta(Y)$ is positive, Y has geometric bad reduction and one of the cases in Table 4.2.2 occurs.

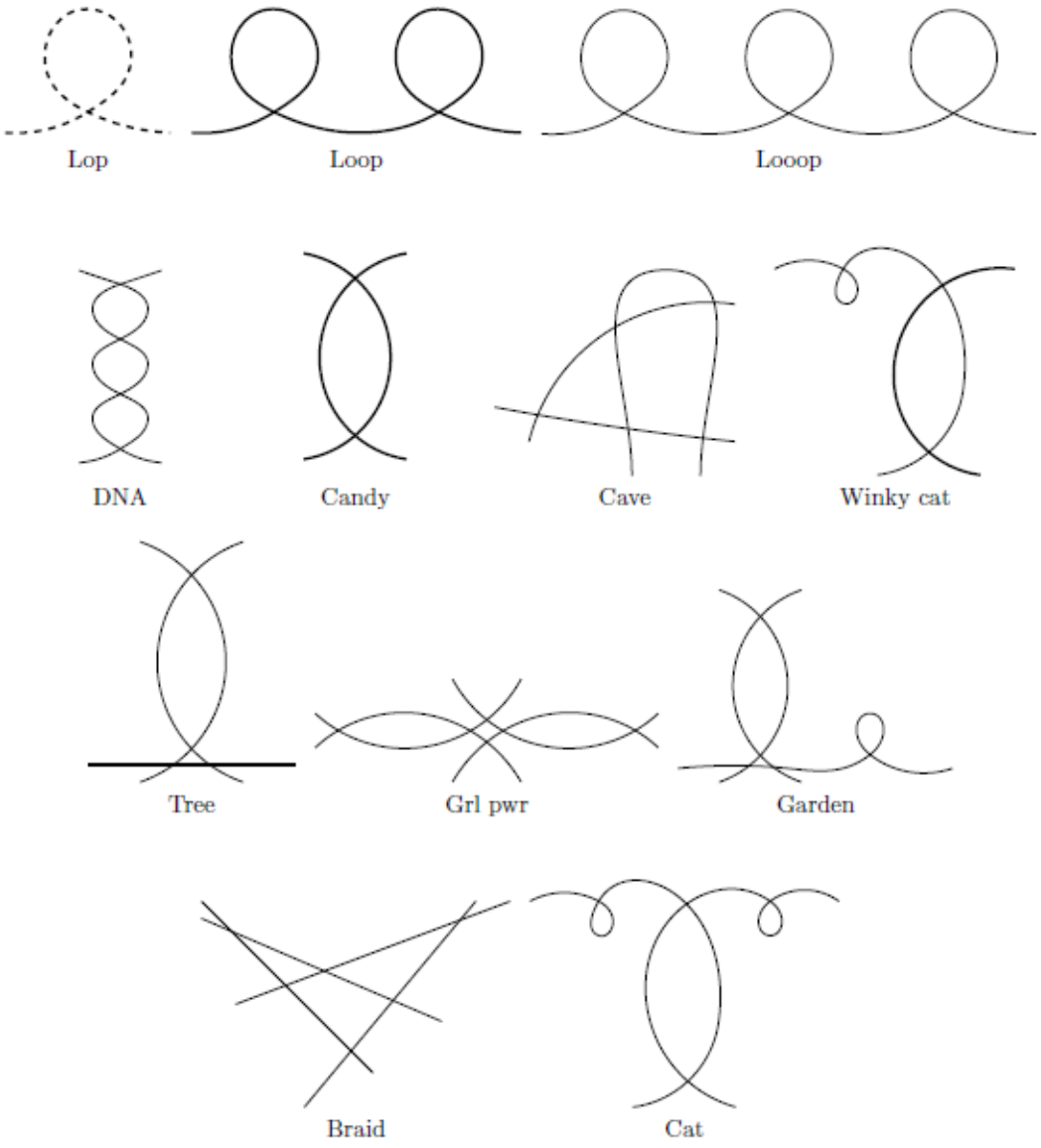
The reduction types corresponding to the names in the last column of Tables 4.2.1 and 4.2.2 are the ones in Figure 4.3. The information on the second-to-last column is about the decorated graph, that is the analogous to the cluster picture but for Galois covers with Galois group the Klein group. I invite the interested reader to check out the paper [BCK+21, Section 2 and Appendix A] for more details.

	$\nu(I_3)$	$\nu(I_3')$	$\nu(I_3'')$	$\nu(I_6)$	$\nu(I)$	Other conditions	Decorated graphs	Stable curve
(a)	$=0$		$=0$	>0	$=0$		II.3	Loop
(b)	$=0$	$=0$	$=0$	>0	>0		III.1	DNA
(c)	$=0$	>0	$=0$	>0	>0		IV*.1	Braid
(d)	>0	$=0$	$=0$	$=0$	$=0$		II.4	Lop
(e)	>0	$=0$	$=0$	>0	$=0$		III.2	Looop
(f.i)	>0	$=0$	$=0$	>0	>0	$2\nu(I)>\nu(I_3)+\nu(I_6)>2\nu(I_3)$ or $\nu(I_3)<\nu(I)<\nu(I_6)$	IV.1	Grl Pwr
(f.ii)						$2\nu(I)>\nu(I_3)+\nu(I_6)>2\nu(I_6)$ or $\nu(I_3)>\nu(I)>\nu(I_6)$	IV.3	Cat
(f.iii)						$2\nu(I)>\nu(I_3)+\nu(I_6)=2\nu(I_3)$ or $\nu(I_3)=\nu(I)=\nu(I_6)$	II.1	Candy
(f.iv)						$\nu(I)<\nu(I_3)$, $\nu(I)<\nu(I_6)$	IV.2	Garden
(f.v)						$\nu(I)=\nu(I_3)<\nu(I_6)$	III.5	Tree
(f.vi)						$\nu(I)=\nu(I_6)<\nu(I_3)$	III.6	Winky Cat
(g)	>0	$=0$	$=0$	$=0$	>0		III.3	Loop
(h)	>0	>0	$=0$	$=0$	>0		IV*.3	Looop

Table 4.2.1: Cases of Theorem 4.2.1 with $\nu(I_3'')=0$.

