MATHEMATICS OF COMPUTATION
Volume 78, Number 266, April 2009, Pages 1173–1191
S 0025-5718(08)02174-1
Article electronically published on September 3, 2008

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 Ω, 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 $\mathrm{Jac}(C_f)$ of dimension 3 which are isomorphic to A_f, where $f \in S_2^{\mathrm{new}}(X_0(N))$, $N \leq 4000$.

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 $\mathrm{Jac}(C) \simeq A$. 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.

Received by the editor February 5, 2007 and, in revised form, March 5, 2008.
2000 *Mathematics Subject Classification.* Primary 14C34, 14G35; Secondary 11G10, 11F11, 14H42.
Key words and phrases. Modular curves, modular Jacobians, non-hyperelliptic curves of genus 3, Torelli's theorem, theta functions.
The research of this paper was done while the author was a Ph.D. student at the Institut für Experimentelle Mathematik (IEM) of the university of Essen under the supervision of Gerhard Frey.

©2008 American Mathematical Society
Reverts to public domain 28 years from publication

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, $\simeq$ means isomorphic over $\mathbb{C}$, and $\overset{\mathbb{Q}}{\simeq}$ 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 $\{\omega_1, \dots, \omega_g\}$ 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

$$\begin{array}{rccl} \phi: & C & \longrightarrow & \mathbb{P}^{g-1} \\ & P & \longmapsto & \phi(P) := (\omega_1(P) : \cdots : \omega_g(P)), \end{array}$$

where $\omega(P) = f(P)$ for any expression $\omega = f dt_P$, with $f, t_P \in k(C)$ and t_P 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

$$\begin{aligned} g(x,y,z) \quad := \quad & a_1x^4 + 4a_2x^3y + 6a_3x^2y^2 + 4a_4xy^3 + a_5y^4 + 4a_6x^3z + 12a_7x^2yz \\ & +12a_8xy^2z + 4a_9y^3z + 6a_{10}x^2z^2 + 12a_{11}xyz^2 + 6a_{12}y^2z^2 \\ & +4a_{13}xz^3 + 4a_{14}yz^3 + a_{15}z^4, \end{aligned}$$

the invariants I_3 and I_6 may be computed from:

$$\begin{aligned} I_3(g) := & a_1a_5a_{15} + 3\left(a_1a_{12}^2 + a_5a_{10}^2 + a_{15}a_3^2\right) \\ & + 4\left(a_2a_9a_{13} + a_6a_4a_{14} - a_1a_9a_{14} - a_5a_6a_{13} - a_{15}a_2a_4\right) + 6a_3a_{10}a_{12} \\ & - 12\left(a_7a_8a_{11} + a_2a_{11}a_{12} + a_6a_8a_{12} + a_4a_{11}a_{10} + a_9a_7a_{10} + a_{13}a_8a_3\right. \\ & \left. + a_{14}a_7a_3 - \left(a_7a_4a_{13} + a_8a_{14}a_2 + a_{11}a_6a_9 + a_3a_{11}^2 + a_{10}a_8^2 + a_{12}a_7^2\right)\right), \end{aligned}$$

and

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

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:

$$i_1 = \frac{I_3^9}{I_{27}}, \quad i_2 = \frac{I_3^7 I_6}{I_{27}}, \quad i_3 = \frac{I_3^6 I_9}{I_{27}}, \quad i_4 = \frac{I_3^5 I_{12}}{I_{27}}, \quad i_5 = \frac{I_3^4 I_{15}}{I_{27}}, \quad i_6 = \frac{I_3^3 I_{18}}{I_{27}}.$$

Lemma 1. *If two ternary smooth plane quartics C and C' are isomorphic, then*

$$i_j(C) = i_j(C') \qquad \textit{for} \quad j = 1, \ldots, 6\,.$$

Proof. Let $C' = C^\alpha$ with $\alpha \in \mathrm{GL}_3(\mathbb{C})$ and $D := \det(\alpha) \neq 0$. From [32] we get the following relations between I_j and I'_j:

$$I'_j = (D^4)^{\frac{j}{3}} \cdot I_j\,,$$

for $j = 3, 6, 9, 12, 15, 18, 27$. The lemma then follows from the definitions of i_j. □

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 $\xi \in C(\bar{k})$ we denote by T_ξ the tangent line to C at ξ. The intersection divisor $(C \cdot T_\xi)$ is of the form

$$(C \cdot T_\xi) = 2\xi + \xi' + \xi''$$

for some $\xi', \xi'' \in C(\bar{k})$. The point $\xi \in C(\bar{k})$ is called an ordinary flex (resp. special flex or hyperflex) if

$$(C \cdot T_\xi) = 3\xi + \xi' \text{ for some } \xi' \neq \xi \quad (\text{resp. } \quad (C \cdot T_\xi) = 4\xi\ ).$$

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 hyperfexes 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 $\bar{k}$ 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, ξ) is defined over k if C is a curve defined over k and ξ 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, ξ) defined over k, there is a coordinate system (x, y, z) of $\mathbb{P}^2$ such that (C, ξ) is given by*

$$(1) \qquad C:\ 0 = y^3 z + y(p_0 z^3 + p_1 z^2 x + x^3) + q_0 z^4 + q_1 z^3 x + q_2 z^2 x^2 + q_3 z x^3 + q_4 x^4,$$
$$\xi = (0:1:0), \qquad T_\xi:\ z = 0.$$

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

$$\lambda = (p_i, q_j) \sim \lambda' = (p'_i, q'_j) \Longleftrightarrow p'_i = u^{6-2i} p_i, \quad q'_j = u^{9-2j} q_j, \quad (i = 0, 1,\ j = 0, 1, \ldots, 4)$$

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, ξ) defined over k, there is a coordinate system (x, y, z) of $\mathbb{P}^2$ such that (C, ξ) is given by*

$$C:\ 0 = y^3 z + y(p_0 z^3 + p_1 z^2 x + p_2 z x^2) + q_0 z^4 + q_1 z^3 x + q_2 z^2 x^2 + x^4, \tag{2}$$
$$\xi = (0 : 1 : 0), \qquad T_\xi :\ z = 0.$$

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

$$\lambda = (p_i, q_j) \sim \lambda' = (p'_i, q'_j) \Longleftrightarrow p'_i = u^{8-3i} p_i, \quad q'_j = u^{12-3j} q_j, \quad (i, j = 0, 1, 2)$$

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_ξ. 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_ξ by letting $q_4 = 1$. Even if $q_4 = 0$, it is always possible to describe (C, ξ) by a unique normal form C_ξ. If, for instance, ξ is an ordinary flex and $q_4 = 0, p_1, q_3 \neq 0$, then by choosing $u = \frac{q_3}{p_1}$ 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 $p'_1 = q'_3$.

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 4):

$$X_{369}^D \ :\ 0 = y^3 z + y\left(x^3 - \frac{2}{2187} x z^2 - \frac{22}{1594323} z^3\right) - \frac{2}{2187} x^3 z + \frac{1}{19683} x^2 z^2 + \frac{10}{4782969} x z^3 + \frac{151}{10460353203} z^4 .$$

Note that one cannot view λ in the above propositions as a set of invariants for the curve C since λ depends on the flex ξ 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

$$\omega : S_2(N) \longrightarrow \Omega^1(X_0(N)),\ \ f(\tau) \longmapsto 2\pi i f(\tau) d\tau$$

induces an isomorphism between the vector spaces $S_2(N)$ and $\Omega^1(X_0(N))$.

