An algorithm for computing Hilbert modular varieties

Chloe Martindale
(supervised by Marco Streng)

September 30, 2014

Abstract

We describe an algorithm for computing an analogue of the modular polynomial for elliptic curves, for principally polarised abelian varieties with real multiplication. Given a principally polarised abelian variety with real multiplication by $\mathcal{O}_{K_0}$, where $\mathcal{O}_{K_0}$ is the maximal order in a totally real number field K_0, for any totally positive prime μ in $\mathcal{O}_{K_0}$ one can find a "μ-isogenous" principally polarised abelian variety with real multiplication by $\mathcal{O}_{K_0}$. We describe an algorithm to compute a birational model for an algebraic variety which parametrises μ-isogeny classes of principally polarised abelian varieties with real multiplication by $\mathcal{O}_{K_0}$.

Contents

1 Motivation: from elliptic curves to abelian varieties

We first present a brief background on the theory of modular polynomials for elliptic curves before explaining our generalisation to higher genus. Let

$$E_\tau \cong \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$$

be an elliptic curve defined over $\mathbb{C}$, where $\tau \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$, with j-invariant $j(\tau)$.

Recall. The j-invariant of an elliptic curve is a modular function for $\mathrm{SL}_2(\mathbb{Z})$ which generates the function field of $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$. A modular function for $\mathrm{SL}_2(\mathbb{Z})$ is a modular form for $\mathrm{SL}_2(\mathbb{Z})$ of weight 0 which is only meromorphic at infinity, i.e. a function $j : \mathbb{H} \to \mathbb{C}$ which is holomorphic everywhere (but only meromorphic at infinity) such that for all $M \in \mathrm{SL}_2(\mathbb{Z})$, $j(M\tau) = j(\tau)$. Here $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathbb{H}$ on the left by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau \mapsto \frac{a\tau + b}{c\tau + d}.$$

Definition 1.1. An *isogeny* is a surjective morphism with finite kernel. An N-isogeny of elliptic curves for some $N \in \mathbb{Z}$ is an isogeny with kernel of size N.

Definition 1.2. The *modular polynomial of level* N, $\Phi_N(X, Y) \in \mathbb{Q}[X, Y]$, is a polynomial such that $\Phi_N(j(\tau), Y) = 0$ if and only if there exists an N-isogeny $\phi : E_\tau \to E_{\tau'}$ such that $Y = j(\tau')$. (Then in particular $\Phi_N(j(\tau), j(N\tau)) = 0$).

Some small examples of modular polynomials were given last week in Yuri Bilou's talk.
Knowing this polynomial means that, given an elliptic curve, one can easily find all those N-isogenous to it (or at least their j-invariants). One application for this is the computation of isogeny graphs. Our motivation for computing an equivalent of the modular polynomial in higher genus, especially genus 2, is to be able to easily compute isogeny graphs in genus 2.

2 Generalising the modular polynomial

The goal of our paper is to compute an equivalent of the modular polynomial for elliptic curves for principally polarised abelian varieties with real multiplication. We will first recall the essential background on abelian varieties.

Abelian varieties are described in the following way for example in [Str], Chapter 5.1. Let A be g-dimensional abelian variety over $\mathbb{C}$. Then A is a Lie group, so there exists a natural complex analytic group homomorphism $\exp : T_0A \to A$ which lies in the following exact sequence:

$$0 \to \Lambda \to T_0A \to A \to 0.$$

Further, Λ is a lattice of rank $2g$. From the exact sequence above, and from the isomorphism $T_0A \cong \mathbb{C}^g$, we see that $A \cong \mathbb{C}^g/\Lambda$ (*).

From this point on, K_0 will denote a totally real number field with $[K_0 : \mathbb{Q}] = g$.

Definition 2.1. An abelian variety A has *real multiplication by* $\mathcal{O}_{K_0}$ if there exists an embedding

$$\iota : \mathcal{O}_{K_0} \hookrightarrow \mathrm{End}(A).$$

If we consider an abelian variety A with real multiplication by $\mathcal{O}_{K_0}$ with $[K_0 : \mathbb{Q}] = g$, then it is often useful to write $A \cong (K_0 \otimes \mathbb{C})/\Lambda$ in place of (*).

Definition 2.2. An abelian variety A is *principally polarised* if there exists an isomorphism

$$\xi : A \longrightarrow A^\vee$$

from A to its dual. We will not go into defining the technicalities of the dual abelian variety here, but this can be found in for example [Sij]. (Intuitively, a polarisation on an abelian variety over $\mathbb{C}$ given by $\mathbb{C}^g/\Lambda$ is a geometric structure related to a certain type of alternating bilinear form on Λ).