	$\nu(I_3)$	$\nu(I_3')$	$\nu(I_3'')$	$\nu(I_6)$	$\nu(I)$	Other conditions	Decorated graphs	Stable curve
(a)	$=0$		>0	$=0$			II.2	DNA
(b.i)	$\nu(I_3+I_3')=0$		>0	>0	$=0$	$0<\nu(I_3'')<\nu(I_6)$	IV*.2	DNA
(b.ii)						$\nu(I_3'')>\nu(I_6)>0$	IV.5	Braid
(b.iii)						$\nu(I_3'')=\nu(I_6)>0$	III.4	Candy
(c.i)	$=0$	>0	>0	>0	>0	$\nu(I_6^2)=\nu(I_3I_3''^3)$, $\nu(I_3'^4)\geq\nu(I_3I_3'')$	I	Good (hyper.)
(c.ii)						$\nu(I_6^2)>\nu(I_3I_3''^3)$, $\nu(I_3'^4)\geq\nu(I_3I_3'')$, and $\nu(I_3'^4-4I_3I_3'')=\nu(I_3I_3'')$	II.3	Loop
(c.iii)						$\nu(I_6^2)>\nu(I_3I_3''^3)$, $\nu(I_3'^4)=\nu(I_3I_3'')$, and $\nu(I_3'^4-4I_3I_3'')>\nu(I_3I_3'')$	III.1	DNA
(c.iv)						$\nu(I_6^2)<\nu(I_3I_3''^3)$ and $\nu(I_3'^4)\geq\nu(I_3I_6)$	II.2	DNA
(c.v)						$12\nu(I_3')<3\nu(I_3I_3'')<2\nu(I_3I_6)$	IV*.2	DNA
(c.vi)						$12\nu(I_3')<2\nu(I_3I_6)<3\nu(I_3I_3'')$	IV.5	Braid
(c.vii)						$12\nu(I_3')<2\nu(I_3I_6)=3\nu(I_3I_3'')$	III.4	Candy
(d)	>0		>0	$=0$	$=0$		III.7	Cave
(e)	>0	$=0$	>0		>0		IV.4	Braid

Table 4.2.2: Cases of Theorem 4.2.1 with $\nu(I_3'')>0$.



Admissible covers. The genus-2 components correspond to the thick dashed lines, and the genus-1 components correspond to the thick solid lines. The remaining components have genus 0.

Figure 4.3: Bad reduction types for Ciani plane quartics.

Chapter 5

Bounds on the primes of bad reduction of genus 3 curves

As we mentioned in the Introduction, in order to prove the correctness of class polynomials computed by approximating the value of modular invariants we need to control their denominators. Even if different choices for these absolute modular invariants are possible, a natural condition to impose is to have a power of the discriminant of the curves in their denominators. So under some conditions only primes of bad reduction will appear in the denominators of the coefficients of the class polinomials, e.g. [IKL+19, Thm 1.1]. The purpose of this section is to state the results by me and my many collaborators on bounding and controlling the primes of bad reduction of CM curves of genus 3, see [BCL+15, KLL+20, IKL+20]. Some results on bounding their exponents on the discriminant are also showed.

In this section we assume that X is a genus 3 curve with CM by a sextic order $\mathcal{O} \subseteq K$ with primitive CM-type Φ, i.e., with simple Jacobian. We will define a generalization of the embedding problem for genus 3 as it is done in [GL07] for genus 2. This will allow us to give a bound depending on $\mathrm{disc}(\mathcal{O})$ for the primes of bad reduction of X.

5.1 Bounds for the primes

We start by proving the existence of a special embedding when having a prime of bad reduction. We will next bound the primes for which such an embedding may exist.

Proposition 5.1.1. *Let X be a curve of genus 3 defined over a number field L with CM by an order $\mathcal{O}$ in a sextic CM-field K. Suppose that the Jacobian J of X is simple. Let M be a finite extension of L such that J has good reduction everywhere and the stable model of X is defined over $\mathcal{O}_M$. If X has bad reduction modulo a prime ideal $\mathfrak{p} \subset \mathcal{O}_M$, then there exists a supersingular elliptic curve E defined over $\overline{\mathbb{F}}_p$ with endomorphism ring $\mathcal{R}$, a polarization $\lambda = \begin{pmatrix} \alpha & \beta \\ \beta^\vee & \gamma \end{pmatrix}$ on E^2 where $\alpha, \gamma \in \mathbb{Z}_{>0}$, $\beta \in \mathcal{R}$, $n := \alpha\gamma - \beta\beta^\vee \in \mathbb{Z}_{>0}$ and a ring embedding*

$$\iota : \mathcal{O} \hookrightarrow \mathcal{M}_3(\mathcal{R}/n) \tag{5.1.1}$$

such that the Rosati involution coming from the polarization $1\times\lambda$ *induces complex conjugation on* $\mathcal{O}$ *and the entries of the first row of each matrix in* $\iota(\mathcal{O})$ *are in* $\mathcal{R}$*.*

The ideas of the proof of Proposition 5.1.1 are the following: if $\mathfrak{p}$ is a prime of bad reduction then the reduction of the Jacobian is still a principally polarized abelian threefold (since it has CM and hence always potentially good reduction [ST68]). This implies that it is isomorphic to a product $E \times A$ where A is principally polarized abelian surface. By a dimension argument on the endomorphism ring we prove that $A \sim E^2$ and E is a supersingular elliptic curve. We write $K = \mathbb{Q}(\sqrt{-\mu})$ for some $\mu \in K^+$ and we consider the reduction of the endomorphism μ as an endomorphism of $E \times A$. With this we construct a particular isogeny from A to E^2 and by conjugation of the embedding $\mathcal{O} = \mathrm{End}(J) \hookrightarrow \mathrm{End}(\overline{J}) = \mathrm{End}(E \times A)$ by this isogeny we obtain an embedding as the one in the statement of Proposition 5.1.1.

