Algorithmic number theory and the allied theory of theta functions

Christophe Ritzenthaler

Institut de Mathématiques de Luminy, CNRS

Edinburgh 10-10

e-mail: ritzenth@iml.univ-mrs.fr
web: http://iml.univ-mrs.fr/∼ritzenth/

Outline

Diffie-Hellman key exchange

Let $(G =< g >, \times)$ be a cyclic group of order N.

Alice		Bob
a random k_A		a random k_B
$h_A = g^{k_A}$		$h_B = g^{k_B}$
	$\xrightarrow{h_A}$	
	$\xleftarrow{h_B}$	
secret $= {h_B}^{k_A}$		secret $= {h_A}^{k_B}$

$\boxed{g^{k_A k_B} \text{ is the common secret}}$

A priori, the difficulty for an adversary is to compute $g^{k_A k_B}$ knowing g^{k_A} et g^{k_B}.

DLP and Jacobians

In many cases, it is known to be equivalent to the Discrete Logarithm Problem:

$$\text{giving } g \text{ and } g^a \text{ find } a.$$

Two constraints:

- the operations in G are fast;
- the best attack to solve the DLP is the 'generic attack' which requires $\approx \sqrt{\#G}$ operations.

Currently, the best G are the groups of rational points on the Jacobians of curves over finite fields with prime order.

Problem: how to construct/find such curves ?

- No brute force method: the finite field is typically $\mathbb{F}_{2^{127}-1}$ for a genus 2 curve.
- Many methods have been developed to get 'polynomial time' algorithms: ℓ-adic cohomology, p-adic cohomology, deformation, CM,. . .

The algorithms

CM method: CM-type + fundamental unit $\rightsquigarrow$ lattice + polarization $\rightsquigarrow$ period matrix $\rightsquigarrow$ Thetanullwerte $\rightsquigarrow \begin{cases} \text{the curve over } \mathbb{C} \\ \text{invariants} \end{cases} \rightsquigarrow$ curve $/\mathbb{F}_q$.

AGM for point counting: curve $/\mathbb{F}_q \rightsquigarrow$ lift $\rightsquigarrow$ quotients of Thetanullwerte $\rightsquigarrow$ canonical lift + info on Weil polynomial $\rightsquigarrow$ Weil polynomial.

Important points:

- the theory must be developed over any field (however the intuition comes from $\mathbb{C}$);
- the theory must be explicit;
- computations should be fast.

Coding theory origin

Context: to construct good error-correcting codes, one needs curves over finite fields with many rational points.

Problem: find a closed formula for the maximal number of points of a curve of genus g over a finite field k.
$\rightsquigarrow$ For $g = 1, 2, 3$ prove that a certain $(A, a)/k$ is a Jacobian.

Proposition (Precise Torelli theorem)

Let $(A, a)/K$ be a principally polarized abelian variety which is the Jacobian of a curve C over $\bar{K}$, then it is the Jacobian of a curve over $L = K(\sqrt{d})$ for a unique $d \in K^*/(K^*)^2$. Moreover if C is hyperelliptic then we can take $L = K$.

Serre's strategy for $g = 3$: d is the product of the 36 Thetanullwerte (correctly normalized).

1. Link with number theory, cryptography and coding theory

2. Period matrices and Thetanullwerte
   - Period matrices
   - Thetanullwerte
   - From the Thetanullwerte to the Riemann matrix
   - From the Riemann matrix to the (quotients of) Thetanullwerte

3. From the curve to its Jacobian
   - Hyperelliptic case and the first tool: s_ε
   - Non hyperelliptic case and the second tool: Jacobian Nullwerte

4. From the Jacobian to its curve
   - Even characteristics
   - Odd characteristics

Definitions

Let C be a curve over $k \subset \mathbb{C}$ of genus $g > 0$.

