NON-HYPERELLIPTIC MODULAR JACOBIANS OF DIMENSION 3

ROGER OYONO

ABSTRACT. We present a method to solve in an efficient way the problem of constructing the curves given by Torelli’s theorem in dimension 3 over the complex numbers: For an absolutely simple principally polarized abelian threefold $A$ over $\mathbb{C}$ given by its period matrix $\Omega$, compute a model of the curve of genus three (unique up to isomorphism) whose Jacobian, equipped with its canonical polarization, is isomorphic to $A$ as a principally polarized abelian variety. We use this method to describe the non-hyperelliptic modular Jacobians of dimension 3. We investigate all the non-hyperelliptic new modular Jacobians $\text{Jac}(C_f)$ of dimension 3 which are isomorphic to $A_f$, where $f \in S_2^{\text{new}}(X_0(N))$, $N \leq 4000$.

INTRODUCTION

In this article, we consider a 3-dimensional absolutely simple principally polarized abelian variety $A$ defined over the complex numbers. Due to the well-known results about the moduli space of genus 3 curves, the abelian variety $A$ is isomorphic to the Jacobian variety of a genus 3 curve $C$ defined over the complex numbers. Moreover, Torelli’s theorem asserts, with respect to the attached polarization, that the curve $C$ is unique up to isomorphism. In the generic case, the curve $C$ is non-hyperelliptic. The problem of determining if the curve $C$ is hyperelliptic or not was first solved by Poor [28]. His approach consists of testing whether some even theta constants vanish or not, i.e. the values of Riemann’s theta function at even 2-torsion points. In the case of hyperelliptic curves, Weber [38, 39] also used even theta constants to explicitly construct the Rosenhain model of the curve $C$ with $\text{Jac}(C) \simeq A$. Using only even theta constants seemed natural since Riemann’s theta function always vanishes at odd 2-torsion points. The first use of odd 2-torsion points for solving Torelli’s theorem is due to Guàrdia et al. [17, 18, 14], who used a geometric property of derivatives of the theta function at odd 2-torsion points. Based on this idea, we present a method to solve the non-hyperelliptic case of Torelli’s theorem in dimension 3.
We use this method to describe modular Jacobians of dimension 3. We implemented programs in Magma to determine all 3-dimensional non-hyperelliptic \( \mathbb{Q} \)-simple new modular Jacobians of level \( N \leq 4000 \).

In what follows, the objects we are dealing with, when no field is specified, are defined over \( \mathbb{C} \). For instance, \( \cong \) means isomorphic over \( \mathbb{C} \), and \( \cong \) means isomorphic over \( \mathbb{Q} \).

1. Preliminaries on Non-hyperelliptic Curves of Genus 3

In the following, let \( C \) be a non-hyperelliptic curve of genus 3 defined over an arbitrary field \( k \) and let \( \{\omega_1, \ldots, \omega_9\} \) be a basis of the space \( \Omega^1(C) \) of holomorphic differential forms on \( C \). The canonical embedding of \( C \) with respect to this basis is given by

\[
\phi : C \longrightarrow \mathbb{P}^9 \quad \quad P \longrightarrow \phi(P) := (\omega_1(P) : \cdots : \omega_9(P)),
\]

where \( \omega(P) = f(P) \) for any expression \( \omega = f dt \), with \( f, t \in k(C) \) and \( t \) a local parameter at \( P \). The image \( \phi(C) \) of \( C \) by the canonical embedding is a smooth plane quartic, and conversely any smooth plane quartic is the image by the canonical embedding of a genus 3 non-hyperelliptic curve. From now on, we restrict ourselves to smooth plane quartics when we are speaking about non-hyperelliptic curves of genus 3 and we denote \((x_1 : x_2 : x_3)\) (or sometimes \((x : y : z)\)) the coordinates in the projective plane \( \mathbb{P}^2 \).

1.1. Dixmier invariants. To classify ternary smooth plane quartics (up to isomorphism over \( \mathbb{C} \)), Dixmier [6] introduced a system \( I_3, I_6, I_9, I_{12}, I_{15}, I_{18}, I_{27} \) of invariants: For a general ternary quartic given by

\[
g(x, y, z) := a_1 x^4 + 4a_2 x^3 y + 6a_3 x^2 y^2 + 4a_4 xy^3 + a_5 y^4 + 4a_6 x^3 z + 12a_7 x^2 y z + 12a_8 x y^2 z + 6a_{10} x^2 z^2 + 12a_{11} x y z^2 + 6a_{12} y^2 z^2 + 4a_{13} x^2 z^3 + 4a_{14} x y z^3 + a_{15} z^4,
\]

the invariants \( I_3 \) and \( I_6 \) may be computed from:

\[
I_3(g) := a_1 a_3 a_5 + 3 (a_1 a_3^2 + a_3 a_5^2 + a_5 a_7^2)
\]
\[
+ 4 (a_2 a_9 a_{13} + a_6 a_{14} - a_1 a_9 a_{14} - a_5 a_9 a_{13} - a_5 a_2 a_4) + 6a_3 a_{10} a_{12}
\]
\[
- 12 (a_7 a_8 a_{11} + a_9 a_{13} a_{12} + a_6 a_{14} a_{12} + a_4 a_{11} a_{10} + a_9 a_{13} a_{10} + a_{13} a_8 a_{13})
\]
\[
+ a_{14} a_{17} a_{13} - (a_7 a_8 a_{11} + a_9 a_{13} a_{12} + a_6 a_{14} a_{12} + a_4 a_{11} a_{10} + a_{13} a_8 a_{13} + a_{13} a_{11} + a_{10} a_{12} + a_{12} a_{17} + a_{12} a_{17}),
\]

and

\[
I_6(g) := \det \begin{bmatrix}
a_1 & a_3 & a_{10} & a_7 & a_6 & a_2 \\
a_3 & a_5 & a_{12} & a_9 & a_8 & a_4 \\
a_{10} & a_{12} & a_{15} & a_{14} & a_{13} & a_{11} \\
a_7 & a_9 & a_{14} & a_{12} & a_{11} & a_8 \\
a_6 & a_8 & a_{13} & a_{11} & a_{10} & a_7 \\
a_2 & a_4 & a_{11} & a_8 & a_7 & a_3
\end{bmatrix}.
\]

For the definition of the other invariants \( I_9, I_{12}, I_{15}, I_{18}, I_{27} \), see [6]. The computation of \( I_9, I_{12}, I_{15}, I_{18}, I_{27} \) via explicit formulae is too exhaustive; for example, the discriminant \( I_{27} \) has about 50,000,000 terms.

The plane quartic \( C : g(x, y, z) = 0 \) has genus 3 if and only if the discriminant \( I_{27} \neq 0 \) (see [6]). From the above Dixmier invariants we can deduce the following
absolute Dixmier invariants:
\[ i_1 = \frac{t_2^3}{t_2}, \quad i_2 = \frac{t_3}{t_2}, \quad i_3 = \frac{t_4}{t_2}, \quad i_4 = \frac{t_5}{t_2}, \quad i_5 = \frac{t_6}{t_2}, \quad i_6 = \frac{t_7}{t_2}. \]

**Lemma 1.** If two ternary smooth plane quartics \( C \) and \( C' \) are isomorphic, then
\[ i_j(C) = i_j(C') \quad \text{for} \quad j = 1, \ldots, 6. \]

**Proof.** Let \( C' = C^\alpha \) with \( \alpha \in \text{GL}_3(\mathbb{C}) \) and \( D := \det(\alpha) \neq 0 \). From [32] we get the following relations between \( I_j \) and \( I'_j \):
\[ I'_j = (D^4)^{\frac{j}{6}} \cdot I_j, \]
for \( j = 3, 6, 9, 12, 15, 18, 27 \). The lemma then follows from the definitions of \( i_j \). \( \square \)

**Remark 1.**
(i) Recently, Ohno gave a complete system of invariants to classify ternary smooth plane quartics up to isomorphism \([26, 10]\). Unfortunately, we became aware of these results only once our computations were done. For this reason, the Dixmier invariants were used throughout this paper.

(ii) After necessary adjustments, Dixmier-Ohno invariants can be extended to any field of characteristic different from 2 and 3.

