Universiteit Leiden

Algebra, Geometry and Number Theory — ALGANT Erasmus Mundus Master

université de BORDEAUX

# Modular Polynomials for Hilbert Modular Forms


Chloe Martindale

Supervisor: Marco Streng


## Motivation

**Definition 1** *The* modular polynomial of prime level $p$ *is a polynomial*

$$\Phi_p(X,Y)\in\mathbb{Z}[X,Y]$$

*which, for all* $\tau\in\mathbb{H}$, *satisfies*

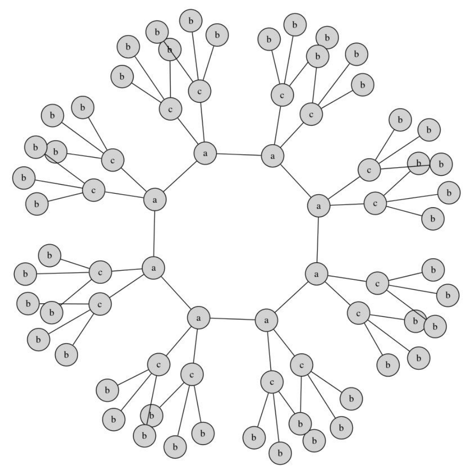
$$\Phi_p(j(\tau),j(p\tau))=0,$$

*where* $j(\tau)$ *is the* $j$*-invariant for elliptic curves.*

- Given the **$j$-invariant $j$ of en elliptic curve over $k$**, we can find the $j$-invariants of all those elliptic curves which are $p$-isogenous to it by computing the roots of $\Phi_p(j,Y)\in k(Y)$.
- Analogues have been computed so that given an **Igusa invariant of a genus 2 curve**, we can find the Igusa invariants of all those genus 2 curves which are $p$-isogenous to it, but these analogues have **huge coefficients** and are **difficult to handle** in practise.
- In our work, we add the constraint of **real multiplication**, and compute modular polynomials for genus 2 which are much **smaller and easier to handle**. We also give a theoretical algorithm to compute modular polynomials for **abelian varieties of any dimension**.

## An application - isogeny graphs

- Using the structure of **isogeny graphs** together with our modular polynomials we have a fast method for **computing endomorphism rings**.
- The isogeny graphs that we have for abelian varieties without taking into account the real multiplication do not in general have a nice structure.
- **Taking into account real multiplication gives a 'nice' structure** in many (maybe all) cases, here is an example computed by Sorina Ionica using AVIsogenies:



## Example in genus 2

**INPUT:**

- Totally real number field $F=\mathbb{Q}(\sqrt{5})$.
- Functions in $Q(\mathcal{M}_F)$ satisfying the conditions of Definition 3 given by

$$J_1(\tau)=C_1\frac{E_6(\tau)-E_2(\tau)^3}{E_2(\tau)^3},\ J_2(\tau)=\frac{C_2E_{10}(\tau)-C_3E_2(\tau)^2E_6(\tau)+C_4E_2(\tau)^5}{E_2(\tau)^5},$$

  where $E_2(\tau)$, $E_6(\tau)$ and $E_{10}(\tau)$ are Eisenstein series for $\mathrm{SL}_2(\mathcal{O}_F)$ of weights 2, 6 and 10 respectively, and the $C_i$ are explicit rational numbers. (The functions $J_1$ and $J_2$ are called **Gundlach invariants**).
- The level, a totally positive prime element in $\mathcal{O}_F$, for example $\mu=5-2\sqrt{5}$ (which has norm 5).

**OUTPUT:**

The 4 polynomials described under 'The algorithm':

$$G_1\in\mathbb{Q}(X_1,X_2,Z_1),\quad G_2\in\mathbb{Q}(X_1,X_2,Z_2),$$
$$H_{1,2}\in\mathbb{Q}(X_1,X_2,Z_1,Z_2),\quad H_{2,1}\in\mathbb{Q}(X_1,X_2,Z_1,Z_2).$$

- The largest coefficients are of the order $10^{30}$.
- The amount of bits required to write down the polynomials is estimated to be 15 (in comparison with $\sim 5^{12}$ for the Siegel modular polynomials).