The Jacobian of C is a torus $\mathrm{Jac}(C) \simeq \mathbb{C}^g/\Lambda$ where

- the lattice $\Lambda = \Omega\mathbb{Z}^{2g}$,
- the matrix $\Omega = [\Omega_1,\ \Omega_2] \in \mathrm{M}_{g,2g}(\mathbb{C})$ is a period matrix and
- $$\tau = \Omega_2^{-1}\Omega_1 \in \mathbb{H}_g = \{M \in \mathrm{GL}_g(\mathbb{C}),\ {}^tM = M,\ \mathrm{Im}\, M > 0\}$$

  is a Riemann matrix.

Construction

- $v_1, \ldots, v_g$ be a k-basis of $H^0(C, \Omega^1)$,
- $\delta_1, \ldots, \delta_{2g}$ be generators of $H_1(C, \mathbb{Z})$ such that $(\delta_i)_{1 \ldots 2g}$ form a symplectic basis for the intersection pairing on C.

$$\Omega := [\Omega_1,\ \Omega_2] = \left[\int_{\delta_j} v_i\right]_{\substack{i=1,\ldots,g \\ j=1,\ldots,2g}} .$$

- Magma (Vermeulen): can compute Ω for a hyperelliptic curve.
- Maple (Deconinck, van Hoeij) can compute Ω for any plane model.

Remark: it would be nice to have a free implementation (in SAGE).

Example

Ex: $E : y^2 = x^3 - 35x - 98 = (x-7)(x-a)(x-\bar{a})$ which has complex multiplication by $\mathbb{Z}[\alpha]$ with $\alpha = \frac{-1-\sqrt{-7}}{2}$ and $a = \frac{-7}{2} - \frac{\sqrt{-7}}{2}$.

$$\Omega = \left[\, 2\int_a^{\bar{a}} \frac{dx}{2y}, 2\int_a^{7} \frac{dx}{2y} \right] = c \cdot [\alpha,\ 1].$$

(Chowla, Selberg 67) formula gives

$$c = \frac{1}{8\pi\sqrt{7}} \cdot \Gamma(\frac{1}{7}) \cdot \Gamma(\frac{2}{7}) \cdot \Gamma(\frac{4}{7})$$

with

$$\Gamma(x) = \int_0^{\infty} t^{z-1} \exp(-t)\, dt.$$

1. Link with number theory, cryptography and coding theory

2. Period matrices and Thetanullwerte
   - Period matrices
   - Thetanullwerte
   - From the Thetanullwerte to the Riemann matrix
   - From the Riemann matrix to the (quotients of) Thetanullwerte

3. From the curve to its Jacobian
   - Hyperelliptic case and the first tool: s_ε
   - Non hyperelliptic case and the second tool: Jacobian Nullwerte

4. From the Jacobian to its curve
   - Even characteristics
   - Odd characteristics

Projective embedding

The intersection pairing on C induces a principal polarization j on $\mathrm{Jac}(C)$.
$\iff$ The map $\mathbf{Sym}^{g-1} C \to \mathrm{Jac}(C)$ defines an ample divisor D on $\mathrm{Jac}(C)$ (up to translation).

Theorem (Lefschetz, Mumford, Kempf)

For $n \geq 3$, nD is very ample, i.e. one can embed $\mathrm{Jac}(C)$ in a $\mathbb{P}^{n^g-1}$ with a basis of sections of $\mathcal{L}(nD)$.

For $n = 4$, the embedding is given by intersection of quadrics, whose equations are completely determined by the image of 0.

Thetanullwert

A basis of sections of $\mathcal{L}(4D)$ is given by theta functions $\theta[\varepsilon](2z,\tau)$ with integer characteristics $[\varepsilon] = (\epsilon, \epsilon') \in \{0,1\}^{2g}$ where

$$\theta\begin{bmatrix}\epsilon\\ \epsilon'\end{bmatrix}(z,\tau) = \sum_{n\in\mathbb{Z}^g} \exp\left(i\pi\ (n+\frac{\epsilon}{2})\tau^t(n+\frac{\epsilon}{2}) + 2i\pi\ (n+\frac{\epsilon}{2})^t(z+\frac{\epsilon'}{2})\right).$$

When $\epsilon^t\epsilon' \equiv 0 \pmod 2$, $[\varepsilon]$ is said even and one calls Thetanullwert

$$\theta\begin{bmatrix}\epsilon\\ \epsilon'\end{bmatrix}(0,\tau) = \theta\begin{bmatrix}\epsilon\\ \epsilon'\end{bmatrix}(\tau) = \theta[\varepsilon](\tau) = \theta_{ab}$$

where the binary representations of a and b are ϵ, ϵ'.

