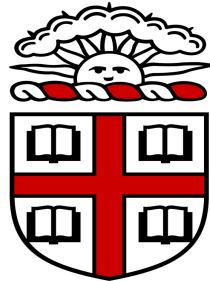


Abelian surfaces with extra endomorphisms

Reinier Bröker



BROWN

joint work with Kristin Lauter (Microsoft Research)
and Marco Streng (University of Leiden)

A tale of two polynomials

Let $j : \mathbf{H} \rightarrow \mathbf{C}$ be the complex analytic function with Fourier expansion $j(z) = 1/q + 744 + 196884q + \dots$ in $q = \exp(2\pi iz)$.

Definition. For $m > 1$, the modular polynomial Φ_m is the minimal polynomial of $j(mz)$ over $\mathbf{C}(j)$.

The modular polynomial parametrizes elliptic curves together with a cyclic m -isogeny.

Properties.

- $\Phi_m(X) \in \mathbf{Z}[X, j]$;
- $\Phi_m(X, j) = \Phi_m(j, X)$;
- m prime $\implies \deg_X(\Phi_m) = m + 1$.

An example

$$\begin{aligned}\Phi_5 = & X^6 - X^5Y^5 + 3720X^5Y^4 - 4550940X^5Y^3 + 2028551200X^5Y^2 \\ & - 246683410950X^5Y + 1963211489280X^5 + 3720X^4Y^5 \\ & + 1665999364600X^4Y^4 + 107878928185336800X^4Y^3 \\ & + 383083609779811215375X^4Y^2 + 1285179890682881638400X^4Y \\ & + 1284733132841424456253440X^4 - 4550940X^3Y^5 \\ & + 107878928185336800X^3Y^4 - 441206965512914835246100X^3Y^3 \\ & + 26898488858380731577417728000X^3Y^2 \\ & - 192457934618928299655108231168000X^3Y \\ & + 280244777828439527804321565297868800X^3 \\ & \quad \vdots \\ & + 53274330803424425450420160273356509151232000X + Y^6 \\ & + 1963211489280Y^5 + 1284733132841424456253440Y^4 \\ & + 280244777828439527804321565297868800Y^3 \\ & + 6692500042627997708487149415015068467200Y^2 \\ & + 53274330803424425450420160273356509151232000Y \\ & + 141359947154721358697753474691071362751004672000\end{aligned}$$

A tale of two polynomials

For an imaginary quadratic order \mathcal{O} , let $H_{\mathcal{O}}$ be the minimal polynomial of $j(\mathbf{C}/\mathcal{O})$ over \mathbf{Q} .

Properties.

- $H_{\mathcal{O}} \in \mathbf{Z}[X]$;
- $\deg(H_{\mathcal{O}}) = \#\text{Pic}(\mathcal{O}) \approx \sqrt{|\text{disc}(\mathcal{O})|}$.

Example.

- $H_{\mathbf{Z}[i]}(X) = X - 1728$;
- $H_{\mathbf{Z}[\sqrt{-5}]}(X) = X^2 - 1264000X - 681472000$.

A tale of two polynomials

Theorem. (Kronecker) *For every integer $m > 1$ we have*

$$\Phi_m(X, X) = \pm \prod_{\mathcal{O}} H_{\mathcal{O}}^{e(\mathcal{O})}(X).$$

The product ranges over all \mathcal{O} that contain a primitive element of norm m and

$$e(\mathcal{O}) = |\{\text{primitive } \alpha \in \mathcal{O} \text{ of norm } m\} / \mathcal{O}^*| \in \mathbf{Z}_{>0}.$$

Example.

$$\Phi_5(X, X) = H_{\mathbf{Z}[i]}^2 H_{\mathbf{Z}[2i]}^2 H_{\mathbf{Z}[(-1+\sqrt{-11})/2]}^2 H_{\mathbf{Z}[(-1+\sqrt{-19})/2]}^2 H_{\mathbf{Z}[\sqrt{-5}]}.$$

Today: 2-dimensional analogue

The modular polynomial for elliptic curves can be generalized to principally polarized abelian surfaces (p.p.a.s.).