If $M|N$ and $d|\frac{N}{M}$, then $z \mapsto d \cdot z$ 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 $J_0(N) := \mathrm{Jac}(X_0(N))$. The old subspace $S_2^{\mathrm{old}}(N)$ 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 $d|\frac{N}{M}$. Similarly, we define the old subvariety $J_0(N)^{\mathrm{old}}$ of $J_0(N)$. Let $S_2^{\mathrm{new}}(N)$ be the orthogonal complement to $S_2^{\mathrm{old}}(N)$ with respect to the Petersson inner product in

$S_2(N)$. For $n \geq 1$ 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 $S_2^{\mathrm{new}}(N)$ 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 $I_f = \{\sigma_1, \ldots, \sigma_d\}$ be the set of all isomorphisms of K_f into $\mathbb{C}$, and let $\{f^{\sigma_1}, \ldots, f^{\sigma_d}\}$ be the complete set of newform conjugates to f over $\mathbb{Q}$. Shimura [33, 34] attached to the newform $f \in S_2^{\mathrm{new}}(N)$ a subvariety A_f of $J_0(N)$ defined over $\mathbb{Q}$ with the following properties: A_f is a simple factor of $J_0(N)^{\mathrm{new}}$ over $\mathbb{Q}$, $\dim(A_f) = d$ and $\Omega^1(A_f) \simeq \sum_{\sigma\in I_f} \mathbb{C}\omega(f^\sigma)$. 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

$$\pi_f : J_0(N)^{\mathrm{new}} \twoheadrightarrow A_f\,.$$

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

$$J_0(N)^{\mathrm{new}} \overset{\mathbb{Q}}{\sim} \prod_{f\in B_N} A_f \quad \text{and} \quad J_0(N)^{\mathrm{old}} \overset{\mathbb{Q}}{\sim} \prod_{M|N, M\neq N} \prod_{f\in B_M} A_f^{\sigma_0(\frac{N}{M})},$$

where $\sigma_0(n)$ denotes the number of positive divisors of n.

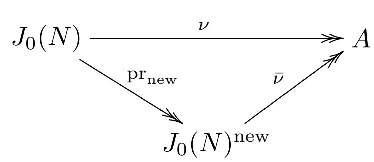
Definition 1 ([13, 2])**.** An abelian variety A over $\mathbb{Q}$ is said to be $\mathbb{Q}$-modular of level N, if there exists a surjective $\mathbb{Q}$-morphism

$$\nu : J_0(N) \twoheadrightarrow A\,.$$

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

$$\bar\nu : J_0(N)^{\mathrm{new}} \twoheadrightarrow A\,.$$

The following diagram is then commutative:



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

$$\pi : X_0(N) \twoheadrightarrow C\,.$$

The curve C is then said to be new of level N if its Jacobian $\mathrm{Jac}(C)$ is new of level N.

For a modular curve C, the following diagram commutes:

$$\begin{array}{ccc} J_0(N) & \xrightarrow{\pi_*} & \mathrm{Jac}(C) \\ \uparrow & & \uparrow \\ X_0(N) & \xrightarrow{\pi} & C \end{array}$$

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 1, for each $g \geq 2$ the set of 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 Λ is a full $\mathbb{Z}$-lattice in $\mathbb{C}^g$ and E is a non-degenerate Riemann form on the lattice Λ. The Riemann form E induces a polarization on Λ. The abelian variety A is principally polarized if there exists a symplectic basis $\{\lambda_1, \ldots, \lambda_{2g}\}$ of Λ, such that the Riemann form E with respect to this basis has the following representation:

$$(E_{ij}) := (E(\lambda_i, \lambda_j))_{1 \leq i,j \leq 2g} = \begin{pmatrix} 0 & E_g \\ -E_g & 0 \end{pmatrix}.$$

If the polarization is principal, the lattice $\Lambda = \Omega_1\mathbb{Z}^g + \Omega_2\mathbb{Z}^g$ is isomorphic to the lattice $\mathbb{Z}^g + \Omega\mathbb{Z}^g$, where $\Omega_i := (\lambda_{1+(i-1)g}, \ldots, \lambda_{g+(i-1)g}) \in \mathbb{C}^{g\times g}$ and $\Omega := \Omega_2^{-1}\Omega_1$. The period matrix Ω of A is in the Siegel upper half-plane

$$\mathbb{H}_g := \left\{ z \in \mathbb{C}^{g\times g} : z^t = z, \Im\mathrm{m}(z) > 0 \right\}$$

and the symplectic group

$$\mathrm{Sp}(2g, \mathbb{Z}) := \left\{ \gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{GL}(2g, \mathbb{Z}) |\ \gamma^t J \gamma = J \text{ where } J := \begin{pmatrix} 0 & E_g \\ -E_g & 0 \end{pmatrix} \right\}$$

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 $\mathrm{Sp}(2g, \mathbb{Z})\Omega$ represent the isomorphy class of A in $\mathrm{Sp}(2g, \mathbb{Z}) \setminus \mathbb{H}_g$.

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

$$[2] : A \longrightarrow A, \quad a \longmapsto 2a$$

is given by

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

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 Π the normalized degree $g-1$ Abel-Jacobi map, $\Pi : C_{g-1} \longrightarrow \mathrm{Jac}(C)$, whose image $\Pi(C_{g-1})$ is precisely the theta divisor Θ, i.e. the zero locus of Riemann theta function

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

To the analytic theta characteristic $\begin{bmatrix}\delta\\ \epsilon\end{bmatrix}$ with $\delta, \epsilon \in \mathbb{Z}^g \bmod 2\mathbb{Z}^g$, we will attach the holomorphic theta function

$$\theta\begin{bmatrix}\delta\\ \epsilon\end{bmatrix} : \mathbb{C}^g \times \mathbb{H}_g \longrightarrow \mathbb{C}$$

defined by

$$\begin{aligned}\theta\begin{bmatrix}\delta\\ \epsilon\end{bmatrix}(z,\Omega) &:= \sum_{n\in\mathbb{Z}^g} \exp\left(\pi i\left((n+\frac{1}{2}\delta)\Omega(n+\frac{1}{2}\delta)^t + 2(n+\frac{1}{2}\delta)(z+\frac{1}{2}\epsilon^t)\right)\right)\\ &= \exp\left(\frac{\pi i}{4}\delta\Omega\delta^t + \pi i\delta(z+\frac{\epsilon^t}{2})\right)\cdot\theta\left(z+\frac{1}{2}\Omega\delta^t+\frac{\epsilon^t}{2},\Omega\right).\end{aligned}$$

The map

$$(\mathbb{Z}^g \bmod 2\mathbb{Z}^g)^2 \longrightarrow \mathrm{Jac}(C)[2],\ m = \begin{bmatrix}\delta\\ \epsilon\end{bmatrix} \longmapsto z_m := \frac{1}{2}\Omega\delta^t + \frac{\epsilon^t}{2}$$

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

The functions

$$\theta\begin{bmatrix}\delta\\ \epsilon\end{bmatrix}(0,\Omega) : \mathbb{H}_g \longrightarrow \mathbb{C}$$

are called theta constants and are said to be even, if $\delta\epsilon^t \equiv 0 \pmod 2$ and odd otherwise. All the odd theta constants vanish due to the fact that

$$\theta\begin{bmatrix}\delta\\ \epsilon\end{bmatrix}(-z,\Omega) = (-1)^{\delta\epsilon^t}\theta\begin{bmatrix}\delta\\ \epsilon\end{bmatrix}(z,\Omega).$$

They are exactly $2^{g-1}(2^g+1)$ even and $2^{g-1}(2^g-1)$ odd theta constants.

