Modular Jacobians of dimension 3

Roger Oyono

University of Waterloo

Computational challenges arising in algorithmic number theory and Cryptography, Toronto 2006

Modular Jacobians of dimension 3

Modular Jacobians of dimension 3

Definition

A non-hyperelliptic curve C is a curve for which there exists no morphism $C \longrightarrow \mathbb{P}^1$ of degree 2.

Canonical embedding

Let $\{\omega_1, \cdots, \omega_g\}$ a basis of $\Omega^1(C)$. The curve C is non-hyperelliptic iff the canonical morphism

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

is an embedding.

In that case, $\varphi(C)$ is a curve of degree $2g - 2$.

Definition

A non-hyperelliptic curve C is a curve for which there exists no morphism $C \longrightarrow \mathbb{P}^1$ of degree 2.

Canonical embedding

Let $\{\omega_1, \cdots, \omega_g\}$ a basis of $\Omega^1(C)$. The curve C is non-hyperelliptic iff the canonical morphism

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

is an embedding.
In that case, $\varphi(C)$ is a curve of degree $2g-2$.

Properties for $g(C) = 3$

- $\varphi(C)$ is a smooth plane quartic,
- Any smooth plane quartic is the image by the canonical embedding of a genus 3 non-hyperelliptic curve.
- If $\mathrm{char}(k) \neq 2$, there are exactly 28 bitangents.
- If $\mathrm{char}(k) \neq 2, 3$, there are 24 Weierstrass points (with multiplicity).
- There exists a complete system of invariants for plane quartics (Dixmier-Ohno).

Theorem (*Shioda*)

Let k be a field with $\mathrm{char}(k) \neq 3$. Given a plane quartic with an ordinary flex (C, ξ) defined over k, there is a coordinate system (x, y, z) of $\mathbb{P}^2$ s.t. C, ξ are given by

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

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:

$$\lambda = (p_i, q_j) \sim \lambda' = (p_i', q_j') \Longleftrightarrow p_i' = u^{6-2i} p_i,\ \ q_j' = u^{9-2j} q_j,\ \ (i = 0, 1,\ j = 0, 1, \cdots, 4)$$

for some $u \neq 0$.

Modular Jacobians of dimension 3

Definition

Hecke subgroups of Level N in $\mathrm{SL}_2(\mathbb{Z})$:

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) | \quad c \equiv 0 \mod N \right\}$$

$\Gamma_0(N)$ acts on the extended upper half plane $\mathbb{H}^* := \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$ with $\mathbb{H} := \{\tau \in \mathbb{C} | \quad \Im\mathrm{m}(\tau) > 0\}$ via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z \longmapsto \frac{az+b}{cz+d}.$$

The orbits of this action are the modular curves $X_0(N)$:

$$\Gamma_0(N) \backslash \mathbb{H}^* =: X_0(N).$$

- For the $\mathbb{C}$-vector space $S_2(N)$ of cusp forms of weigth 2:

$$S_2(N) \simeq \Omega^1(X_0(N))$$

- Fourier expansion of cusp forms:

$$f(\tau) := \sum_{n=1}^{\infty} a_n q^n, q := e^{2\pi i \tau}, \;\; a_n \in \mathbb{C},$$

  and $f \equiv 0 \iff a_n = 0$ for $0 \leq n \leq \mu k/12$ where

$$\mu := [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)].$$

- The Hecke algebra induces an action on $S_2(N)$ as well as on $J_0(N)$.

- The vector space $S_2^{\mathrm{new}}(N)$ of newforms is the orthogonal complement of

$$S_2^{\mathrm{old}}(N) := \langle g(d\tau) | \quad g(\tau) \in S_2(M) \text{ with } M|N, M \neq N, d|\frac{N}{M}\rangle.$$

with respect to the Petersson inner product.
- There exists a unique basis of $S_2^{\mathrm{new}}(N)$ consisting of eigenforms with respect to all the Hecke operators T_p ($\mathrm{gcd}(p, N) = 1$).