Explicitly: let $j_i : \mathbf{H}_2 \rightarrow \mathbf{C}$ be the three ‘Igusa functions’. They satisfy:

- if $J(C_1) \cong J(C_2)$, then $j_i(C_1) = j_i(C_2)$;
- if $(j_1, j_2, j_3) \neq (*, *, 0)$, then there is a unique C with $j_i(C) = j_i$.

A generalization of Φ_p is the ideal W_p generated by the minimal polynomials of $j_i(p\tau)$ over $\mathbf{C}(j_1, j_2, j_3)$.

Generators of W_p are polynomials in $X_1, Y_1, Z_1, X_2, Y_2, Z_2$. Writing $X_i = Y_i$ gives an ideal V_p which is an analogue of $\Phi_p(X, X)$.

However: V_p has an ‘unnatural’ moduli interpretation. Reasons: \mathcal{A}_2 is not affine and j_3 can be zero.

Moduli interpretation

Let (A, L) and (A', L') be abelian surfaces with principal polarizations L, L' .

An isogeny $f : (A, L) \rightarrow (A', L')$ induces a polarization on A . Put $A = \mathbf{C}^2/\Lambda$, $A' = \mathbf{C}^2/\Lambda'$ and write $L' : \Lambda' \times \Lambda' \rightarrow \mathbf{Z}$. Then:

$$f^* L' : (u, v) \mapsto L'(f(u), f(v))$$

is a Riemann form on Λ .

Definition. A (p, p) -isogeny $f : (A, L) \rightarrow (A', L')$ is an isogeny $f : A \rightarrow A'$ of surfaces with $f^* L' = pL$.

The kernel $\text{Ker}(f) \subset A[p]$ is 2-dimensional as \mathbf{F}_p -vector space and isotropic with respect to the Weil pairing.

Our object of study

Definition. Let $\mathcal{M}_2^{(p,p)} \subset \mathcal{A}_2$ parametrize p.p.a.s. (A, L) admitting a (p, p) -isogeny $(A, L) \rightarrow (A, L)$.

If $(A, L) \in \mathcal{M}_2^{(p,p)}$ is not the product of elliptic curves with the product polarization, then its Igusa invariants are finite and are contained in V_p .

By looking at $\mathcal{M}_2^{(p,p)}$ we will also find *which* products of curves admit (p, p) -endomorphisms.

The ‘technicality $\mathcal{M}_2^{(p,p)} \leftrightarrow V_p$ ’ does not occur for genus 1 because the map

$$j : \mathcal{A}_1 \rightarrow \mathbf{C}$$

is bijective.

Dimensions

The subvariety $\mathcal{M}_2^{(p,p)} \subset \mathcal{A}_2$ has co-dimension 1 and is a finite union of

- surfaces
- curves
- points.

If $(A, L) \in \mathcal{M}_2^{(p,p)}$ is *simple*, then we can use

- surfaces \longleftrightarrow real multiplication
- curves \longleftrightarrow quaternion multiplication
- points \longleftrightarrow complex multiplication.

Our approach is different and handles the split case as well.

Finding points in $\mathcal{M}_2^{(p,p)}$

Fix a point $(A, L, x) \in \mathcal{M}_2^{(p,p)}$ with $x \in \text{End}(A)$ a (p, p) -isogeny.

Let $\bar{\cdot} : \text{End}(A) \rightarrow \text{End}(A)$ be the Rosati involution, so that

$$\bar{\alpha} = \varphi_L^{-1} \hat{\alpha} \varphi_L$$

with $\varphi_L : A \xrightarrow{\sim} \hat{A}$ the isomorphism induced by L .

Claim. *We have $\bar{x}x = p$.*

Proof. Write $A = \mathbf{C}^2/\Lambda$ and compute $L(u, \bar{x}xv) = L(xu, xv) \stackrel{!}{=} pL(u, v) = L(u, pv)$. □

The ring $\mathbf{Z}[x]$

Write $K = \mathbf{Q}(x) \subseteq \text{End}(A) \otimes_{\mathbf{Z}} \mathbf{Q}$ and $\mathcal{O} = \mathbf{Z}[x]$.

Two cases:

- (A) \mathcal{O} is a domain
- (B) \mathcal{O} is not a domain.

Until further notice: assume we are in case (A).

The ring K is a *number field* and $\deg(K/\mathbf{Q}) \mid 4$.