The choice 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

$$\begin{array}{cccl}\phi: & C & \longrightarrow & \mathbb{P}^{g-1}\\ & P & \longmapsto & \phi(P) := (\omega_1(P):\cdots:\omega_g(P)).\end{array}$$

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 $P_1, \dots, P_{g-1} \in C(\bar{K})$ such that the divisor $D = P_1 + \dots + P_{g-1}$ satisfies $l(D) = 1$. The equation:*

$$(3) \qquad H_D(X_1, \dots, X_g) := \left(\frac{\partial \theta}{\partial z_1}(\Pi(D)), \dots, \frac{\partial \theta}{\partial z_g}(\Pi(D)) \right) \Omega_1^{-1} \begin{pmatrix} X_1 \\ \vdots \\ X_g \end{pmatrix} = 0$$

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 $\mathrm{Jac}(C_1)$ and $\mathrm{Jac}(C_2)$. Furthermore, Torelli's theorem [40] asserts that the Jacobian $\mathrm{Jac}(C)$ with its principal polarization E determines the curve C up to isomorphism: If $(\mathrm{Jac}(C), E)$ and $(\mathrm{Jac}(C'), E')$ 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 $\mathrm{Jac}(C)$. If we just consider $\mathrm{Jac}(C)$ 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 Ω, 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. *Ω is hyperelliptic if and only if exactly one even theta constant vanishes in Ω.*
2. *Ω is non-hyperelliptic if and only if no even theta constant vanishes in Ω.*

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 $\mathrm{Jac}(C)$ (see [16]). Due to Proposition 3, the bitangent associated to the odd 2-torsion point z_0 is given by the line with equation:

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

Definition 3 ([7])**.** Let $S = ([\epsilon_i])_{i=1,\dots,7}$ 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 $S := ([\epsilon_i])_{i=1,\dots,7}$ where

$$\epsilon_1 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix} \quad \epsilon_2 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix} \quad \epsilon_3 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \quad \epsilon_4 = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$
$$\epsilon_5 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \quad \epsilon_6 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \quad \epsilon_7 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

We denote by β_i the bitangent associated to $[\epsilon_i]$ and by β_{ij} the bitangent associated to $[\epsilon_i] + [\epsilon_j]$. The set (β_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

$$\begin{cases} \beta_1 : x_1 = 0, & \beta_5 : a_1x_1 + a_2x_2 + a_3x_3 = 0, \\ \beta_2 : x_2 = 0, & \beta_6 : a_1'x_1 + a_2'x_2 + a_3'x_3 = 0, \\ \beta_3 : x_3 = 0, & \beta_7 : a_1''x_1 + a_2''x_2 + a_3''x_3 = 0, \\ \beta_4 : x_1 + x_2 + x_3 = 0. & \end{cases} \tag{5}$$

It is well known as a classical result since the first work of Riemann [30], how to construct a quartic for which the $(\beta_i)_{i=1,\dots,7}$ 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 $(\beta_i)_{i=1,\dots,7}$. 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)*

$$\sqrt{x_1v_1} + \sqrt{x_2v_2} + \sqrt{x_3v_3} = 0, \tag{6}$$

where v_1, v_2, v_3 satisfy

$$\begin{cases} v_1 + v_2 + v_3 + x_1 + x_2 + x_3 = 0, \\ \frac{v_1}{a_1} + \frac{v_2}{a_2} + \frac{v_3}{a_3} + ka_1x_1 + ka_2x_2 + ka_3x_3 = 0, \\ \frac{v_1}{a_1'} + \frac{v_2}{a_2'} + \frac{v_3}{a_3'} + k'a_1'x_1 + k'a_2'x_2 + k'a_3'x_3 = 0, \\ \frac{v_1}{a_1''} + \frac{v_2}{a_2''} + \frac{v_3}{a_3''} + k''a_1''x_1 + k''a_2''x_2 + k''a_3''x_3 = 0, \end{cases}$$

with k, k', k'' solutions of

$$\begin{pmatrix} \frac{1}{a_1} & \frac{1}{a'_1} & \frac{1}{a''_1} \\ \frac{1}{a_2} & \frac{1}{a'_2} & \frac{1}{a''_2} \\ \frac{1}{a_3} & \frac{1}{a'_3} & \frac{1}{a''_3} \end{pmatrix} \begin{pmatrix} \lambda \\ \lambda' \\ \lambda'' \end{pmatrix} = \begin{pmatrix} -1 \\ -1 \\ -1 \end{pmatrix},$$

$$\begin{pmatrix} a_1 & a'_1 & a''_1 \\ a_2 & a'_2 & a''_2 \\ a_3 & a'_3 & a''_3 \end{pmatrix} \begin{pmatrix} \lambda k \\ \lambda' k' \\ \lambda'' k'' \end{pmatrix} = \begin{pmatrix} -1 \\ -1 \\ -1 \end{pmatrix}.$$

The 28 bitangents can be expressed through the following equations:

$$\beta_1 : x_1 = 0, \quad \beta_2 : x_2 = 0, \quad \beta_3 : x_3 = 0,$$
$$\beta_{23} : v_1 = 0, \quad \beta_{13} : v_2 = 0, \quad \beta_{12} : v_3 = 0,$$

$$\beta_4 : x_1 + x_2 + x_3 = 0, \qquad \beta_5 : a_1x_1 + a_2x_2 + a_3x_3 = 0,$$
$$\beta_6 : a'_1x_1 + a'_2x_2 + a'_3x_3 = 0, \quad \beta_7 : a''_1x_1 + a''_2x_2 + a''_3x_3 = 0,$$

$$\beta_{14} : v_1 + x_2 + x_3 = 0, \qquad \beta_{15} : \frac{v_1}{a_1} + ka_2x_2 + ka_3x_3 = 0,$$
$$\beta_{16} : \frac{v_1}{a'_1} + k'a'_2x_2 + k'a'_3x_3 = 0, \quad \beta_{17} : \frac{v_1}{a''_1} + k''a''_2x_2 + k''a''_3x_3 = 0,$$

$$\beta_{24} : x_1 + v_2 + x_3 = 0, \qquad \beta_{25} : ka_1x_1 + \frac{v_2}{a_2} + ka_3x_3 = 0,$$
$$\beta_{26} : k'a'_1x_1 + \frac{v_2}{a'_2} + k'a'_3x_3 = 0, \quad \beta_{27} : k''a''_1x_1 + \frac{v_2}{a''_2} + k''a''_3x_3 = 0,$$

$$\beta_{34} : x_1 + x_2 + v_3 = 0, \qquad \beta_{35} : ka_1x_1 + ka_2x_2 + \frac{v_3}{a_3} = 0,$$
$$\beta_{36} : k'a'_1x_1 + k'a'_2x_2 + \frac{v_3}{a'_3} = 0, \quad \beta_{37} : k''a''_1x_1 + k''a''_2x_2 + \frac{v_3}{a''_3} = 0,$$

$$\beta_{67} : \frac{x_1}{1-ka_2a_3} + \frac{x_2}{1-ka_3a_1} + \frac{x_3}{1-ka_1a_2} = 0,$$
$$\beta_{57} : \frac{x_1}{1-k'a'_2a'_3} + \frac{x_2}{1-k'a'_3a'_1} + \frac{x_3}{1-k'a'_1a'_2} = 0,$$
$$\beta_{56} : \frac{x_1}{1-k''a''_2a''_3} + \frac{x_2}{1-k''a''_3a''_1} + \frac{x_3}{1-k''a''_1a''_2} = 0,$$

$$\beta_{45} : \frac{v_1}{a_1(1-ka_2a_3)} + \frac{v_2}{a_2(1-ka_3a_1)} + \frac{v_3}{a_3(1-ka_1a_2)} = 0,$$
$$\beta_{46} : \frac{v_1}{a'_1(1-k'a'_2a'_3)} + \frac{v_2}{a'_2(1-k'a'_3a'_1)} + \frac{v_3}{a'_3(1-k'a'_1a'_2)} = 0,$$
$$\beta_{47} : \frac{v_1}{a''_1(1-ka''_2a''_3)} + \frac{v_2}{a''_2(1-k''a''_3a''_1)} + \frac{v_3}{a''_3(1-k''a''_1a''_2)} = 0.$$

Remark 2. By Riemann's notation $\sqrt{x_1v_1} + \sqrt{x_2v_2} + \sqrt{x_3v_3} = 0$, we mean the plane quartic with equation $(x_1v_1 + x_2v_2 - x_3v_3)^2 - 4x_1x_2v_1v_2 = 0$.