Proposition 5.1.2. *If* K *contains no imaginary quadratic field then the entries of* ι *are not contained in a field. Otherwise the entries of* ι *are neither contained in a field except if* $p \mid 6dn$ *where* $\mathbb{Q}(\sqrt{d}) \subseteq K$*.*

The proof of this proposition is a consequence of the results in [KLL+20, Sec. 5] and it is based on the primitivity of the CM-type.

Proposition 5.1.3. *([IKL+20, Sec. 4.1]) If* C *has extra automorphisms, i.e., automorphisms inducing elements different from* ± 1 *in* $J(C)$*, then* K *contains an imaginary quadratic field* $\mathbb{Q}(\sqrt{d})$*,* $p \mid 6dn$ *and* $\iota(\sqrt{d})$ *is a multiple of the identity.*

This extra automorphism condition is for instance verified when $\mathbb{Q}(i) \subseteq K$. Which is a very interesting case as explained at the end of Section 2.2.

Theorem 5.1.4. *([KLL+20, Thm. 1.1] improved as in [IKL+20]) Let* $K = \mathbb{Q}(\eta)$ *be a sextic CM-field with* η *defined by an integral equation* $\eta^6 + A\eta^4 + B\eta^2 + C = 0$*. Let* $\mathcal{O}$ *be an order in* K *containing* η*. Let* X/M *be a curve of genus 3 with absolutely simple Jacobian and CM by* $\mathcal{O}$*. Let* $\mathfrak{p} \subset \mathcal{O}_M$ *(lying above* p*) be a prime of geometrically bad reduction. Then we have* $p < A^8$*.*

In the case in which X has extra automorphisms the previous theorem can be substantially improved to produced not only a bound but a very small and precise list of primes, see [IKL+20, Sec. 6].

The proof of Theorem 5.1.4 is based on clever manipulations on the entries of the embedding problem to bound the norms of certain elements. Then the "Small norm elements commute" Lemma in [GL07, Lemma 2.2.1] and Proposition 5.1.2 give a contradiction for the existence of such an embedding if the prime p is too big.

5.1.1 Picard curves

Even if Theorem 5.1.4 holds for CM Picard curves, in [KLS20] we considered different invarians for Picard curves and we also computed a bound for the primes in the denominators of such invariants (see Section 3.3).

Theorem 5.1.5. *([KLS20, Thm. 2.2]) Let X be a Picard curve of genus 3 over a number field L with $\mathrm{End}(\mathrm{Jac}(X)_{\bar{L}})$ isomorphic to an order $\mathcal{O}$ of a number field K of degree 6. Let K_+ be the real cubic subfield of K. Let $\mu \in \mathbb{Z} + 2\mathcal{O}$ be such that $K_+ = \mathbb{Q}(\mu)$.*

Let $j = u/b^\ell$ be an absolute Picard curve invariant. Let $\mathfrak{p}$ be a prime of L lying over a rational prime p. If $\mathrm{ord}_{\mathfrak{p}}(j(X)) < 0$, then

$$p \leq \mathrm{tr}_{K_+/\mathbb{Q}}(\mu^2)^3 \qquad \text{and} \qquad p \leq \left(1 + \frac{16}{\pi}|\Delta(\mathcal{O}_+)|^{1/2}\right)^3 < 196|\Delta(\mathcal{O}_+)|^{3/2}.$$

This theorem has been used by Arora and Eisenträger [AE19] to implement class polynomials for CM Picard curves.

5.2 Solutions for the embedding problem

In order to bound the primes in the denominators we need to compute solutions to the embedding problem, and in order to find the exponents in the denominators we have to understand the geometry of the solutions.

We implemented in Sage [S+20] an algorithm to compute the solutions [IKL+20], and we computed them for several CM-fields. This algorithm that was extremely slow in its first versions, it is now very optimized and compute the solutions for each field in just a few hours (just few seconds if the extra-automorphisms condition is satisfied).

If a prime is of bad reduction we will find a solution to the embedding problem and we will detect it. However, and contrary to the genus 2 case, we are not able to prove the reciprocal; that is, that finding a solution to the embedding problem for $(\mathcal{O}, p)$ implies the existence of a genus 3 curve with CM by $\mathcal{O}$ and bad reduction at a prime $\mathfrak{p} \mid p$. This is due to the lack of control of the primitivity of the CM-type of the solutions we compute. More details on this may be found in [IKL+20, Sec. 2.1]. Nevertheless, the algorithm is useful to find bounds for the primes in the denominators, and after inspection of the run examples we have not found so far a solution for a pair $(\mathcal{O}, p)$ not providing a curve with bad reduction.

5.2.1 Examples and explanations

We start by considering the list of CM hyperelliptic curves of genus 3 defined over $\mathbb{Q}$ (the CM-fields are computed in [Kıl16, Kıl17] and the equations are computed with the algorithm in [Wen01, BILV16] with the corrections in [LS20, Appendix]). These equations are showed in [IKL+19, Sec. 5.2]. By Proposition 3.1.2 and its generalization we know that all primes $p \neq 2$ appearing in the minimal discriminant of these curves are indeed primes of bad reduction.