We have $\bar{\cdot} \in \text{Aut}(K)$ and the Rosati involution equals complex conjugation for every $K \hookrightarrow \mathbf{C}$.

\mathcal{O} is a domain

Three subcases:

- $K = \mathbf{Q}(\sqrt{p})$. Now: $x\bar{x} = p$ and this happens if there is a real embedding.
- K is imaginary quadratic. Now: $x + \bar{x} \in \mathbf{Q}$ has absolute value $< 2\sqrt{p}$.
- K is a degree 4 CM-field. Now: $x + \bar{x} \in K^+ \hookrightarrow \mathbf{R}$ has absolute value $< 2\sqrt{p}$.

We get a *finite* list of possibilities for K .

Next step: go from \mathcal{O} to $(A = \mathbf{C}^2/\Lambda, L)$.

Making the polarization easier

The tensor product $\Lambda \otimes_{\mathbf{Z}} \mathbf{Q} \cong K^s$ is a K -vector space of dimension $s = 4/\deg(K/\mathbf{Q})$ over K .

The polarization L is a \mathbf{Q} -linear form $K^s \times K^s \rightarrow \mathbf{Q}$.

Lemma. *There is a unique matrix $T \in \text{Mat}_s(K)$ such that:*

$$\forall u, v \in K^2 : \quad L(u, v) = \text{Tr}(u^T T \bar{v}).$$

We also have $\overline{T}^T = -T$.

Proof. Use all properties of $L : \mathbf{C}^2 \times \mathbf{C}^2 \rightarrow \mathbf{R}$. □

Finding pairs (Λ, T)

New goal: for every \mathcal{O} , list all pairs (Λ, T) satisfying:

- $\Lambda \subset K^s$ has rank 4 over \mathbf{Z}
- $T \in \text{Mat}_2(K)$ satisfies $\overline{T}^T = -T$
- $\text{Tr}(u^T T \overline{v}) \in \mathbf{Z}$ for $u, v \in \Lambda$ and $\det(T) = 1$ on Λ .

The answer depends on the field $K = \mathbf{Q}(x)$.

- If K is real quadratic and if \mathcal{O} is maximal, then

$$(\Lambda, T) = (\mathcal{O} \times \mathcal{O}, \frac{1}{2x - \text{Tr}_{K/\mathbf{Q}}(x)} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}),$$

up to isomorphism.

Finding pairs (Λ, S)

- If K is imaginary quadratic and if \mathcal{O} is maximal, you can list the *Hermitian* matrices $S = (x - \bar{x})T$. (*Hayashida/Nishi*)
 - ◊ $K = \mathbf{Q}(\sqrt{-2})$ gives

$$S = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & \sqrt{-2} + 1 \\ -2\sqrt{-2} + 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

- If K is a degree 4 CM-field, then:
 - ◊ Λ is a fractional \mathcal{O} -ideal
 - ◊ $T \in K$ gives the polarization.

This boils down to computing the ideal classes of \mathcal{O} .

Last step in the classification: consider $A = \mathbf{C}^2/\Lambda$ and see if T indeed defines a polarization. (*Shimura*)

Putting everything together

- If K is real quadratic, we find an irreducible surface. (*Humbert surface*)
- If K is imaginary quadratic, we find a point if S is definite and a curve (*Shimura curve*) if S is indefinite.
- If K is degree 4 CM, we find a point.

This is an ‘analytic answer’. To make everything algebraic:

- Humbert surface: compute equation
- indefinite S : find a quaternion order contained in $\text{End}(A)$. The intersection of the Humbert surfaces corresponding to the real quadratic suborders is our Shimura curve.
- the CM-points are algebraic.

The other case: \mathcal{O} is not a domain

Theorem. *Let β_1, β_2 be the eigenvalues of x acting on \mathbf{C}^2 . Then: β_i is imaginary quadratic of norm p . The traces of β_1, β_2 are distinct. Furthermore: there exist elliptic curves E_1, E_2 and there is an integer $k \mid (\text{Tr}(\beta_1) - \text{Tr}(\beta_2))$ such that there is a (k, k) -isogeny*

$$\lambda : E_1 \times E_2 \rightarrow A$$

with $\text{End}(E_i) \supseteq \mathbf{Z}[\beta_i]$ and $x\lambda = \lambda(\beta_1, \beta_2)$.