Theorem

- Shimura (1973): *To the eigenform* $f = \sum_{n=1}^{\infty} a_n q^n \in S_2^{\mathrm{new}}(N)$ *there exists a* $\mathbb{Q}$*-simple abelian subvariety of* $J_0^{\mathrm{new}}(N)$ *of dimension* $[K_f, \mathbb{Q}]$ *where* $K_f := \mathbb{Q}(a_n)$.
- Eichler-Shimura relation: *For the characteristic polynomial* χ_{T_p} *of the Hecke operator* T_p *:*

$$\#A_f(\mathbb{F}_p) = \chi_{T_p}(p+1).$$

Definition

$A_{/\mathbb{Q}}$ is a *modular abelian variety of level* N if

$$\exists \tau_{/\mathbb{Q}} : J_0(N) \twoheadrightarrow A.$$

Theorem

- Shimura (1973): *To the eigenform* $f = \sum_{n=1}^{\infty} a_n q^n \in S_2^{\mathrm{new}}(N)$ *there exists a* $\mathbb{Q}$*-simple abelian subvariety of* $J_0^{\mathrm{new}}(N)$ *of dimension* $[K_f, \mathbb{Q}]$ *where* $K_f := \mathbb{Q}(a_n)$.
- Eichler-Shimura relation: *For the characteristic polynomial* χ_{T_p} *of the Hecke operator* T_p *:*

$$\# A_f(\mathbb{F}_p) = \chi_{T_p}(p+1).$$

Definition

$A_{/\mathbb{Q}}$ is a *modular abelian variety of level* N if

$$\exists \tau_{/\mathbb{Q}} : J_0(N) \twoheadrightarrow A.$$

Definition

$C_{/\mathbb{Q}}$ is a *modular curve of level N* if

$$\exists \pi_{/\mathbb{Q}} : X_0(N) \longrightarrow\!\!\!\!\!\rightarrow C\,.$$

$$X_0(N) \xrightarrow{\quad\pi\quad}\!\!\!\!\!\rightarrow C$$

Definition

$C_{/\mathbb{Q}}$ is a *modular curve of level N* if

$$\exists \pi_{/\mathbb{Q}} : X_0(N) \twoheadrightarrow C\,.$$

$$J_0(N) \xrightarrow{\pi_*} J(C)$$

$$X_0(N) \xrightarrow{\pi} C$$

Definition

$C_{/\mathbb{Q}}$ is a *modular curve of level N* if

$$\exists \pi_{/\mathbb{Q}} : X_0(N) \twoheadrightarrow C .$$

In that case, $J(C)$ is modular of level N, since we have

$$J_0(N) \xrightarrow{\pi_*} J(C)$$

$$X_0(N) \xrightarrow{\pi} C$$

Definition

$C_{/\mathbb{Q}}$ is a *modular curve of level N* if

$$\exists \pi_{/\mathbb{Q}} : X_0(N) \twoheadrightarrow C .$$

In that case, $J(C)$ is modular of level N, since we have

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

Definition

$C_{/\mathbb{Q}}$ is a *modular curve of level N* if

$$\exists \pi_{/\mathbb{Q}} : X_0(N) \twoheadrightarrow C\,.$$

In that case, $J(C)$ is modular of level N, since we have

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

The converse is not true in general.

Definition

$C_{/\mathbb{Q}}$ is a *modular curve of level* N if

$$\exists \pi_{/\mathbb{Q}} : X_0(N) \twoheadrightarrow C \,.$$

In that case, $J(C)$ is modular of level N, since we have

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

The converse is not true in general.