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 $\mathrm{Jac}(C) \simeq A$:

(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 $A \simeq \mathrm{Jac}(C)$ 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 (4), we then compute the equations of the 7 bitangents β_i of the Aronhold system S.

(iii) Using linear transformations, we rewrite the 7 bitangents β_i associated to $[\epsilon_i]_{i=1\ldots,7}$ 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 $\mathrm{Jac}(C) \simeq A$.

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 $\mathrm{Sp}_6(\mathbb{F}_2)$ 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 extension, 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 $J_0(N)^{\mathrm{new}}, N \leq 4000$, 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 Ω_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 $\mathrm{Jac}(C_f) \simeq A_f$. In our computations, we had to use the first $20,000$ Fourier coefficients of the newform $f \in S_2^{\mathrm{new}}(N)$ 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 $J_0(N)^{\mathrm{new}}$ 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 1. Principally polarized A_f with $\dim A_f = 3$ and $N \leq 4000$

$\#A_f$	3334
# p.p. A_f	79
# p.p. and hyperelliptic A_f	12
# p.p. and non-hyperelliptic A_f	67

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 $A_f \simeq \mathrm{Jac}(C_f)$ which admit a model C_{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 ξ_j, compute the *unique* Shioda normal form C_{ξ_j} relative to (C, ξ_j).
(iii) The curve (C_f, ξ) admits a $\mathbb{Q}$-rational model if and only if one of the above equations C_{ξ_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, ξ) defined over $\mathbb{Q}$. With this algorithm we are also able to determine the structure of the automorphism group $\mathrm{Aut}(C)$ of C : An automorphism $\varphi \neq \mathrm{Id}$ of C fixes at most $2g-2=8$ points of C, i.e. φ cannot act trivially on the set of Weierstrass points of C. The normal forms C_{ξ_1} and C_{ξ_2} at two distinct Weierstrass points ξ_1, ξ_2 are equal if and only if $\xi_1 = \xi_2^{\varphi}$ for a $\varphi \in \mathrm{Aut}(C)$.

In the following, we label the genus 3 curves coming from $\mathbb{Q}$-simple new modular Jacobians A_f of level N by X_N^A, where N denotes the level of X_N^A and the letter A denotes the position with respect to the ordering given as output of the Magma-function `SortDecomposition`.In the appendix (see Table 6) we listed out all $\mathbb{Q}$-simple quotients A_f of $J_0(N)^{\mathrm{new}}$ 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 [11]). 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 $\mathrm{Jac}(C)$ and $\mathrm{Jac}(C')$ 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, $f \in S_2^{\mathrm{new}}(N)$.

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 $S_2^{\mathrm{new}}(369)$ 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[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

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

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

with diagonal matrix

$$\Delta_f = 8 \cdot \mathrm{Id}\,,$$

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

$$\Omega_f = \begin{pmatrix} 0.55467\cdots+3.07521\ldots i & -0.79883\cdots+0.11922\ldots i & 0.85186\cdots+0.79061\ldots i \\ -0.79883\cdots+0.11922\ldots i & 0.74004\cdots+0.43861\ldots i & -0.04497\cdots-0.32299\ldots i \\ 0.85186\cdots+0.79061\ldots i & -0.04497\cdots-0.32299\ldots i & 0.65132\cdots+0.97328\ldots i \end{pmatrix}.$$

Using Theorem 1, there is a curve C_f of genus 3 with $A_f \simeq \mathrm{Jac}(C_f)$. 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 (4), the bitangents associated to the canonical Aronhold system $S=(\epsilon_i)$ (cf. page 1181) have the equations

$$\begin{aligned}
\beta_1 &: 0 = x-(1.62009\cdots-0.88123\ldots i)y+(0.60794\cdots-1.09289\ldots i)z\,,\\
\beta_2 &: 0 = x-(1.62009\cdots+0.88123\ldots i)y+(0.60794\cdots+1.09289\ldots i)z\,,\\
\beta_3 &: 0 = x-(1.18597\cdots-0.01375\ldots i)y+(0.07649\cdots+0.00738\ldots i)z\,,\\
\beta_4 &: 0 = x-(0.13444\cdots-0.32339\ldots i)y+(0.79703\cdots-0.39889\ldots i)z\,,\\
\beta_5 &: 0 = x+(2.88498\cdots+2.57527\ldots i)y+(2.95024\cdots-6.21143\ldots i)z\,,\\
\beta_6 &: 0 = x+(0.02710\cdots+0.18672\ldots i)y+(0.75712\cdots-0.74717\ldots i)z\,,\\
\beta_7 &: 0 = x+(0.90241\cdots-1.65452\ldots i)y-(2.06151\cdots+1.61189\ldots i)z\,,
\end{aligned}$$

which become

$$\begin{aligned}
\beta_1 &: 0 = x\,,\\
\beta_2 &: 0 = y\,,\\
\beta_3 &: 0 = z\,,\\
\beta_4 &: 0 = x+y+z\,,\\
\beta_5 &: 0 = x+(0.99571\cdots+0.01530\ldots i)y+(0.99050\cdots-0.00242\ldots i)z\,,\\
\beta_6 &: 0 = x+(0.99999\cdots+0.00218\ldots i)y+(0.99655\cdots+0.00029\ldots i)z\,,\\
\beta_7 &: 0 = x+(1.00406\cdots+0.01543\ldots i)y+(0.98864\cdots-0.00065\ldots i)z\,,
\end{aligned}$$

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

$$\begin{aligned}
v_1 &= (2.41739\cdots+0.67174\ldots i)x+(1.39123\cdots+0.65332\ldots i)y+(1.40882\cdots+0.65261\ldots i)z\,,\\
v_2 &= -(1.55957\cdots+0.16076\ldots i)x-(0.52956\cdots+0.15658\ldots i)y-(1.54558\cdots+0.14781\ldots i)z\,,\\
v_3 &= -(1.85781\cdots+0.51098\ldots i)x-(1.86167\cdots+0.49673\ldots i)y-(0.86323\cdots+0.50480\ldots i)z\,.
\end{aligned}$$

Up to a certain precision, the curve C_f has the $\mathbb{Q}$-rational Dixmier invariants

$$i_1 = \frac{7^9}{2^{44}\cdot 3^{18}\cdot 41^3}\,,\qquad i_2 = \frac{-7^7\cdot 97}{2^{48}\cdot 3^{21}\cdot 41^3}\,,$$

$$i_3 = \frac{7^6\cdot 6353}{2^{36}\cdot 3^{16}\cdot 41^3}\,,\qquad i_4 = \frac{7^5\cdot 73\cdot 31337}{2^{36}\cdot 3^{18}\cdot 41^3}\,,$$

$$i_5 = \frac{7^4\cdot 43\cdot 4662331}{2^{34}\cdot 3^{15}\cdot 41^3}\,,\qquad i_6 = \frac{-7^3\cdot 1307\cdot 1601\cdot 5303}{2^{32}\cdot 3^{16}\cdot 41^3}\,.$$

