

# Computing endomorphism rings of abelian varieties of dimension two

Gaetan Bisson

## Abstract

Generalizing a method of Sutherland and the author for elliptic curves [5, 1], we design a subexponential algorithm for computing the endomorphism ring structure of ordinary abelian varieties of dimension two over finite fields. Although its correctness and complexity bound rely on several assumptions, we report on practical computations showing that it performs very well and can easily handle previously intractable cases.

**Note.** Certain results of this paper previously appeared in the author's thesis [2].

## 1 Introduction

Let  $\mathcal{A}$  be an absolutely simple abelian variety of dimension  $g$  defined over a field with  $q$  elements; its Frobenius endomorphism  $\pi$  admits a monic characteristic polynomial  $\chi_\pi \in \mathbb{Z}[t]$  of which the  $2g$  complex roots have absolute value  $\sqrt{q}$ . Pila [24] proved that this polynomial can be computed in time polynomial in  $\log(q)$ . In the generic case where  $\mathcal{A}$  is ordinary,  $\chi_\pi$  is irreducible and the endomorphisms of  $\mathcal{A}$  form a discrete subring of maximal rank (an *order*)  $\text{End}(\mathcal{A})$  of  $\mathbb{Q}(\pi)$  that is unchanged by base field extensions.

Tate [28] showed that  $\chi_\pi$  not only encodes the cardinality of  $\mathcal{A}$  over extension fields but also uniquely identifies its isogeny class. The endomorphism ring structure of an abelian variety is a finer invariant than  $\chi_\pi$  which is better suited to isogeny-related problems such as those considered in [16] and has also found constructive applications to cryptography, for instance in [27].

Kohel [17] first addressed the computation of this structure and obtained an exponential method for ordinary elliptic curves. It was recently improved by Sutherland and the author [5] yielding an algorithm with subexponential complexity under heuristic assumptions that were later proved to hold under the generalized Riemann hypothesis [1]. Although Kohel's method does not extend to dimensions  $g > 1$  [7, Example 8.3], other exponential methods exist for arbitrary  $g$ , namely those of Eisenträger and Lauter [13], and of Wagner [29].

This paper generalizes the techniques of [5, 1] to ordinary abelian varieties of dimension  $g = 2$  and obtains the first subexponential algorithm for computing their endomorphism rings; its asymptotic complexity is

$$L(q)^{g^2 \sqrt{3}/2 + o(1)} \quad \text{where} \quad L(q) = \exp \sqrt{\log(q) \cdot \log \log(q)}$$

as  $q$  goes to infinity. We stress that both its correctness and complexity bound rely on heuristic assumptions besides the generalized Riemann hypothesis, and

require the exclusion of a zero-density set of worst-case varieties. In practice, we find that our algorithm performs very well on examples of moderate size. When relevant, we avoid specializing the variable  $g$  to 2 in our complexity estimates, as they would also hold for  $g > 2$  if certain tasks turned out to be computationally feasible; see Section 6.

Section 2 discusses the relation between isogenies and endomorphism rings on which our algorithm, outlined in Section 3, is based. Sections 4 and 5 then explain how short relations are generated and corresponding isogenies evaluated. Heuristic assumptions and worst cases are reviewed in Section 6, while practical runtimes are reported in Section 7.

## 2 Isogenies and Endomorphism Rings

We assume some familiarity with abelian varieties, isogenies, and endomorphism rings; we refer to [10, Chapter V] for background material and to [25] for complex multiplication.

Consider again an absolutely simple, ordinary abelian variety  $\mathcal{A}$  of dimension  $g$  defined over a field with  $q$  elements, and fix an isomorphism of its endomorphism algebra  $\mathbb{Q}(\pi) = \mathbb{Q} \otimes \text{End}(\mathcal{A})$  with a number field  $K$ ; this field is called the *complex multiplication field* of  $\mathcal{A}$  and is a totally imaginary quadratic extension of a totally real number field  $K_0$  of degree  $g$ . Waterhouse [30] showed that the endomorphism rings of abelian varieties isogenous to  $\mathcal{A}$  are exactly those orders of  $K$  that contain  $\mathbb{Z}[\pi, \bar{\pi}]$ , where  $\bar{\pi} = q/\pi$ ; they form a finite lattice (in the set-theoretic sense of the word) with supremum the ring of integers  $\mathcal{O}_K$ .

Following Fouquet and Morain [14], we say that an isogeny  $\phi : \mathcal{A} \rightarrow \mathcal{B}$  is *horizontal* when  $\text{End}(\mathcal{A})$  and  $\text{End}(\mathcal{B})$  are the same order in  $K$ , and *vertical* otherwise. In a sense, horizontal isogenies are the prevalent case.

**Lemma 2.1.** *If  $\phi : \mathcal{A} \rightarrow \mathcal{B}$  is an isogeny with kernel isomorphic to  $(\mathbb{Z}/\ell\mathbb{Z})^g$ , the index  $[\text{End}(\mathcal{A}) + \text{End}(\mathcal{B}) : \text{End}(\mathcal{A}) \cap \text{End}(\mathcal{B})]$ , which we call the distance between the orders  $\text{End}(\mathcal{A})$  and  $\text{End}(\mathcal{B})$ , is a divisor of  $\ell^{2g-1}$ .*

*Proof.* Since  $\phi$  splits the multiplication-by- $\ell$  map, we have  $\ell \text{End}(\mathcal{A}) \subset \text{End}(\mathcal{B})$  and, the latter being an order, we further have  $\mathbb{Z} + \ell \text{End}(\mathcal{A}) \subset \text{End}(\mathcal{B})$ ; we thus obtain the lattice of Figure 1. As they are indices of the form  $[\mathcal{O} : \mathbb{Z} + \ell\mathcal{O}]$ , the products  $bcd$ ,  $ace$ , and  $cde$  are all equal to  $\ell^{2g-1}$  which implies  $bcd \cdot ace/cde = \ell^{2g-1}$  and finally  $ab = \ell^{2g-1}/c$ .  $\square$

The distance between the endomorphism rings of isogenous abelian varieties necessarily divides the index  $[\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]]$ ; vertical isogenies thus only exist for finitely many primes  $\ell$ . On the other hand, horizontal isogenies occur for a positive density of primes  $\ell$ , which follows from the following result.