### 1.2. Shioda’s normal forms.
Let \( C \) be a smooth plane quartic defined over the field \( k \). For any point \( \xi \in C(\overline{k}) \) we denote by \( T_\xi \) the tangent line to \( C \) at \( \xi \). The intersection divisor \((C \cdot T_\xi)\) is of the form
\[ (C \cdot T_\xi) = 2\xi + \xi' + \xi'' \]
for some \( \xi', \xi'' \in C(\overline{k}) \). The point \( \xi \in C(\overline{k}) \) is called an ordinary flex (resp. special flex or hyperflex) if
\[ (C \cdot T_\xi) = 3\xi + \xi' \quad \text{for some} \quad \xi' \neq \xi \quad (\text{resp.} \quad (C \cdot T_\xi) = 4\xi). \]
The ordinary and special flexes are exactly the ordinary and special Weierstrass points of the curve \( C \). The hyperflex of a plane quartic with exactly one hyperflex has to be rational since it has to be Galois invariant. According to [37], a \( k \)-rational smooth plane quartic with a hyperflex has generically a \( k \)-rational flex since the locus of smooth plane quartics with two or more hyperflexes has codimension one in the locus of smooth plane quartics with a hyperflex. However, one can find \( k \)-rational families of quartics with at least two hyperflexes which are not defined over \( k \). For instance, the roots in \( \overline{k} \) of the irreducible degree four polynomial \( f(x) \in k[x] \) provide hyperflexes (not defined over \( k \)) of the curve with affine model \( y^4 = f(x) \).

In what follows, we say that the pair \((C, \xi)\) is defined over \( k \) if \( C \) is a curve defined over \( k \) and \( \xi \) a \( k \)-rational flex of \( C \). In the case of smooth plane quartics we have the following propositions:

**Proposition 1** ([35]). Let \( k \) be an arbitrary field of characteristic \( \neq 3 \). Given a plane quartic with an ordinary flex \((C, \xi)\) defined over \( k \), there is a coordinate system \((x, y, z)\) of \( \mathbb{P}^2 \) such that \((C, \xi)\) is given by
\begin{align*}
C: \quad & 0 = y^2z + y(p_0z^3 + p_1z^2x + x^2) + q_0z^4 + q_1z^3x + q_2z^2x^2 + q_3zx^3 + q_4x^4, \\
\xi: \quad & (0:1:0), \quad T_\xi: \quad z = 0.
\end{align*}
Moreover, the parameter
\[ \lambda = (p_0, p_1, q_0, q_1, q_2, q_3, q_4) \in k^7 \]
is uniquely determined up to the equivalence
\[ \lambda = (p_1, q_1) \sim \lambda' = (p'_1, q'_1) \iff p'_i = u^{6-2i} p_i, \quad q'_j = u^{9-2j} q_j, \quad (i = 0, 1, j = 0, 1, \ldots, 4) \]
for some \( u \neq 0 \).

**Proposition 2** ([35]). Let \( k \) be an arbitrary field of characteristic \( \neq 2, 3 \). Given a plane quartic with a special flex \( (C, \xi) \) defined over \( k \), there is a coordinate system \((x, y, z)\) of \( \mathbb{P}^2 \) such that \((C, \xi)\) is given by
\[ C : 0 = y^3 z + y(p_0 z^3 + p_1 z^2 x + p_2 x^2) + q_0 z^4 + q_1 z^3 x + q_2 z^2 x^2 + x^4, \]
\[ \xi = (0 : 1 : 0), \quad T_\xi : \quad z = 0. \]
Moreover, the parameter
\[ \lambda = (p_0, p_1, p_2, q_0, q_1, q_2) \in k^6 \]
is uniquely determined up to the equivalence
\[ \lambda = (p_1, q_1) \sim \lambda' = (p'_1, q'_1) \iff p'_i = u^{8-3i} p_i, \quad q'_j = u^{12-3j} q_j, \quad (i, j = 0, 1, 2) \]
for some \( u \neq 0 \).

A curve with an equation of the form (1) or (2) is called a normal form and we denote it by \( C_\xi \). Indeed, a flex of a plane quartic is generically an ordinary flex. The coefficient \( q_4 \) in the normal form (1) is generically different from 0. In this case we can uniquely normalize \( C_\xi \) by letting \( q_4 = 1 \). Even if \( q_4 = 0 \), it is always possible to describe \((C, \xi)\) by a unique normal form \( C_\xi \). If, for instance, \( \xi \) is an ordinary flex and \( q_4 = 0, p_1, q_3 \neq 0 \), then by choosing \( u = \frac{2}{p_1} \) we then have a unique normal form
\[ 0 = y^3 z + y(p'_0 z^3 + p'_1 z^2 x + x^3) + q'_0 z^4 + q'_1 z^3 x + q'_2 z^2 x^2 + q'_3 z x^3, \]
where \( p'_1 = q'_4 \).

With this argumentation, we were able to compute up to a certain precision a \( \mathbb{Q} \)-rational model of the curve \( X_{369}^D \) from a Riemann model over \( \mathbb{C} \) (see Example 1 in Section 3).

\[ X_{369}^D : \quad 0 = y^3 z + y(x^3 - \frac{22}{2187} x z^2 - \frac{1594323}{10460353203} z^3) \]
\[ - \frac{2}{2187} x^3 + \frac{10}{4782969} x^2 z^2 + \frac{10}{4782969} x z^3. \]

Note that one cannot view \( \lambda \) in the above propositions as a set of invariants for the curve \( C \) since \( \lambda \) depends on the flex \( \xi \) under consideration.

2. MODULAR JACOBIANS AND MODULAR CURVES

Let \( N > 2 \) be an integer and \( X_0(N) \) the associated modular curve of genus \( g \).
Let \( S_2(N) \) be the set of cusp forms of weight 2 for the Hecke subgroup \( \Gamma_0(N) \).
The map
\[ \omega : S_2(N) \longrightarrow \Omega^1(X_0(N)), \quad f(\tau) \longrightarrow 2\pi i f(\tau) d\tau \]
induces an isomorphism between the vector spaces \( S_2(N) \) and \( \Omega^1(X_0(N)) \).

If \( M|N \) and \( d \) is \( \frac{N}{M} \), then \( z \rightarrow d \cdot z \) induces a morphism \( X_0(N) \longrightarrow X_0(M) \), which also induces morphisms \( S_2(M) \longrightarrow S_2(N) \) and \( J_0(M) \longrightarrow J_0(N) \), where \( J_0(N) := \text{Jac}(X_0(N)) \). The old subspace \( S_2^{\text{old}}(N) \) of \( S_2(N) \) is defined as the sum of the images of all such maps \( S_2(M) \longrightarrow S_2(N) \) for all \( d \) and \( M \) such that \( M|N, M \neq N \) and \( d \) is \( \frac{N}{M} \). Similarly, we define the old subvariety \( J_0(N)^{\text{old}} \) of \( J_0(N) \). Let \( S_2^{\text{new}}(N) \) be the orthogonal complement to \( S_2^{\text{old}}(N) \) with respect to the Petersson inner product in
S_2(N). For n ≥ 1 with gcd(N,n) = 1, there exist correspondences T_n on X_0(N), which induce endomorphisms of S_2(N) and of J_0(N) known as Hecke operators, also denoted by T_n. There exists a unique basis of S_2^{new}(N) consisting of eigenforms with respect to all the T_p (for gcd(N,p) = 1), i.e., cusp forms f = q + \sum_{i \geq 2} a_i q^i such that T_n(f) = a_n f whenever gcd(n,N) = 1. The elements of this basis are called newforms of level N. Given the newform f = q + \sum_{i \geq 2} a_i q^i, let K_f = \mathbb{Q}(a_n) be the real algebraic number field generated by the coefficients a_n of f, let I_f = {σ_1, ..., σ_d} be the set of all isomorphisms of K_f into \mathbb{C}, and let \{f^{σ_1}, ..., f^{σ_d}\} be the complete set of newform conjugates to f over \mathbb{Q}. Shimura [33][34] attached to the newform f ∈ S_2^{new}(N) a subvariety A_f of J_0(N) defined over \mathbb{Q} with the following properties: A_f is a simple factor of J_0(N)^{new} over \mathbb{Q}, dim(A_f) = d and Ω^1(A_f) \cong \sum_{σ ∈ I_f} Cω(f^σ). Furthermore, A_f is absolutely simple if f does not admit a twist, in particular, A_f is absolutely simple for square-free module N. The definition of A_f directly implies the existence of a surjective morphism

$$\pi_f : J_0(N)^{new} \longrightarrow A_f.$$ 

Let B_M be a basis of non-conjugate newforms. Then

$$J_0(N)^{new} \cong \mathbb{Q} \prod_{f ∈ B_N} A_f \quad \text{and} \quad J_0(N)^{old} \cong \mathbb{Q} \prod_{M | N, M ≠ N} \prod_{f ∈ B_M} A_f^{σ_0(\frac{N}{M})},$$

where σ_0(n) denotes the number of positive divisors of n.