We note that by using Shioda's transformations at the ordinary flex

$$\xi \quad = \quad (0.60900\cdots - 0.79316\ldots i : -1.62391\cdots + 0.77629\ldots i : 1)$$

with tangent line

$$T_\xi : \quad 0 = -(0.03895\cdots + 0.02027\ldots i)x - (0.03870\cdots + 0.01924\ldots i) - (0.03799\cdots + 0.01975\ldots i)z$$

we obtain the model

$$C'_f : \quad 0 = \quad y^3z + y(x^3 - 9,14494\ldots 10^{-4}xz^2 - 1.37989\ldots 10^{-5}z^3) - 9,14494\ldots 10^{-4}x^3z$$
$$+5.08052\ldots 10^{-5}x^2z^2 + 2.09075\ldots 10^{-6}xz^3 + 1.44354\ldots 10^{-8}z^4,$$

which is, up to a certain precision, the $\mathbb{Q}$-rational curve with the equation

$$0 = y^3z + y(x^3 - \frac{2}{2187}xz^2 - \frac{22}{1594323}z^3) - \frac{2}{2187}x^3z + \frac{1}{19683}x^2z^2 + \frac{10}{4782969}xz^3 + \frac{151}{10460353203}z^4.$$

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 $\mathrm{Jac}(C_f) \simeq A_f$ 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 $\#\mathrm{Jac}(C)(\mathbb{F}_q)$ has a large prime divisor. The computation of $\#\mathrm{Jac}(C)(\mathbb{F}_q)$ 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 χ_{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, 3, 29]). 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.

6. Appendix: Table of non-hyperelliptic new modular Jacobian A_f of $J_0(N)^{\text{new}}, N \leq 600$

curves	*Dixmier invariants*	*curves*	*Dixmier invariants*
X_{97}^{A}	$i_1 = \frac{-23^9}{2^{53}.3^{27}.97^3}$ $i_2 = \frac{5^2\cdot 23^7}{2^{57}.3^{29}.97^3}$ $i_3 = \frac{23^6\cdot 109}{2^{39}.3^{24}.97^3}$ $i_4 = \frac{-23^5\cdot 106649}{2^{37}.3^{25}.97^3}$ $i_5 = \frac{7\cdot 13\cdot 23^4\cdot 29\cdot 47}{2^{32}.3^{23}.97^3}$ $i_6 = \frac{7\cdot 23^3\cdot 4446899}{2^{29}.3^{22}.97^3}$	X_{149}^{A}	$i_1 = \frac{83^9}{2^{53}.3^{27}.149^3}$ $i_2 = \frac{83^7\cdot 1823}{2^{57}.3^{29}.149^3}$ $i_3 = \frac{5\cdot 83^6\cdot 239\cdot 947}{2^{41}.3^{24}.149^3}$ $i_4 = \frac{83^5\cdot 432110321}{2^{41}.3^{25}.149^3}$ $i_5 = \frac{7\cdot 83^4\cdot 236140337759}{2^{38}.3^{23}.149^3}$ $i_6 = \frac{5\cdot 7\cdot 17\cdot 23\cdot 83^3\cdot 239\cdot 853\cdot 58049}{2^{36}.3^{22}.149^3}$
X_{109}^{B}	$i_1 = \frac{11^9}{2^{53}.3^{27}.109^3}$ $i_2 = \frac{11^7\cdot 47^2}{2^{57}.3^{29}.109^3}$ $i_3 = \frac{11^6\cdot 101\cdot 1259}{2^{43}.3^{24}.109^3}$ $i_4 = \frac{11^5\cdot 5894347}{2^{40}.3^{25}.109^3}$ $i_5 = \frac{11^5\cdot 5087\cdot 10889}{2^{37}.3^{23}.109^3}$ $i_6 = \frac{5\cdot 11^3\cdot 39330808093}{2^{36}.3^{22}.109^3}$	X_{151}^{A}	$i_1 = \frac{7^9}{2^{53}.3^{27}.151^3}$ $i_2 = \frac{-7^7\cdot 17\cdot 617}{2^{57}.3^{29}.151^3}$ $i_3 = \frac{7^6\cdot 23\cdot 251\cdot 577}{2^{43}.3^{24}.151^3}$ $i_4 = \frac{7^5\cdot 11\cdot 1621\cdot 5087}{2^{40}.3^{25}.151^3}$ $i_5 = \frac{-7^4\cdot 31\cdot 37\cdot 113\cdot 587\cdot 6733}{2^{37}.3^{23}.151^3}$ $i_6 = \frac{7^3\cdot 38767\cdot 945648167}{2^{36}.3^{22}.151^3}$
X_{113}^{C}	$i_1 = \frac{-1}{2^{53}.3^{27}.113^3}$ $i_2 = \frac{13\cdot 61}{2^{57}.3^{29}.113^3}$ $i_3 = \frac{-19\cdot 23\cdot 269}{2^{43}.3^{24}.113^3}$ $i_4 = \frac{-836063}{2^{39}.3^{25}.113^3}$ $i_5 = \frac{5\cdot 13\cdot 38562143}{2^{37}.3^{23}113^3}$ $i_6 = \frac{-11\cdot 37\cdot 62711911}{2^{36}.3^{22}.113^3}$	X_{169}^{B}	$i_1 = \frac{5^{18}}{2^{53}.3^{27}.13^6}$ $i_2 = \frac{-5^{14}\cdot 7\cdot 79}{2^{57}.3^{29}.13^6}$ $i_3 = \frac{5^{12}\cdot 155887}{2^{43}.3^{24}.13^6}$ $i_4 = \frac{5^{10}\cdot 11\cdot 216829}{2^{39}.3^{25}.13^6}$ $i_5 = \frac{5^8\cdot 131\cdot 463\cdot 69847}{2^{37}.3^{23}.13^6}$ $i_6 = \frac{5^8\cdot 89\cdot 162518641}{2^{36}.3^{22}.13^6}$
X_{127}^{A}	$i_1 = \frac{71^9}{2^{53}.3^{27}.127^3}$ $i_2 = \frac{-43\cdot 71^7\cdot 139}{2^{57}.3^{29}.127^3}$ $i_3 = \frac{7\cdot 71^6\cdot 13933}{2^{40}.3^{24}127^3}$ $i_4 = \frac{-7\cdot 71^5\cdot 23840251}{2^{41}.3^{25}.127^3}$ $i_5 = \frac{13\cdot 71^4\cdot 1336920521}{2^{38}3^{23}.127^3}$ $i_6 = \frac{53\cdot 71^3\cdot 607\cdot 3251\cdot 26681}{2^{36}.3^{22}.127^3}$	X_{179}^{B}	$i_1 = \frac{-17^9}{2^{53}.3^{27}.179^3}$ $i_2 = \frac{17^8\cdot 89}{2^{57}.3^{29}.179^3}$ $i_3 = \frac{5^3\cdot 13\cdot 17^7}{2^{41}.3^{24}.179^3}$ $i_4 = \frac{-7\cdot 17^6\cdot 89\cdot 227}{2^{41}.3^{25}.179^3}$ $i_5 = \frac{17^5\cdot 41\cdot 2478937}{2^{38}.3^{23}.179^3}$ $i_6 = \frac{-17^3\cdot 36829407137}{2^{36}.3^{22}.179^3}$
X_{139}^{B}	$i_1 = \frac{-17^9}{2^{53}.3^{27}.139^3}$ $i_2 = \frac{13\cdot 17^7\cdot 349}{2^{57}.3^{29}139^3}$ $i_3 = \frac{-7\cdot 17^6\cdot 41\cdot 367}{2^{43}.3^{24}.139^3}$ $i_4 = \frac{-7\cdot 17^5\cdot 2835667}{2^{40}.3^{25}.139^3}$ $i_5 = \frac{5\cdot 7\cdot 17^5\cdot 383\cdot 12161}{2^{34}.3^{23}.139^3}$ $i_6 = \frac{7\cdot 11\cdot 17^3\cdot 53\cdot 149854519}{2^{36}.3^{22}.139^3}$	X_{187}^{E}	$i_1 = \frac{7^9}{2^{44}.3^{27}.11^3.17^4}$ $i_2 = \frac{-7^7\cdot 59}{2^{48}.3^{29}.11^3.17^3}$ $i_3 = \frac{5\cdot 7^6\cdot 157\cdot 283}{2^{35}.3^{24}.11^3.17^4}$ $i_4 = \frac{-7^5\cdot 13\cdot 16456963}{2^{36}.3^{25}.11^3.17^4}$ $i_5 = \frac{7^4\cdot 111770067821}{2^{34}.3^{23}.11^3.17^4}$ $i_6 = \frac{-7^3\cdot 37\cdot 131\cdot 181\cdot 101419}{2^{32}.3^{22}.11^3.17^4}$