**Theorem 2.2** ([25, §7], [30, §7]). *For every ideal  $\mathfrak{a}$  of  $\text{End}(\mathcal{A})$ , denote by  $\phi_{\mathfrak{a}}$  the quotient isogeny*

$$\mathcal{A} \longrightarrow \mathcal{A} / \bigcap_{\alpha \in \mathfrak{a}} \ker(\alpha).$$

*If  $\mathfrak{a}$  is invertible and coprime to the characteristic,  $\phi_{\mathfrak{a}}$  is a horizontal isogeny of degree  $N_{K/\mathbb{Q}}(\mathfrak{a})$  and all such isogenies arise in that way; this induces a free and transitive action of  $\text{cl}(\text{End}(\mathcal{A}))$  on the isogeny class of  $\mathcal{A}$  up to isomorphisms.*

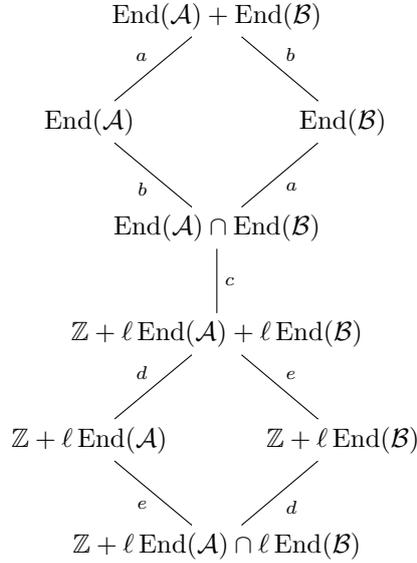


Figure 1: Lattice of orders for an isogeny  $\mathcal{A} \rightarrow \mathcal{B}$  of kernel  $(\mathbb{Z}/\ell\mathbb{Z})^g$ .

However, isogenies cannot be computed efficiently unless abelian varieties are equipped with polarizations, which this theorem disregards. From now on, we will therefore assume that  $\mathcal{A}$  is endowed with a principal polarization, and require that morphisms preserve this extra structure; this implies that  $\text{End}(\mathcal{A})$  is stable under complex conjugation. To state an equivalent to Theorem 2.2 in this setting, we need a slightly different type of class group:

**Definition 2.3.** *For any order  $\mathcal{O}$  in a complex multiplication field  $K$ , denote by  $I_{\mathcal{O}}$  the group consisting of all pairs  $(\mathfrak{a}, \rho)$  satisfying  $\mathfrak{a}\bar{\mathfrak{a}} = \rho\mathcal{O}$ , where  $\mathfrak{a}$  is an invertible fractional ideal of  $\mathcal{O}$  and  $\rho$  is a totally positive element of  $K_0$ , endowed with component-wise multiplication; also, let  $P_{\mathcal{O}}$  be its subgroup formed by pairs of the form  $(\mu\mathcal{O}, \mu\bar{\mu})$  for  $\mu \in K$ . The quotient group  $I_{\mathcal{O}}/P_{\mathcal{O}}$  is called the polarized class group of  $\mathcal{O}$  and is denoted by  $\mathfrak{C}(\mathcal{O})$ .*

Note that this group is unchanged if we additionally require that  $\mathfrak{a}$  (and  $\mu$ ) be coprime to a fixed integer  $\nu$ ; from now on, it will be understood that we exclusively consider class representatives of this type with  $\nu = \text{disc}(\mathbb{Z}[\pi, \bar{\pi}])$ . By the following theorem, such elements correspond to horizontal isogenies that preserve the polarization.

**Theorem 2.4** ([25, §14]). *Provided that  $\text{End}(\mathcal{A})$  is maximal, one can associate a horizontal isogeny of degree  $N_{K/\mathbb{Q}}(\mathfrak{a})$  to every  $(\mathfrak{a}, \rho) \in I_{\text{End}(\mathcal{A})}$ , where  $\mathfrak{a}$  is coprime to the characteristic, so as to induce a free action of  $\mathfrak{C}(\text{End}(\mathcal{A}))$  on the isogeny class of  $\mathcal{A}$  up to isomorphisms.*

For elliptic curves, this result coincides with Theorem 2.2 due to the uniqueness of principal polarizations, and thus holds for non-maximal endomorphism rings as well. It is also believed to hold for general endomorphism rings in higher dimension, and we will assume that it does; see Section 6 for details on the extent of our assumptions.

### 3 Locating Endomorphism Rings

Our main idea to compute the endomorphism ring of  $\mathcal{A}$  originates from [5] and consists in locating it in the lattice of orders of  $K$  containing  $\mathbb{Z}[\pi, \bar{\pi}]$  by comparing the structure of the graph of horizontal isogenies with that of polarized class groups of candidate rings. Sections 4 and 5 describe this and obtain the result below under the assumptions of Section 6, namely  $g = 2$ , certain heuristics, and the exclusion of a zero-density set of varieties.

**Proposition 3.1.** *Subject to the restrictions listed in Section 6, Algorithm 5.4 determines whether  $\text{End}(\mathcal{A})$  contains a prescribed order  $\mathcal{O}$  with negligible error probability using an expected*

$$L(|\text{disc}(\mathcal{O})|)^{g\sqrt{3}/2+o(1)}$$

*operations in the base field.*

This enables us to test whether  $\text{End}(\mathcal{A}) = \mathcal{O}_K$  in subexponential time, a particular case that was deemed sufficient for early complex multiplication methods in dimension two [15]. Nevertheless, to compute the endomorphism ring entirely (as newer methods require [18]), we must first bound the number of orders containing  $\mathbb{Z}[\pi, \bar{\pi}]$  and their discriminants.

