Arithmetic on Picard curves of CM-type

Anna Somoza
Universitat Politècnica de Catalunya

25 January 2015

Introduction

Abelian varieties

An abelian variety over $\mathbb{C}$ is

- a g-dimensional complex torus:

$$A = \mathbb{C}^g/\Lambda\,, \quad \Lambda = w_1\mathbb{Z} + \cdots + w_{2g}\mathbb{Z}\,,$$

  the w_i in $\mathbb{C}^g$ being $\mathbb{R}$-linearly independent,

- that can be polarized: admits a Riemann form with respect to Λ

$$E\colon \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{R}$$

  (1) E is an alternating non-degenerate $\mathbb{R}$-bilinear form.
  (2) It takes integral values on $\Lambda \times \Lambda$.
  (3) the form $(x, y) \mapsto E(ix, y)$ is positive definite.

Abelian varieties

Given $A = (\mathbb{C}^g/\Lambda, E)$ an abelian variety, $\Lambda = w_1\mathbb{Z} + \cdots + w_{2g}\mathbb{Z}$, the matrix

$$P = (E(w_i, w_j)) \in \mathrm{Mat}_{2g}(\mathbb{Z})$$

is antisymmetric (skew-symmetric) $P^t = -P$. Frobenius shows that there is a canonical basis:

$$\Lambda = e_1\mathbb{Z} + \cdots + e_{2g}\mathbb{Z}$$

such that

$$Q = (E(e_i, e_j)) = \left[\begin{array}{c|c} O_g & D \\ \hline -D & O_g \end{array}\right], \quad D = \mathrm{diag}(d_1, d_2, \ldots, d_g),$$

with $d_1 \mid d_2 \mid \cdots \mid d_g$ called the elementary divisors of E.
When $d_1 = d_2 = \cdots = d_g = 1$, we call (A, E) principally polarized.

Abelian varieties of CM-type

We say that $A = (\mathbb{C}^g/\Lambda, E)$ is of *CM*-type if

$$\mathrm{End}(A) \otimes \mathbb{Q}$$

contains a commutative subring of dimension $2g$ over $\mathbb{Q}$.

Note that in this case A is defined over a number field.

Advantages:

- The more endomorphisms A has, the better arithmetic we can do.
- Its Hasse-Weil L-function can be computed as a Hecke L-function.

And it is easy to manufacture A of CM-type!

We ought all this to Shimura-Taniyama (and Deuring for $g = 1$).

Abelian varieties of CM-type

A number field $K/\mathbb{Q}$ is a *CM*-field if it is a quadratic extension K/K_0 where the base field K_0 is totally real but K is totally imaginary:

- $K_0 \hookrightarrow \mathbb{R}$ (all embeddings are real)
- $[K : K_0] = 2$ and $K \hookrightarrow \mathbb{C}$ (no real embedding).

Examples: $K =$ quadratic imaginary, cyclotomic fields, Picard fields, ...

Abelian varieties of CM-type

A CM-type (K, Φ) is a CM-field K of degree $2g$ along with

$$\Phi = \{\sigma_1, \dots, \sigma_g\}$$

where $\sigma_i \colon K \hookrightarrow \mathbb{C}$ are different embeddings and $\overline{\sigma}_i$ is not in Φ.

An abelian variety $A = (\mathbb{C}^g/\Lambda, E)$ is of CM-type (K, Φ) if there is an isomorphism

$$\mathcal{O}_K \hookrightarrow \mathrm{End}(A)\,, \quad \gamma \mapsto \mathrm{diag}(\sigma_1(\gamma), \dots, \sigma_g(\gamma))\,.$$

Abelian varieties of CM-type

Let (K, Φ) be a CM-type.

Given an ideal $\mathfrak{b}$ of the ring of integers $\mathcal{O}_K$, we consider the lattice

$$\Phi(\mathfrak{b}) = \{(\sigma_1(\beta), \ldots, \sigma_g(\beta))\colon \beta \in \mathfrak{b}\}.$$

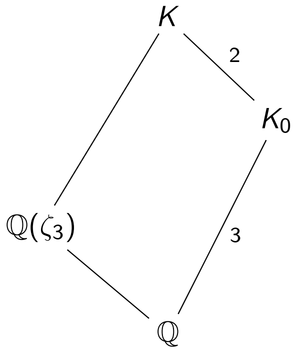
The torus $A = \mathbb{C}^g/\Phi(\mathfrak{b})$ can be polarized, giving rise to an abelian variety of CM-type

$$\begin{aligned} \mathcal{O}_K &\hookrightarrow \mathrm{End}(A) \\ \gamma &\mapsto \mathrm{diag}(\sigma_1(\gamma), \ldots, \sigma_g(\gamma)) \end{aligned}$$

Up to isogeny, all abelian varieties of CM-type can be constructed in this way. Moreover, A is simple if and only if the CM-type Φ is primitive.