The CM-fields corresponding to the curves (6)–(8) in Table 5.2.1 have $h_K/h_{K_+} = 4$. Hence, by Theorem 4.3.1 in [Kıl16], there are 4 curves with CM by the maximal orders of these three CM-fields: only one of them is defined over $\mathbb{Q}$ and the other three are defined over K_+. The ones defined over K_+ are represented by the cases marked by *. These curves defined over K_+ are Galois conjugate, we show the norm of their discriminant in the second column of the table.

Curve X	Minimal discriminant of X	No. of embeddings
(1)	$7^{24} \cdot 11^{12}$	$7 \cdot 11$
(2)	3^8	3
(3)	1	1
(4)	1	1
(5)	$3^8 \cdot 5^{16}$	$3 \cdot 5$
(6)	$2^? \cdot 11^{24}$	$2^? \cdot 11^2 \cdot 47$
(6)*	$2^? \cdot 11^{12} \cdot 47^{24}$	
(7)	$2^?$	$2^? \cdot 23$
(7)*	$2^? \cdot 23^{24}$	
(8)	$2^? \cdot 3^8$	$2^? \cdot 3^4 \cdot 7 \cdot 31 \cdot 47 \cdot 79$
(8)*	$2^? \cdot 3^? \cdot 7^? \cdot 31^{12} \cdot 47^{24} \cdot 79^{24}$	

Table 5.2.1: The number of embeddings is showed multiplicatively and up to equivalence.

There are 29 non-hyperelliptic curves of genus 3, i.e., plane quartics, with CM by a maximal order in a sextic CM-field and defined over the rationals, see [KLL+18] for the curve equations[1]. The corresponding CM-fields were computed in [Kıl16]. We also run our algorithm for some of them: namely $X_3, X_5, X_6, X_9, X_{10}$ and X_{12} in [KLL+18]. In [LLLR20, Table 4], the reduction type of these plane quartics at every prime $p \neq 7$ is determined with the results in the loc. cit. paper. However, the reduction type at 7 cannot be decided to be geometrically bad or potentially good hyperelliptic. We run our algorithm (see Table 5.2.2) and we did not find any solution for $p = 7$ for the last three curves, proving in this way that the they have potentially good hyperelliptic reduction. For the first three we found solutions, which seems to support that the reduction type is geometrically bad. However, since for genus 3 we have not proved yet that finding a solution to the embedding problems implies bad reduction, we cannot conclude.

Curve	$I_{27}^{\min}$	Number of solutions for $p = 7$
X_3	$2^{29} \cdot 3^{36} \cdot 5^{36} \cdot 7^7 \cdot 233^{14} \cdot 356399^{14}$	> 0
X_5	$2^{29} \cdot 3^{51} \cdot 7^7 \cdot 37^{14} \cdot 127^{14}$	> 0
X_6	$2^{29} \cdot 3^{51} \cdot 7^7 \cdot 17^{12} \cdot 127^{14} \cdot 211^{14} \cdot 20707^{14}$	> 0
X_9	$-2^{42} \cdot 3^{18} \cdot 5^{12} \cdot 7^{14} \cdot 79^{14} \cdot 233^{14} \cdot 857^{14}$	0
X_{10}	$-2^{42} \cdot 3^{18} \cdot 7^{14} \cdot 41^{14} \cdot 71^{14}$	0
X_{12}	$2^5 \cdot 3^{18} \cdot 7^{14} \cdot 11^9 \cdot 5711^{14} \cdot 730642034 93^{14}$	0

Table 5.2.2: CM plane quartics over $\mathbb{Q}$ for which the reduction type at 7 was not known.

[1]The correctness of some of these curve equations is verified with the results in [CMSV19]

5.3 Bounds for the exponents

Let X be CM hyperelliptic curve of genus 3 defined over a number field L. Let M/L be a finite extension such that $J(X)$ has good reduction over M and the theta constants of X are also defined over M. Let $\mathfrak{p} \subset \mathcal{O}_M$ be a prime ideal lying above p. Let ν be the valuation in M given by $\nu(p) = 1$. Suppose that X has bad reduction at $\mathfrak{p}$. Then, by Proposition 6.2 in [Lor20] and its proof we can assume that the valuations of the theta constants with theta characteristics

$$\left[\begin{smallmatrix}011\\011\end{smallmatrix}\right], \left[\begin{smallmatrix}011\\111\end{smallmatrix}\right], \left[\begin{smallmatrix}111\\011\end{smallmatrix}\right], \left[\begin{smallmatrix}101\\101\end{smallmatrix}\right], \left[\begin{smallmatrix}101\\111\end{smallmatrix}\right], \left[\begin{smallmatrix}111\\101\end{smallmatrix}\right], \left[\begin{smallmatrix}110\\110\end{smallmatrix}\right], \left[\begin{smallmatrix}110\\111\end{smallmatrix}\right], \left[\begin{smallmatrix}111\\110\end{smallmatrix}\right], \tag{5.3.1}$$

are $v_1, v_1, v_1, v_1 + v_2, v_1 + v_2, \infty, v_2, v_2, v_2$ with $0 \leq v_1 \leq v_2$ and $v_2 > 0$, while all other theta constants have zero valuation. In this situation, $\nu(\Delta) = 12(v_1 + v_2) \leq 24v_2$.

