

# Abelian surfaces admitting an $(\ell, \ell)$ -endomorphism

Marco Streng\*

Talk given at Max-Planck-Institut für Mathematik, Bonn  
September 17, 2009

## Abstract

We give a classification of all principally polarized abelian surfaces that admit  $(\ell, \ell)$ -isogenies to themselves. We make the classification explicit in the simplest cases  $\ell = 1$  and  $\ell = 2$  and show how to compute all the abelian surfaces that occur.

This talk is about research done during an internship of the speaker at Microsoft Research. It is joint work with Reinier Bröker (Microsoft Research, now Brown University) and Kristin Lauter (Microsoft Research)

Let  $\ell$  be a positive integer. For this talk, we assume  $\ell$  to be square-free and greater than 1. An  $\ell$ -**isogeny** is a morphism of degree  $\ell$  of elliptic curves. This notion gives rise to the *modular polynomial*, which is a polynomial  $\Phi_\ell \in \mathbf{Z}[X, Y]$  such that for all elliptic curves  $E, F/\mathbf{C}$ , there is an  $\ell$ -isogeny  $E \rightarrow F$  if and only if we have  $\Phi_\ell(j(E), j(F)) = 0$ .

A related polynomial is the *Hilbert class polynomial*  $H_{\mathcal{O}} \in \mathbf{Z}[X]$ , defined for any imaginary quadratic order  $\mathcal{O}$  by

$$H_{\mathcal{O}} = \prod_{\substack{E/\mathbf{C} \\ \text{End}(E) \cong \mathcal{O}}} (X - j(E)).$$

These polynomials satisfy

$$\Phi_\ell(X, X) = \prod H_{\mathcal{O}}^{e(\mathcal{O})}, \tag{1}$$

where the product is taken over all  $\mathcal{O}$  that have an element of norm  $\ell$  and  $e(\mathcal{O})$  is a positive integer related to the number of such elements. This identity is useful for understanding one type of polynomial from the other. For example, one of the proofs that  $H_{\mathcal{O}}$  has integer coefficients uses this identity.

---

\*Universiteit Leiden.

If we go to **dimension 2**, then we need the notion of an  $(\ell, \ell)$ -isogeny of *principally polarized abelian surfaces*. We introduce both notions, as well as the *moduli space*  $\mathcal{A}_2$  of such surfaces, later. The analogue of  $\Phi_\ell$  is then a variety

$$W_\ell \subset \mathcal{A}_2 \times \mathcal{A}_2$$

that parametrizes  $(\ell, \ell)$ -isogenies. The variety  $V_\ell$  obtained by intersecting  $W_\ell$  with the diagonal in  $\mathcal{A}_2 \times \mathcal{A}_2$  is then a subvariety of  $\mathcal{A}_2$  that gives all abelian varieties that have an  $(\ell, \ell)$ -isogeny to themselves.

Our **GOAL** is to give the 2-dimensional analogue of (1), that is, a decomposition of  $V_\ell^{\text{red}}$  into irreducible algebraic subvarieties.

One possible application is to *Igusa class polynomials*, that is, the dimension-2 analogue of the Hilbert class polynomial. These polynomials aren't integral, but perhaps the analogue of (1) could be used for bounding the denominators of their coefficients.

Let's now give the **definitions**. A *complex torus*  $T$  is a  $\mathbf{C}$ -vector space  $V$  modulo a lattice  $\Lambda$  of full rank. A *morphism* of complex tori is a morphism as complex analytic Lie groups. Such a morphism is always induced from a complex linear map of vector spaces that maps one lattice to the other. An *isogeny* is a surjective morphism with finite degree (i.e. order of the kernel).

A *polarization* on  $V/\Lambda$  is a non-degenerate  $\mathbf{R}$ -bilinear form  $E : V \times V \rightarrow \mathbf{R}$  satisfying

- $E$  is alternating, i.e.  $E(u, v) = -E(v, u)$  for all  $u, v \in V$ ,
- $E(\Lambda, \Lambda) \subset \mathbf{Z}$ , and
- $(u, v) \mapsto E(iu, v)$  is symmetric and positive definite.

We define an *abelian variety over  $\mathbf{C}$*  to be a complex torus for which there exists a polarization. This gives an equivalence of categories between our definition of abelian varieties and the more algebraic definition of proper group variety. A *polarized abelian variety* is a pair consisting of a complex torus *together* with a polarization.

The determinant of a polarization  $E$  with respect to a  $\mathbf{Z}$ -basis of  $\Lambda$  is an integer that does not depend on the choice of basis. It is always a square and we call its positive square root the *degree*  $\deg(E)$  of  $E$ . By *principal*, we mean 'of degree 1'.

Let  $f : T \rightarrow T'$  be an isogeny and  $E'$  a polarization on  $T'$ . Then

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

defines a polarization on  $T$  of degree  $\deg f \cdot \deg E'$ .