**Lemma 3.2.** *We have:*

$$|\text{disc}(\mathbb{Z}[\pi, \bar{\pi}])| < 4^{g(2g-1)} q^{g^2},$$

$$[\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]] < 2^{g(2g-1)} q^{g^2/2}.$$

*Proof.* All  $2g$  complex roots of  $\chi_\pi$  have absolute value  $\sqrt{q}$ , so we have  $|\text{disc}(\chi_\pi)| < (2\sqrt{q})^{2g(2g-1)}$ . The bounds then follow from the classical relation  $[\mathcal{O} : \mathcal{O}']^2 = \text{disc}(\mathcal{O}')/\text{disc}(\mathcal{O})$  and, for the first one, the identity  $[\mathbb{Z}[\pi, \bar{\pi}] : \mathbb{Z}[\pi]] = q^{g(g-1)/2}$  and, for the second one, the triviality  $|\text{disc}(\mathcal{O}_K)| > 1$ .  $\square$

These bounds are nearly tight so there might be exponentially many candidate endomorphism rings; to efficiently locate  $\text{End}(\mathcal{A})$  among them, we perform an  $n$ -ary search in the lattice of orders using the following algorithm borrowed from [1].

**Algorithm 3.3.**

- INPUT: *An absolutely simple, ordinary, principally polarized abelian variety  $\mathcal{A}$  of dimension  $g$  defined over a field with  $q$  elements.*
- OUTPUT: *The endomorphism ring of  $\mathcal{A}$ .*
1. *Compute the Frobenius polynomial  $\chi_\pi$  of  $\mathcal{A}$ .*
  2. *Factor its discriminant and construct the order  $\mathcal{O}' = \mathbb{Z}[\pi, \bar{\pi}]$ .*
  3. *For orders  $\mathcal{O}$  directly above  $\mathcal{O}'$ :*
  4. *If  $\mathcal{O} \subset \text{End}(\mathcal{A})$ , set  $\mathcal{O}' \leftarrow \mathcal{O}$  and go to Step 3.*
  5. *Return  $\mathcal{O}'$ .*

By *directly above*, we mean that  $\mathcal{O}$  contains  $\mathcal{O}'$  and no order lies strictly between them; the distance between two such orders necessarily divides  $\ell^{2g-1}$  for some prime factor  $\ell$  of  $[\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]]$ , since  $\mathcal{O}'$  must then contain  $\mathbb{Z} + \ell\mathcal{O}$ .

For Step 2, we use the unconditional factoring method of Lenstra and Pomerance [20]; its complexity is  $L(|\text{disc}(\chi_\pi)|)^{1+o(1)}$ , that is, at most  $L(q)^{g\sqrt{2}+o(1)}$ . Alternatively, one may rely on the number field sieve [19] which has a heuristically better runtime.

**Theorem 3.4.** *Subject to the restrictions listed in Section 6, the expected running time of Algorithm 3.3 is bounded by*

$$L(q)^{g^2\sqrt{3}/2+o(1)}.$$

*Proof.* Section 6.1 will show that enumerating the orders directly above a given one can almost always be done in negligible time compared to the overall complexity. The bottleneck of our algorithm is thus Step 4, which by Proposition 3.1 uses  $L(|\text{disc}(\mathbb{Z}[\pi, \bar{\pi}])|)^{g\sqrt{3}/2+o(1)}$  operations. Using Lemma 3.2, we may therefore bound the total complexity by  $L(q)^{g^2\sqrt{3}/2+o(1)}$ .  $\square$

## 4 Evaluating Isogenies

The next section will establish Proposition 3.1 by exploiting Theorem 2.4: to compare  $\mathcal{O}$  to  $\text{End}(\mathcal{A})$ , we will compare the structures of their polarized class groups by testing whether trivial products in  $\mathfrak{C}(\mathcal{O})$  yield isogeny chains mapping  $\mathcal{A}$  to isomorphic varieties. This only requires us to compute isogenous varieties  $\phi_\alpha(\mathcal{A})$  for given elements  $\alpha \in I_{\mathcal{O}}$ , not to actually evaluate the isogenies  $\phi_\alpha$  and push points of  $\mathcal{A}$  through them; however, there is currently no way of doing the former more efficiently than the latter.

In fact, evaluating isogenies in dimension  $g > 1$  became feasible only recently due to the work of Lubicz and Robert [22] implemented in the AVIsogenies library [3]. At the time of this writing, only isogenies with maximal isotropic kernel of degree coprime to the characteristic may be evaluated [11]; more precisely, we have the following result (see [11, Theorem 1.2] for a more explicit statement specialized to  $g = 2$ ):

**Proposition 4.1.** *Let  $\mathcal{H}$  be a given isotropic subgroup isomorphic to  $(\mathbb{Z}/\ell\mathbb{Z})^g$  of an abelian variety of dimension  $g$ . The separable isogeny with kernel  $\mathcal{H}$  can be evaluated with a worst-case complexity of  $\ell^{3g+o(1)}$  operations in the base field.*

Prior to evaluating an isogeny, we must identify its kernel  $\mathcal{H}$  as corresponding to a given element  $(\mathfrak{a}, \ell)$  of the polarized class group  $\mathfrak{C}(\mathbb{Z}[\pi, \bar{\pi}])$ . Assuming that  $\mathfrak{a}$  is a prime above some  $\ell \in \mathbb{Z}$ , and writing it as  $\ell\mathcal{O} + f(\pi)\mathcal{O}$  for some factor  $f$  of  $\chi_\pi \bmod \ell$ , we can take  $\mathcal{H}$  to be the subgroup of  $\mathcal{A}[\ell]$  on which the Frobenius acts with characteristic polynomial  $f$ ; it is unique since we restrict to ideals  $\mathfrak{a}$  coprime to  $\nu = \text{disc}(\mathbb{Z}[\pi, \bar{\pi}])$ . In effect, this identification fixes an isomorphism between  $\mathbb{Q} \otimes \text{End}(\mathcal{A})$  and the complex multiplication field  $K$  (mapping a fixed root of  $\chi_\pi$  to the Frobenius endomorphism) as was required in Section 2, and it only matters that this be done consistently within a given isogeny class.