Proof. Let V_i be the β_i -eigenspace. Write $E_i = V_i / (V_i \cap \Lambda)$. Now check that we can take λ to be addition on A . \square

Conclusion: It is a finite computation to find all possibilities for E_1, E_2, k and $\text{Ker}(\lambda)$.

Example: $p = 2$, surfaces

We find one (Humbert) surface:

$$\begin{aligned} H_8 = & -12008187649867604184j_1^{10} + 46966009581837720j_1^9j_2^2 \\ & -281796057491026320j_1^9j_2j_3 + 74323144140993953726400j_1^9j_2 \\ & +422694086236539480j_1^9j_3^2 - 188308985155317427104000j_1^9j_3 \\ & +6525527376491882166412800000j_1^9 - 40922652296790j_1^8j_2^4 \\ & \vdots \\ & +160j_1^2j_2^{13} - 1920j_1^2j_2^{12}j_3 + 25973784j_1^2j_2^{12} + 8640j_1^2j_2^{11}j_3^2 \\ & -85753728j_1^2j_2^{11}j_3 - 17280j_1^2j_2^{10}j_3^3 + 12960j_1^2j_2^9j_3^4 - 80j_1j_2^{14} \\ & +480j_1j_2^{13}j_3 - 720j_1j_2^{12}j_3^2 + 16j_2^{15} \end{aligned}$$

corresponding to $\mathcal{O} = \mathbf{Z}[\sqrt{2}]$.

Example: $p = 2$, positive definite matrices S

- $\mathcal{O} = \mathbf{Z}[i]$ gives $S = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. This yields the surface $E_{-4} \times E_{-4}$.
- $\mathcal{O} = \mathbf{Z}[(-1 + \sqrt{7})/2]$ gives $S = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. This yields the surface $E_{-7} \times E_{-7}$.
- $\mathcal{O} = \mathbf{Z}[\sqrt{-2}]$ gives $S = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & \sqrt{-2} + 1 \\ -\sqrt{-2} + 1 & 2 \end{pmatrix}$.
The first S yields $E_{-8} \times E_{-8}$.

The second S gives $E_{-8} \times E_{-8}$ a different polarization. It becomes the Jacobian of a curve C .

Historic detour: finding C

The curve E_{-8} has j -invariant 8000. Its two torsion is defined over $L = \mathbf{Q}(\sqrt{8})$.

The curve $E/L : Y^2 = X(X - 1)(X - \lambda)$ has j -invariant 8000 for $\lambda = -2\sqrt{2} + 3$. Let $F/L : Y^2 = X(X - 1)(X - (1/\lambda))$.

Let $\psi : E[2] \rightarrow F[2]$ be the map with

$$(1, 0) \mapsto (1, 0), \quad (\lambda, 0) \mapsto (\lambda, 0).$$

Legendre gluing. For this ψ , the quotient $(E \times F)/\text{graph}(\psi)$ is the Jacobian of a genus 2 curve.

Historic detour: finding C

Legendre gave a formula for $(E \times F)/\text{graph}(\psi)$, too.

With

$$C : Y^2 = (X^2 - 1) \left(X^2 - \frac{1}{\lambda} \right) \left(X^2 - \frac{\frac{1}{\lambda} - 1}{\lambda - 1} \right),$$

we have $\text{Jac}(C) = (E \times F)/\text{graph}(\psi)$.

This Jacobian has absolute Igusa invariants

$$(400000, -20000, -2000)$$

and also equals $\text{Jac}(C')$ with $C' : Y^2 = X^5 - X$.

We have $\text{Jac}(C) \in H_8$.

Example: $p = 2$, negative definite matrices S

- $\mathcal{O} = \mathbf{Z}[i]$ gives $S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. This yields 2 Shimura curves.
- $\mathcal{O} = \mathbf{Z}[(-1 + \sqrt{-7})/2]$ gives $S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. This yields 1 Shimura curve.
- $\mathcal{O} = \mathbf{Z}[\sqrt{-2}]$ gives $S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. This yields 2 Shimura curves.

The image of the quadratic form $(a, b) \mapsto (a, b)S(\bar{a}, \bar{b})^T$ contains 1 for $S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and only elements of $\text{Tr}(\mathcal{O}_K)$ for $S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

This explains the difference for $\text{disc}(\mathcal{O})$ odd.