**Definition 1** ([13][2]). An abelian variety A over \mathbb{Q} is said to be \mathbb{Q}-modular of level N, if there exists a surjective \mathbb{Q}-morphism

$$\nu : J_0(N) \longrightarrow A.$$ 

In that case, we say that A is new (of level N), if there exists a \mathbb{Q}-morphism

$$\bar{\nu} : J_0(N)^{new} \longrightarrow A.$$ 

The following diagram is then commutative:

$$\begin{array}{ccc}
J_0(N) & \xrightarrow{\nu} & A \\
\downarrow{pr_{new}} & & \downarrow{\bar{\nu}} \\
J_0(N)^{new} & \xrightarrow{\bar{\nu}} & A
\end{array}$$

**Definition 2** ([13][2]). A non-singular curve C defined over \mathbb{Q} is said to be \mathbb{Q}-modular of level N, if there exists a non-constant \mathbb{Q}-morphism

$$\pi : X_0(N) \longrightarrow C.$$ 

The curve C is then said to be new of level N if its Jacobian Jac(C) is new of level N.
For a modular curve $C$, the following diagram commutes:

$$
\begin{aligned}
J_0(N) & \xrightarrow{\pi^*} \text{Jac}(C) \\
X_0(N) & \xrightarrow{\pi} C
\end{aligned}
$$

The modularity of the Jacobian does not imply (in general) the modularity of the corresponding curve (cf. [13, section 7]).

The well-known results of Wiles et al. [41, 36] about (new) modular elliptic curves (over $\mathbb{Q}$) implies that there are infinitely many new modular curves of genus 1. In contrast to new modular curves of genus $g$ (up to isomorphism) over $\mathbb{Q}$ is finite and computable [2], and in the case of genus 2, [2, 13] provide a complete list of new modular curves.

3. Explicit version of Torelli’s theorem in dimension 3

3.1. Abelian varieties over $\mathbb{C}$. An abelian variety $A$ of dimension $g$ defined over the complex numbers can be viewed as a pair $(\mathbb{C}^g / \Lambda, E)$ where $\Lambda$ is a full $\mathbb{Z}$-lattice in $\mathbb{C}^g$ and $E$ is a non-degenerate Riemann form on the lattice $\Lambda$. The Riemann form $E$ induces a polarization on $\Lambda$.

If the polarization is principal, the lattice $\Lambda = \Omega \mathbb{Z}^g$ is isomorphic to the lattice $\mathbb{Z}^g + \Omega \mathbb{Z}^g$, where $\Omega := \Omega_1 + \Omega_2 \mathbb{Z}^g$ and $\Omega_1 := (\lambda_1, \ldots, \lambda_g, \ldots, \lambda_g) \in \mathbb{C}^g$ and $\Omega := \Omega^{-1}$. The period matrix $\Omega$ of $A$ is in the Siegel upper half-plane $\mathbb{H}_g := \{ z \in \mathbb{C}^g : z = z, \Im(z) > 0 \}$ and the symplectic group $\text{Sp}(2g, \mathbb{Z}) := \left\{ \gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \text{GL}(2g, \mathbb{Z}) \mid \gamma^t J \gamma = J \right\}$ acts on $\mathbb{C}^g \times \mathbb{H}_g$ by

$$
\gamma(z, \Omega) := ((C\Omega + D)^{-1} z, (A\Omega + B)(C\Omega + D)^{-1}).
$$

The period matrix of the principally polarized abelian variety $A$ and the cosets $\text{Sp}(2g, \mathbb{Z}) \Omega$ represent the isomorphy class of $A$ in $\text{Sp}(2g, \mathbb{Z}) \setminus \mathbb{H}_g$.

The set of 2-torsion points $A[2]$ of $A$, i.e. the kernel of the isogeny

$$
A[2] : A \rightarrow A, \quad a \mapsto 2a
$$

is given by

$$
A[2] = \left\{ z_m = \frac{1}{2} \Omega \delta^t + \frac{1}{2} \epsilon^t \mid m = \begin{pmatrix} \delta \\ \epsilon \end{pmatrix} \text{ with } \delta, \epsilon \in \mathbb{Z}^g \mod 2 \mathbb{Z}^g \right\}.
$$

The 2-torsion point $z_m$ is said to be even (resp. odd) if $\delta \epsilon^t \equiv 0 \mod 2$ (resp. $\delta \epsilon^t \equiv 1 \mod 2$).
The Jacobian variety of a genus $g$ curve $C$ defined over the complex numbers is principally polarized.

Let us denote by $C_d$ the $d$-fold symmetric product of $C$, which can be identified with the set of effective divisors of degree $d$ on $C$ and by $\Pi$ the normalized degree $g - 1$ Abel-Jacobi map, $\Pi : C_{g - 1} \longrightarrow \text{Jac}(C)$, whose image $\Pi(C_{g - 1})$ is precisely the theta divisor $\Theta$, i.e. the zero locus of Riemann theta function

$$\theta(z, \Omega) := \sum_{n \in \mathbb{Z}^g} \exp(\pi i (n\Omega t + 2nz)).$$

To the analytic theta characteristic $\delta \epsilon \in \mathbb{Z}^g \mod \mathbb{Z}^g$, we will attach the holomorphic theta function $\theta[\delta \epsilon](z, \Omega) : \mathbb{C}^g \times \mathbb{H}_g \longrightarrow \mathbb{C}$

defined by

$$\theta[\delta \epsilon](z, \Omega) := \exp \left( \pi i \left( (n + \frac{1}{2}\delta)\Omega(n + \frac{1}{2}\delta)^t + 2(n + \frac{1}{2}(z + \frac{1}{2}\epsilon)^t) \right) \right) \cdot \theta \left( z + \frac{1}{2}\Omega \delta^t + \frac{\epsilon^t}{2}, \Omega \right).$$

The map

$$(\mathbb{Z}^g \mod 2\mathbb{Z}^g)^2 \longrightarrow \text{Jac}(C)[2], \quad m = [\delta \epsilon] \longmapsto z_m := \frac{1}{2}\Omega \delta^t + \frac{\epsilon^t}{2}$$

is a bijection between the set of analytic theta characteristics and the set of 2-torsion points of $\text{Jac}(C)$.

The choices of the basis $\omega_1, \ldots, \omega_g$ of the space of holomorphic differential forms on $C$ provides the canonical map from $C$ to $\mathbb{P}^{g - 1}$, given by

$$\phi : C \longrightarrow \mathbb{P}^{g - 1}, \quad \phi(P) := (\omega_1(P) : \cdots : \omega_g(P)).$$

Note that if the curve and the differentials are all defined over the same number field $K$, then the canonical map is also defined over $K$. The following result relates the canonical images of certain divisors with their images through the Abel-Jacobi map:
Proposition 3 ([17]). Let $P_1, \ldots, P_{g-1} \in C(\bar{K})$ such that the divisor $D = P_1 + \cdots + P_{g-1}$ satisfies $l(D) = 1$. The equation:

$$H_D(X_1, \ldots, X_g) := \left( \frac{\partial \theta}{\partial z_1}(\Pi(D)), \ldots, \frac{\partial \theta}{\partial z_g}(\Pi(D)) \right) \Omega^{-1} \begin{pmatrix} X_1 \\ \vdots \\ X_g \end{pmatrix} = 0$$

determines a hyperplane $H_D$ of $\mathbb{P}^{g-1}$ which cuts the curve $\phi(C)$ on the divisor $\phi(D)$.