An  $(\ell, \ell, \dots, \ell)$ -isogeny (with  $g$  times an ' $\ell$ ')  $f : (T, E) \rightarrow (T', E')$  of principally polarized abelian varieties is an isogeny  $f : T \rightarrow T'$  such that  $f^*E' = \ell E$ . An *isomorphism* of principally polarized abelian varieties is defined in the same way but with  $\ell = 1$ .

Let  $\mathcal{A}_g$  be the coarse moduli space of principally polarized abelian varieties of dimension  $g$ . Its set of  $\mathbf{C}$ -points is the set of principally polarized abelian varieties of dimension  $g$  up to isomorphism.

By  $\text{End}(A)$  for a principally polarized abelian variety  $A$ , we mean the ring of endomorphisms of the underlying abelian variety (without the polarization).

Our **GOAL** is now to list all pairs  $(A, x)$  with  $A \in \mathcal{A}_2$  and  $x \in \text{End}(A)$  an  $(\ell, \ell)$ -isogeny. From now on, let  $(A, x)$  be such a pair.

The **Rosati involution** is the unique map  $\text{End}(A) \rightarrow \text{End}(A) : y \mapsto \bar{y}$  such that  $E(yu, v) = E(u, \bar{y}v)$  for all  $u, v \in V$ . Indeed, non-degeneracy of  $E$  implies that a unique  $\mathbf{R}$ -linear  $\bar{y} : V \rightarrow V$  with the defining property exists, and the definition of a principal polarization shows  $\bar{y} \in \text{End}(A)$ . It is easy to see that the Rosati involution is an anti homomorphism of rings, i.e. respects addition and reverses multiplication.

Note that we have  $E(u, \bar{x}xv) = E(xu, xv) = \ell E(u, v) = E(u, \ell v)$  for all  $u, v$ , so  $\bar{x}x = \ell$ .

Our first approach was to list all decomposition types of  $A$  (simple, isogenous to a product of elliptic curves, isomorphic to a product of elliptic curves) and the corresponding possibilities for  $\text{End}(A)$ . However, it turned out to work much better to just look at  $K = \mathbf{Q}[x] \subset \text{End}(A) \otimes \mathbf{Q}$  and its subring  $\mathcal{O} = \mathbf{Z}[x] \subset \text{End}(A)$  and forget about the rest of  $\text{End}(A)$ . Then there are two possibilities:

- I  $\mathcal{O}$  is a domain,
- II  $\mathcal{O}$  is not a domain.

Shimura has described the moduli spaces corresponding to I. We will show how to list them explicitly. At the end of this talk, we show how to use the ring  $\mathcal{O}$  to decompose  $A$  into a product of elliptic curves in case II.

In **case I**, the ring  $K$  is a number field of degree dividing 4. As we have  $\bar{x} = \ell x^{-1} \in K$ , the Rosati involution is an automorphism of  $K$ , and it is known that it is equal to complex conjugation for every embedding of  $K$  into  $\mathbf{C}$ . There are thus three cases.

1. There is a real embedding, so  $x^2 = \bar{x}x = \ell$  and hence  $K = \mathbf{Q}(\sqrt{\ell})$ , where  $x = \pm\sqrt{\ell}$ .
2. The field  $K$  is imaginary quadratic, so  $x$  is an imaginary quadratic integer satisfying  $\bar{x}x = \ell$ . In particular,  $x + \bar{x}$  is a rational integer of absolute value less than  $2\sqrt{\ell}$ , so there are finitely many possibilities. For example, for  $\ell = 1$ , there are only the primitive third, fourth, and sixth roots of unity, and for  $\ell = 2$ , we have  $x \in \{\pm\sqrt{-2}, \frac{1}{2}(\pm 1 \pm \sqrt{-7}), \pm 1 \pm \sqrt{-1}\}$ .
3. The field  $K$  has degree 4 and no real embeddings. It is then a *CM field*, i.e. a non-real field  $K$  such that complex conjugation is an automorphism of  $K$  that does not depend on a choice of complex embedding. The element  $x$  is again a non-real algebraic integer and thus  $x + \bar{x}$  is in every real absolute value less than  $2\sqrt{\ell}$ . This again makes the list of possibilities finite. For  $\ell = 1$ , we only have the primitive fifth, eighth, tenth, and twelfth roots of

unity. For  $\ell = 2$ , there are 12 possibilities up to complex conjugation and sign.

There are thus only finitely many possibilities for  $\mathcal{O}$ . For each, note that  $\Lambda$  is an  $\mathcal{O}$ -module that is free of rank 4 over  $\mathbf{Z}$ , hence  $\Lambda \otimes \mathbf{Q}$  is a  $K$ -vector space of dimension  $s = 4/\deg K$  over  $K$ . We choose a basis of this vector space and identify it with  $K^s$ . Then  $E$  becomes a  $\mathbf{Q}$ -bilinear form  $K^s \times K^s \rightarrow \mathbf{Q}$ .