Lemma 5.3.1. *([IKL+20]) With notation above, we have:*

$$v_2 = \max\{e : J(X) \simeq_{ppav} \tilde{E} \times \tilde{A} \mod \mathfrak{p}^e\}.$$

We want to be able to read a bound for v_2 in terms of a solution to the embedding problem. For this we will use the following result by Gross:

Theorem 5.3.2. *[Gro86, Proposition 3.3] Let $\tilde{E}$ be a CM elliptic curve over a number field M such that $E = \tilde{E} \mod \mathfrak{p}$ is supersingular. Let $\mathcal{R}_\infty = \mathrm{End}(\tilde{E})$ and $\mathcal{R} = \mathcal{R}_1 = \mathrm{End}(E)$, then $\mathrm{End}(\tilde{E} \mod \mathfrak{p}^e) = \mathcal{R}_e = \mathcal{R}_\infty + p^{e-1}\mathcal{R}$, where $p = \mathfrak{p} \cap \mathbb{Z}$.*

We also give a generalization of the "Small norm elements commute" Lemma in [GL07, Lemma 2.2.1]:

Lemma 5.3.3. *([IKL+20]) Let $x, y \in \mathcal{R}_{e+1}$ not commuting, then $p^{2e+1} \leq 4N(x)N(y)$.*

That we use to prove the following:

Proposition 5.3.4. *Let S be a solution to the embedding problem with $p \nmid n$ or K not containing an imaginary quadratic field. Then*

$$v_2 \leq \frac{1}{2}(1 + \log_p(4 \max(\mathrm{N}(x_i)^2)))$$

where x_i are as in [IKL+20, Sec. 3.2].

We are still working on a general bound that works for any sextic CM-field.

5.3.1 An arithmetic intersection formula

Let $\mathcal{A}_3$ be the Siegel modular space of p.p.a.v. of dimension 3. The locus of hyperelliptic Jacobians is given by the following conditions on the Siege modular forms: $\chi_{18} = 0$ and $\Sigma_{140} \neq 0$, see [Igu67, Lemma 11]. The locus $\chi_{18} = \Sigma_{140} = 0$ corresponds to the elements of $\mathcal{A}_3$ with decomposable Jacobian, denote it by G_1.

Let K be any sextic CM-field. The primes of bad reduction of curves with CM by K are those which appear in the arithmetic intersection of the CM points by K with the locus G_1.

Our bound for the number of solutions to the embedding problem and Proposition 5.3.4 give us a bound (at least in the case in which K does not contain an imaginary quadratic field) for $(CM(K)_{pr}.G_1)_\ell$ where

$$CM(K)_{pr} = \sum CM(K, \Phi),$$

with $CM(K, \Phi)$ the set of points in $\mathcal{A}_3$ such that there is an embedding $\iota : \mathcal{O}_K \to End(A)$ of type Φ, where Φ is a primitive CM-type and the sum goes through all equivalence classes of such CM-types.

Assuming a relation as in [Yan13, Sec. 9] between this number and the discriminant of the curves, we also obtain a bound for the denominators of genus 3 class polynomials.

The fact of only getting a bound and not an exact formula as in [LV15, Thm. 2.1] is due to not having proved yet a statement as in the genus 2 case asserting that a solutions to the embedding problem in genus 3 implies the existence of a CM curve by the given order with bad reduction at the given prime.

Chapter 6

Conclusion

As a very brief summary of the results I obtained during the last years and I expounded in this report, I can say that together with my collaborators I:

- obtained *modular expressions* for genus 3 hyperelliptic curves invariants. I also found *useful invariant expressions* in terms of the differences of their roots.
- computed *generators for the invariant ring* of Ciani Plane quartics in characteristic different from 2.
- distinguished between potentially good quartic reduction, potentially good *hyperelliptic reduction* and geometrically bad reduction for plane quartic curves.
- determined and characterized the *reduction type* of Ciani plane quartics in terms of the valuations of their invariants.
- idem with genus 3 hyperelliptic curves.
- found *bounds for the primes in the denominators* of class polynomials for hyperelliptic genus 3 curves, Picard curves and in general for primes of bad reduction of CM curves of genus 3.
- implemented an algorithm for computing the *solutions to the embedding problem* in genus 3.
- gave *bounds for the exponents* of primes of bad reduction under some mild conditions.

Some of my projects for the next years are the following:

Invariant rings computation. In the paper [LLLR20] we need to have a HSOP for plane quartic curves in order to determine the reduction type of the primes in their discriminants. Except for some subtleties in characteristic 3 we provided such a HSOP. But even if a HSOP is known in all characteristic, we still do not have generator for the full invariant ring of plane quartics in positive characteristic. With my collaborators in this paper we

are working on computing this invariant ring. Techniques from Classical Invariant Theory and computer assisted proofs are needed. Another interesting question in this direction, and related with the characteristic 3 subtlety, it is the computation of invariant rings for Artin-Scheier curves.

Bad reduction types of plane quartics. As mentioned in the introduction of Chapter 4 the computation of the reduction type of different families of genus 3 curves is based on the study of the degeneration of a Galois morphism from the curve to $\mathbb{P}^1$. In general there is no reason for this morphism to exist. This is why we have to try different techniques. My idea is to find an analog of the cluster picture of hyperelliptic curves for non-hyperelliptic curves. The cluster picture contains the information about the collision of the ramification points. This ramification points are related to the 2-torsion of the Jacobian of the curve. So a possibility would be to consider the bitangents of a plane quartic which are also related with the 2-torsion of its Jacobian and their collision while reducing modulo p. Somehow this was used for the case of hyperelliptic reduction in my paper [LLR18].

Conductor computations. The conductor of a curve is an important arithmetic invariant related with its discriminant. It gives information on the reduction type, but it is also related with the ramification of the field generated by the torsion of its Jacobian. It is in general difficult to compute and there are many open question concerning it. For instance, how to determine the rational plane quartic with the smallest conductor? After my work [BCK+21] and with my collaborators in this paper, we are planning to pursue this research direction. We will start by inspecting closer the family of Ciani quartics. We will also deal with questions concerning the construction of plane quartic curves with good reduction outside a finite set of primes.

Arithmetic intersection formulas. I want to give several arithmetic intersection formulas for genus 2 and 3 curves. In [LV15] they give an arithmetic intersection formula for primitive CM-fields with the cycle G_1 of decomposable polarizations. Also by using the embedding problem, we obtain a bound for the corresponding arithmetic intersection in the case of genus 3 and a sextic CM-field not containing an imaginary quadratic field. I want to consider now the non-primitive case in genus 2 and 3. Totally different techniques are expected to be needed here: an example of this is found in [RV00]. This project will be a collaboration with C. Ritzenthaler and F. Rodríguez-Villegas.