Definition

$C_{/\mathbb{Q}}$ is a modular curve of level N if

$$X_0(N) \xrightarrow{\pi_{/\mathbb{Q}}} C$$

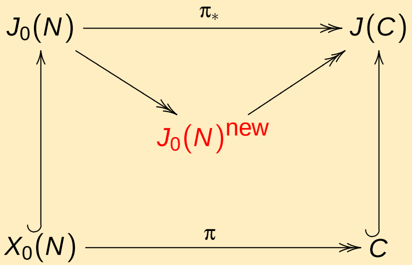
Definition

$C_{/\mathbb{Q}}$ is a modular curve of level N if

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

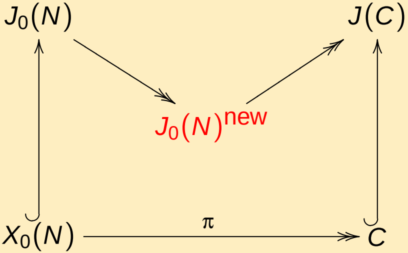
Definition

$C_{/\mathbb{Q}}$ is a *new modular curve of level* N if



Definition

$C_{/\mathbb{Q}}$ is a *new modular curve of level N* if

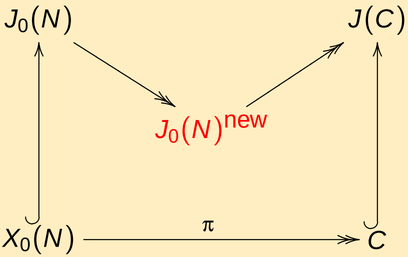


Then

$$\pi^* \Omega^1(C) \hookrightarrow S_2(N)^{\mathrm{new}} \frac{dq}{q}$$

Definition

$C_{/\mathbb{Q}}$ is a *new modular curve of level N* if



Then

$$\pi^* \Omega^1(C) \hookrightarrow S_2(N)^{\text{new}} \frac{dq}{q}$$

Notation

Let $g \in \mathbb{Z}$ such that $g \geq 0$, we denote by

$$\begin{aligned} \mathcal{MC}_g &= \{\text{modular curves of genus } g\}_{/\overset{\mathbb{Q}}{\simeq}}, \\ \mathcal{MC}_g^{\text{new}} &= \{[C] \in \mathcal{MC}_g \,|\, C \text{ is new}\}. \end{aligned}$$

$g = 1$, Wiles et. al.

$\mathcal{MC}_1 = \mathcal{MC}_1^{\text{new}} = \{\text{elliptic curves defined over } \mathbb{Q}\}_{/\overset{\mathbb{Q}}{\simeq}}.$

$\#\mathcal{MC}_1 = \#\mathcal{MC}_1^{\text{new}} = \infty.$

Theorem (Baker et. al.)

Let $g \geq 2$ be an integer. Then $\mathcal{MC}_g^{new}$ is finite and computable.

Notation

Let $g \in \mathbb{Z}$ such that $g \geq 0$, we denote by

$$\mathcal{MC}_g = \{\text{modular curves of genus } g\}_{/\overset{\mathbb{Q}}{\simeq}},$$
$$\mathcal{MC}_g^{\text{new}} = \{[C] \in \mathcal{MC}_g \,|\, C \text{ is new}\}.$$

$g = 1$, Wiles et. al.

$\mathcal{MC}_1 = \mathcal{MC}_1^{\text{new}} = \{\text{elliptic curves defined over } \mathbb{Q}\}_{/\overset{\mathbb{Q}}{\simeq}}$.

$\#\mathcal{MC}_1 = \#\mathcal{MC}_1^{\text{new}} = \infty$.

Theorem (Baker et. al.)

Let $g \geq 2$ be an integer. Then $\mathcal{MC}_g^{new}$ is finite and computable.

Notation

Let $g \in \mathbb{Z}$ such that $g \geq 0$, we denote by

$$\begin{aligned} \mathcal{MC}_g &= \{\text{modular curves of genus } g\}_{/\underset{\simeq}{\mathbb{Q}}}, \\ \mathcal{MC}_g^{\text{new}} &= \{[C] \in \mathcal{MC}_g \,|\, C \text{ is new}\}. \end{aligned}$$

$g = 1$, Wiles et. al.

$$\mathcal{MC}_1 = \mathcal{MC}_1^{\text{new}} = \{\text{elliptic curves defined over } \mathbb{Q}\}_{/\underset{\simeq}{\mathbb{Q}}}.$$

$$\#\mathcal{MC}_1 = \#\mathcal{MC}_1^{\text{new}} = \infty.$$

Theorem (Baker et. al.)