**Lemma.** There exists a unique matrix  $T \in \text{Mat}_s(K)$  such that for all  $u, v \in K^s$ , we have

$$E(u, v) = \text{Tr}(u^t T \bar{v}). \quad (2)$$

This matrix satisfies  $\bar{T}^t = -T$  holds.

*Proof.* Given  $u, v \in K^s$ , consider the  $\mathbf{Q}$ -linear map  $K \rightarrow \mathbf{Q} : y \mapsto E(yu, v)$ . As the bilinear map  $K \times K \rightarrow \mathbf{Q} : (w, y) \mapsto \text{Tr}(wy)$  is non-degenerate, there is a unique  $w = w(u, v) \in K$  such that  $E(yu, v) = \text{Tr}(wy)$  for all  $y$ . By taking  $y = 1$ , we get  $E(u, v) = \text{Tr}(w(u, v))$ . It is not hard to check that  $w$  is  $K$ -linear on the left, and that it is  $K$ -linear via  $\bar{\cdot}$  on the right. This shows that  $T$  exists. The fact that  $E$  is alternating shows that so is  $T$ .  $\square$

Our **GOAL** for case I is now, for each  $\mathcal{O}$ , to list all pairs  $\Lambda \subset K^s$  and  $T \in \text{Mat}_s(K)$  such that  $\Lambda$  has rank 4 over  $\mathbf{Z}$ , that  $\bar{T}^t = -T$  holds, and that  $E$  defined by (2) takes values in  $\mathbf{Z}$  and has determinant 1 on  $\Lambda$ , up to change of  $K$ -basis of  $K^s$  (and to compute the corresponding abelian varieties).

Let  $\delta = x - \bar{x}$  and  $S = \delta T$ . Here is how to enumerate those pairs for the three kinds of fields.

1. If  $\mathcal{O}$  is the maximal order, then we only need  $\Lambda = \mathcal{O} \times \mathcal{O}$  with

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

For general orders, there are still not many options, so this is easy.

2. We have  $\bar{S}^t = S$ , so  $S$  is Hermitian. The method for enumerating the pairs with  $S$  positive definite and  $\mathcal{O}$  maximal is given by Hayashida and Nishi [2] in the context of enumerating principal polarizations on products of elliptic curves over finite fields.
3. Here  $\Lambda$  is a fractional  $\mathcal{O}$ -ideal and  $T$  is an element of  $K$ . The pairs  $(\Lambda, T)$  are related to CM theory and can be enumerated if one can compute the set of ideal classes of  $\mathcal{O}$ .

Once we have found all pairs  $(\Lambda, T)$ , we need to enumerate the corresponding abelian varieties. Note that we have

$$\Lambda \subset K^s \otimes \mathbf{R} \cong_{\mathbf{R}} \mathbf{C}^2,$$

where the  $\mathbf{R}$ -vector space isomorphism is a choice. One can then look at  $(\mathbf{C}^2/\Lambda, E)$ , where  $E$  is of (2), and see for which choices  $E$  is a polarization

and  $x$  extends  $\mathbf{C}$ -linearly to  $\mathbf{C}^2$ . The set of correct choices has been made explicit by Shimura and can be found in [1, §9.2] if  $K$  is real and [1, §9.6] otherwise. We have that the variety in  $\mathcal{A}_2$  corresponding to each  $(\Lambda, T)$  is (depending on the type of field  $K$ )

1. an irreducible surface (called an *Humbert surface*),
2. a point if  $S$  is definite and an irreducible curve (called a *Shimura curve*) if  $S$  is indefinite,
3. a point.

As Shimura's construction is explicit, we now know exactly how to compute all isomorphism classes for case I complex analytically.

To get an **algebraic answer**, one needs to compute equations for the surfaces, curves, and points that we just mentioned. David Gruenewald [?] gives an algorithm for computing the Humbert surfaces. Computing algebraic equations for the points from numerical approximations is easy. Finally, in case 2, if  $S$  is indefinite, it is possible to compute from  $\Lambda$  and  $T$  an indefinite quaternion order that is contained in the endomorphism ring of  $A$ . By computing the real quadratic orders inside that quaternion order, one could theoretically find the Shimura curve as an intersection of Humbert surfaces.