curves	*Dixmier invariants*
X_{203}^{F}	$i_1 = \frac{7^4\cdot 17^9}{2^{53}.3^{27}.29^3}$ $i_2 = \frac{5^3\cdot 7^2\cdot 17^7\cdot 283}{2^{57}.3^{29}.29^3}$ $i_3 = \frac{5\cdot 7\cdot 17^6\cdot 353\cdot 29327}{2^{43}.3^{24}.29^3}$ $i_4 = \frac{7^2\cdot 17^5\cdot 487\cdot 216577}{2^{40}.3^{25}.29^3}$ $i_5 = \frac{17^4\cdot 6737\cdot 8849\cdot 359417}{2^{36}.3^{23}.7.29^3}$ $i_6 = \frac{17^3\cdot 149\cdot 131679238350523}{2^{36}.3^{22}.7^2.29^3}$
X_{217}^{A}	$i_1 = \frac{5^9\cdot 227^9}{2^{53}.3^{55}.7^3.31^3}$ $i_2 = \frac{-5^8\cdot 227^7\cdot 342821}{2^{57}.3^{57}.7^3.31^3}$ $i_3 = \frac{5^6\cdot 227^6\cdot 439\cdot 3871663}{2^{39}.3^{52}.7^3.31^3}$ $i_4 = \frac{5^5\cdot 19\cdot 113\cdot 227^5\cdot 3181\cdot 4410097}{2^{41}.3^{53}.7^3.31^3}$ $i_5 = \frac{5^4\cdot 227^4\cdot 3264116968231423459}{2^{38}.3^{51}.7^3.31^3}$ $i_6 = \frac{5^3\cdot 227^3\cdot 11320571\cdot 514794731537767}{2^{36}.3^{50}.7^3.31^3}$
X_{239}^{A}	$i_1 = \frac{5^9\cdot 7^9}{2^{53}.3^{27}.239^3}$ $i_2 = \frac{-5^7\cdot 7^7\cdot 433}{2^{57}.3^{29}.239^3}$ $i_3 = \frac{-5^6\cdot 7^6\cdot 43963}{2^{39}.3^{24}.239^3}$ $i_4 = \frac{-5^5\cdot 7^5\cdot 509\cdot 112481}{2^{41}.3^{25}.239^3}$ $i_5 = \frac{-5^4\cdot 7^4\cdot 27827\cdot 3496799}{2^{38}.3^{23}.239^3}$ $i_6 = \frac{-5^4\cdot 7^3\cdot 68503144613}{2^{36}.3^{22}.239^3}$
X_{295}^{A}	$i_1 = \frac{-11^9}{2^{53}.3^{27}.5^3.59^3}$ $i_2 = \frac{11^7\cdot 13\cdot 181}{2^{57}.3^{29}.5^3.59^3}$ $i_3 = \frac{-7\cdot 11^6\cdot 23203}{2^{42}.3^{24}.5^3.59^3}$ $i_4 = \frac{-7^2\cdot 11^5\cdot 370631}{2^{41}.3^{25}.5^3.59^3}$ $i_5 = \frac{7\cdot 11^5\cdot 19\cdot 769\cdot 2287}{2^{38}.3^{23}.5^2.59^3}$ $i_6 = \frac{-7\cdot 11^3\cdot 197\cdot 415664659}{2^{36}.3^{22}.5^3.59^3}$
X_{329}^{C}	$i_1 = \frac{-19^9}{2^{53}.3^{27}.7^3.47^3}$ $i_2 = \frac{5\cdot 19^7\cdot 1181}{2^{57}.3^{29}.7^3.47^3}$ $i_3 = \frac{-19^6\cdot 29\cdot 61\cdot 67}{2^{40}.3^{24}.7^3.47^3}$ $i_4 = \frac{-13\cdot 19^5\cdot 701\cdot 7723}{2^{41}.3^{25}.7^3.47^3}$ $i_5 = \frac{19^4\cdot 163061001821}{2^{38}.3^{23}.7^3.47^3}$ $i_6 = \frac{5\cdot 19^3\cdot 41\cdot 7369\cdot 904573}{2^{36}.3^{22}.7^3.47^3}$

curves	*Dixmier invariants*
X_{369}^{D}	$i_1 = \frac{7^9}{2^{44}.3^{18}.41^3}$ $i_2 = \frac{-7^7\cdot 97}{2^{48}.3^{21}.41^3}$ $i_3 = \frac{7^6\cdot 6353}{2^{36}.3^{16}.41^3}$ $i_4 = \frac{7^5\cdot 73\cdot 31337}{2^{36}.3^{18}.41^3}$ $i_5 = \frac{7^4\cdot 43\cdot 4662331}{2^{34}.3^{15}.41^3}$ $i_6 = \frac{-7^3\cdot 1307\cdot 1601\cdot 5303}{2^{32}.3^{16}.41^3}$
X_{369}^{E}	$i_1 = \frac{7^9}{2^{44}.3^{18}.41^3}$ $i_2 = \frac{-7^7\cdot 97}{2^{48}.3^{21}.41^3}$ $i_3 = \frac{7^6\cdot 6353}{2^{36}.3^{16}.41^3}$ $i_4 = \frac{7^5\cdot 73\cdot 31337}{2^{36}.3^{18}.41^3}$ $i_5 = \frac{7^4\cdot 43\cdot 4662331}{2^{34}.3^{15}.41^3}$ $i_6 = \frac{-7^3\cdot 1307\cdot 1601\cdot 5303}{2^{32}.3^{16}.41^3}$
X_{388}^{A}	$i_1 = \frac{-1}{2^{46}.3^{27}.97^3}$ $i_2 = \frac{-233}{2^{50}.3^{29}.97^3}$ $i_3 = \frac{5293513}{2^{41}.3^{24}.97^3}$ $i_4 = \frac{624203}{2^{35}.3^{25}.97^3}$ $i_5 = \frac{71\cdot 3533\cdot 300997}{2^{38}.3^{23}.97^3}$ $i_6 = \frac{-29\cdot 409326261863}{2^{36}.3^{22}.97^3}$
X_{436}^{B}	$i_1 = \frac{181^9}{2^{37}.3^{18}.11^{14}.109^3}$ $i_2 = \frac{-5\cdot 23\cdot 113\cdot 181^7}{2^{42}.3^{20}.11^{14}.109^3}$ $i_3 = \frac{181^6\cdot 4727066557}{2^{35}.3^{15}.11^{14}.109^3}$ $i_4 = \frac{181^5\cdot 499\cdot 56343733}{2^{33}.3^{15}.11^{14}.109^3}$ $i_5 = \frac{151\cdot 181^4\cdot 381481\cdot 538018951}{2^{34}.3^{14}.11^{14}.109^3}$ $i_6 = \frac{181^3\cdot 239273\cdot 480133\cdot 133676033}{2^{32}.3^{14}.11^{14}.109^3}$
X_{452}^{A}	$i_1 = \frac{31^9}{2^{10}.3^{41}.113^3}$ $i_2 = \frac{13\cdot 17\cdot 31^7\cdot 521}{2^{21}.3^{43}.113^3}$ $i_3 = \frac{31^6\cdot 157\cdot 336931631}{2^{17}.3^{38}.113^3}$ $i_4 = \frac{5\cdot 31^5\cdot 71\cdot 53551058051}{2^{18}.3^{39}.113^3}$ $i_5 = \frac{5\cdot 31^4\cdot 774401181277897891}{2^{22}.3^{37}.113^3}$ $i_6 = \frac{7\cdot 23\cdot 31^3\cdot 421\cdot 10301727084532427}{2^{22}.3^{36}.113^3}$