Points of  $\mathcal{H}$  are defined over an extension field whose degree is the multiplicative order of  $x$  in  $\mathbb{Z}[x]/(f)/(\ell)$ , that is, at most  $N_{K/\mathbb{Q}}(\mathfrak{a}) - 1$ . Over that extension, assuming that points of  $\mathcal{A}$  can be drawn uniformly at random in an efficient manner, the  $\ell$ -torsion subgroup of  $\mathcal{A}$  can be computed using an algorithm of Couveignes [12, §8].

Once the isogenous abelian variety has been computed, we must find a representative of its isomorphism class over the base field, so that this process can be iterated. When  $g = 2$ , abelian varieties can be represented as Jacobian varieties of hyperelliptic curves, which allows us to efficiently draw points uniformly at random as well as to exploit the theory of invariants and Mestre's algorithm [23] in order to find representatives of isomorphism classes defined over the smallest possible field (that is, the field of definition of  $\mathcal{H}$ ).

In dimension  $g > 3$ , where only general representations of abelian varieties are available (such as those given by theta functions), there is to the best of our knowledge no efficient method to draw points uniformly at random or to find representatives of isomorphism classes defined over minimal fields. When  $g = 3$ , abelian varieties can still be represented as Jacobian varieties of algebraic curves, which gives a solution to the first problem, and we note that recent work such as [21] comes close to solving the second one.

## 5 Generating Short Relations

To determine whether a given order  $\mathcal{O}$  is contained in the endomorphism ring of  $\mathcal{A}$ , we generalize the approach of [5, 1]. It rests on Theorem 2.4 and the simple result below.

**Lemma 5.1.** *For any two orders  $\mathcal{O} \subset \mathcal{O}'$  containing  $\mathbb{Z}[\pi, \bar{\pi}]$ , the map  $(\mathfrak{a}, \rho) \in I_{\mathcal{O}} \rightarrow (\mathfrak{a}\mathcal{O}', \rho) \in I_{\mathcal{O}'}$  induces a natural morphism of polarized class groups  $\mathfrak{C}(\mathcal{O}) \rightarrow \mathfrak{C}(\mathcal{O}')$ ; this morphism is surjective when restricted and corestricted to elements such that  $\rho \in \mathbb{Q}$ .*

Denote by  $\mathfrak{C}'(\mathcal{O})$  the subgroup of  $\mathfrak{C}(\mathcal{O})$  formed by elements whose  $\rho$  are rationals. Now, define a *relation* as a tuple  $(\alpha_1, \dots, \alpha_k)$  of elements of  $\mathfrak{C}'(\mathbb{Z}[\pi, \bar{\pi}])$ , say that it *holds in  $\mathcal{O}$*  if the product  $\alpha_1 \cdots \alpha_k$  is trivial in  $\mathfrak{C}(\mathcal{O})$  through the map of the above lemma, and that it *holds in  $\mathcal{A}$*  if the corresponding isogeny chain  $\phi_{\alpha_1} \circ \cdots \circ \phi_{\alpha_k}$  maps  $\mathcal{A}$  to an isomorphic abelian variety. By Theorem 2.4, if every relation that holds in  $\mathcal{O}$  also does in  $\mathcal{A}$ , the group  $\mathfrak{C}'(\text{End}(\mathcal{A}))$  must be a quotient of  $\mathfrak{C}'(\mathcal{O})$ , which is almost always equivalent to  $\mathcal{O} \subset \text{End}(\mathcal{A})$  as we will see in Section 6.2.

The computation of class groups of algebraic orders is a classical topic that has led to the development of fast algorithms for generating ideal relations. However, our requirement that corresponding isogenies be efficiently computable places two additional constraints:

- Elements  $(\alpha_i)$  of our relations must correspond to maximal isotropic isogenies.
- Their number  $k$  and norms  $(N_{K/\mathbb{Q}}(\alpha_i))$  must be bounded.

The latter constraint is already addressed in [1, §6] whose results and proofs carry directly over to arbitrary dimension; we now explain how to additionally satisfy the former.

Let  $\Phi$  be a type for  $K$ , that is, a set of representatives for embeddings of  $K$  into its normal closure  $K^c$  up to complex conjugation. Its *type norm*

$$N_{\Phi} : x \longmapsto \prod_{\phi \in \Phi} \phi(x)$$

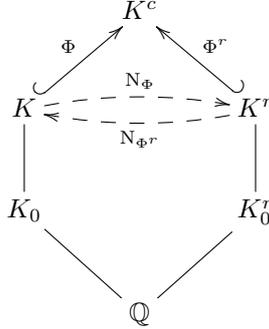


Figure 2: The complex multiplication field, its reflex field, and type norm maps.

maps  $K$  to its reflex field  $K^r$ , the fixed field of  $\{\sigma \in \text{Gal}(K^c/\mathbb{Q}) : \sigma\Phi = \Phi\}$ , and induces a morphism taking ideals  $\mathfrak{a}$  of  $K$  to elements  $(N_{\Phi}(\mathfrak{a}), N_{K/\mathbb{Q}}(\mathfrak{a}))$  of  $\mathfrak{C}'(\mathcal{O}^r)$  for any order  $\mathcal{O}^r$  of  $K^r$  with discriminant coprime to  $\nu$ . Types of absolutely simple abelian varieties are primitive, which implies that  $K^{rr} = K$ ; hence the type norm of the reflex type  $\Phi^r$ , the restriction to  $K^r$  of inverses of automorphisms of  $K^c$  induced by  $\Phi$ , or *reflex type norm*, maps ideals of  $K^r$  to  $\mathfrak{C}'(\mathcal{O})$  for any order  $\mathcal{O}$  containing  $\mathbb{Z}[\pi, \bar{\pi}]$ . See Figure 2.