3.2. Explicit version of Torelli’s theorem in dimension 3. An isomorphism between principally polarized abelian varieties $(A_1, E_1)$ and $(A_2, E_2)$ is an isomorphism between the varieties $A_1$ and $A_2$ which conserves the polarization (i.e. transforms $E_1$ into $E_2$). An isomorphism between two curves $C_1$ and $C_2$ induces (up to translation) an isomorphism between their (principally polarized) Jacobians $\text{Jac}(C_1)$ and $\text{Jac}(C_2)$. Furthermore, Torelli’s theorem [40] asserts that the Jacobian $\text{Jac}(C)$ with its principal polarization $E$ determines the curve $C$ up to isomorphism: If $(\text{Jac}(C), E)$ and $(\text{Jac}(C'), E')$ are isomorphic as principally polarized abelian varieties, then the curve $C$ and $C'$ are also isomorphic. By Torelli’s theorem the curve $C$ is completely determined by its principally polarized Jacobian $\text{Jac}(C)$. If we just consider $\text{Jac}(C)$ only as an unpolarized abelian variety, then there could exist a curve $C'$ non-isomorphic to $C$ but with the same unpolarized Jacobian [20, 21, 11, 19].

The following theorem holds in the case of absolutely simple principally polarized abelian variety of dimension 3:

**Theorem 1.** An absolutely simple principally polarized abelian variety of dimension 3 over the complex numbers is the Jacobian of a genus 3 curve. This curve is unique up to isomorphism.

In the following we are interested in finding an efficient algorithmic method to make Torelli’s theorem explicit in dimension 3:

For a given absolutely simple principally polarized abelian variety $A$ of dimension 3 given by its normalized period matrix $\Omega$, decide if $A$ is the Jacobian of a hyper- or a non-hyperelliptic curve $C$ of genus 3, and if so find the equation of such a curve.

The following theorem gives us an answer to this decisional problem, whether the curve $C$ (in Torelli’s theorem) is hyperelliptic or non-hyperelliptic:

**Theorem 2.** Let $\Omega \in \mathbb{H}_3$ be a period matrix of an absolutely simple principally polarized abelian variety of dimension 3. Then

1. $\Omega$ is hyperelliptic if and only if exactly one even theta constant vanishes in $\Omega$.
2. $\Omega$ is non-hyperelliptic if and only if no even theta constant vanishes in $\Omega$.

A non-hyperelliptic curve of genus 3 defined over a field of characteristic different from 2 has exactly 28 different bitangents, where bitangents are lines $l$, such that the intersection divisor $(l \cdot C)$ is of the form $2P + 2Q$ for some (not necessarily distinct) points $P, Q$ of $C$. There is a canonical bijection between the set of bitangents and the set of odd 2-torsion points of the Jacobian $\text{Jac}(C)$ (see [16]). Due to Proposition 3, the bitangent associated to the odd 2-torsion point $z_0$ is given by the line with
We denote by $\beta$ to construct a quartic for which the equation:

$$
(4) \quad \left( \frac{\partial \theta}{\partial z_1}(z_0), \frac{\partial \theta}{\partial z_2}(z_0), \frac{\partial \theta}{\partial z_3}(z_0) \right) \Omega_1^{-1} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = 0.
$$

**Definition 3** \([\text{[7]}]\). Let $S = \{[\epsilon_i]\}_{i=1,...,7}$ be a subset of characteristics. The subset $S$ is called a principal set if

(i) every odd characteristic can be written as $[\epsilon_i]$ or $[\epsilon_i] + [\epsilon_j]$, $i \neq j$, and

(ii) every even characteristic can be written as $[0]$ or $[\epsilon_i] + [\epsilon_j] + [\epsilon_k]$, with distinct $i, j, k$.

In the following we use the canonically principal system $S := \{[\epsilon_i]\}_{i=1,...,7}$ where

$$
\epsilon_1 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \quad \epsilon_2 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}, \quad \epsilon_3 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}, \quad \epsilon_4 = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix},
$$

$$
\epsilon_5 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad \epsilon_6 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}, \quad \epsilon_7 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}.
$$

We denote by $\beta_i$ the bitangent associated to $[\epsilon_i]$ and by $\beta_{ij}$ the bitangent associated to $[\epsilon_i] + [\epsilon_j]$. The set $(\beta_i)$ forms an Aronhold system, i.e. a set of bitangents with the property, that the intersection points (with the quartic) of three arbitrary bitangents in this set are never on a conic \([7]\).

After performing some adequate linear transformations, we may suppose

$$
(5) \quad \begin{cases} 
\beta_1 : x_1 = 0, & \beta_5 : a_1 x_1 + a_2 x_2 + a_3 x_3 = 0, \\
\beta_2 : x_2 = 0, & \beta_6 : a'_1 x_1 + a'_2 x_2 + a'_3 x_3 = 0, \\
\beta_3 : x_3 = 0, & \beta_7 : a''_1 x_1 + a''_2 x_2 + a''_3 x_3 = 0,
\end{cases}
$$

It is well known as a classical result since the first work of Riemann \([30]\), how to construct a quartic for which the $(\beta_i)_{i=1,...,7}$ are one of its Aronhold systems. Recently, Caporaso and Sernesi \([4]\) as well as Lehavi \([22, 23]\) proved that such a quartic is uniquely determined by the set of the 7 bitangents $(\beta_i)_{i=1,...,7}$. In the following theorem, we describe the Riemann construction in order to find the equation of a plane quartic with given bitangents associated to a principal system (cf. \([31]\)):

**Theorem 3** (Riemann, \([30]\)). The curve $C$ is isomorphic to the quartic (which we call a Riemann model)

$$
(6) \quad \sqrt{x_1 v_1} + \sqrt{x_2 v_2} + \sqrt{x_3 v_3} = 0,
$$

where $v_1, v_2, v_3$ satisfy

$$
\begin{align*}
&v_1 + v_2 + v_3 + x_1 + x_2 + x_3 = 0, \\
&\frac{v_1}{a_1} + \frac{v_2}{a_2} + \frac{v_3}{a_3} + k a_1 x_1 + k a_2 x_2 + k a_3 x_3 = 0, \\
&\frac{v_1}{a'_1} + \frac{v_2}{a'_2} + \frac{v_3}{a'_3} + k' a'_1 x_1 + k' a'_2 x_2 + k' a'_3 x_3 = 0, \\
&\frac{v_1}{a''_1} + \frac{v_2}{a''_2} + \frac{v_3}{a''_3} + k'' a''_1 x_1 + k'' a''_2 x_2 + k'' a''_3 x_3 = 0,
\end{align*}
$$

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
with $k, k', k''$ solutions of
\[
\begin{pmatrix}
\frac{1}{a_1} & \frac{1}{a_1'} & \frac{1}{a_1''} \\
\frac{1}{a_2} & \frac{1}{a_2'} & \frac{1}{a_2''} \\
\frac{1}{a_3} & \frac{1}{a_3'} & \frac{1}{a_3''}
\end{pmatrix}
\begin{pmatrix}
\lambda \\
\lambda' \\
\lambda''
\end{pmatrix} =
\begin{pmatrix}
-1 \\
-1 \\
-1
\end{pmatrix}.
\]