Let $g \geq 2$ be an integer. Then $\mathcal{MC}_g^{new}$ is finite and computable.

Non-Hyperelliptic Curves

Let $C_{/\mathbb{Q}}$ be a non-hyperelliptic curve of genus $g \geq 3$, and

$$\Omega^1(C) = \langle \omega_1, \ldots, \omega_g \rangle_{\mathbb{C}}.$$

Then there exists the *canonical embedding* defined by:

$$i : C \hookrightarrow \mathbb{P}^{g-1} \ : \ z \mapsto [\omega_1(z) : \cdots : \omega_g(z)]$$

where $i(C)$ is a nonsingular projective curve of degree $2g - 2$.

Example: $g = 3$

Algorithm $g = 3$ (joint work with Enrique González)

INPUT: $f_1, \dots, f_n \in \mathrm{New}_N$ such that $\dim A = 3$, $A = A_{f_1} \times \cdots \times A_{f_n}$.

Step 1: Compute a rational basis $\{h_1, \dots, h_3\}$ of $\Omega^1(A)$.Using Gauss elimination check if

$$\begin{cases} h_1 = & q + & O(q^2) & \\ h_2 = & & q^2 + & O(q^3) \\ h_3 = & & & O(q^3) \end{cases}$$

Step 2: embeding

$$\begin{cases} x = h_1 \\ y = h_2 \\ z = h_3 \end{cases}$$

Algorithm (cont.)

Step 3: Compute if there exists

$$F(X,Y,Z) = \sum_{i+j+k=4} a_{ijk} X^i Y^j Z^k \in \mathbb{Q}[X,Y,Z]$$

such that

$$F(x,y,z) = O(q^{c_N}),\ c_N = \frac{4}{3}[SL_2(\mathbb{Z}) : \Gamma_0(N)],$$

Step 4: If $C : F(X,Y,Z) = 0$ is smooth and of genus 3 then C is a non-hyperelliptic modular curve of genus 3, level N such that

$$J(C) \overset{\mathbb{Q}}{\sim} A.$$

OUTPUT: $C : F(X,Y,Z) = 0$ or ERROR.

$$C \quad : \quad F(x,y,z) = 0$$

C^A_{97} : $x^3z - x^2y^2 - 5x^2z^2 + xy^3 + xy^2z + 3xyz^2 + 6xz^3 - 3y^2z^2 - yz^3 - 2z^4 = 0$

C^B_{109} : $x^3z - 2x^2yz - x^2z^2 - xy^3 + 6xy^2z - 6xyz^2 + 3xz^3 + y^4 - 6y^3z + 10y^2z^2 - 5yz^3 = 0$

C^C_{113} : $x^3z - x^2y^2 - 4x^2z^2 + xy^3 + 2xy^2z + 6xz^3 - y^3z - 3y^2z^2 + yz^3 - 3z^4 = 0$

C^A_{127} : $x^3z - x^2y^2 - 3x^2z^2 + xy^3 - xyz^2 + 4xz^3 + 2y^3z - 3y^2z^2 + 3yz^3 - 2z^4 = 0$

C^B_{139} : $x^3z - x^2y^2 - 2x^2z^2 + xy^3 - 2xy^2z + 2xyz^2 + xz^3 + y^4 - 2y^3z + 4y^2z^2 - 3yz^3 = 0$

C^A_{149} : $x^3z - x^2y^2 - 3x^2z^2 + xy^3 + 3xy^2z - 2xyz^2 + 2xz^3 - y^4 - y^2z^2 + yz^3 = 0$