Example

Let $q = \exp(\pi i \tau)$. There are 3 genus 1 Thetanullwerte:

$$\theta_{00} = \theta\begin{bmatrix}0\\0\end{bmatrix}(0,\tau) = \sum_{n\in\mathbb{Z}} q^{n^2},$$

$$\theta_{10} = \theta\begin{bmatrix}1\\0\end{bmatrix}(0,\tau) = \sum_{n\in\mathbb{Z}} q^{\left(n+\frac{1}{2}\right)^2},$$

$$\theta_{01} = \theta\begin{bmatrix}0\\1\end{bmatrix}(0,\tau) = \sum_{n\in\mathbb{Z}} (-1)^n q^{n^2}.$$

1. Link with number theory, cryptography and coding theory

2. Period matrices and Thetanullwerte
   - Period matrices
   - Thetanullwerte
   - From the Thetanullwerte to the Riemann matrix
   - From the Riemann matrix to the (quotients of) Thetanullwerte

3. From the curve to its Jacobian
   - Hyperelliptic case and the first tool: s_ε
   - Non hyperelliptic case and the second tool: Jacobian Nullwerte

4. From the Jacobian to its curve
   - Even characteristics
   - Odd characteristics

Case $g = 1$ Gauss, Cox 84, Dupont 07

- Let $z = \theta_{01}(\tau)^2/\theta_{00}(\tau)^2$.
- Duplication formulae vs AGM formulae :

$$\begin{array}{rcl|rcl}
\theta_{00}(2\tau)^2 & = & \frac{\theta_{00}(\tau)^2+\theta_{01}(\tau)^2}{2} & a_n & = & \frac{a_{n-1}+b_{n-1}}{2}, \\
\theta_{01}(2\tau)^2 & = & \theta_{00}(\tau)\cdot\theta_{01}(\tau) & b_n & = & \sqrt{a_{n-1}\cdot b_{n-1}}, \\
\theta_{10}(2\tau)^2 & = & \frac{\theta_{00}(\tau)^2-\theta_{01}(\tau)^2}{2} & AGM(a_0,b_0) & := & \lim a_n = \lim b_n
\end{array}$$

$\Rightarrow$ $AGM(\theta_{00}(\tau)^2, \theta_{01}(\tau)^2) = \lim \theta_{00}(2^n\tau)^2 = 1 \Rightarrow AGM(1,z) = \frac{1}{\theta_{00}(\tau)^2}$.

$\Rightarrow \theta_{10}(\tau)^2 = \sqrt{\theta_{00}(\tau)^4 - \theta_{01}(\tau)^4}$.

- Transformation formula :

$$\theta_{00}(\tau)^2 = \frac{i}{\tau} \cdot \theta_{00}\left(\frac{-1}{\tau}\right)^2, \quad \theta_{10}(\tau)^2 = \frac{i}{\tau} \cdot \theta_{01}\left(\frac{-1}{\tau}\right)^2.$$

$\Rightarrow AGM(\theta_{00}(\tau)^2, \theta_{10}(\tau)^2) = \frac{i}{\tau} \cdot \lim \theta_{00}(2^n \cdot \frac{-1}{\tau})^2 = \frac{i}{\tau} \cdot 1$

$\Rightarrow AGM(1, \sqrt{1-z^2}) = \frac{i}{\tau} \cdot \frac{1}{\theta_{00}(\tau)^2}$.

Proposition

$$\frac{i \cdot AGM(1,z)}{AGM(1,\sqrt{1-z^2})} = \tau.$$

Difficulty: define the correct square root when the values are complex.