Notation 2.3. We define the following for ease of notation:

$$K_0 \otimes \mathbb{H} := \{\tau \in K_0 \otimes \mathbb{C} : \mathrm{Im}(\tau) > 0\}.$$

Note that $K_0 \otimes \mathbb{H} \cong \mathbb{H}^g$.

It can be seen in for example [Gor] that if the abelian variety with real multiplication $A \cong (K_0 \otimes \mathbb{C})/\Lambda$ is also principally polarised, then the lattice Λ can be written in the form $\Lambda = \mathcal{O}_{K_0} + \tau\mathcal{O}_{K_0}$ for some $\tau \in \mathrm{SL}_2(\mathcal{O}_{K_0})\backslash(K_0 \otimes \mathbb{H})$. Hence define

$$A_\tau := (K_0 \otimes \mathbb{C})/(\mathcal{O}_{K_0} + \tau\mathcal{O}_{K_0}).$$

Now let

$$f : A \longrightarrow A'$$

be an isogeny of abelian varieties, and

$$\phi : \mathrm{End}(A) \otimes \mathbb{Q} \longrightarrow \mathrm{End}(A') \otimes \mathbb{Q}$$

be the induced map on endomorphism rings. This map is induced from the dual of the isogeny f.

Definition 2.4. We say that f *preserves real multiplication* if the following diagram commutes:

$$\begin{array}{ccc} \mathrm{End}(A) \otimes \mathbb{Q} & \xrightarrow{\phi} & \mathrm{End}(A') \otimes \mathbb{Q} \\ {\scriptstyle \iota}\uparrow & \nearrow_{\iota'} & \\ K_0. & & \end{array}$$

Definition 2.5. For μ a totally positive prime in $\mathcal{O}_{K_0}$, we say that f is an *μ-isogeny* if it preserves real multiplication and if the multiplication map $\mu : A \to A$ makes the following diagram commute:

$$\begin{array}{ccccc} A & \xleftarrow{\mu} & A & \xrightarrow{f} & A' \\ & {\scriptstyle \phi_A}\searrow & & & \downarrow{\scriptstyle \phi_{A'}} \\ & & A^\vee & \xleftarrow{f^\vee} & A'^\vee. \end{array}$$

Then, in analogue with the case of elliptic curves, $|\ker(f)| = \mathrm{N}_{K_0/\mathbb{Q}}(\mu)$.

Recall. A Hilbert modular function for $\mathrm{SL}_2(\mathcal{O}_{K_0})$ is a Hilbert modular form for $\mathrm{SL}_2(\mathcal{O}_{K_0})$ of weight 0, that is, it is a holomorphic function $f : K_0 \otimes \mathbb{H} \to \mathbb{C}$ such that for all $M \in \mathrm{SL}_2(\mathcal{O}_{K_0})$ and for all $\tau \in K_0 \otimes \mathbb{H}$, $f(M\tau) = f(\tau)$. Here $\mathrm{SL}_2(\mathcal{O}_{K_0})$ acts on $K_0 \otimes \mathbb{H}$ on the left by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau \mapsto \left(\frac{\sigma_1(a)\tau_1 + \sigma_1(b)}{\sigma_1(c)\tau_1 + \sigma_1(d)}, ..., \frac{\sigma_g(a)\tau_g + \sigma_g(b)}{\sigma_g(c)\tau_g + \sigma_g(d)} \right),$$

where $\tau = (\tau_1, ..., \tau_g)$ and $(\sigma_1, ..., \sigma_g)$ are the g embeddings of K_0 into $\mathbb{C}$.

In analogue with the j-invariant of elliptic curves, given s modular functions for $\mathrm{SL}_2(\mathcal{O}_{K_0})$, $J_1(\tau), ..., J_s(\tau)$, which generate the function field of $\mathrm{SL}_2(\mathcal{O}_{K_0})\backslash(\mathbb{H} \otimes K_0)$, for most τ these s functions uniquely determine the abelian variety A_τ. Hence we will use A_τ and its $(J_1(\tau), ..., J_s(\tau))$-invariant interchangeably.