The image of  $N_{\Phi^r}$  in  $\mathfrak{C}'(\mathcal{O})$  only contains elements for which the corresponding isogenies can be computed via Proposition 4.1. Therefore, to generate relations of  $\mathcal{O}$  as efficiently as evaluating the corresponding isogeny chains, we first generate tuples of ideals  $(\mathfrak{a}_i)$  whose product is principal in  $\mathcal{O}$  using the method of Buchmann [8] as modified in [1, §6], and then use the relation  $(N_{\Phi^r} N_{\Phi}(\mathfrak{a}_i))$ , whose total norm is  $\sum N_{K/\mathbb{Q}}(\mathfrak{a}_i)^{g^2}$ . Formally, this gives:

**Algorithm 5.2.**

INPUT: An order  $\mathcal{O}$  and a parameter  $\gamma > 0$ .

OUTPUT: A relation holding in  $\mathcal{O}$  whose associated isogeny can be computed efficiently.

1. Form the set  $\mathfrak{B}$  of prime ideals  $\mathfrak{p}$  of  $\mathcal{O}$  with norm less than  $N = L(\Delta)^\gamma$ .
2. Draw a vector  $x \in \mathbb{Z}^{\mathfrak{B}}$  uniformly at random with coordinates  $|x_{\mathfrak{p}}| < \log(\Delta)^{4+\epsilon}$  when  $N_{K/\mathbb{Q}}(\mathfrak{p}) < \log(\Delta)^{2+\epsilon}$  and  $x_{\mathfrak{p}} = 0$  otherwise.
3. Compute the reduced ideal representative  $\mathfrak{a}$  of  $\prod \mathfrak{p}^{x_{\mathfrak{p}}}$ .
4. If  $\mathfrak{a}$  factors over  $\mathfrak{B}$  as  $\prod \mathfrak{p}^{y_{\mathfrak{p}}}$ :
5. Return the relation containing  $N_{\Phi^r}(N_{\Phi}(\mathfrak{p}))$  with multiplicity  $x_{\mathfrak{p}} - y_{\mathfrak{p}}$  for  $\mathfrak{p} \in \mathfrak{B}$ .
6. Go back to Step 2.

For details on Step 4 (and more generally on computing ideal relations in number fields), we refer to [9]. From [8, Theorem 3.1], we obtain:

**Proposition 5.3.** *Assuming that reduced ideals are as smooth as random integers, this algorithm generates a relation with total norm  $L(\Delta)^{g^2\gamma+o(1)}$  in expected time  $L(\Delta)^{\gamma+o(1)} + L(\Delta)^{1/(4\gamma)+o(1)}$ .*

The relations we so obtain form only a sublattice of all relations of  $\mathfrak{C}'(\mathcal{O})$ ; nevertheless, Section 6.2 will show that they suffice to uniquely characterize  $\mathcal{O}$

from other orders containing  $\mathbb{Z}[\pi, \bar{\pi}]$  except locally at small primes and except for a zero-density set of Weil numbers  $\pi$ . Similarly to [1, §6], one can prove that those relations are quasi-uniformly distributed in this sublattice, so that  $\log(q)$  of them suffice to identify  $\mathcal{O}$  with error probability at most  $1/q$ .

To balance the cost of Algorithm 5.2 with that of evaluating corresponding isogenies via Proposition 4.1, we set  $\gamma = 1/(2g\sqrt{3})$ . The proof of Proposition 3.1 can now be concluded with the following algorithm.

**Algorithm 5.4.**

- INPUT: *An absolutely simple, ordinary, principally polarized abelian variety  $\mathcal{A}$  of dimension  $g$  defined over  $\mathbb{F}_q$  and an order  $\mathcal{O}$  containing  $\mathbb{Z}[\pi, \bar{\pi}]$ .*
- OUTPUT: *Whether  $\mathcal{O} \subset \text{End}(\mathcal{A})$ .*
1. *Repeat  $\log(q)$  times:*
  2. *Find a relation  $(\alpha_1, \dots, \alpha_k)$  of  $\mathfrak{C}(\mathcal{O})$  using Algorithm 5.2.*
  3. *If  $\phi_{\alpha_1} \circ \dots \circ \phi_{\alpha_k}$  does not map  $\mathcal{A}$  to an isomorphic variety, return false.*
  4. *Return whether  $\mathcal{O} \subset \text{End}(\mathcal{A})$  locally at small primes (see next section).*

**Note.** Rather than generating independent relations for each order  $\mathcal{O}$  of the lattice to be tested, one might be tempted to first compute the full class group structure of the maximal order  $\mathcal{O}_K$  and then deduce relations of smaller orders  $\mathcal{O}$  via the exact sequence:

$$1 \rightarrow \mathcal{O}^\times \rightarrow \mathcal{O}_K^\times \rightarrow (\mathcal{O}_K/\mathfrak{f})^\times / (\mathcal{O}/\mathfrak{f})^\times \rightarrow \text{Pic}(\mathcal{O}) \rightarrow \text{Pic}(\mathcal{O}_K) \rightarrow 1$$

where  $\mathfrak{f}$  is the conductor of  $\mathcal{O}$ , that is, the largest ideal of both  $\mathcal{O}$  and  $\mathcal{O}_K$ . This has two disadvantages: first, computing class groups is much more expensive than generating just  $\log(q)$  relations; second, the relations of  $\mathcal{O}$  given directly by the exact sequence above grow linearly in the index  $[\mathcal{O}_K : \mathcal{O}]$ , and deriving subexponential-size relations requires using an algorithm similar to 5.2 anyway.