Case $g \geq 2$

Particular case: real Weierstrass points and $g = 2$ (Bost-Mestre 88).

General case (Dupont 07): under some (experimentally verified) conjectures.

Proposition

One can compute τ in terms of $\theta[\varepsilon](\tau)^2/\theta[0](\tau)^2$ in time

$$O(g^2 \cdot 2^g \cdot n^{1+\epsilon})$$

for n digits of precision.

For comparison, integration takes $O(n^{2+\epsilon})$.

1. Link with number theory, cryptography and coding theory

2. Period matrices and Thetanullwerte
   - Period matrices
   - Thetanullwerte
   - From the Thetanullwerte to the Riemann matrix
   - From the Riemann matrix to the (quotients of) Thetanullwerte

3. From the curve to its Jacobian
   - Hyperelliptic case and the first tool: s_ε
   - Non hyperelliptic case and the second tool: Jacobian Nullwerte

4. From the Jacobian to its curve
   - Even characteristics
   - Odd characteristics

The work of (Dupont 07)

Naive method: $O(n\sqrt{n})$ for $g=1$ and $O(n^{2+\epsilon})$ for $g=2$.

New method: invert the AGM. Complexity for n bits of precision on the quotients

- $O(n^{1+\epsilon})$ for $g=1$,
- $O(n^{1+\epsilon})$ for $g=2$ (conjectural algorithm).

Main idea for $g=1$: let

$$f(z) = i \cdot AGM(1,z) - \tau \cdot AGM(1, \sqrt{1-z^2}).$$

Then $f(\theta_{01}(\tau)^2/\theta_{00}(\tau)^2)=0$. Do a Newton algorithm on f.

- can we get rid of the conjectures ?
- can we generalize to all genera ?
- can we compute the Thetanullwerte alone ?

Thomae's formulae

Let C be a hyperelliptic curve $C : y^2 = \prod_{i=1}^{2g+1}(x - \lambda_i)$.

Theorem (Thomae's formulae)

$$\theta[\varepsilon](\tau)^4 = \pm \left(\frac{\det \Omega_2}{\pi^g}\right)^2 \prod_{(i,j)\in I} (\lambda_i - \lambda_j)$$

with the choice of the basis of differentials $x^i dx/y$ (the set I depends on $[\varepsilon]$ and on the basis of $H_1(C, \mathbb{Z})$).

Proof: see (Fay 73) using a variational method.

Proof for the quotients:

- study the zeroes of the section

$$s_\varepsilon(P) = \theta[\varepsilon](\phi_{P_0}(P))$$

  where $P_0 \in C$ and $\phi_{P_0}(P) = P - P_0 \in \mathrm{Jac}(C)$.

- $c \cdot f(P) = \frac{s_\varepsilon(P)^2}{s_{\varepsilon'}(P)^2}$ for an explicit $f \in \mathbb{C}(C)$.
- $c = \frac{s_\varepsilon(P_1)^2}{s_{\varepsilon'}(P_1)^2 f(P_1)} = \frac{s_\varepsilon(P_2)^2}{s_{\varepsilon'}(P_2)^2 f(P_2)}$ for P_1, P_2 such that $\frac{s_\varepsilon(P_2)^2}{s_{\varepsilon'}(P_2)^2} = \frac{s_{\varepsilon'}(P_1)^2}{s_\varepsilon(P_1)^2}$.

1. Link with number theory, cryptography and coding theory

2. Period matrices and Thetanullwerte
   - Period matrices
   - Thetanullwerte
   - From the Thetanullwerte to the Riemann matrix
   - From the Riemann matrix to the (quotients of) Thetanullwerte

3. From the curve to its Jacobian
   - Hyperelliptic case and the first tool: s_ε
   - Non hyperelliptic case and the second tool: Jacobian Nullwerte

4. From the Jacobian to its curve
   - Even characteristics
   - Odd characteristics

Non hyperelliptic case genus 3

Let C be a smooth plane quartic.