$\vdots$ $\vdots$

21 new modular curves with $\mathbb{Q}$-simple Jacobians

$\vdots$ $\vdots$

C^L_{855} : $x^3z - x^2z^2 - xy^3 + 3xyz^2 - 3xz^3 + 2y^3z - 3y^2z^2 + 3yz^3 = 0$

C^D_{1175} : $x^3z - x^2y^2 + x^2z^2 + xy^3 - 2xy^2z + 2xyz^2 - xz^3 + y^4 - 2y^3z + y^2z^2 + yz^3 = 0$

C^P_{1215} : $x^3z - xy^3 + 3xyz^2 + 5xz^3 - 6y^2z^2 - 3yz^3 + z^4 = 0$

How to compute a basis of $S_2(C)$ if C is a "non-new" modular curve?

Lemma

Let $\pi : X_0(N) \longrightarrow C$ a non-constant $\mathbb{Q}$-morphism. The vector space $S_2(C)$ admits a $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-invariant basis B consisting of cusp forms

$$h(q) = \sum_{d \mid \frac{N}{M}} c_d f(q^d)$$

for $M \mid N$, $f \in S_2^{\mathrm{new}}(M)$ and $c_d \in K_f$.

Example:

$J_0(178) \sim_{\mathbb{Q}} A_{f_1}^{(1)} \times A_{f_2}^{(1)} \times A_{f_3}^{(2)} \times A_{f_4}^{(3)} \times (B_{g_1}^{(1)})^2 \times (B_{g_2}^{(1)})^2 \times (B_{g_3}^{(5)})^2$.
Let $A_{f_3,g_2} := A_{f_3}^{(2)} \times B_{g_2}^{(1)}$

$$f_3(q) = q + q - q^2 + aq^3 + q^4 + (-2a-3)q^5 + O(q^6) \in S_2^{\mathrm{new}}(178)$$

$$g_2(q) = q - q^2 - q^3 - q^4 - q^5 + O(q^6) \in S_2^{\mathrm{new}}(89)$$

where $K_{f_3} = \mathbb{Q}(a)$ with $a^2 + 2a - 1 = 0$. Let $S_2(A_{f_3}) = \langle f_{31}, f_{32} \rangle$ with

$$f_{31}(q) = q - q^2 + q^4 - 3q^5 - 2q^7 - q^8 - 2q^9 + O(q^{10})$$

$$f_{32}(q) = q^3 - 2q^5 - q^6 - 2q^9 + O(q^{10})$$

We have

$$F(f_{31}(q), f_{32}(q), g_2(q) + 2g_2(q^2)) = 0,$$

where $C : F = 0$ is the smooth plane quartic given by

$$F(x,y,z) = x^4 - 8x^3y + 38x^2y^2 - 2x^2z^2 - 24xy^3 - 8xyz^2 - 7y^4 + 6y^2z^2 + z^4.$$

Modular Jacobians of dimension 3

- Abelian varieties (of dimension g) over $\mathbb{C}$ are isomorphic to tori $\mathbb{C}^g/\Lambda$, with a well defined Riemann form E.
- Example: A Riemann form of the elliptic curve $E(\mathbb{C}) \simeq \mathbb{C}/(\mathbb{Z}+i\mathbb{Z})$ is given by

$$E(x+iy, x'+iy') := x'y - y'x.$$

- $\mathbb{C}^g/\Lambda$ is principally polarized (p.p.), if there exists a basis $\{\lambda_1, \cdots, \lambda_{2g}\}$ of Λ with

$$(E(\lambda_i, \lambda_j)) = \begin{pmatrix} 0 & E_g \\ -E_g & 0 \end{pmatrix}$$

In this case: $A \simeq \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$ with $\Omega \in \mathbb{H}_g$.
- Jacobian varieties are principally polarized.

Theorem

An absolute simple p.p.a.v. A of dimension $g \leq 3$ is isomorphic to the Jacobian of a genus g curve.