Picard fields

Here after, a Picard field is a CM-field obtained as a Kummer extension of $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$ that is normal over $\mathbb{Q}$:



$\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma \rangle \simeq \mathbb{Z}/6\mathbb{Z}$.
Primitive CM-type: $\Phi = \{1, \sigma, \sigma^2\}$.

Picard fields

As an application of the Louboutin and Yamamura lower bounds for the relative class number $h^{-}(K)$:

$$h(K) = h^{-}(K) \cdot h(K_0)\,,$$

Park and Kwon (1997) give reasonable upper bounds for the conductors of the abelian sextic CM-fields with small class numbers. In particular, there are only 5 Picard fields with class number $h(K) = 1$, none with $h(K) = 2$ and a few dozens with $h(K) = 3$.

Classification theorem

Let (K, Φ) be a CM-type of degree $2g$ and let $\delta_{K/\mathbb{Q}}$ be the different of K.

Theorem (Shimura)

Let $\mathfrak{b}$ be an ideal in $\mathcal{O}_K$ such that $\delta_{K/\mathbb{Q}}\mathfrak{b}\overline{\mathfrak{b}} = (b)$.
Assume there is a unit $\varepsilon \in \mathcal{O}_{K_0}^*$ such that εb is totally imaginary and $\operatorname{Im}\sigma(\varepsilon b) < 0$ for all $\sigma \in \Phi$. Write $\xi = (\varepsilon b)^{-1}$.
Then, the bilinear form

$$E_\xi(x, y) = \sum_{i=1}^{g} \sigma_i(\xi)\,(\overline{x}_i y_i - x_i \overline{y}_i)$$

defines a principal polarization on $\Phi(\mathfrak{b})$. Moreover, two such $(\mathbb{C}^g/\Phi(\mathfrak{b}_1), E_{\xi_1})$ and $(\mathbb{C}^g/\Phi(\mathfrak{b}_2), E_{\xi_2})$ are isomorphic if and only if there exists $\gamma \in K$ such that $\gamma\,\mathfrak{b}_1 = \mathfrak{b}_2$ and $\xi_1 = \gamma\overline{\gamma}\xi_2$.

Algorithm

Input: K a Picard CM-field, $\Phi = \{1, \sigma, \sigma^2\}$ where $\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma \rangle$.

Output: Complete (finite) set of isomorphism classes of principally polarized abelian varieties having complex multiplication by $\mathcal{O}_K$.

Step 1: Compute:

- the different $\delta_{K/\mathbb{Q}}$ and the class group $\mathrm{Cl}(K)$.
- representatives $\{\varepsilon_1, \ldots, \varepsilon_d\}$ for the cosets U^+/U_1.
- representatives $\{u_1, \ldots, u_e\}$ for the cosets $\mathcal{O}_K^*/U^+$.

Step 2: For every ideal class represented by $\mathfrak{b}$ such that $\delta_{K/\mathbb{Q}}\mathfrak{b}\overline{\mathfrak{b}} = (b)$, and for every u_j check:

- whether $u_j b$ is totally imaginary and $\mathrm{Im}(\sigma(u_j b)) < 0$ for all $\sigma \in \Phi$.
- let $\xi = (u_j b)^{-1}$. List $\{(\mathbb{C}^3/\Phi(\mathfrak{b}), E_{\xi\varepsilon_i}) \colon i = 1, \ldots, d\}$.

Algorithm

For every isomorphism class represented by $(\mathbb{C}^3/\Phi(\mathfrak{b}), E_\xi)$, we comupte a Frobenius basis $\mathfrak{b} = \langle \beta_1, \ldots, \beta_6 \rangle$:

$$(E_\xi(\Phi(\beta_i), \Phi(\beta_j)))_{1\le i,j\le 6} = \left[\begin{array}{c|c} O_3 & \mathrm{Id} \\ \hline -\mathrm{Id} & O_3 \end{array}\right]$$

Finally, arrange by columns

$$\mathcal{A}_1 = (\Phi(\beta_1), \Phi(\beta_2), \Phi(\beta_3)) \text{ and } \mathcal{A}_2 = (\Phi(\beta_4), \Phi(\beta_5), \Phi(\beta_6))$$

and we get the period matrix

$$\mathcal{A}_2^{-1}\mathcal{A}_1 \in \mathbb{H}_3 = \left\{\Omega \in \mathrm{GL}_3(\mathbb{C})\colon \Omega = \Omega^t\,, \mathrm{Im}(\Omega) \text{ is positive definite}\right\}$$

in the Siegel upper half space.

Torelli's theorem and Picard curves

Given an abelian variety A; does there exist an algebraic curve C such that there is an isogeny between A and the Jacobian of C?

- for $\dim(A) = 1$: this is clear;
- for $\dim(A) = 2$: it has been proved;
- for $\dim(A) = 3$: Principally polarized abelian varieties of dimension two or three are Jacobian varieties.