## 6 Assumptions and Worst Cases

Throughout this paper, we have made the following assumptions:

- (1) *Theorem 2.4 holds for non-maximal orders.* (Section 2)
- (2) *Orders directly above a given one can be enumerated in subexponential time.* (Section 3)
- (3) *Isogenies  $\mathcal{A} \rightarrow \mathcal{A}/\mathfrak{a}$  can effectively be evaluated over the base field.* (Section 4)
- (4) *No two orders have the same polarized class group structure.* (Section 5)
- (5) *Reduced ideals are as likely to be smooth as integers of comparable size.* (Section 5)

We have seen in Section 4 that Assumption (3) is satisfied when  $g = 2$ , and we restrict to this case. Assumptions (1) and (5) are well-established heuristics which we gladly accept. Assumptions (2) and (4) do not hold in general but we will now show that they do outside of a zero-density set of abelian varieties  $\mathcal{A}/\mathbb{F}_q$  of fixed genus  $g$ , as  $q$  goes to infinity.

## 6.1 Enumerating orders

The lattice of orders containing  $\mathbb{Z}[\pi, \bar{\pi}]$  typically consists entirely of orders that are either minimal or maximal locally at large primes  $\ell$ ; indeed, integers  $v = [\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]$  are not likely to be divisible by squares of large primes. More precisely, for any  $\tau > 0$ , we have

$$\#\{v \in \{1, \dots, n\} : \exists \ell \in \mathcal{P}_{>L(n)^\tau, \ell^2|v}\} \leq \sum_{\ell \in \mathcal{P}_{>L(n)^\tau}} \frac{n}{\ell^2} \leq \frac{n}{L(n)^\tau},$$

which is negligible compared to  $n$  as it goes to infinity; therefore, assuming that  $v$  has similar divisibility properties to random integers less than  $n = 2^{g(2g-1)}q^{g^2/2}$  (as per Lemma 3.2), only a zero-density set of abelian varieties of dimension  $g$  over  $\mathbb{F}_q$  have lattices of orders that, locally at some prime  $\ell > L(n)^\tau$ , have height greater than 1.

Discarding that set, there is only one order directly above (resp. below) any given one locally at large primes  $\ell$ , and they can be found using a Gröbner basis algorithm [2, §III.2.3] in time subexponential in  $\log(q)$ . Locally at primes  $\ell \leq L(n)^\tau$ , we resort to the much more direct method of enumerating all subgroups of  $\frac{1}{\ell}\mathcal{O}/\mathcal{O}$  and selecting those which are orders; this takes time polynomial in  $\ell$ , that is, subexponential in  $\log(q)$ , and we select  $\tau$  small enough so that this complexity is negligible compared to our overall complexity bound.

## 6.2 Orders with identical class group structure

To compute endomorphism rings locally at small primes  $\ell$ , we rely on the direct method of Eisenträger and Lauter [13, §6.5], which uses  $\ell^{2gv+o(1)}$  operations in the base field, where  $v$  is the valuation of  $[\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]$  at  $\ell$ . As above, to ensure that this cost is negligible relative to our overall complexity bound, we make  $\tau > 0$  small enough and omit the zero-density set of abelian varieties for which this index is divisible by a power greater than  $L(q)^\tau$  of a prime less than  $L(q)^\tau$ .

Consequently, we only need to show that the set of relations generated by Algorithm 5.2 (that is, the image through the map  $N_{\Phi^r} N_\Phi$  of the set  $p_{\mathcal{O}}$  of ideals of  $\mathbb{Z}[\pi, \bar{\pi}]$  that are principal in  $\mathcal{O}$ ) discriminates  $\mathcal{O}$  from other orders of the lattice locally at every prime  $\ell > L(q)^\tau$ , and we may assume that such primes  $\ell$  only divide the index  $[\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]$  with multiplicity 1. To establish this, let  $\mathcal{O}'$  be another order containing  $\mathbb{Z}[\pi, \bar{\pi}]$  such that  $N_{\Phi^r} N_\Phi(p_{\mathcal{O}}) \subset P_{\mathcal{O}'}$  where  $P_{\mathcal{O}'}$  is as in Definition 2.3. From [26, Lemma 1.8.4], we have the identity

$$N_{\Phi^r} N_\Phi(\mathfrak{a}) = N_{K/\mathbb{Q}}(\mathfrak{a})\mathfrak{a}/\bar{\mathfrak{a}}$$

from which it follows that the square of any element  $(\mathfrak{a}, \alpha) \in P_{\mathcal{O}}$  is principal if and only if  $N_{\Phi^r} N_\Phi(\mathfrak{a})$  is. Therefore,  $N_{\Phi^r} N_\Phi(p_{\mathcal{O}}) \subset P_{\mathcal{O}'}$  implies  $P_{\mathcal{O}}^2 \subset P_{\mathcal{O}'}$  and hence

$$\ker(\mathfrak{C}(\mathcal{O}^\circ) \rightarrow \mathfrak{C}(\mathcal{O}))^2 \subset \ker(\mathfrak{C}(\mathcal{O}^\circ) \rightarrow \mathfrak{C}(\mathcal{O}'))$$

where  $\mathcal{O}^\circ = \mathcal{O} \cap \mathcal{O}'$ . Since, locally at all primes  $\ell > L(q)^\tau$ , either  $\mathcal{O} = \mathcal{O}'$  or one of them is maximal, we may apply [4, Theorem 5.1] which establishes that  $\mathcal{O} \subset \mathcal{O}'$  except possibly if  $\ell$  divides  $M \cdot N_{K_0/\mathbb{Q}} \text{disc}(K/K_0)$  where  $M$  is a fixed integer. We thus discard yet another zero-density set of abelian varieties, namely those for which  $M \cdot N_{K_0/\mathbb{Q}} \text{disc}(K/K_0)$  and  $[\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]$  have a common prime factor greater than  $L(q)^\tau$ . See [4] for details.