Theorem (Weber 1876)

$$\left(\frac{\theta[\varepsilon](\tau)}{\theta[\varepsilon'](\tau)}\right)^4 = \frac{[b_i, b_j, b_{ij}][b_{ik}, b_{jk}, b_{ij}][b_j, b_{jk}, b_k][b_i, b_{ik}, b_k]}{[b_j, b_{jk}, b_{ij}][b_i, b_{ik}, b_{ij}][b_i, b_j, b_k][b_{ik}, b_{jk}, b_k]}$$

where the b_i, b_{ij} are linear equations of certain bitangents of C and $[b_i, b_j, b_k]$ is the determinant of the matrix of the coefficients of (once for all fixed) equations of the bitangents.

- Weber's proof uses $s_\varepsilon(P)$.
- Nart, R. unpublished: more natural proof using derivative of theta functions and a generalization of Jacobi's derivative formula.

Question: can we find a formula for a Thetanullwert alone like in the hyperelliptic case ?

Derivative of theta functions

When $\epsilon^t \epsilon' \equiv 1 \pmod 2$, $[\varepsilon]$ is said odd and we write $[\boldsymbol{\mu}]$ instead.

Definition

The theta gradient (with odd characteristic $[\boldsymbol{\mu}]$) is the vector

$$\nabla\theta[\boldsymbol{\mu}] := \left(\frac{\partial\theta[\boldsymbol{\mu}](z,\tau)}{\partial z_1}(0,\tau), \ldots, \frac{\partial\theta[\boldsymbol{\mu}](z,\tau)}{\partial z_g}(0,\tau) \right).$$

The theta hyperplane is the projective hyperplane

$$\nabla\theta[\boldsymbol{\mu}] \cdot (X_1, \ldots, X_g) = 0$$

of $\mathbb{P}^{g-1}$ defined by a theta gradient.
We denote the matrix

$$J[\boldsymbol{\mu}_1, \ldots, \boldsymbol{\mu}_g] := \left(\nabla\theta[\boldsymbol{\mu}_1], \ldots, \nabla\theta[\boldsymbol{\mu}_g] \right)$$

and $[\boldsymbol{\mu}_1, \ldots, \boldsymbol{\mu}_g]$ its determinant (called Jacobian Nullwerte).

Case of Riemann-Mumford-Kempf singularity theorem

Let C be any curve of genus $g > 0$ and let κ_0 be such that $\mathbf{Sym}^{g-1}\, C - \kappa_0 = \{z,\ \theta[0](z,\tau) = 0\}$.

Theorem

Let ϕ be the canonical map

$$\phi : C \to \mathbb{P}^{g-1},\ P \mapsto (\omega_1(P), \ldots, \omega_g(P)).$$

Let D be an effective divisor of degree $g-1$ on C such that $h^0(D) = 1$. Then

$$\left(\frac{\partial\theta(z,\tau)}{\partial z_1}(D - \kappa_0, \tau), \frac{\partial\theta(z,\tau)}{\partial z_g}(D - \kappa_0, \tau) \right) \Omega_2^{-1}\, {}^t(X_1, \ldots, X_g) = 0$$

is an hyperplane of $\mathbb{P}^{g-1}$ which contains the divisor $\phi(D)$ on the curve $\phi(C)$.

Remarks

- Jacobi's derivative formula expresses $[\boldsymbol{\mu}_1, \ldots, \boldsymbol{\mu}_g]$ as a precise polynomial in the Thetanullwerte.
- For $g \leq 5$ it is known that $[\boldsymbol{\mu}_1, \ldots, \boldsymbol{\mu}_g]$ is in $\mathbb{C}[\theta]$.In general, it is not true but $[\boldsymbol{\mu}_1, \ldots, \boldsymbol{\mu}_g]$ can be expresses as a quotient of two polynomials in the Thetanullwerte. There is also a precise conjectural formula (Igusa 80).
- Could we directly invert the formula, i.e. express a Thetanullwert is terms of Jacobian Nullwerte (at least for $g \leq 5$) ?
- (Nakayashili 97, Enolski, Grava 06): Thomae's formula for $y^n = \prod_{i=1}^m (x - \lambda_i)^{n-1} \cdot \prod_{i=m+1}^{2m} (x - \lambda_i)$.
- a general theory exists (Klein vol.3 p.429, Matone-Volpato 07 over $\mathbb{C}$, Shepherd-Barron preprint 08 over any field). Their expressions involve determinants of bases of $H^0(C, \mathcal{L}(2K_C + \boldsymbol{\mu}))$. But no formula or implementation has been done.