## Setup

- Let $F$ be a totally real number field of degree $g$ over $\mathbb{Q}$.
- Let $\mathcal{O}_F$ be the maximal order of $F$, and let $\mathcal{O}_F^\vee$ be its trace dual.
- Let $\mathbb{H}^g$ denote $g$ copies of the complex upper half plane.
- Let $\mathrm{SL}(\mathcal{O}_F\oplus\mathcal{O}_F^\vee)$ be the matrix group given by

$$\left\{\begin{pmatrix} a & b\\ c & d\end{pmatrix}\in\mathrm{SL}_2(F): a,d\in\mathcal{O}_F, b\in\mathcal{O}_F^\vee, c\in(\mathcal{O}_F^\vee)^{-1}\right\}.$$

**Definition 2** *Let $\mathcal{A}$ be an abelian variety of genus $g$, with a principal polarization given by $\xi:\mathcal{A}\xrightarrow{\sim}\mathcal{A}^\vee$ and real multiplication via the embedding $\iota:\mathcal{O}_F\hookrightarrow\mathrm{End}(\mathcal{A})$ such that the image of $\mathcal{O}_F$ in $\mathrm{End}(\mathcal{A})$ is stable under the Rosati involution. Then we say that $(\mathcal{A},\xi,\iota)$ is a* **principally polarized abelian variety of genus $g$ with real multiplication by $\mathcal{O}_F$**.

We can define an action of $\mathrm{SL}(\mathcal{O}_F\oplus\mathcal{O}_F^\vee)$ on $\mathbb{H}^g$, under which the moduli space of prinicipally polarized complex abelian varieties of genus $g$ with real multiplication by $\mathcal{O}_F$ is given by

$$\mathrm{SL}(\mathcal{O}_F\oplus\mathcal{O}_F^\vee)\backslash\mathbb{H}^g.$$

- Denote by $\mathcal{M}_F$ the $\mathbb{C}$-algebra of Hilbert modular forms for $\mathrm{SL}(\mathcal{O}_F\oplus\mathcal{O}_F^\vee)$.
- Denote by $Q(\mathcal{M}_F)$ the $\mathbb{C}$-algebra of quotients of elements of $\mathcal{M}_F$ of equal weight (inside the fraction field).

**Definition 3** *Let $(\mathcal{A},\xi,\iota)$ be a principally polarized complex abelian variety of genus $g$ with real multiplication by $\mathcal{O}_F$ which corresponds to $\tau\in\mathrm{SL}(\mathcal{O}_F\oplus\mathcal{O}_F^\vee)\backslash\mathbb{H}^g$ under the moduli correspondence. Fix an $r$-tuple $(J_1,\dots,J_r)\in Q(\mathcal{M}_F)^{\times r}$ such that, for every $\tau\in\mathrm{SL}(\mathcal{O}_F\oplus\mathcal{O}_F^\vee)\backslash\mathbb{H}^g$, the $r$-tuple $(J_1(\tau),\dots,J_r(\tau))\in(\mathbb{C}\cup\{\infty\})^{\times r}$ determines $(\mathcal{A},\xi,\iota)$ up to isomorphism. We will call*

$$(J_1(\tau),\dots,J_r(\tau))$$

*the* **isomorphism invariant** *of $(\mathcal{A},\xi,\iota)$. This is our analogue of the $j$-invariant for elliptic curves.*

## The algorithm

**INPUT:**

- An integer $g\geq 2$, and a totally real number field $F$ of degree $g$ over $\mathbb{Q}$.
- An appropriate choice of functions $\{J_1,\dots,J_r\}$ for $Q(\mathcal{M}_F)$, and $q$-expansions for each numerator and denominator.
- A totally positive prime element $\mu$ of $\mathcal{O}_F$.