### 6.3 Certifying the result

As an aside, let us describe how one may certify the output endomorphism ring  $\mathcal{O}$  under Assumption (1), using relations that discriminate  $\mathcal{O}$  from other orders of the lattice.

**Definition 6.1.** *A certificate for an order  $\mathcal{O}$  consists of:*

- a family of orders  $\mathcal{O}_i$  and relations  $r_i$  that hold in  $\mathcal{O}_i$  but not in  $\mathcal{O}$ ,
- a family of orders  $\mathcal{O}_j$  and relations  $r_j$  that hold in  $\mathcal{O}$  but not in  $\mathcal{O}_j$ ,

*such that  $\mathcal{O}$  is the only order containing  $\mathbb{Z}[\pi, \bar{\pi}]$  satisfying  $\mathcal{O}_i \not\subseteq \mathcal{O}$  and  $\mathcal{O}_j \not\supseteq \mathcal{O}$  for all  $i$  and  $j$ .*

As a direct consequence of Theorem 2.4, the endomorphism ring of an abelian variety  $\mathcal{A}$  with Frobenius endomorphism  $\pi$  is  $\mathcal{O}$  if and only if the isogenies corresponding to the  $r_j$ 's map  $\mathcal{A}$  to isomorphic varieties while those corresponding to the  $r_i$ 's do not. In practice, the  $\mathcal{O}_i$ 's can be chosen to be all orders considered in Step 3 of Algorithm 3.3 found not to be contained in  $\mathcal{O} = \text{End}(\mathcal{A})$  and the  $\mathcal{O}_j$ 's to be all orders directly below  $\mathcal{O}$ .

When two orders  $\mathcal{O}$  and  $\mathcal{O}'$  cannot be distinguished using relations, the same technique can be used except locally at prime factors of  $[\mathcal{O} + \mathcal{O}' : \mathcal{O} \cap \mathcal{O}']$ ; the verification process then takes on the additional burden of verifying the endomorphism ring locally at those primes. Since they are almost always small, the associated cost is asymptotically negligible; therefore, by Propositions 4.1 and 5.3, it takes  $L(q)^{g\gamma+o(1)} + L(q)^{g/(4\gamma)+o(1)}$  time to generate a certificate that can subsequently be verified in  $L(q)^{3g^3\gamma+o(1)}$  operations, for any  $\gamma > 0$ .

## 7 Practical Computations

We give two examples illustrating different patterns for the index  $v = [\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]]$ . Previous algorithms [13, 29] compute endomorphism rings efficiently when  $\mathcal{A}[\ell^n]$  remains defined over small extension fields as  $\ell^n$  ranges through prime-power factors of  $v$ , while ours performs well as soon as no order directly above  $\mathbb{Z}[\pi, \bar{\pi}]$  has an overly large discriminant.

Computations reported here were performed by a straightforward Magma [6] implementation using the AVIsogenies library [3] and running on one Intel i7-2620M core.

### 7.1 Example with nearly prime $v$

Let us first consider a very favorable case where  $v$  is both large and nearly prime, that of the Jacobian variety  $\mathcal{A}$  of the hyperelliptic curve with equation

$$y^2 = x^5 + 523747x^4 + 306186x^3 + 744660x^2 + 415524x + 261884$$

over the field with  $q = 1250407$  elements; its Frobenius endomorphism  $\pi$  admits the characteristic polynomial  $z^4 + 1251z^3 + 1772074z^2 + 1251qz + q^2$  from which one can derive that  $\mathbb{Z}[\pi, \bar{\pi}]$  is an order of index  $v = 2 \cdot 538259$  in the ring of integers of  $K = \mathbb{Q}(\pi)$ .

We start by computing  $\text{End}(\mathcal{A})$  locally at 2, that is, determining whether it contains the order in which  $\mathbb{Z}[\pi, \bar{\pi}]$  has index 2; this order is generated by  $\pi$  and  $\alpha/(2q)$  where

$$\alpha = 417q + 1346084914086\pi + 497115559392\pi^2 + \pi^3.$$

To determine whether  $\alpha/(2q)$  belongs to  $\text{End}(\mathcal{A})$  or, equivalently, whether  $\alpha/2$  does (as  $q$  is coprime to  $v$ ), we use the method of Eisenträger and Lauter [13]: it takes 102ms to determine that  $\alpha$  kills the full 2-torsion of  $\mathcal{A}$ , which establishes that  $\text{End}(\mathcal{A})$  is locally maximal at 2.

Now denote by  $\mathfrak{p}\bar{\mathfrak{p}}$  the factorization of 7 in  $\mathbb{Z}[\pi, \bar{\pi}]$  and observe that  $\mathfrak{p}$  is principal in  $\mathcal{O}_K$ . We evaluate the corresponding isogeny, spending 10.9s to find its kernel and 1.37s to identify the isogenous variety; since it is not isomorphic to  $\mathcal{A}$  we have established, in just 12.3s, that

$$\text{End}(\mathcal{A}) \simeq \mathbb{Z}[\pi, \alpha/(2q)].$$

This computation is clearly intractable using previous algorithms: the full 538259-torsion of  $\mathcal{A}$  is defined over an extension of degree  $e = 869166638466$ , so it would require a rough minimum of  $\log(q^e) \log(q^{e^g}) \approx 2^{90}$  operations just to find a random 538259-torsion point.