The 28 bitangents can be expressed through the following equations:
\[
\beta_1 : x_1 = 0, \quad \beta_2 : x_2 = 0, \quad \beta_3 : x_3 = 0,
\]
\[
\beta_{21} : v_1 = 0, \quad \beta_{13} : v_2 = 0, \quad \beta_{12} : v_3 = 0,
\]
\[
\beta_4 : x_1 + x_2 + x_3 = 0, \quad \beta_5 : a_1 x_1 + a_2 x_2 + a_3 x_3 = 0,
\]
\[
\beta_6 : a_1' x_1 + a_2' x_2 + a_3' x_3 = 0, \quad \beta_7 : a_1'' x_1 + a_2'' x_2 + a_3'' x_3 = 0,
\]
\[
\beta_{14} : v_1 + v_2 + x_3 = 0, \quad \beta_{15} : \frac{v_1}{a_1} + k a_2 x_2 + k a_3 x_3 = 0,
\]
\[
\beta_{16} : \frac{v_1}{a_1} + k' a_2' x_2 + k' a_3' x_3 = 0, \quad \beta_{17} : \frac{v_1}{a_1} + k'' a_2'' x_2 + k'' a_3'' x_3 = 0,
\]
\[
\beta_{24} : x_1 + v_2 + x_3 = 0, \quad \beta_{25} : k a_1 x_1 + \frac{v_2}{a_2} + k a_3 x_3 = 0,
\]
\[
\beta_{26} : k' a_1' x_1 + \frac{v_2}{a_2} + k' a_3' x_3 = 0, \quad \beta_{27} : k'' a_1'' x_1 + \frac{v_2}{a_2} + k'' a_3'' x_3 = 0,
\]
\[
\beta_{34} : x_1 + x_2 + v_3 = 0, \quad \beta_{35} : k a_1 x_1 + k a_2 x_2 + \frac{v_3}{a_3} = 0,
\]
\[
\beta_{36} : k' a_1' x_1 + k' a_2' x_2 + \frac{v_3}{a_3} = 0, \quad \beta_{37} : k'' a_1'' x_1 + k'' a_2'' x_2 + \frac{v_3}{a_3} = 0,
\]
\[
\beta_{57} : \frac{x_1}{1-ka_2a_3} + \frac{x_2}{1-ka_1a_3} + \frac{x_3}{1-ka_1a_2} = 0,
\]
\[
\beta_{56} : \frac{x_1}{1-k'a_2'a_3} + \frac{x_2}{1-k'a_1'a_3} + \frac{x_3}{1-k'a_1'a_2} = 0,
\]
\[
\beta_{35} : \frac{v_1}{a_1(1-ka_2a_3)} + \frac{v_2}{a_2(1-ka_1a_3)} + \frac{v_3}{a_3(1-ka_1a_2)} = 0,
\]
\[
\beta_{46} : \frac{v_1}{a_1(1-k'a_2'a_3)} + \frac{v_2}{a_2(1-k'a_1'a_3)} + \frac{v_3}{a_3(1-k'a_1'a_2)} = 0,
\]
\[
\beta_{47} : \frac{v_1}{a_1'(1-ka_2'a_3)} + \frac{v_2}{a_2'(1-k'a_1'a_3)} + \frac{v_3}{a_3'(1-k'a_1'a_2)} = 0.
\]

Remark 2. By Riemann’s notation $\sqrt{x_1 v_1} + \sqrt{x_2 v_2} + \sqrt{x_3 v_3} = 0$, we mean the plane quartic with equation $(x_1 v_1 + x_2 v_2 - x_3 v_3)^2 - 4x_1 x_2 v_1 v_2 = 0$.

Let $A$ be an absolutely simple principally polarized abelian variety of dimension 3 given by its torus representation $A = \mathbb{C}^3/(\Omega_1 \mathbb{Z}^3 + \Omega_2 \mathbb{Z}^3)$ with $\Omega := \Omega_1^{-1} \Omega_2 \in \mathbb{H}_3$. The following procedure could be used to reconstruct the equation of the Riemann model of a plane quartic $C/\mathbb{C}$ with $\text{Jac}(C) \simeq A$:

(i) From the computation of the 36 even theta constants given by $A$, we decide if $A$ is the Jacobian of a non-hyperelliptic curve $C$ using Theorem 2.

(ii) If $A \simeq \text{Jac}(C)$ for a non-hyperelliptic curve $C$, then we can efficiently compute the derivatives of the theta function evaluated at odd 2-torsion points $z_{\epsilon_i}$ ($\epsilon_i \in S$). With (1), we then compute the equations of the 7 bitangents $\beta_i$ of the Aronhold system $S$.

(iii) Using linear transformations, we rewrite the 7 bitangents $\beta_i$ associated to $[\epsilon_i]_{i=1}^{7}$ in the form given in (5). With Theorem 3 it is an easy task to compute the equation of the Riemann model of a curve $C/\mathbb{C}$ with $\text{Jac}(C) \simeq A$. 

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
Remark 3. For a genus 3 non-hyperelliptic curve $C$ defined over a field $k$ of characteristic different from 2, the field of definition $k'$ of the 28 bitangents of $C$ is exactly the field of definition of the odd 2-torsion points of its Jacobian, so the maximal degree of the extension $k'/k$ is the order of $\text{Sp}_6(\mathbb{F}_2)$ which is equal to $1451520 = 28 \cdot 27 \cdot 10 \cdot 8 \cdot 6 \cdot 4$ (cf. [24]). This maximal degree occurs generically for curves defined over $\mathbb{Q}$. In order to obtain an equation defined over smaller fields, it is more appropriate to study models arising from Shioda’s transformations which lead to equations defined over an extension $k''$ of $k$ of maximal degree 24.

4. NON-HYPERELLIPTIC MODULAR JACOBIANS OF DIMENSION 3

Our goal in this section is to apply the method described in the previous section to describe all the principally polarized 3-dimensional abelian varieties $A_f$ of $J_0(N)_{\text{new}}, N \leq 4000$, which are Jacobian of non-hyperelliptic curves of genus 3.

As an optimal quotient of the Jacobian of $X_0(N)$, the abelian variety $A_f$ has a natural polarization induced by the canonical polarization defined on the Jacobian $J_0(N)$. We will consider this natural polarization $H_f$ on $A_f$ to check if $A_f$ is principally polarized. The computations for $A_f$ were performed in MAGMA [25] using the package MAV [15] written by González-Jiménez and Guàrdia. We are then able to test if the polarization $H_f$ is principal, and we can also compute the period matrix $\Omega_f$ relative to the polarization $H_f$. After computing theta constants, we use the method described in the previous section to compute (in the case that $A_f$ is absolutely simple) the equation of a curve $C_f$ such that $\text{Jac}(C_f) \simeq A_f$. In our computations, we had to use the first 20,000 Fourier coefficients of the newform $f \in S_2^{\text{new}}(N)$ to reach the precision required to find rational Dixmier invariants. For more technical details on the precision of our computations (of the Riemann model and the associated Dixmier invariants) see [27].

We looked at all the abelian varieties $A_f$ of $J_0(N)_{\text{new}}$ with $N \leq 4000$. Table 1 provides the number of abelian varieties $A_f$ which are principally polarized, hyperelliptic, and non-hyperelliptic modular Jacobians of dimension 3. These results are not surprising, indeed a generic curve of genus 3 is non-hyperelliptic and the moduli space of hyperelliptic curves of genus 3 has codimension 1 in the moduli of curves of genus 3.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>3334</td>
<td>79</td>
<td>12</td>
</tr>
</tbody>
</table>

Unfortunately, numerical evidence indicates that the models are, in general, not defined over $\mathbb{Q}$. The Dixmier invariants are defined over $\mathbb{Q}$ as expected. However, it is a difficult task to solve the following problem:

*From a complete set of given Dixmier-Ohno invariants $\{i_1, \ldots, i_{12}\}$ defined over a field $k$, compute a model of a smooth plane quartic $C$ defined over the same field $k$ which has exactly these invariants.*
However, if modular Jacobians are also expected (as in [14, 12]) to be described by curves with small integer coefficients, we may try to compute the equations of such models by brute force.

For the special case of modular Jacobians $A_f \simeq \text{Jac}(C_f)$ which admit a model $C_{\text{rat}}$ defined over $\mathbb{Q}$ with a $\mathbb{Q}$-rational flex, we can use the following deterministic algorithm to compute such a $\mathbb{Q}$-rational equation:

(i) Compute all the 24 flexes $\xi_1, \ldots, \xi_{24}$ of $C_f$.
(ii) For each $\xi_j$, compute the unique Shioda normal form $C_{\xi_j}$ relative to $(C, \xi_j)$.
(iii) The curve $(C_f, \xi_j)$ admits a $\mathbb{Q}$-rational model if and only if one of the above equations $C_{\xi_j}$ has only $\mathbb{Q}$-rational coefficients.

In fact, this method gives us an efficient algorithm to test (and compute) if a given curve $C/\mathbb{C}$ admits a model $(C, \xi)$ defined over $\mathbb{Q}$. With this algorithm we are also able to determine the structure of the automorphism group $\text{Aut}(C)$ of $C$ : An automorphism $\varphi \neq \text{Id}$ of $C$ fixes at most $2g - 2 = 8$ points of $C$, i.e. $\varphi$ cannot act trivially on the set of Weierstrass points of $C$. The normal forms $C_{\xi_1}$ and $C_{\xi_2}$ at two distinct Weierstrass points $\xi_1, \xi_2$ are equal if and only if $\xi_1 = \xi_2^\varphi$ for a $\varphi \in \text{Aut}(C)$.