curves	*Dixmier invariants*
X_{475}^E	$i_1 = \frac{3067^9}{2^{53} \cdot 3^{27} \cdot 5^6 \cdot 19^3}$ $i_2 = \frac{479 \cdot 3067^7 \cdot 15937}{2^{57} \cdot 3^{29} \cdot 5^6 \cdot 19^3}$ $i_3 = \frac{193 \cdot 3067^6 \cdot 115419877}{2^{39} \cdot 3^{24} \cdot 5^6 \cdot 19^3}$ $i_4 = \frac{41 \cdot 3067^5 \cdot 41903 \cdot 2234129}{2^{37} \cdot 3^{25} \cdot 5^4 \cdot 19^3}$ $i_5 = \frac{13 \cdot 397 \cdot 479 \cdot 3067^4 \cdot 6619 \cdot 8887 \cdot 25349}{2^{32} \cdot 3^{23} \cdot 5^6 \cdot 19^3}$ $i_6 = \frac{3067^3 \cdot 1587899065951933060901}{2^{29} \cdot 3^{22} \cdot 5^5 \cdot 19^3}$
X_{475}^G	$i_1 = \frac{3067^9}{2^{53} \cdot 3^{27} \cdot 5^6 \cdot 19^3}$ $i_2 = \frac{479 \cdot 3067^7 \cdot 15937}{2^{57} \cdot 3^{29} \cdot 5^6 \cdot 19^3}$ $i_3 = \frac{193 \cdot 3067^6 \cdot 115419877}{2^{39} \cdot 3^{24} \cdot 5^6 \cdot 19^3}$ $i_4 = \frac{41 \cdot 3067^5 \cdot 41903 \cdot 2234129}{2^{37} \cdot 3^{25} \cdot 5^4 \cdot 19^3}$ $i_5 = \frac{13 \cdot 397 \cdot 479 \cdot 3067^4 \cdot 6619 \cdot 8887 \cdot 25349}{2^{32} \cdot 3^{23} \cdot 5^6 \cdot 19^3}$ $i_6 = \frac{3067^3 \cdot 1587899065951933060901}{2^{29} \cdot 3^{22} \cdot 5^5 \cdot 19^3}$
X_{511}^B	$i_1 = \frac{5^9 \cdot 37^9 \cdot 43133^9}{2^{53} \cdot 3^{30} \cdot 7^8 \cdot 11^{14} \cdot 73^3 \cdot 101^{14}}$ $i_2 = \frac{-5^8 \cdot 37^7 \cdot 263 \cdot 43133^7 \cdot 197689 \cdot 6021091}{2^{57} \cdot 3^{32} \cdot 7^8 \cdot 11^{14} \cdot 73^3 \cdot 101^{14}}$ $i_3 = \frac{5^6 \cdot 13 \cdot 37^6 \cdot 43133^6 \cdot 142702121 \cdot 25535098000501}{2^{43} \cdot 3^{28} \cdot 7^8 \cdot 11^{14} \cdot 73^3 \cdot 101^{14}}$ $i_4 = \frac{5^5 \cdot 17 \cdot 37^5 \cdot 577 \cdot 43133^5 \cdot 3563719 \cdot 164875199 \cdot 160402791737}{2^{39} \cdot 3^{28} \cdot 7^8 \cdot 11^{14} \cdot 73^3 \cdot 101^{14}}$ $i_5 = \frac{-5^4 \cdot 13^2 \cdot 37^4 \cdot 43133^4 \cdot 4115376046670328285328841328058909 9}{2^{33} \cdot 3^{24} \cdot 7^8 \cdot 11^{14} \cdot 73^3 \cdot 101^{14}}$ $i_6 = \frac{-5^3 \cdot 37^3 \cdot 43133^3 \cdot 688333 \cdot 28685999 \cdot 3031471393386674295606558437642759}{2^{36} \cdot 3^{26} \cdot 7^8 \cdot 11^{14} \cdot 73^3 \cdot 101^{14}}$
X_{567}^H	$i_1 = \frac{5^4}{2^{53} \cdot 3^9 \cdot 7^3}$ $i_2 = \frac{5 \cdot 17}{2^{57} \cdot 3^{12} \cdot 7^3}$ $i_3 = \frac{5 \cdot 3821}{2^{42} \cdot 3^8 \cdot 7^3}$ $i_4 = \frac{17 \cdot 8363}{2^{41} \cdot 3^9 \cdot 5 \cdot 7^3}$ $i_5 = \frac{5^2 \cdot 313}{2^{38} \cdot 3^6 \cdot 7^3}$ $i_6 = \frac{-19 \cdot 83 \cdot 11119}{2^{36} \cdot 3^7 \cdot 5^2 \cdot 7^3}$
X_{596}^A	$i_1 = \frac{359^9}{2^{55} \cdot 3^{27} \cdot 149^3}$ $i_2 = \frac{13 \cdot 23 \cdot 73 \cdot 359^7}{2^{57} \cdot 3^{29} \cdot 149^3}$ $i_3 = \frac{23 \cdot 359^6 \cdot 89348191}{2^{47} \cdot 3^{24} \cdot 149^3}$ $i_4 = \frac{5^2 \cdot 359^5 \cdot 39644905697}{2^{45} \cdot 3^{25} \cdot 149^3}$ $i_5 = \frac{47 \cdot 359^4 \cdot 370708577229919}{2^{42} \cdot 3^{23} \cdot 149^3}$ $i_6 = \frac{13 \cdot 19 \cdot 359^3 \cdot 16529 \cdot 794641 \cdot 2599117}{2^{40} \cdot 3^{22} \cdot 149^3}$