Therefore,
K Picard CM-field $\rightsquigarrow \Omega \in \mathbb{H}_3$ abelian variety $\rightsquigarrow C$ Picard curve

Theta functions

The Riemann theta function is the function

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

for $(z,\Omega) \in \mathbb{C}^g \times \mathbb{H}_g$. Quasi-periodicity: for a, b in $\mathbb{Z}^g$ one has

$$\theta(z + a + \Omega b) = \exp(-\pi i(2b^t z + b^t \Omega b))\theta(z,\omega)\,.$$

Let δ, $\epsilon \in \mathbb{Q}^g$. The theta function with characteristic (δ,ϵ) is

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

The lambda modular function

$\Omega = (\tau) \in \mathbb{H}$ $\quad q = \exp(\pi i \tau)$

$A = \mathbb{C}/\langle 1, \tau \rangle$

The function

$$\lambda(\tau) = \left(\frac{\sqrt{2}\eta(\frac{\tau}{2})\eta^2(2\tau)}{\eta^3(\tau)} \right)^8 = \frac{\theta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right]^4(0,\tau)}{\theta\left[\begin{smallmatrix}0\\1/2\end{smallmatrix}\right]^4(0,\tau)}$$

$$\lambda(\tau) = 16q - 128q^2 + 704q^3 - 3072q^4 + 11488q^5 - 38400q^6 + \dots$$

is a Hauptmodul for the modular curve $X(2)$.

Legendre's model:

$$y^2 = x(x-1)(x-\lambda)$$

$$j(\tau) = \frac{256(1-\lambda+\lambda^2)^3}{\lambda^2(1-\lambda)^2}$$

Picard curves of CM-type

$\Omega \in \mathbb{H}_3$
$A = \mathbb{C}^3 / \langle 1_3, \Omega \rangle$

$$C\colon y^3 = x(x-1)(x-\lambda)(x-\mu)$$

$$D_i = \begin{bmatrix} a \\ b \end{bmatrix} \in (\frac{1}{3}\mathbb{Z}/\mathbb{Z})^6 \text{ with } \{a + b\,\Omega\}_{i=1,27} = J(C)[1-\zeta_3] \subseteq J(C)[3]\,.$$

$$\lambda = \left(\frac{\theta[D_2 + 2D_3 - D_1 - \Delta]\,(0,\Omega)}{\theta[2D_2 + D_3 - D_1 - \Delta]\,(0,\Omega)} \right)^3 ; \quad \mu = \left(\frac{\theta[D_2 + 2D_4 - D_1 - \Delta]\,(0,\Omega)}{\theta[2D_2 + D_3 - D_1 - \Delta]\,(0,\Omega)} \right)^3$$

where $D_1 + D_2 + D_3 + D_4 = 0$ but each three are linearly independent, and Δ is the Riemann constant.

Picard curves of CM-type

Shimura: If $J(C)$ is defined over $\mathbb{Q}$ then $K/\mathbb{Q}$ is normal.

From a Picard CM-field K we obtain:

$$y^3 = x(x-1)(x-\lambda)(x-\mu) \text{ with } \lambda, \mu \in \overline{\mathbb{Q}}$$

Then invariant theory gives us:

$$y^3 = x^4 + g_2 x^2 + g_3 x + g_4 \text{ with } g_i \in \overline{\mathbb{Q}}$$

$$j_1 = \frac{g_3^2}{g_2^3}\,, \qquad j_2 = \frac{g_4}{g_2^2}$$

$$C\colon\, y^3 = x^4 + j_1 x^2 + j_1^2 x + j_1^2 j_2\,.$$

Sage implementation. Example

$h = 1$

K_0	Picard curve
$y^3 - y^2 - 2y + 1$	$y^3 = x^4 - 7^2 \cdot 2x^2 + 7^2 \cdot 2^3 x - 7^3 2$
$y^3 - y^2 - 4y - 1$	$y^3 = x^4 - 13 \cdot 2 \cdot 7^2 x^2 + 2^3 \cdot 13 \cdot 5 \cdot 47x - 5^2 \cdot 31 \cdot 13^2$

$h = 3$

$$y^3 = x(x-1)(x-\lambda)(x-\mu)$$

K_0	λ	μ
$x^3 - 21x - 28$	$-8.19 \cdot 10^{-22} + 1.49 \cdot 10^{-21} i$	$-0.0148 + 0.00057i$

Sage implementation. Example

$h = 1$

K_0	j_1	j_2
$y^3 - y^2 - 2y + 1$	$-2^3/7^2$	$-1/7 \cdot 2^2$
$y^3 - y^2 - 4y - 1$	$-2^3 47^2 5^2/7^6 13$	$-31 \cdot 5^2/2^2 7^4$

$h = 3$

K_0	j_1	j_2
$x^3 - 21x - 28$	$-0.29595 - 0.0000264i$	$-0.083206 - 9.71 \cdot 10^{-6} i$

Arithmetic on Picard curves of CM-type

Anna Somoza
Universitat Politècnica de Catalunya

25 January 2015