1. Link with number theory, cryptography and coding theory

2. Period matrices and Thetanullwerte
   - Period matrices
   - Thetanullwerte
   - From the Thetanullwerte to the Riemann matrix
   - From the Riemann matrix to the (quotients of) Thetanullwerte

3. From the curve to its Jacobian
   - Hyperelliptic case and the first tool: s_ε
   - Non hyperelliptic case and the second tool: Jacobian Nullwerte

4. From the Jacobian to its curve
   - Even characteristics
   - Odd characteristics

Torelli theorem: classical versions

Let C/k be a curve of genus $g > 0$.

Theorem

C is uniquely determined up to k-isomorphism by $(\mathrm{Jac}(C), j)$.

Corollary

C is uniquely determined up to $\mathbb{C}$-isomorphism by Ω or by the Thetanullwerte.

From the Jacobian to its curve: hyperelliptic case

$$C : y^2 = \prod_{i=1}^{2g+1} (x - \lambda_i).$$

Idea: invert quotient Thomae's formulae (Mumford Tata II p.136, Takase 96, Koizumi 97)

$$\frac{\lambda_k - \lambda_l}{\lambda_k - \lambda_m} = i^c \cdot \frac{\theta[\varepsilon_1]^2 \cdot \theta[\varepsilon_2]^2}{\theta[\varepsilon_3]^2 \cdot \theta[\varepsilon_4]^2}, \quad c \in \{0, 1, 2, 3\}.$$

- For genus 1: $\lambda_1 = \theta_1^4 / \theta_0^4$.
- For genus 2 (Rosenhain formula):

$$\lambda_1 = -\frac{\theta_{01}^2 \theta_{21}^2}{\theta_{30}^2 \theta_{10}^2}, \quad \lambda_2 = -\frac{\theta_{03}^2 \theta_{21}^2}{\theta_{30}^2 \theta_{12}^2}, \quad \lambda_3 = -\frac{\theta_{03}^2 \theta_{01}^2}{\theta_{10}^2 \theta_{12}^2}.$$

- For genus 3 (Weng 01):

$$\lambda_1 = \frac{(\theta_{15}\theta_3)^4 + (\theta_{12}\theta_1)^4 - (\theta_{14}\theta_2)^4}{2(\theta_{15}\theta_3)^4}, \lambda_2 = \frac{(\theta_4\theta_9)^4 + (\theta_6\theta_{11})^4 - (\theta_{13}\theta_8)^4}{2(\theta_4\theta_9)^4}, \ldots$$

From the Jacobian to its curve : non hyperelliptic genus 3

(Weber 1876) shows how to find the Riemann model:

$$C : \sqrt{x(a_1x + a_1'y + a_1''z)} + \sqrt{y(a_2x + a_2'y + a_2''z)} + \sqrt{z(a_3x + a_3'y + a_3''z)} = 0$$

with

$$a_1 = i\frac{\theta_{41}\theta_{05}}{\theta_{50}\theta_{14}}, \quad a_1' = i\frac{\theta_{05}\theta_{66}}{\theta_{33}\theta_{50}}, \quad a_1'' = -\frac{\theta_{66}\theta_{41}}{\theta_{14}\theta_{33}},$$

$$a_2 = i\frac{\theta_{25}\theta_{61}}{\theta_{34}\theta_{70}}, \quad a_2' = i\frac{\theta_{61}\theta_{02}}{\theta_{57}\theta_{34}}, \quad a_2'' = \frac{\theta_{02}\theta_{25}}{\theta_{70}\theta_{57}},$$

$$a_3 = i\frac{\theta_{07}\theta_{43}}{\theta_{16}\theta_{52}}, \quad a_3' = i\frac{\theta_{40}\theta_{20}}{\theta_{75}\theta_{16}}, \quad a_3'' = \frac{\theta_{20}\theta_{07}}{\theta_{52}\theta_{75}}.$$

Question: can something be done for $g \geq 4$?