Theorem (*Torelli (1957)*)

$\mathrm{Jac}(C_1) \simeq \mathrm{Jac}(C_2)$ *(as p.p.a.v.)* $\Longleftrightarrow C_1 \simeq C_2$.

Remark

There exists non-isomorphic curves C and C' with isomorphic unpolarized Jacobian (Howe, Rotger, ...).

(Theta)-characteristic (odd / even)

- A (theta)-charactersitic is a vector of the form $m = \begin{bmatrix} \delta \\ \varepsilon \end{bmatrix}$ with $\delta, \varepsilon \in \mathbb{Z}^g \bmod 2\mathbb{Z}^g$. The charactersitic m is odd (resp. even) iff $\delta \cdot \varepsilon^T \equiv 1 \mod 2$ (resp. $\delta \cdot \varepsilon^T \equiv 0 \mod 2$).
- There are $2^{g-1}(2^g - 1)$ odd characteristics and $2^{g-1}(2^g + 1)$ even characteristics.

Riemann Theta functions:

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

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

$$\vartheta \begin{bmatrix} \delta \\ \varepsilon \end{bmatrix} (0, \Omega) \quad := \quad \exp\left(\frac{\pi i}{4}\delta\Omega\delta^t + \pi i \delta \frac{\varepsilon^t}{2} \right) \cdot \vartheta\left(\frac{1}{2}\Omega\delta^t + \frac{\varepsilon^t}{2}, \Omega \right)$$

- For an absolute simple p.p.a.v. $A = \mathbb{C}^3/(\mathbb{Z}^3 + \Omega\mathbb{Z}^3)$ there exists a curve C with $A \simeq \mathrm{Jac}(C)$.
- The curve C is hyperelliptic $\Longleftrightarrow$ exactly one even ϑ- constants of $\mathrm{Jac}(C)$ vanishes.
- For a smooth plane quartic: The odd 2-torsion points of $\mathrm{Jac}(C)$ correspond to divisor classes $[P_1 + P_2 - (P_1^\infty + P_2^\infty)]$ coming from bitangents of C.
- *Goal:* From the p.p.a.v. $A = \mathbb{C}^3/(\mathbb{Z}^3 + \Omega\mathbb{Z}^3)$ compute the equation of a curve C with $\mathrm{Jac}(C) \simeq_{\mathbb{C}} A$.

Hyperelliptic Shottky problem

- Rosenhain model using even ϑ-constants (Spalleck, Weng, ...).
- "Symmetric model" using derivatives of ϑ-function at odd 2-torsion points (Guardia).

- For an absolute simple p.p.a.v. $A = \mathbb{C}^3/(\mathbb{Z}^3 + \Omega\mathbb{Z}^3)$ there exists a curve C with $A \simeq \mathrm{Jac}(C)$.
- The curve C is hyperelliptic $\iff$ exactly one even ϑ- constants of $\mathrm{Jac}(C)$ vanishes.
- For a smooth plane quartic: The odd 2-torsion points of $\mathrm{Jac}(C)$ correspond to divisor classes $[P_1 + P_2 - (P_1^\infty + P_2^\infty)]$ coming from bitangents of C.
- *Goal:* From the p.p.a.v. $A = \mathbb{C}^3/(\mathbb{Z}^3 + \Omega\mathbb{Z}^3)$ compute the equation of a curve C with $\mathrm{Jac}(C) \simeq_{\mathbb{C}} A$.

Hyperelliptic Shottky problem

- Rosenhain model using even ϑ-constants (Spalleck, Weng, ...).
- "Symmetric model" using derivatives of ϑ-function at odd 2-torsion points (Guardia).

A set of characteristics $S := ([\varepsilon_i])_{i=1,\dots,7}$ is an Aronhold system if:

- Any odd characteristic is of the form $[\varepsilon_i]$ or $[\varepsilon_i] + [\varepsilon_j]$, $i \neq j$, and,
- Any even characteristic is of the form $[0]$ or $[\varepsilon_i] + [\varepsilon_j] + [\varepsilon_k]$, with distincts i, j, k.