**In practice**, for  $\ell = 1, 2$ , we used a different method to compute the Shimura curves and many of the points. From the  $\Lambda$ 's and  $T$ 's, we can see how many points and curves there are and find out which are isogenous to each other and/or to products of elliptic curves. It is also possible to see what kind of isogeny there is, e.g. the degree of the isogeny and whether it is a  $(k, k)$ -isogeny for some  $k$ . We can then compute example points and curves by taking products of elliptic curves. Classical formulas of Legendre and Jacobi give curves of genus 2 with Jacobian  $(2, 2)$ -isogenous to a product of elliptic curves. More modern formulas generalize this to  $(k, k)$ -isogenies for  $k = 3, 4$ , and higher. We know that we are done if we have the correct number of points and curves.

**For example**, let  $E, F$  be a pair of elliptic curves with a 2-isogeny  $f$  and consider  $A = E \times F$  with

$$x = \begin{pmatrix} 0 & \hat{f} \\ -f & 0 \end{pmatrix},$$

where  $\hat{f}$  is the dual of  $f$ , i.e., satisfies  $\hat{f}f = 2$ . The pairs  $E, F$  form the zero set of the modular polynomial  $\Phi_2$  in the plane, hence the set of all  $A$  forms a curve in  $\mathcal{A}_2$ . Note that we have  $\bar{x}x = 2$  and  $x^2 = -2$ , so this family is one of the Shimura curves for  $\mathcal{O} = \mathbf{Z}[\sqrt{-2}]$ .

Using the formulas of Legendre and Jacobi, we find a family of curves  $C$  of genus 2 that are  $(2, 2)$ -isogenous to the  $E, F$  above and on which  $x$  induces an endomorphism. This family is our second Shimura curve for  $\mathcal{O} = \mathbf{Z}[\sqrt{-2}]$  and one can show that there exist only two pairs  $(\Lambda, T)$  (up to equivalence) with  $S$  indefinite, hence we have found all Shimura curves for this ring.

For **case II**, we have the following result.

**Lemma.** Suppose that  $\mathcal{O} = \mathbf{Z}[x]$  is not a domain. Let  $\beta_1, \beta_2$  be the eigenvalues of  $x$  acting on  $V$ . Then for each  $i$ , we have that  $\beta_i$  is an imaginary quadratic integer of norm  $\ell$  and the traces of  $\beta_1$  and  $\beta_2$  are distinct.

Moreover, there exist a pair  $E_1, E_2$  of elliptic curves, a positive integer  $k$  dividing the difference of the traces of  $\beta_1$  and  $\beta_2$  and a  $(k, k)$ -isogeny  $\lambda : E_1 \times E_2 \rightarrow A$  such that we have  $\text{End}(E_i) \supset \mathbf{Z}[\beta_i]$  and  $x\lambda = \lambda(\beta_1, \beta_2)$ .

In the proof of the lemma, the elliptic curves  $E_i$  are subvarieties of  $A$  given by  $E_i = V_i/(V_i \cap \Lambda)$ , where  $V_i$  is the  $\beta_i$ -eigenspace, and  $\lambda : E_1 \times E_2 \rightarrow A$  is the addition map inside  $A$ .

Note that there are only finitely many possibilities for  $E_1, E_2$ , and  $k$ , and hence also for  $\ker \lambda$ . It is therefore possible to enumerate all possibilities for  $A$ .

This finishes case II.

Here are some **examples** of what we have computed with these methods:

- For  $\ell = 1$ , some results and definitions need to be adapted, but then everything works: we get a list of all possible automorphism groups of principally polarized abelian varieties  $A$ , with the corresponding subvarieties of  $\mathcal{A}_2$ . Such a list (obtained by different methods) is already known. The case where  $A$  is a product of elliptic curves is easy. The only other case is where  $A$  is the Jacobian of a hyperelliptic curve  $C$  of genus 2 and we have  $\text{Aut}(A) = \text{Aut}(C)$ . The automorphism groups of curves of genus 2 have been computed by [?]. Actually, the possibilities for  $\text{Aut}(C)$  modulo the hyperelliptic involution, and the modular variety for each group, have been known since Bolza [?] who classified binary sextic forms with extra automorphisms.
- For  $\mathcal{O} = \mathbf{Z}[\sqrt{-2}]$  with  $S$  indefinite, we have seen that there are exactly two Shimura curves. There are also exactly two points for  $S$  definite.
- The reduced variety  $V_2^{\text{red}}$  is the union of the Humbert surface for  $\mathbf{Z}[\sqrt{2}]$  and 13 points. These 13 points correspond to 3 products of elliptic curves from case II, 3 Jacobians of curves of genus 2 from case II, and 7 Jacobians of curves of genus 2 from case II for 4 distinct CM fields of degree 4. All Shimura curves that appeared already lie on the Humbert surface.

## References

- [1] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der mathematischen Wissenschaften*. Springer, second edition, 2004.
- [2] Tsuyoshi Hayashida and Mieno Nishi. Existence of curves of genus two on a product of two elliptic curves. *J. Math. Soc. Japan*, 17(1):1–16, 1965.