**OUTPUT:**

A set of $r^2$ polynomials

$$\left\{\begin{array}{c} G_i(X_1,\dots,X_r,Z_i)\in\mathbb{Q}[X_1,\dots,X_r,Z_i]\\ H_{i,j}(X_1,\dots,X_r,Z_i,Z_j)\in\mathbb{Q}[X_1,\dots,X_r,Z_i,Z_j]\end{array}\right\}_{\substack{i=1,\dots,r\\ j=1,\dots,r,\, j\neq i}},$$

where the $H_{i,j}$ are **linear in $Z_1,\dots,Z_{i-1},Z_{i+1},\dots,Z_r$**.

- **This looks like the modular polynomial for elliptic curves:** after carefully defining a '$\mu$-isogeny' in an analogous way to a $p$-isogeny for elliptic curves, but taking into account the real multiplication and the polarizations, we can deduce the following:

For $(\mathcal{A},\xi,\iota)$ a principally polarized abelian variety with isomorphism invariant $(J_1(\tau),\dots,J_r(\tau))$, define

$$\mathcal{S}:=\left\{\begin{array}{c} G_i(J_1(\tau),\dots,J_r(\tau),Z_i)\in\mathbb{Q}[X_1,\dots,X_r,Z_i]\\ H_{i,j}(J_1(\tau),\dots,J_r(\tau),Z_i,Z_j)\in\mathbb{Q}[X_1,\dots,X_r,Z_i,Z_j]\end{array}\right\}_{\substack{i=1,\dots,r\\ j=1,\dots,r,\, j\neq i.}}$$

Then generically

$$(\mathcal{A}',\xi',\iota')\text{ is }\mu\text{-isogenous to }(\mathcal{A},\xi,\iota)$$
$$\Leftrightarrow$$
$$\text{its isomorphism invariant }(J_1(\tau'),\dots,J_r(\tau'))\text{ is a common zero of the polynomials in }\mathcal{S}.$$

- The zeroes of the polynomials in $\mathcal{S}$ are **easy to compute**: $G_i(J_1(\tau),\dots,J_r(\tau),Z_i)$ is univariate and $H_{i,j}(J_1(\tau),\dots,J_r(\tau),Z_i,Z_j)$ is linear in $Z_j$!


### References

- G. Bisson, R. Cosset, D. Robert et al. *AVIsogenies (Abelian Varieties and Isogenies)*, MAGMA package.
- E. Z. Goren, *Lectures on Hilbert Modular Varieties and Modular Forms*, CRM Monograph Series (2002) Volume 14.
- K.-B. Gundlach, *Die Bestimmung der Funktionen zur Hilbertschen Modulgruppe des Zahlkrpers* $\mathbb{Q}(\sqrt{5})$, Math. Ann. 152 (1963) 226-256.
- J. Igusa, *On Siegel modular forms of genus two*, Amer. J. Math. 84 (1962), 175-200.
- S. Ionica, E. Thomé, *Isogeny graphs with maximal real multiplication*, Cryptology ePrint Archive, Report 2014/230 (2014).
- K. Lauter, T. Yang, *Computing genus 2 curves from invariants on the Hilbert moduli space*, Journal of Number Theory 131 (2011) 936-958.
- S. Nagaoka, *On the ring of Hilbert modular forms over* $\mathbb{Z}$, J. Math. Soc. Japan 35 (1983) 589-608.
- H.L. Resnikoff, *On the Graded Ring of Hilbert modular forms associated with* $\mathbb{Q}(\sqrt{5})$, Math. Ann. 208 (1974) 161-170.
- M. Streng, *Complex Multiplication of Abelian Surfaces* PhD thesis, Universiteit Leiden (2010).
- G. van der Geer, *Hilbert Modular Surfaces*, Springer-Verlag (1987).



2015 Universiteit Leiden, The Netherlands, E-mail: chloe.martindale@math.leidenuniv.nl