1. Link with number theory, cryptography and coding theory

2. Period matrices and Thetanullwerte
   - Period matrices
   - Thetanullwerte
   - From the Thetanullwerte to the Riemann matrix
   - From the Riemann matrix to the (quotients of) Thetanullwerte

3. From the curve to its Jacobian
   - Hyperelliptic case and the first tool: s_ε
   - Non hyperelliptic case and the second tool: Jacobian Nullwerte

4. **From the Jacobian to its curve**
   - Even characteristics
   - **Odd characteristics**

Torelli theorems: odd versions

Theorem (Grushevsky, Salvati Manni 04)

A generic abelian variety of dimension $g \geq 3$ is uniquely determined by its theta gradients.

Theorem (Caporaso, Sernesi 03)

A general curve C of genus $g \geq 3$ is uniquely determined by its theta hyperplanes.

Rem: the second result is not a corollary of the first.

Hyperelliptic case: genus 2 example (Guàrdia 01,07)

Let $[\mu_1], \ldots, [\mu_6]$ be the odd characteristics. Then C admits a symmetric model

$$y^2 = x\left(x - \frac{[\mu_1,\mu_3]}{[\mu_2,\mu_3]}\right)\left(x - \frac{[\mu_1,\mu_4]}{[\mu_2,\mu_4]}\right)\left(x - \frac{[\mu_1,\mu_5]}{[\mu_2,\mu_5]}\right)\left(x - \frac{[\mu_1,\mu_6]}{[\mu_2,\mu_6]}\right).$$

Remarks:

- his theory of symmetric models has nice invariants, nice reduction properties.

Non hyperelliptic curves of genus 3: Guàrdia 09

Refinement of Riemann model: a smooth plane quartic over k is k-isomorphic to

$$\sqrt{\frac{[b_7\,b_2\,b_3][b_7\,b_2'\,b_3']}{[b_1\,b_2\,b_3][b_1'\,b_2'\,b_3']}X_1X_1'}+\sqrt{\frac{[b_1\,b_7\,b_3][b_7\,b_1'\,b_3']}{[b_1\,b_2\,b_3][b_1'\,b_2'\,b_3']}X_2X_2'}+\sqrt{\frac{[b_1\,b_2\,b_7][b_7\,b_1'\,b_2']}{[b_1\,b_2\,b_3][b_1'\,b_2'\,b_3']}X_3X_3'}=0$$

where X_i, X_i' are the equations of the bitangents b_i, b_i'.

Ex: Take $A = E^3$ where E has CM by $\sqrt{-19}$ + the unique undecomposable principal polarization. Then $A = \mathrm{Jac}(C)$ where

$$C : x^4 + (1/9)y^4 + (2/3)x^2y^2 - 190y^2 - 570x^2 + (152/9)y^3 - 152x^2y - 1083 = 0.$$

Summary

	$g=1$	$g=2$	$g \geq 3$ h.	$g=3$ n.h.	$g>3$ n.h.
$\theta \to \tau$	fast	fast conj.	fast conj.	fast conj.	fast conj.
$\tau \to \theta$	algo fast quotient	algo fast quot.	algo	algo	algo
$C \to \Omega$	fast	(free) algo	algo	algo	plane model
$C \to \theta$	fast	algo	algo	algo quot.	theory
$\theta \to C$	fast	fast	fast	fast	?
$\nabla\theta \to C$	fast	fast	fast	fast	?

algo: there exists an algorithm but slow.
fast (conj.): there exists a fast (conjectural) algorithm.
quot.: for the quotient of Thetanullwerte.
theory: the theory is done but no implementation has been done.
?: nothing is done.