Example

$$\varepsilon_1 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix} \quad \varepsilon_2 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix} \quad \varepsilon_3 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \quad \varepsilon_4 = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\varepsilon_5 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \quad \varepsilon_6 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \quad \varepsilon_7 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

Theorem (Riemann (1898))

For the canonical Aronhold system $(\beta_i)_{i=1,\dots,7}$ there exists a smooth plane quartic C admitting the $(\beta_i)_{i=1,\dots,7}$ as bitangents:

$$\sqrt{xv_1} + \sqrt{yv_2} + \sqrt{zv_3} = 0,$$

The linear functions v_1, v_2, v_3 are explicitly given.

Theorem (Lehavi (2002))

Any smooth plane quartic is uniquely (up to isomorphism) determined by an Aronhold system $(\beta_i)_{i=1,\cdots,7}$.

Theorem (Riemann (1898))

For the canonical Aronhold system $(\beta_i)_{i=1,\ldots,7}$ there exists a smooth plane quartic C admitting the $(\beta_i)_{i=1,\ldots,7}$ as bitangents:

$$\sqrt{xv_1} + \sqrt{yv_2} + \sqrt{zv_3} = 0,$$

The linear functions v_1, v_2, v_3 are explicitly given.

Theorem (Lehavi (2002))

Any smooth plane quartic is uniquely (up to isomorphism) determined by an Aronhold system $(\beta_i)_{i=1,\cdots,7}$.

Let $\mathrm{Jac}(C) \simeq \mathbb{C}^3/(\Omega_1\mathbb{Z}^3 + \Omega_2\mathbb{Z}^3)$, with $\Omega := \Omega_2\Omega_1^{-1} \in \mathbb{H}_3$.

How to compute the bitangents of C?

The bitangents $(\beta_i)_{i=1,\ldots,7}$ associated to the Aronhold system $([\varepsilon_i])_{i=1,\ldots,7}$ are given by

$$\left(\frac{\partial\vartheta}{\partial z_1}(\varepsilon_i), \frac{\partial\vartheta}{\partial z_2}(\varepsilon_i), \frac{\partial\vartheta}{\partial z_3}(\varepsilon_i)\right)\Omega_1^{-1}\begin{pmatrix} Z \\ X \\ Y \end{pmatrix} = 0.$$

Algorithm for Torelli in dimension 3

INPUT: $A = \mathbb{C}^3/(\mathbb{Z}^3 + \Omega\mathbb{Z}^3)$ p.p. and absolute simple.
OUTPUT: A smooth plane quartic C with $A \simeq_{\mathbb{C}} \mathrm{Jac}(C)$.

Step 1: Compute the 36 even ϑ-constant and decide whether $A \in \mathrm{Jac}(\mathcal{N}\mathcal{H}_3(\mathbb{C}))$ or not.

Step 2: Compute the derivatives of the ϑ-functions at the odd 2-torsion points $z_{\varepsilon_i}(\varepsilon_i \in S_{\mathrm{can}})$ and compute then the 7 associated bitangents β_i.

Step 3: Compute the Riemann model corresponding to the Aronhold system (β_i).

Theorem (Hida, Wang)

Let A_f be new modular p.p.a.v. and

$$\Omega_{1,f} := \left(\int_{w_i} \omega(f^{\sigma_j}) \right)_{i,j=1,\ldots,d} \in \mathbb{C}^{d \times d}$$

and

$$\Omega_{2,f} := \left(\int_{w_i} \omega(f^{\sigma_j}) \right)_{\substack{i=d+1,\ldots,2d \\ j=1,\ldots,d}} \in \mathbb{C}^{d \times d}.$$