We have now given enough background to state the goal of the paper in a more precise form:

Goal. Given s modular functions for $\mathrm{SL}_2(\mathcal{O}_{K_0})$, $J_1, ..., J_s$, which generate the function field of $\mathrm{SL}_2(\mathcal{O}_{K_0})\backslash(\mathbb{H} \otimes K_0)$, we must find polynomials $F(Y, X_1), G_i(Y, X_1, X_i) \in \mathbb{Q}[X_1, ..., X_s][Y]$ for $i = 2, ..., s$ with G_i linear in X_i such that for most $\tau \in \mathrm{SL}_2(\mathcal{O}_{K_0})\backslash(\mathbb{H} \otimes K_0)$, we have

$$F(J(\tau), X_1) = 0 \quad \Leftrightarrow \quad \exists \mu - \text{isogeny } A_\tau \to A_{\tau'} \text{ s.t. } X_1 = J_1(\tau'), \qquad (1)$$

$$\text{and if so, then } \forall i = 2, ..., s,\ G_i(J(\tau), J_1(\tau'), J_i(\tau')) = 0,$$

where $J(\tau)$ is something coming from $(J_1(\tau), ..., J_s(\tau))$.

This would give a 'Hilbert modular variety' i.e. an analogue of the modular polynomial Φ_N in the following way. Set

$$I = (F(Y, X_1), G_2(Y, X_1, X_2), ..., G_s(Y, X_1, X_s)).$$

Then the affine variety

$$X^0(\mu, K_0) := \mathrm{Spec} \frac{\mathbb{Q}[X_1, ..., X_s][Y]}{I}$$

has rational points $(X_1, ..., X_s)$ given by the $(J_1, ..., J_s)$-invariants of abelian varieties in the same μ-isogeny class.

3 Computing the Hilbert modular variety

For practical purposes, we restrict to genus 2. Recent work of Costello, Deines-Schartz, Lauter, Yang ([C-DS-L-Y]) shows that in this case we always need only 2 modular functions to generate the function field of $\mathrm{SL}_2(\mathcal{O}_{K_0})\backslash(K_0 \otimes \mathbb{H})$, so that $A_\tau = (J_1(\tau), J_2(\tau))$. In particular, the ideal defining the Hilbert modular

variety has 2 defining polynomials, F and G_2. For now, we assume that the Fourier expansions of J_1 and J_2 are known. We first want to write down an F which satisfies (1). A μ-isogeny is given by

$$\begin{array}{cccc} f: & (K_0 \otimes \mathbb{C})/(\mathcal{O}_{K_0} + \tau\mathcal{O}_{K_0}) & \longrightarrow & (K_0 \otimes \mathbb{C})/(\mathcal{O}_{K_0} + \mu\tau\mathcal{O}_{K_0}) \\ & z & \mapsto & \mu z, \end{array}$$

so the roots of $F(J(\tau), X_1)$ are given by

$$J_1(\mu M\tau), \quad \text{for each } M \in \mathrm{SL}_2(\mathcal{O}_{K_0}).$$

Now if $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then

$$J_1(\mu M\tau) = J_1\left(\begin{pmatrix} a & \mu b \\ \mu^{-1}c & d \end{pmatrix}(\mu\tau)\right),$$

which by modularity is equal to $J_1(\mu\tau)$ if and only if $c \in \mu\mathcal{O}_{K_0}$. So define the modular group of level μ to be

$$\Gamma^0(\mu) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathcal{O}_{K_0}) : c \in \mu\mathcal{O}_{K_0} \right\},$$

and further define

$$\mathcal{C} = \Gamma^0(\mu)\backslash \mathrm{SL}_2(\mathcal{O}_{K_0}),$$

giving

$$F(J(\tau), X_1) = \prod_{M \in \mathcal{C}} \left(X_1 - J_1(\mu M\tau)\right).$$

Define $F|_\tau(X_1) := F(J(\tau), X_1)$. We are left with the task of defining a G_2 that satisfies (1), so we should have that $G_2(J(\tau), J_1(\tau'), X_2) = 0$ implies that $X_2 = J_2(\tau')$. We first consider a polynomial $G(Y, X_1) \in \mathbb{Q}[X_1][Y]$ such that

$$G(J(\tau), X_1) := \sum_{M \in \mathcal{C}} J_2(\mu M\tau) \prod_{\substack{M' \in \mathcal{C} \\ M' \neq M}} \left(\frac{X_1 - J_1(\mu M'\tau)}{J_1(\mu M\tau) - J_1(\mu M'\tau)} \right),$$

then for all $M \in \mathcal{C}$, $G(J(\tau), J_1(\mu M\tau)) = J_2(\mu M\tau)$. However, we want to clear denominators, so we consider $\widetilde{G}(Y, X_1) \in \mathbb{Q}[X_1][Y]$ such that

$$\widetilde{G}|_\tau(X_1) := \widetilde{G}(J(\tau), X_1) = \sum_{M \in \mathcal{C}} J_2(\mu M\tau) \prod_{\substack{M' \in \mathcal{C} \\ M' \neq M}} \left(X_1 - J_1(\mu M'\tau)\right)$$

and note that

$$\widetilde{G}(J(\tau), J_1(\mu M\tau)) = J_2(\mu M\tau) \frac{dF|_\tau}{dX_1}(J_1(\mu M\tau)).$$