In the following, we label the genus 3 curves coming from $\mathbb{Q}$-simple new modular Jacobians $A_f$ of level $N$ by $X^3_N$, where $N$ denotes the level of $X^3_N$ and the letter $A$ denotes the position with respect to the ordering given as output of the MAGMA-function $\text{SortDecomposition}$. In the appendix (see Table 6) we listed out all $\mathbb{Q}$-simple quotients $A_f$ of $J_0(N)^{\text{new}}$ with $N \leq 600$, as well as their Dixmier invariants. In the thesis of the author [27], this table was extended to $N \leq 4000$.

**Remark 4.** As an abelian variety of the $GL_2$-type, the abelian variety $A_f$ has exactly $2^M$ isomorphic classes of principal polarizations over $\mathbb{Q}$, where $0 \leq M \leq [K_f : \mathbb{Q}] - 1$ (see [14]). We only studied $A_f$ with respect to its canonical polarization $H_f$. However, it is clear that another non-isomorphic principal polarization $P_f$ of the absolutely simple variety $A_f$ should give a non-isomorphic model $C'$ for which the Jacobians $\text{Jac}(C)$ and $\text{Jac}(C')$ are both isomorphic to $A_f$ as unpolarized abelian varieties. It is also possible to have non-hyperelliptic curves and hyperelliptic curves of genus 3 whose Jacobians are (as unpolarized abelian varieties) isomorphic to $A_f$, $f \in S_2^{\text{new}}(N)$.

To conclude, we illustrate our algorithm with the following example.

**Example 1.** Let $N = 369 = 3^2 \cdot 41$ and $f$ be the newform in $S_2^{\text{new}}(369)$ with Fourier expansion

$$f = q + aq^2 + (a^2 - 2)q^4 + (-a - 2)q^5 + (-a^2 - a + 2)q^7 + (-2a^2 - 2a + 2)q^8 + O(q^{10}),$$

where $a^3 + 2a^2 - 2a - 2 = 0$. The modular abelian variety $A_f$ is absolutely simple (it can be checked using MAGMA that the newform $f$ has no CM\textsuperscript{1} and thus $A_f$ is absolutely simple (cf. [12])). Furthermore, $A_f$ is isomorphic to a torus which has a symplectic basis $\{\lambda_1, \ldots, \lambda_6\}$ such that the intersection pairing $H_f$ has the representation

$$(H_f(\lambda_i, \lambda_j))_{1 \leq i, j \leq 6} = \begin{pmatrix} 0 & \Delta_f \\ -\Delta_f & 0 \end{pmatrix} \in \mathbb{Z}^{6 \times 6}$$

\textsuperscript{1}The newform $f = q + \sum_{i \geq 2} a_i q^i \in S_2^{\text{new}}(N)$ has complex multiplication (CM) if there exists a non-trivial character $\chi$ of $\text{Gal}(\mathbb{Q}^{\text{ab}})$ such that $a_p = \chi(p) a_p$ for all primes $p$ not dividing $N$. 

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
with diagonal matrix
\[ \Delta_f = 8 \cdot \text{Id}, \]
that means, \( A_f \) is a principally polarized abelian variety, which has the torus representation \( \mathbb{C}^3 / (\mathbb{Z}^3 + \Omega_f \mathbb{Z}^3) \) with period matrix
\[
\Omega_f = \begin{pmatrix}
0.55467 \cdots + 3.07521 \cdots & -0.79883 \cdots + 0.11922 \cdots & 0.85186 \cdots + 0.79061 \cdots \\
-0.79883 \cdots + 0.11922 \cdots & 0.74004 \cdots + 0.43861 \cdots & -0.04497 \cdots - 0.32299 \cdots \\
0.85186 \cdots + 0.79061 \cdots & -0.04497 \cdots - 0.32299 \cdots & 0.65132 \cdots + 0.97328 \cdots
\end{pmatrix}.
\]

Using Theorem 1, there is a curve \( C_f \) of genus 3 with \( A_f \cong \text{Jac}(C_f) \). Straightforward computations with an appropriate precision for computations over the complex field show that no even theta constant vanishes and Theorem 2 implies that \( C_f \) is non-hyperelliptic. By equation (1), the bitangents associated to the canonical Aronhold system \( S = (\epsilon_i) \) (cf. page 1181) have the equations
\[
\beta_1 : 0 = x - (1.62009 \cdots - 0.88123 \cdots i) y + (0.60794 \cdots - 1.09289 \cdots i) z,
\beta_2 : 0 = x - (1.62009 \cdots + 0.88123 \cdots i) y + (0.60794 \cdots + 1.09289 \cdots i) z,
\beta_3 : 0 = x - (1.18597 \cdots - 0.01375 \cdots i) y + (0.07649 \cdots + 0.00738 \cdots i) z,
\beta_4 : 0 = x - (0.13444 \cdots - 0.32339 \cdots i) y + (0.79703 \cdots - 0.39889 \cdots i) z,
\beta_5 : 0 = x - (2.88498 \cdots + 2.57527 \cdots i) y + (2.95024 \cdots - 6.21143 \cdots i) z,
\beta_6 : 0 = x - (0.02710 \cdots + 0.18672 \cdots i) y + (0.75712 \cdots - 0.74714 \cdots i) z,
\beta_7 : 0 = x - (0.90241 \cdots - 1.65452 \cdots i) y - (2.06151 \cdots + 1.61189 \cdots i) z,
\]
which become
\[
\beta_1 : 0 = x,
\beta_2 : 0 = y,
\beta_3 : 0 = z,
\beta_4 : 0 = x + y + z,
\beta_5 : 0 = x + (0.99571 \cdots + 0.01530 \cdots i) y + (0.99650 \cdots - 0.00242 \cdots i) z,
\beta_6 : 0 = x + (0.99999 \cdots + 0.00218 \cdots i) y + (0.99655 \cdots + 0.00029 \cdots i) z,
\beta_7 : 0 = x + (1.00406 \cdots + 0.01543 \cdots i) y + (0.98864 \cdots - 0.00065 \cdots i) z,
\]
after performing the adequate linear transformations.

Using Theorem 3, we compute the Riemann model for the canonical embedding of \( C_f \), and obtain
\[
C_f : (xv_1 + yv_2 - zv_3)^2 = 4xyv_1v_2,
\]
where
\[
v_1 = (2.41739 \cdots + 0.67174 \cdots i) x + (1.39123 \cdots + 0.65332 \cdots i) y + (1.40882 \cdots + 0.65261 \cdots i) z,
v_2 = -(1.55957 \cdots + 0.16076 \cdots i) x - (0.52956 \cdots + 0.15658 \cdots i) y - (1.54558 \cdots + 0.14781 \cdots i) z,
v_3 = -(1.85781 \cdots + 0.51098 \cdots i) x - (1.86167 \cdots + 0.49673 \cdots i) y - (0.86323 \cdots + 0.50480 \cdots i) z.
\]

Up to a certain precision, the curve \( C_f \) has the \( \mathbb{Q} \)-rational Dixmier invariants
\[
i_1 = \frac{7^6}{2^{24} \cdot 3^8 \cdot 41^3}, \quad i_2 = \frac{7^7 \cdot 97}{2^{24} \cdot 3^8 \cdot 41^3},
i_3 = \frac{7^6 \cdot 6353}{2^{24} \cdot 3^8 \cdot 41^3}, \quad i_4 = \frac{7^7 \cdot 73 \cdot 31337}{2^{24} \cdot 3^8 \cdot 41^3},
i_5 = \frac{7^4 \cdot 43 \cdot 4662331}{2^{24} \cdot 3^8 \cdot 41^3}, \quad i_6 = \frac{7^5 \cdot 1307 \cdot 1691 \cdot 5303}{2^{24} \cdot 3^8 \cdot 41^3}.
\]
We note that by using Shioda’s transformations at the ordinary flex
\[ \xi = (0.60900 \cdots - 0.79316 \cdots i : -1.62391 \cdots + 0.77629 \cdots i : 1) \]
with tangent line
\[ T_\xi: 0 = -(0.03895 \cdots + 0.2027 \cdots i)x - (0.03870 \cdots + 0.01924 \cdots i) - (0.03799 \cdots + 0.01975 \cdots i)z \]
we obtain the model
\[ C'_f: 0 = y^3z + y(x^3 - 9.14494 \cdots 10^{-4}xz^2 - 1.37989 \cdots 10^{-5}z^3) - 9.14494 \cdots 10^{-4}x^3z \
+ 5.08502 \cdots 10^{-5}x^2z^2 + 2.09075 \cdots 10^{-6}xz^3 + 1.44354 \cdots 10^{-8}z^4, \]
which is, up to a certain precision, the \( \mathbb{Q} \)-rational curve with the equation
\[ 0 = y^3 + y(x^3 - \frac{2}{2187}xz^2 - \frac{22}{1943523}z^3) - \frac{2}{2187}x^3z + \frac{1}{19683}z^2 + \frac{10}{4782969}xz^3 + \frac{151}{10460353203}z^4. \]

For some modular Jacobians, we get additional bad reductions for the curve \( C_f \) at some primes \( p \) not dividing the level \( N \). For all the modular Jacobians \( \text{Jac}(C_f) \simeq A_f \) of level \( N \leq 4000 \), whenever this phenomenon appears, the discriminant of the smooth plane quartic \( C_f \) always admits a factor \( p^{14} \) at such primes \( p \) (cf. Appendix). At this time, the author cannot give a reasonable explanation for this phenomenon.