The period matrix Ω_f of A_f is given by

$$\Omega_f = \Omega_{1,f}^{-1} \Omega_{2,f}.$$

Example

Let $N = 511 = 7 \cdot 73$ and $f \in S_2^{\mathrm{new}}(511)$ be the eigenform with Fourier expansion

$$f = q + aq^2 + 2q^3 + (a^2 - 2)q^4 + (-a+1)q^5 + 2aq^6 + O(q^7),$$

where $a^3 - 5a + 1 = 0$.
$A_f \simeq_{\mathbb{C}} \mathrm{Jac}(C_f)$ for a smooth plane quartic C_f given by

$$C_f : (xv_1 + yv_2 - zv_3)^2 = 4xyv_1v_2,$$

where

$$\begin{aligned}
v_1 &= \quad (7.883\cdots - 10.600\ldots i)x + (8.108\cdots - 11.222\ldots i)y + (6.920\cdots - 11.383\ldots i)z,\\
v_2 &= -(7.602\cdots - 6.770\ldots i)x - (7.566\cdots - 7.038\ldots i)y - (7.694\cdots - 7.382\ldots i)z,\\
v_3 &= -(1.282\cdots - 3.829\ldots i)x - (1.542\cdots - 4.184\ldots i)y - (0.227\cdots - 4.001\ldots i)z.
\end{aligned}$$

Example (cont.)

After Shioda transformation (with a specific Weierstrass point):

$$\begin{aligned} C_f:\ 0 &= y^3z + y(x^3 + 8.09331\ldots xz^2 + 376513626.19508\ldots z^3) \\ &\quad + x^4 - 30364.69321\ldots x^3z + 11220519.80408\ldots \\ &\quad + x^2z^2 + 46628578544.41879\ldots xz^3 + 19617959110841.35239\ldots z^4 \end{aligned}$$

defined over some real algebraic number field K, with the following $\mathbb{Q}$-rational Dixmier invariants:

$$\begin{aligned} i_1 &= \frac{5^9\cdot 37^9\cdot 43133^9}{2^{53}\cdot 3^{30}\cdot 7^8\cdot 11^{14}\cdot 73^3\cdot 101^{14}}, \\ i_2 &= \frac{-5^8\cdot 37^7\cdot 263\cdot 43133^7\cdot 197689\cdot 6021091}{2^{57}\cdot 3^{32}\cdot 7^8\cdot 11^{14}\cdot 73^3\cdot 101^{14}}, \\ i_3 &= \frac{5^6\cdot 13\cdot 37^6\cdot 43133^6\cdot 142702121\cdot 25535098000501}{2^{43}\cdot 3^{28}\cdot 7^8\cdot 11^{14}\cdot 73^3\cdot 101^{14}}, \\ i_4 &= \frac{5^5\cdot 17\cdot 37^5\cdot 577\cdot 43133^5\cdot 3563719\cdot 164875199\cdot 160402791737}{2^{39}\cdot 3^{28}\cdot 7^8\cdot 11^{14}\cdot 73^3\cdot 101^{14}}, \\ i_5 &= \frac{-5^4\cdot 13^2\cdot 37^4\cdot 43133^4\cdot 41153760466703282853288413280589099}{2^{33}\cdot 3^{24}\cdot 7^8\cdot 11^{14}\cdot 73^3\cdot 101^{14}}, \\ i_6 &= \frac{-5^3\cdot 37^3\cdot 43133^3\cdot 688333\cdot 28685999\cdot 30314713933866742956065584376 42759}{2^{36}\cdot 3^{26}\cdot 7^8\cdot 11^{14}\cdot 73^3\cdot 101^{14}} \end{aligned}$$

- For $N < 4000$:

$\#A_f$	3334
$\#$ p.p. A_f	79
$\#A_f \in \mathrm{Jac}(\mathcal{H}_3(\mathbb{C}))$	12
$\#A_f \in \mathrm{Jac}(\mathcal{NH}_3(\mathbb{C}))$	67

- The obtained equations are defined over $\bar{\mathbb{Q}}$.
- However: The Dixmier invariants of the C_f are defined over $\mathbb{Q}$.
- We are able to compute a $\mathbb{Q}$-rational model for curves C_f having a $\mathbb{Q}$-rational Weierstrass point.