So choose $G_2 \in \mathbb{Q}[X_1, X_2][Y]$ in such a way that

$$G_2(J(\tau), X_1, X_2) = \widetilde{G}|_\tau(X_1) - X_2 \frac{dF|_\tau}{dX_1}(X_1).$$

Now both $F|_\tau$ and $\widetilde{G}|_\tau$ can be written as

$$F|_\tau = \sum_{j=0}^{m} c_j X_1^j \quad \widetilde{G}|_\tau = \sum_{j=0}^{n} d_j X_1^j$$

for $m = |\mathcal{C}|$, $n = |\mathcal{C}| - 1$ and coefficients c_j, d_j given by modular functions for $\mathrm{SL}_2(\mathcal{O}_{K_0})$. But J_1 and J_2 generate the function field of $\mathrm{SL}_2(\mathcal{O}_{K_0})\backslash(K_0 \otimes \mathbb{H})$, so for each c_j, d_j there exist rational numbers $a_{j,k,l}, b_{j,k,l}$ such that

$$c_j = \sum_{k,l \in \mathbb{Z}_{\geq 0}} a_{j,k,l} J_1^k J_2^l \quad \text{and} \quad d_j = \sum_{k,l \in \mathbb{Z}_{\geq 0}} b_{j,k,l} J_1^k J_2^l.$$

If Fourier expansions are known for J_1 and J_2, then using the above, Fourier expansions can be calculated for $F|_\tau$, $\widetilde{G}|_\tau$. One can then calculate Fourier expansions for $J_1^k J_2^l$ for each k and l, and then compare the coefficients with the coefficients of the Fourier expansions for $F|_\tau$, $\widetilde{G}|_\tau$ to determine the rational numbers $a_{j,k,l}$ and $b_{j,k,l}$. Furthermore, since the space of modular functions is finite dimensional, only finitely many of these rational numbers need to be computed to completely determine each c_j and d_j.

4 Future work

The code to compute the defining polynomials F, G_2 is currently implemented in one form, but we are still implementing some speed ups. We are also working on some time estimates with these speed ups. Enea Milio will talk next week about another method to compute analogues of modular polynomials in genus 2. We are now working on the next step together with Damien Robert.

References

[C-DS-L-Y] C. Costello, A. Deines-Schartz, K. Lauter, T. Yang, *Constructing Abelian Surfaces for Cryptography via Rosenhain Invariants*, https://eprint.iacr.org/2014/424.pdf, (2014).

[Gor] E.Z. Goren, *Lectures on Hilbert Modular Varieties and Modular Forms*, CRM Monograph Series (2002) Volume 14.

[Gun] K.-B. Gundlach, *Die Bestimmung der Funktionen zur Hilbertschen Modulgruppe des Zahlkrpers* $\mathbb{Q}(\sqrt{5})$, Math. Ann. 152 (1963) 226-256.

[Igu] J. Igusa. *On Siegel modular forms of genus two*, Amer. J. Math. 84 (1962), 175200. MR0141643 (25:5040)

[L-Y] K. Lauter, T. Yang, *Computing genus 2 curves from invariants on the Hilbert moduli space*, Journal of Number Theory 131 (2011) 936-958.

[Nag] S. Nagaoka, *On the ring of Hilbert modular forms over* $\mathbb{Z}$, J. Math. Soc. Japan 35 (1983) 589-608.

[Res] H.L. Resnikoff, *On the Graded Ring of Hilbert modular forms associated with* $\mathbb{Q}(\sqrt{5})$, Math. Ann. 208 (1974) 161-170.

[Sij] J. Sijsling, *What is... a polarization?*, http://pub.math.leidenuniv.nl/strengtc/cm/polariz.pdf, Universiteit Leiden (2009).

[Str] M. Streng, *Complex multiplication of abelian surfaces*, PhD thesis, Universiteit Leiden (2010).

[vdG] G. van der Geer, *Hilbert Modular Surfaces*, Springer-Verlang (1987).