5. Conclusion

Initially, our intention behind the computation of the equations of genus 3 non-hyperelliptic new modular curves with \( \mathbb{Q} \)-simple Jacobian was based on their presumably attractive application to cryptosystems based on the discrete logarithm problem (DLP) on finite abelian groups. Generically, the fact that a curve \( C \) is secure lies on the fact that the group order \( \#\text{Jac}(C)(\mathbb{F}_q) \) has a large prime divisor. The computation of \( \#\text{Jac}(C)(\mathbb{F}_q) \) is thus an important milestone for testing the security of those cryptosystems. From this point of view, modular Jacobians provided attractive groups for the DLP. Then by using the characteristic polynomials \( \chi_{T_p} \) of the Hecke operators \( T_p \) acting on the Tate module of \( A_f \), the Eichler-Shimura relation enables us to compute \( \#A_f(\mathbb{F}_p) \) at primes \( p \) with good reduction by
\[ \#A_f(\mathbb{F}_p) = \chi_{T_p}(p + 1). \]
Moreover, there exists fast algorithms for performing the group law on the Jacobians of non-hyperelliptic curves of genus 3 (see [8, 9, 32]). Meanwhile, Diem and Thomé [5] provided a method to solve the DLP on Jacobians of smooth plane quartics which has an heuristic complexity of \( \tilde{O}(q) \), where \( q \) is the number of elements of the finite field \( \mathbb{F}_q \); this attack makes the use of non-hyperelliptic curves of genus 3 in comparison to other cryptosystem (ECC and HECC see for example [1]) at this time no longer competitive. In fact, the size of the parameters should then be enlarged by about 50% (i.e. \( q \approx 2^{81} \)) to maintain the security level.
### Dixmier invariants

<table>
<thead>
<tr>
<th>curves</th>
<th>Dixmier invariants</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X_{A}^97$</td>
<td>$i_1 = \frac{23^3}{23^3, 23^2, 23} \ 23^7$</td>
</tr>
<tr>
<td></td>
<td>$i_2 = \frac{23^7}{23^7} \ 23^0$</td>
</tr>
<tr>
<td></td>
<td>$i_3 = \frac{23^9}{23^9} \ 23^0$</td>
</tr>
<tr>
<td></td>
<td>$i_4 = \frac{23^9}{23^9} \ 23^0$</td>
</tr>
<tr>
<td></td>
<td>$i_5 = 23^9 \ 23^0$</td>
</tr>
<tr>
<td></td>
<td>$i_6 = 23^9 \ 23^0$</td>
</tr>
<tr>
<td>$X_{B}^{169}$</td>
<td>$i_1 = \frac{23^3}{23^3} \ 23^0$</td>
</tr>
<tr>
<td></td>
<td>$i_2 = \frac{23^3}{23^3} \ 23^0$</td>
</tr>
<tr>
<td></td>
<td>$i_3 = \frac{23^3}{23^3} \ 23^0$</td>
</tr>
<tr>
<td></td>
<td>$i_4 = \frac{23^3}{23^3} \ 23^0$</td>
</tr>
<tr>
<td></td>
<td>$i_5 = 23^3 \ 23^0$</td>
</tr>
<tr>
<td></td>
<td>$i_6 = 23^3 \ 23^0$</td>
</tr>
<tr>
<td>$X_{C}^{113}$</td>
<td>$i_1 = \frac{23^3}{23^3} \ 23^0$</td>
</tr>
<tr>
<td></td>
<td>$i_2 = \frac{23^3}{23^3} \ 23^0$</td>
</tr>
<tr>
<td></td>
<td>$i_3 = \frac{23^3}{23^3} \ 23^0$</td>
</tr>
<tr>
<td></td>
<td>$i_4 = \frac{23^3}{23^3} \ 23^0$</td>
</tr>
<tr>
<td></td>
<td>$i_5 = 23^3 \ 23^0$</td>
</tr>
<tr>
<td></td>
<td>$i_6 = 23^3 \ 23^0$</td>
</tr>
<tr>
<td>$X_{A}^{127}$</td>
<td>$i_1 = \frac{23^3}{23^3, 23^2, 23} \ 23^7$</td>
</tr>
<tr>
<td></td>
<td>$i_2 = \frac{23^7}{23^7} \ 23^0$</td>
</tr>
<tr>
<td></td>
<td>$i_3 = \frac{23^9}{23^9} \ 23^0$</td>
</tr>
<tr>
<td></td>
<td>$i_4 = \frac{23^9}{23^9} \ 23^0$</td>
</tr>
<tr>
<td></td>
<td>$i_5 = 23^9 \ 23^0$</td>
</tr>
<tr>
<td></td>
<td>$i_6 = 23^9 \ 23^0$</td>
</tr>
<tr>
<td>$X_{B}^{19}$</td>
<td>$i_1 = \frac{23^3}{23^3} \ 23^0$</td>
</tr>
<tr>
<td></td>
<td>$i_2 = \frac{23^3}{23^3} \ 23^0$</td>
</tr>
<tr>
<td></td>
<td>$i_3 = \frac{23^3}{23^3} \ 23^0$</td>
</tr>
<tr>
<td></td>
<td>$i_4 = \frac{23^3}{23^3} \ 23^0$</td>
</tr>
<tr>
<td></td>
<td>$i_5 = 23^3 \ 23^0$</td>
</tr>
<tr>
<td></td>
<td>$i_6 = 23^3 \ 23^0$</td>
</tr>
</tbody>
</table>

### Additional Table

<table>
<thead>
<tr>
<th>curves</th>
<th>Dixmier invariants</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X_{B}^{151}$</td>
<td>$i_1 = \frac{23^3}{23^3} \ 23^0$</td>
</tr>
<tr>
<td></td>
<td>$i_2 = \frac{23^3}{23^3} \ 23^0$</td>
</tr>
<tr>
<td></td>
<td>$i_3 = \frac{23^3}{23^3} \ 23^0$</td>
</tr>
<tr>
<td></td>
<td>$i_4 = \frac{23^3}{23^3} \ 23^0$</td>
</tr>
<tr>
<td></td>
<td>$i_5 = 23^3 \ 23^0$</td>
</tr>
<tr>
<td></td>
<td>$i_6 = 23^3 \ 23^0$</td>
</tr>
</tbody>
</table>