Finding 5 Shimura curves

Our strategy: write down some ‘easy curves’ until we have 5 different ones.

- Let E be an elliptic curve and put $x = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \in \text{End}(E^2)$.
This Shimura curve corresponds to $\mathcal{O} = \mathbf{Z}[i]$.

- Glue E to itself along its 2-torsion to find (the closure of)

$$Y^2 = (X^2 - 1) \left(X^2 - \frac{1-a}{a} \right) \left(X^2 + \frac{a}{a-1} \right)$$

for $a \in \mathbf{C} \setminus \{0, 1\}$. This curve corresponds to $\mathcal{O} = \mathbf{Z}[i]$.

Both curves lie on H_8 .

Finding 5 Shimura curves

- Let $f : E \rightarrow F$ be a 2-isogeny of elliptic curves. Put $x = \begin{pmatrix} 0 & \widehat{f} \\ -f & 0 \end{pmatrix} \in \text{End}(E \times F)$. The Shimura curve is given by $\Phi_2 = 0$ and corresponds to $\mathcal{O} = \mathbf{Z}[\sqrt{-2}]$.
- For the same E, F : glue them along their 2-torsion to find

$$Y^2 = (X^2 - 1) \left(X^2 - \frac{(a-1)^2}{(a+1)^2} \right) \left(X^2 + \frac{4a}{(a+1)^2(a-1)} \right)$$

for $a \in \mathbf{C} \setminus \{-1, 0, 1\}$. This also corresponds to $\mathcal{O} = \mathbf{Z}[\sqrt{-2}]$.

Both curves lie on H_8 .

Finding 5 Shimura curves

- For $\mathcal{O} = \mathbf{Z}[(-1 + \sqrt{-7})/2]$ it turns out that we need the moduli space of tuples

$$(f : E \rightarrow F, P_1, P_2)$$

with f a 7-isogeny and $\langle P_1, P_2 \rangle = E[2]$. A factor $X(a, b) = 0$ of

$$\Phi_7(j(a), j(b)) \in \mathbf{Q}(a, b) \quad \text{with} \quad j(a) = 2^8 \frac{(a^2 - a + 1)^3}{(a - 1)^2 a^2}$$

is birational to the fibered product $Y_0(7) \times_{Y(1)} Y(2)$. The points on this Shimura curve are the Jacobians of

$$Y^2 = X(X^2 - 1) \left(X^2 - \frac{b}{a} \right) \left(X^2 - \frac{b-1}{a-1} \right), \quad (a, b) \in X.$$

The Shimura curve lies on H_8 .

Example: $p = 2$, CM-points

There are 12 degree 4 CM fields K that contain a ‘Weil 2-number’. Four have Galois group D_4 and eight are biquadratic.

Using CM-theory we find 28 points, counted with multiplicity.

The Jacobian of

$$Y^2 = X^6 + X^3 + 1/20$$

occurs 3 times, is $(2, 2)$ -split and does *not* lie on H_8 . The other split surfaces lie on H_8 .

The D_4 -case yields 8 points, 2 of which lie on H_8 .

Example: $p = 2$ and \mathcal{O} is not a domain

It is a finite computation to find all possibilities.

Most of the p.p.a.s. can be found using a $(2, 2)$ -gluing à la Legendre. We find 7 abelian surfaces, 3 of which lie on H_8 .

We needed one $(3, 3)$ -gluing. These have been worked out by Robert Kuhn (1988). We find the two curves

$$Y^2 = X(X \pm 2\sqrt{7} - 6)(X^2 \pm 24\sqrt{7} - 48)(X^2 + (\mp\sqrt{7} - 2)X \pm 2\sqrt{7} + 10).$$

Their Jacobians do not lie on H_8 .

Example: $p = 2$, summary

Theorem. *The variety $\mathcal{M}_2^{(2,2)}$ that parametrizes principally polarized abelian surfaces that admit a $(2, 2)$ -isogeny consists of:*

- *the Humbert surface of discriminant 8*
- *three products of elliptic curves with the product polarization*
- *two $(2, 2)$ -split surfaces*
- *two $(3, 3)$ -split surfaces*
- *6 simple CM-points.*