Bibliography

[ACGH85] E. Arbarello, M. Cornalba, P.A. Griffiths, and J. Harris. *Geometry of algebraic curves, Vol. I*, volume 267. Grundlehren der Mathematischen Wissenschaften, Springer-Verlag, New-York, 1985.

[AE19] Sonny Arora and Kirsten Eisenträger. Constructing Picard curves with complex multiplication using the Chinese remainder theorem. In *Proceedings of the Thirteenth Algorithmic Number Theory Symposium*, volume 2 of *Open Book Ser.*, pages 21–36. Math. Sci. Publ., Berkeley, CA, 2019.

[Bas15] Romain Basson. *Arithmétique des espaces de modules des courbes hyperelliptiques de genre* 3 *en caractéristique positive*. PhD thesis, Université de Rennes 1, Rennes, 2015.

[BBEL08] Juliana Belding, Reinier Broker, Andreas Enge, and Kristin Lauter. Computing Hilbert class polynomials. In *Algorithmic number theory*, volume 5011 of *Lecture Notes in Comput. Sci.*, pages 282–295. Springer, Berlin, 2008.

[BBL18] Eslam Badr, Francesc Bars, and Elisa Lorenzo García. The Picard group of Brauer-Severi varieties. *Open Math.*, 16(1):1196–1203, 2018.

[BBL19] Eslam Badr, Francesc Bars, and Elisa Lorenzo García. On twists of smooth plane curves. *Math. Comp.*, 88(315):421–438, 2019.

[BBW17] Michel Börner, Irene I. Bouw, and Stefan Wewers. Picard curves with small conductor. In *Algorithmic and experimental methods in algebra, geometry, and number theory*, pages 97–122. Springer, Cham, 2017.

[BCK+21] Irene Bouw, Nirvana Coppola, Pinar Kilicer, Sabrina Kunzweiler, Elisa Lorenzo García, and Anna Somoza. Reduction type of genus-3 curves in a special stratum of their moduli space. Women in Numbers Europe, Research Directions in Number Theory, Association for Women in Mathematics Series Volume, Springer, 2021.

[BCL+15] Irene Bouw, Jenny Cooley, Kristin E. Lauter, Elisa Lorenzo García, Michelle Manes, Rachel Newton, and Ekin Ozman. Bad reduction of genus 3 curves with complex multiplication. Women in Numbers Europe, Research Directions

in Number Theory, Association for Women in Mathematics Series Volume 2, Springer, 2015.

[BGL+17] Sean Ballentine, Aurore Guillevic, Elisa Lorenzo García, Chloe Martindale, Maike Massierer, Benjamin Smith, and Jaap Top. Isogenies for point counting on genus two hyperelliptic curves with maximal real multiplication. In *Algebraic geometry for coding theory and cryptography*, volume 9 of *Assoc. Women Math. Ser.*, pages 63–94. Springer, Cham, 2017.

[BILV16] Jennifer S. Balakrishnan, Sorina Ionica, Kristin Lauter, and Christelle Vincent. Constructing genus-3 hyperelliptic Jacobians with CM. *LMS J. Comput. Math.*, 19(suppl. A):283–300, 2016.

[BKSW20] Irene I. Bouw, Angelos Koutsianas, Jeroen Sijsling, and Stefan Wewers. Conductor and discrimant of Picard curves. To appear in *J. London Math. Soc.*, 2020.

[BL20] Eslam Badr and Elisa Lorenzo García. A note on the stratification by automorphisms of smooth plane curves of genus 6. *Colloq. Math.*, 159(2):207–222, 2020.

[Bol87] Oskar Bolza. Darstellung der rationalen ganzen invarianten der binärform sechsten grades durch die nullwerthe der zugehörigen ϑ-functionen. *Math. Ann.*, 30(4):478–495, 1887.

[Bou98] Irene I. Bouw. *Tame covers of curves: p-ranks and fundamental groups*. PhD thesis, Utrecht University, 1998.

[Bro08] Reinier Broker. A p-adic algorithm to compute the Hilbert class polynomial. *Math. Comp.*, 77(264):2417–2435, 2008.

[BS15] Florian Bouyer and Marco Streng. Examples of CM curves of genus two defined over the reflex field. *LMS J. Comput. Math.*, 18(1):507–538, 2015.

[Bur92] Jean-François Burnol. Remarques sur la stabilité en arithmétique. *Internat. Math. Res. Notices*, (6):117–127, 1992.

[BW15] Irene I. Bouw and Stefan Wewers. Semistable reduction of curves and computation of bad Euler factors of L-functions. Notes for a minicourse, ICERM, 2015.

[BW17] Irene I. Bouw and Stefan Wewers. Computing L-functions and semistable reduction of superelliptic curves. *Glasg. Math. J.*, 59(1):77–108, 2017.

[BY06] Jan Hendrik Bruinier and Tonghai Yang. CM-values of Hilbert modular functions. *Invent. Math.*, 163(2):229–288, 2006.

[Cas85] J. W. S. Cassels. The arithmetic of certain quartic curves. *Proc. Roy. Soc. Edinburgh Sect. A*, 100(3-4):201–218, 1985.

[Cia99] E. Ciani. I varii tipi possibili di quartiche piane più volte omologiche armoniche. *Rend. Circ. Mat. Palermo*, 13:347–373, 1899.

[Cle70] A. Clebsch. Zur theorie der binären algebraischen formen. *Math. Ann.*, 3(2):265–267, 1870.