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
<table>
<thead>
<tr>
<th>Curves</th>
<th>Dixmier Invariants</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X_{203}$</td>
<td>$i_1 = \frac{7 \cdot 17^6}{23 \cdot 37 + 29^7}, \quad i_2 = \frac{5^2 \cdot 17^5}{23 \cdot 37 + 29^7}, \quad i_3 = \frac{5 \cdot 7 \cdot 17^6 \cdot 353}{23 \cdot 37 + 29^7}, \quad i_4 = \frac{2 \cdot 17^7}{23 \cdot 37 + 29^7}, \quad i_5 = \frac{\sqrt{11} \cdot 71 \cdot 37017}{23 \cdot 37 + 29^7}, \quad i_6 = \frac{\sqrt{11} \cdot 19 \cdot 197 \cdot 145664659}{23 \cdot 37 + 29^7} $</td>
</tr>
<tr>
<td>$X_{217}$</td>
<td>$i_1 = \frac{5^2 \cdot 271}{23 \cdot 37 + 29^7}, \quad i_2 = \frac{5 \cdot 7 \cdot 17^6}{23 \cdot 37 + 29^7}, \quad i_3 = \frac{5 \cdot 7 \cdot 17^6 \cdot 353}{23 \cdot 37 + 29^7}, \quad i_4 = \frac{2 \cdot 17^7}{23 \cdot 37 + 29^7}, \quad i_5 = \frac{\sqrt{11} \cdot 71 \cdot 37017}{23 \cdot 37 + 29^7}, \quad i_6 = \frac{\sqrt{11} \cdot 19 \cdot 197 \cdot 145664659}{23 \cdot 37 + 29^7} $</td>
</tr>
<tr>
<td>$X_{239}$</td>
<td>$i_1 = \frac{7 \cdot 17^6}{23 \cdot 37 + 29^7}, \quad i_2 = \frac{5^2 \cdot 17^5}{23 \cdot 37 + 29^7}, \quad i_3 = \frac{5 \cdot 7 \cdot 17^6 \cdot 353}{23 \cdot 37 + 29^7}, \quad i_4 = \frac{2 \cdot 17^7}{23 \cdot 37 + 29^7}, \quad i_5 = \frac{\sqrt{11} \cdot 71 \cdot 37017}{23 \cdot 37 + 29^7}, \quad i_6 = \frac{\sqrt{11} \cdot 19 \cdot 197 \cdot 145664659}{23 \cdot 37 + 29^7} $</td>
</tr>
<tr>
<td>$X_{300}$</td>
<td>$i_1 = \frac{7 \cdot 17^6}{23 \cdot 37 + 29^7}, \quad i_2 = \frac{5^2 \cdot 17^5}{23 \cdot 37 + 29^7}, \quad i_3 = \frac{5 \cdot 7 \cdot 17^6 \cdot 353}{23 \cdot 37 + 29^7}, \quad i_4 = \frac{2 \cdot 17^7}{23 \cdot 37 + 29^7}, \quad i_5 = \frac{\sqrt{11} \cdot 71 \cdot 37017}{23 \cdot 37 + 29^7}, \quad i_6 = \frac{\sqrt{11} \cdot 19 \cdot 197 \cdot 145664659}{23 \cdot 37 + 29^7} $</td>
</tr>
</tbody>
</table>

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
<table>
<thead>
<tr>
<th>curves</th>
<th>Dixmier invariants</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X^E_{475}$</td>
<td>$i_1 = \frac{3067^{9}}{2^{24} \cdot 3^{6} \cdot 19}$</td>
</tr>
<tr>
<td></td>
<td>$i_2 = 479 \cdot 3067^{7} \cdot 15937$</td>
</tr>
<tr>
<td></td>
<td>$i_3 = 193 \cdot 3067^{6} \cdot 115419877$</td>
</tr>
<tr>
<td></td>
<td>$i_4 = 41 \cdot 3067^{5} \cdot 41993 \cdot 2234129$</td>
</tr>
<tr>
<td></td>
<td>$i_5 = 13 \cdot 397 \cdot 479 \cdot 3067^{4} \cdot 6619 \cdot 8887 \cdot 25349$</td>
</tr>
<tr>
<td></td>
<td>$i_6 = 3067^{3} \cdot 15879990595193 \cdot 3060901$</td>
</tr>
<tr>
<td>$X^G_{475}$</td>
<td>$i_1 = \frac{3067^{7}}{2^{23} \cdot 3^{1} \cdot 19}$</td>
</tr>
<tr>
<td></td>
<td>$i_2 = 479 \cdot 3067^{7} \cdot 15937$</td>
</tr>
<tr>
<td></td>
<td>$i_3 = 193 \cdot 3067^{6} \cdot 115419877$</td>
</tr>
<tr>
<td></td>
<td>$i_4 = 41 \cdot 3067^{5} \cdot 41993 \cdot 2234129$</td>
</tr>
<tr>
<td></td>
<td>$i_5 = 13 \cdot 397 \cdot 479 \cdot 3067^{4} \cdot 6619 \cdot 8887 \cdot 25349$</td>
</tr>
<tr>
<td></td>
<td>$i_6 = 3067^{3} \cdot 15879990595193 \cdot 3060901$</td>
</tr>
<tr>
<td>$X^B_{511}$</td>
<td>$i_1 = \frac{5^{6} \cdot 13^{6} \cdot 43133^{6}}{2^{25} \cdot 3^{3} \cdot 7 \cdot 11 \cdot 73 \cdot 101^{14}}$</td>
</tr>
<tr>
<td></td>
<td>$i_2 = -5^{5} \cdot 17^{7} \cdot 263 \cdot 43133^{5} \cdot 19768 \cdot 6021091$</td>
</tr>
<tr>
<td></td>
<td>$i_3 = \frac{6 \cdot 13 \cdot 3 \cdot 6 \cdot 43133^{6} \cdot 44702121} {2^{11} \cdot 3^{2} \cdot 7^{2} \cdot 11^{11} \cdot 73^{1} \cdot 101^{14}}$</td>
</tr>
<tr>
<td></td>
<td>$i_4 = 5^{5} \cdot 13^{2} \cdot 3^{7} \cdot 37 \cdot 43133^{4} \cdot 411 \cdot 37 \cdot 6046670328283288413280589099$</td>
</tr>
<tr>
<td></td>
<td>$i_5 = \frac{-5 \cdot 13^{2} \cdot 3^{7} \cdot 37 \cdot 43133^{3} \cdot 683333 \cdot 28659999 \cdot 3031471391388674295606558437642759} {2^{23} \cdot 29^{3} \cdot 7 \cdot 11^{14} \cdot 73^{1} \cdot 101^{14}}$</td>
</tr>
<tr>
<td></td>
<td>$i_6 = -5^{5} \cdot 13^{2} \cdot 3^{7} \cdot 37 \cdot 43133^{3} \cdot 683333 \cdot 28659999 \cdot 3031471391388674295606558437642759$</td>
</tr>
<tr>
<td>$X^H_{567}$</td>
<td>$i_1 = \frac{5^{4}}{2^{24} \cdot 3^{3}}$</td>
</tr>
<tr>
<td></td>
<td>$i_2 = 5 \cdot 17$</td>
</tr>
<tr>
<td></td>
<td>$i_3 = 5 \cdot 3^{3} \cdot 7 \cdot 11$</td>
</tr>
<tr>
<td></td>
<td>$i_4 = 17 \cdot 3 \cdot 9 \cdot 5 \cdot 7$</td>
</tr>
<tr>
<td></td>
<td>$i_5 = 5 \cdot 7 \cdot 3^{3} \cdot 7 \cdot 11$</td>
</tr>
<tr>
<td></td>
<td>$i_6 = -19 \cdot 83 \cdot 11119$</td>
</tr>
<tr>
<td></td>
<td>$2 \cdot 3^{3} \cdot 5 \cdot 7$</td>
</tr>
<tr>
<td>$X^A_{596}$</td>
<td>$i_1 = \frac{359^{9}}{2^{25} \cdot 3^{3} \cdot 149^{2}}$</td>
</tr>
<tr>
<td></td>
<td>$i_2 = 13 \cdot 21 \cdot 3 \cdot 359^{2}$</td>
</tr>
<tr>
<td></td>
<td>$i_3 = 23 \cdot 359^{6} \cdot 89348191$</td>
</tr>
<tr>
<td></td>
<td>$i_4 = 2 \cdot 359^{5} \cdot 3964900597$</td>
</tr>
<tr>
<td></td>
<td>$i_5 = 47 \cdot 359^{5} \cdot 370768577229919$</td>
</tr>
<tr>
<td></td>
<td>$i_6 = 13 \cdot 19 \cdot 359^{5} \cdot 16529 \cdot 784641 \cdot 2599117$</td>
</tr>
</tbody>
</table>
Acknowledgements

I would like to thank my supervisor Gerhard Frey and co-supervisor Enric Nart for their support, help and encouragement. Furthermore, I would like to thank Josep González, Enrique González-Jiménez, Jordi Guàrdia and Christophe Ritzenthaler for useful comments. I am also very grateful to Jordi Guàrdia for providing me his MAGMA-package MAV. Finally, I thank the anonymous referee for an especially helpful report.

References


ÉQUIPE GAATI, UNIVERSITÉ DE POLYNÉSIE FRANÇAISE, BP 6570, 98702 FA’A’A, TAHITI, POLYNÉSIE FRANÇAISE

E-mail address: roger.oyono@upf.pf