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

[1] R. Avanzi, N. Thériault, and Z. Wang, *Rethinking low genus hyperelliptic Jacobian arithmetic over binary fields: Interplay of field arithmetic and explicit formulae*, preprint, 2006.
[2] M. H. Baker, E. González-Jiménez, J. González, and B. Poonen, *Finiteness results for modular curves of genus at least 2*, Amer. J. Math. **127** (2005), no. 6, 1325–1387. MR2183527 (2006i:11065)
[3] A. Basiri, A. Enge, J-C. Faugère, and N. Gürel, *Implementing the arithmetic of $C_{3,4}$ curves*, Algorithmic Number Theory Symposium - ANTS-VI, LNCS, vol. 3076, Springer, 2004, pp. 87–101. MR2137346 (2006a:14101)
[4] L. Caporaso and E. Sernesi, *Recovering plane curves from their bitangents*, J. Alg. Geom. **2** (2003), 225–244. MR1949642 (2003k:14035)
[5] C. Diem and E. Thomé, *Index calculus in class groups of non-hyperelliptic curves of genus 3*, 2006, preprint.
[6] J. Dixmier, *On the projective Invariants of quartic plane curves*, Advances in Math. **64** (1987), 279–304. MR888630 (88c:14064)
[7] I. Dolgachev, *Topics in classical algebraic geometry, part I*, Available on `http://www.math.lsa.umich.edu/~idolga/lecturenotes.html`, 2003.
[8] S. Flon and R. Oyono, *Fast arithmetic on Jacobians of Picard curves*, Public Key Cryptography - PKC 2004, LNCS, vol. 2947, Springer, 2004, pp. 55–68. MR2095638 (2005k:14049)
[9] S. Flon, R. Oyono, and C. Ritzenthaler, *Fast addition on non-hyperelliptic genus* 3 *curves*, Preprint, available on `http://eprint.iacr.org/2004`, 2004.
[10] M. Girard and D. Kohel, *Classification of Genus 3 Curves in Special Strata of the Moduli Space*, To appear in ANTS VII (Berlin, 2006). MR2282935 (2007k:14051)
[11] J. González, J. Guàrdia, and V. Rotger, *Abelian surfaces of GL_2-type as Jacobians of curves*, Acta Arithmetica **116(3)** (2005), 263–287. MR2114780 (2005m:11107)
[12] E. González-Jiménez and R. Oyono, *Non-hyperelliptic modular curves of genus* 3, work in progress, 2007.
[13] E. González-Jiménez and J. González, *Modular curves of genus 2*, Math. Comp. **72** (2003), 397–418. MR1933828 (2003i:11078)
[14] E. González-Jiménez, J. González, and J. Guàrdia, *Computations on modular Jacobian surfaces*, Lecture Notes in Comput. Sci. (2369), Springer, 2002, pp. 189–197. MR2041083 (2005c:11074)
[15] E. González-Jiménez and J. Guàrdia, MAV*, modular abelian varieties for* magma, 2001.
[16] P. Griffiths and J. Harris, *Principles of algebraic geometry*, Reprint of the 1978 original. Wiley Classics Library. John Wiley & Sons, Inc., New York, xiv +813 pp., ISBN: 0-471-05059-8, 1994. MR1288523 (95d:14001)
[17] J. Guàrdia, *Jacobian nullwerte and algebraic equations*, Journal of Algebra **253** (2002), 112–132. MR1925010 (2004a:14032)
[18] ———, *Jacobian nullwerte, periods and symmetric equations for hyperelliptic curves*, Annales de l'Institut Fourier **57 (4)** (2007), 1253–1283. MR2339331
[19] E. W. Howe, *Plane quartics with Jacobians isomorphic to a hyperelliptic Jacobian*, Proc. of the AMS **129(6)** (2000), 1647–1657. MR1814093 (2002a:14028)
[20] G. Humbert, *Sur les fonctions abéliennes singulières (deuxieme mémoire)*, J. Math. Pures Appl. **5(6)** (1900), 279–386.
[21] H. Lange, *Abelian varieties with several principal polarizations*, Duke Math. J. **55(3)** (1987), 617–628. MR904944 (88i:14039)

[22] D. Lehavi, *Bitangents and two level structures for curves of genus* 3, Ph.D. thesis, Hebrew University of Jerusalem, 2002.

[23] ———, *Any smooth plane quartic can be reconstructed from its bitangents*, Israel J. Math. **146 (2)** (2005), 371–379. MR2151609 (2006a:14050)

[24] A. Logan, *The Brauer-Manin obstruction on del Pezzo surfaces of degree* 2 *branched along a plane section of a Kummer surface*, preprint, 2007.

[25] Magma, *Computational Algebra System*, Available on `http://magma.maths.usyd.edu.au/magma/`.

[26] T. Ohno, *Invariant subring of ternary quartics I - generators and relations*, preprint.

[27] R. Oyono, *Arithmetik nicht-hyperelliptischer Kurven des Geschlechts 3 und ihre Anwendung in der Kryptographie*, Ph.D. thesis, Essen, 2006.

[28] C. Poor, *On the hyperelliptic locus*, Duke Math. J. **76/3** (1994), 809–884. MR1309334 (96f:14032)

[29] E. Reinaldo-Barreiro, J. Estrada-Sarlabous, and J-P. Cherdieu, *Efficient reduction on the Jacobian variety of Picard curves*, Coding theory, cryptography, and related areas, vol. 877, Springer, 1998, pp. 13–28. MR1749445 (2001f:14057)

[30] B. Riemann, *Sur la théorie des fonctions abéliennes*, Oeuvres de Riemann, 2nd edition (1898), 487.

[31] C. Ritzenthaler, *Problèmes arithmétiques relatifs à certaines familles de courbes sur les corps finis*, Ph.D. thesis, Université Paris 7, 2003.

[32] T. Shaska and J. L. Thompson, *On the generic curve of genus* 3, Contemporary. Math. **369** (2005), 233–244. MR2126664 (2006c:14042)

[33] G. Shimura, *On the factors of the Jacobian variety of a modular function field*, J. Math. Soc. Japan **25(3)** (1973), 523–544. MR0318162 (47:6709)

[34] ———, *Introduction to the arithmetic theory of automorphic functions*, Reprint of the 1971 original. Publications of the Mathematical Society of Japan, 11. Kâno Memorial lectures, 1. Princeton University Press, Princeton, NJ, xiv + 271 pp., ISBN: 0-691-08092-5, 1994. MR1291394 (95e:11048)

[35] T. Shioda, *Plane quartics and Mordell-Weil lattices of type* E_7, Comment. Math. Univ. St. Pauli **42 (1)** (1993), 61–79. MR1223188 (95f:14056)

[36] A. R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141(3)** (1995), 553–572. MR1333036 (96d:11072)

[37] A.M. Vermeulen, *Weierstrass points of weight two on curves of genus* 3, Ph.D. thesis, Universiteit van Amsterdam, 1983. MR715084 (84j:14036)

[38] H-J. Weber, *Algorithmische Konstruktion hyperelliptischer Kurven mit kryptographischer Relevanz und einem Endomorphismenring echt größer als* $\mathbb{Z}$, Ph.D. thesis, Institut für Experimentelle Mathematik Essen, 1997.

[39] ———, *Hyperelliptic Simple Factors of* $J_0(N)$ *with Dimension at least* 3, Exp. Math. **6(4)** (1997), 273–287. MR1606908 (99e:14054)

[40] A. Weil, *Zum Beweis des Torellischen Satzes*, Nach. der Akad. der Wiss. Göttingen, Math. Phys. Klasse (1957), 33–53. MR0089483 (19:683e)

[41] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141(3)** (1995), 443–551. MR1333035 (96d:11071)

Équipe GAATI, Université de Polynésie Française, BP 6570, 98702 Faa'a, Tahiti, Polynésie Française

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