[CMSV19] Edgar Costa, Nicolas Mascot, Jeroen Sijsling, and John Voight. Rigorous computation of the endomorphism ring of a Jacobian. *Math. Comp.*, 88(317):1303–1339, 2019.

[DDMM18] Tim Dokchitser, Vladimir Dokchitser, Céline Maistret, and Adam Morgan. Arithmetic of hyperelliptic curves over local fields. *Preprint*, 2018. arXiv:1808.02936.

[DDMM19] Tim Dokchitser, Vladimir Dokchitser, Céline Maistret, and Adam Morgan. Semistable types of hyperelliptic curves. In *Algebraic curves and their applications*, volume 724 of *Contemp. Math.*, pages 73–135. Amer. Math. Soc., Providence, RI, 2019.

[Dix87] Jacques Dixmier. On the projective invariants of quartic plane curves. *Adv. in Math.*, 64:279–304, 1987.

[DK02] Harm Derksen and Gregor Kemper. *Computational invariant theory*. Invariant Theory and Algebraic Transformation Groups, I. Springer-Verlag, Berlin, 2002. Encyclopaedia of Mathematical Sciences, 130.

[Elk99] Noam D. Elkies. The Klein quartic in number theory. In *The eightfold way*, volume 35 of *Math. Sci. Res. Inst. Publ.*, pages 51–101. Cambridge Univ. Press, Cambridge, 1999.

[Fav20] Harold Favereau. Characterization of the reduction type for hyperelliptic curves of genus 2 and 3. *In progress*, 2020.

[FLGS18] Francesc Fité, Elisa Lorenzo García, and Andrew V. Sutherland. Sato-Tate distributions of twists of the Fermat and the Klein quartics. *Res. Math. Sci.*, 5(4):Paper No. 41, 40, 2018.

[GL07] Eyal Z. Goren and Kristin E. Lauter. Class invariants for quartic CM fields. *Ann. Inst. Fourier (Grenoble)*, 57(2):457–480, 2007.

[Gor68] Paul Gordan. Beweis, dass jede covariante und invariante einer binären form eine ganze function mit numerischen coefficienten einer endlichen anzahl solcher formen ist. *J. Pure Angew. Math.*, 69:323–354, 1868.

[Gro86] Benedict H. Gross. On canonical and quasicanonical liftings. *Invent. Math.*, 84(2):321–326, 1986.

[ID20] Sorina Ionica and Bogdan A. Dina. Genus 3 hyperelliptic curves with CM via Shimura reciprocity. Proceedings of the ANTS-XIV conference, to appear, 2020.

[Igu60] Jun-ichi Igusa. Arithmetic variety of moduli for genus two. *Ann. of Math. (2)*, 72:612–649, 1960.

[Igu62] Jun-ichi Igusa. On Siegel modular forms of genus two. *Amer. J. Math.*, 84:175–200, 1962.

[Igu67] Jun-ichi Igusa. Modular forms and projective invariants. *Amer. J. Math.*, 89:817–855, 1967.

[IKL+19] Sorina Ionica, Pınar Kılıçer, Kristin Lauter, Elisa Lorenzo García, Adelina Mânzăţeanu, Maike Massierer, and Christelle Vincent. Modular invariants for genus 3 hyperelliptic curves. *Res. Number Theory*, 5(1):Art. 9, 22, 2019.

[IKL+20] Sorina Ionica, Pınar Kılıçer, Kristin Lauter, Elisa Lorenzo García, Adelina Mânzăţeanu, and Christelle Vincent. Bounding denominators of class polynomials for genus 3. *In progress*, 2020.

[Kıl16] Pınar Kılıçer. *The CM class number one problem for curves*. PhD thesis, Leiden University and University of Bordeaux, 2016.

[Kıl17] Pınar Kılıçer. The CM class number one problem for curves of genus 3. In progress, 2017.

[KLL+18] Pınar Kılıçer, Hugo Labrande, Reynald Lercier, Christophe Ritzenthaler, Jeroen Sijsling, and Marco Streng. Plane quartics over $\mathbb{Q}$ with complex multiplication. *Acta Arith.*, 185(2):127–156, 2018.

[KLL+20] Pınar Kılıçer, Kristin Lauter, Elisa Lorenzo García, Rachel Newton, Ekin Ozman, and Marco Streng. A bound on the primes of bad reduction for CM curves of genus 3. *Proc. Amer. Math. Soc.*, 148(7):2843–2861, 2020.

[KLS20] Pınar Kılıçer, Elisa Lorenzo García, and Marco Streng. Primes dividing invariants of CM Picard curves. *Canad. J. Math.*, 72(2):480–504, 2020.

[LG17] Elisa Lorenzo García. Twists of non-hyperelliptic curves. *Rev. Mat. Iberoam.*, 33(1):169–182, 2017.

[LG18] Elisa Lorenzo García. Twists of non-hyperelliptic curves of genus 3. *Int. J. Number Theory*, 14(6):1785–1812, 2018.

[Liu93] Qing Liu. Courbes stables de genre 2 et leur schéma de modules. *Math. Ann.*, 295(2):201–222, 1993.

[LL19] Davide Lombardo and Elisa Lorenzo García. Computing twists of hyperelliptic curves. *J. Algebra*, 519:474–490, 2019.

[LLLR20] Reynald Lercier, Qing Liu, Elisa Lorenzo García, and Christophe Ritzenthaler. Reduction type of smooth quartics. *Algebra & Number Theory, to appear*, 2020.

[LLR18] Reynald Lercier, Elisa Lorenzo García, and Christophe Ritzenthaler. Stable models of plane quartics with hyperelliptic reduction. *Too appear in Arithmetic, Geometry, Cryptography and Coding Theory, AMS Contemporary Mathematics*, 2018.

[LLRS20] Davide Lombardo, Elisa Lorenzo García, Christophe Ritzenthaler, and Jeroen Sijsling. Decomposing jacobians via galois covers. *Exp. Math., to appear*, 2020.

[LMM17] Elisa Lorenzo García, Giulio Meleleo, and Piermarco Milione. Statistics for biquadratic covers of the projective line over finite fields. *J. Number Theory*, 173:448–477, 2017. With an appendix by Alina Bucur.

[Lor17] Elisa Lorenzo García. Construction of Brauer-Severi varieties. *Preprint*, 2017. arXiv:1706.10079.

[Lor20] Elisa Lorenzo García. On different expressions for invariants of hyperelliptic curves of genus 3. *Preprint*, 2020. arXiv:1907.05776.

[LR12] Reynald Lercier and Christophe Ritzenthaler. Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects. *J. Algebra*, 372:595–636, 2012.

[LR20] Reynald Lercier and Christophe Ritzenthaler. Siegle modular forms in dimension 3 and invariants fo ternary quartics. *Proceedings of the American Mathematical Society, to appear*, 2020.

[LS20] Joan-C. Lario and Anna Somoza. An inverse Jacobian algorithm for Picard curves. *Research in Number Theory, to appear*, 2020.

[LV15] Kristin Lauter and Bianca Viray. An arithmetic intersection formula for denominators of Igusa class polynomials. *Amer. J. Math.*, 137(2):497–533, 2015.

[Mai17] Céline Maistret. *Parity of ranks of Jacobians of hyperelliptic curves of genus 2.* PhD thesis, University of Warwick, Warwick, 2017.

[Mes91] Jean-François Mestre. Construction de courbes de genre 2 à partir de leurs modules. In *Effective methods in algebraic geometry (Castiglioncello, 1990)*, volume 94 of *Progr. Math.*, pages 313–334. Birkhäuser Boston, Boston, MA, 1991.

[MO13] Ben Moonen and Frans Oort. The Torelli locus and special subvarieties. In *Handbook of moduli. Vol. II*, volume 25 of *Adv. Lect. Math. (ALM)*, pages 549–594. Int. Press, Somerville, MA, 2013.

[Mum77] David Mumford. Stability of projective varieties. *Enseignement Math. (2)*, 23(1-2):39–110, 1977.

[Mum06] David Mumford. *Tata lectures on theta. III.* Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, 2006. With M. Nori, P. Norman, Reprint of the 1984 original.

[Ohn05] Toshiaki Ohno. The graded ring of invariants of ternary quartics I, 2005. Unpublished.

[RF74] Harry E. Rauch and Hershel M. Farkas. *Theta functions with applications to Riemann surfaces.* The Williams & Wilkins Co., Baltimore, Md., 1974.

[RV00] Fernando Rodriguez-Villegas. Explicit models of genus 2 curves with split CM. In *Algorithmic number theory (Leiden, 2000)*, volume 1838 of *Lecture Notes in Comput. Sci.*, pages 505–513. Springer, Berlin, 2000.

[RW06] Matthieu Romagny and Stefan Wewers. Hurwitz spaces. In *Groupes de Galois arithmétiques et différentiels*, volume 13 of *Sémin. Congr.*, pages 313–341. Soc. Math. France, Paris, 2006.

[S+20] W. A. Stein et al. *Sage Mathematics Software (Version x.y.z).* The Sage Development Team, 2020. `http://www.sagemath.org`.

[Sha80] Jayant Shah. A complete moduli space for $K3$ surfaces of degree 2. *Ann. of Math. (2)*, 112(3):485–510, 1980.

[Shi67] Tetsuji Shioda. On the graded ring of invariants of binary octavics. *Amer. J. Math.*, 89:1022–1046, 1967.

[Sil98] Joseph H. Silverman. The space of rational maps on $\mathbf{P}^1$. *Duke Math. J.*, 94(1):41–77, 1998.

[Som19] Anna Somoza. *Inverse Jacobian and related topics for certain superelliptic curves.* PhD thesis, Leiden University and University of Bordeaux, 2019.

[ST68] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.

[Str14] Marco Streng. Computing Igusa class polynomials. *Math. Comp.*, 83(285):275–309, 2014.

[STW14] Lucien Szpiro, Michael Tepper, and Phillip Williams. Semi-stable reduction implies minimality of the resultant. *J. Algebra*, 397:489–498, 2014.

[Sut11] Andrew V. Sutherland. Computing Hilbert class polynomials with the Chinese remainder theorem. *Math. Comp.*, 80(273):501–538, 2011.

[Tak96] Koichi Takase. A generalization of Rosenhain's normal form for hyperelliptic curves with an application. *Proc. Japan Acad. Ser. A Math. Sci.*, 72(7):162–165, 1996.

[Tat75] J. Tate. Algorithm for determining the type of a singular fiber in an elliptic pencil. In *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 33–52. Lecture Notes in Math., Vol. 476, 1975.

[Tsu86] Shigeaki Tsuyumine. On Siegel modular forms of degree 3. *Amer. J. Math.*, 108:755–862, 1986.

[Was08] Lawrence C. Washington. *Elliptic curves*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, second edition, 2008. Number theory and cryptography.

[Web76] H. Weber. Theory of abelian functions of genus 3. (theorie der abelschen functionen vom geschlecht 3.), 1876.

[Wen01] Annegret Weng. A class of hyperelliptic CM-curves of genus three. *J. Ramanujan Math. Soc.*, 16(4):339–372, 2001.

[Wew99] Stefan Wewers. Deformation of tame admissible covers of curves. In *Aspects of Galois theory (Gainesville, FL, 1996)*, volume 256 of *London Math. Soc. Lecture Note Ser.*, pages 239–282. Cambridge Univ. Press, Cambridge, 1999.

[Yan13] Tonghai Yang. Arithmetic intersection on a Hilbert modular surface and the Faltings height. *Asian J. Math.*, 17(2):335–381, 2013.