## 7.2 Example with composite $v$

For a less degenerate case, let  $\mathcal{A}$  be the Jacobian variety of the curve with equation

$$y^2 = x^5 + 800x^4 + 2471x^3 + 6695x^2 + 1082x + 7062$$

over the field with  $q = 7681$  elements. It takes just 60ms to compute that the characteristic polynomial of its Frobenius endomorphism is  $z^4 + 114z^3 + 7566z^2 + 114qz + q^2$  from which it takes negligible time to derive that  $\mathbb{Z}[\pi, \bar{\pi}]$  has index  $2^2 \cdot 47^2 \cdot 379$  in  $\mathcal{O}_K$ .

Again, we start by computing the endomorphism ring locally at 2 using the method of Eisenträger and Lauter [13]. Only 75ms are needed to find a basis for the full 2-torsion (the 4-torsion is not needed) and evaluate the relevant endomorphism on it; this determined that  $\text{End}(\mathcal{A})$  contains the order  $\mathcal{O}_2 = \mathbb{Z}[\pi, \bar{\pi}] + 47^2 \cdot 379 \cdot \mathcal{O}_K$ . Having established that, we may start Algorithm 3.3 from the order  $\mathcal{O}_2$  instead of  $\mathbb{Z}[\pi, \bar{\pi}]$ ; the two orders directly above  $\mathcal{O}_2$  have index 379 and  $47^2$  in  $\mathcal{O}_K$ .

First consider that of index  $47^2$ : in just 100ms we find that ideals of norm  $3^2$  have order 92 in its class group. Computing the 92 corresponding isogenies takes 37s, that is, 400ms on average. As the isogenous variety is not isomorphic to  $\mathcal{A}$ , we deduce that  $\text{End}(\mathcal{A})$  is minimal locally at 47.

Next we consider the order with index 379; after 150ms, we find that the ideal  $\mathfrak{p}^{62}(\mathfrak{r}\mathfrak{s})^2$  is principal in it, where the primes appear in the splittings  $3 = \mathfrak{p}\bar{\mathfrak{p}}$  and  $19 = \mathfrak{r}\mathfrak{s}\bar{\mathfrak{r}}\bar{\mathfrak{s}}$ . We therefore proceed to test whether the corresponding relation holds in  $\mathcal{A}$ : it takes 67s on average to compute each of the two 19-isogenies, and 400ms for each of the 3-isogenies. The isogenous variety, which is determined after a total of 157s, is not found to be isomorphic to  $\mathcal{A}$ , hence we deduce that  $\text{End}(\mathcal{A})$  is the order containing  $\mathbb{Z}[\pi, \bar{\pi}]$  with index 4.

Note that the full 47-torsion and full 379-torsion live over extensions of degree 34592 and 13609890 respectively, which again makes computing  $\text{End}(\mathcal{A})$  using previous methods quite expensive.

This illustrates that, even when the orders in which we look for relations have moderate class numbers, the bottleneck of our algorithm remains the evaluation of isogenies. Accordingly, in both computations above, we have used a simple baby-step giant-step method in place of Algorithm 5.2, which allowed us to find much smaller relations and therefore to better balance the cost of evaluating isogenies with that of searching for relations.

Overall, we find that our algorithm clearly outperforms previous methods as soon as the index  $[\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]]$  has prime power factors  $\ell^n$  for which the torsion points live over significant extensions of the base field, although those methods are still very useful to compute the endomorphism ring locally at small primes.

## Acknowledgments

This work would never have seen the light of day without the author’s prior collaborations with Andrew V. Sutherland, constant encouragements from Pier-ric Gaudry, and invaluable discussions with Andreas Enge, Igor Shparlinski, and Marco Streng.

## References

- [1] Gaetan BISSON. “Computing endomorphism rings of elliptic curves under the GRH.” In: *Journal of Mathematical Cryptology*. 5.2 (2011), pages 101–113. DOI: 10.1515/JMC.2011.008.
- [2] Gaetan BISSON. “Endomorphism Rings in Cryptography.” PhD thesis. Eindhoven University of Technology and Institut National Polytechnique de Lorraine, 2011. ISBN: 90-386-2519-7.
- [3] Gaetan BISSON, Romain COSSET, and Damien ROBERT. *AVIsogenies*. A library for computing isogenies between abelian varieties. 2010. URL: <http://avisogenies.gforge.inria.fr/>.
- [4] Gaetan BISSON and Marco STRENG. “On polarized class groups of orders in quartic CM fields.” In preparation.
- [5] Gaetan BISSON and Andrew V. SUTHERLAND. “Computing the endomorphism ring of an ordinary elliptic curve over a finite field.” In: *Journal of Number Theory* 131.5 (2011): *Elliptic Curve Cryptography*. Edited by Neal KOBLITZ and Victor S. MILLER, pages 815–831. DOI: 10.1016/j.jnt.2009.11.003.
- [6] Wieb BOSMA, John CANNON, and Catherine PLAYOUST. “The Magma algebra system: the user language.” In: *Journal of Symbolic Computation* 24.3–4 (1997), pages 235–265. DOI: 10.1006/jsc.1996.0125.
- [7] Reinier BRÖKER, David GRUENEWALD, and Kristin LAUTER. “Explicit CM theory for level 2-structures on abelian surfaces.” In: *Algebra & Number Theory* 5.4 (2011), pages 495–528. DOI: 10.2140/ant.2011.5.495.

- [8] Johannes BUCHMANN. “A subexponential algorithm for the determination of class groups and regulators of algebraic number fields.” In: *Séminaire de Théorie des Nombres, Paris*. Edited by Catherine GOLDSTEIN. Volume 91. Progress in Mathematics. Birkhäuser, 1989, pages 27–41.
- [9] Henri COHEN, Francisco DIAZ Y DIAZ, and Michel OLIVIER. “Subexponential algorithms for class group and unit computations.” In: *Journal of Symbolic Computation* 24.3–4 (1997): *Special issue on computational algebra and number theory: proceedings of the first MAGMA conference*, pages 433–441. DOI: 10.1006/jscs.1996.0143.
- [10] Gary CORNELL and Joseph H. SILVERMAN, editors. *Arithmetic Geometry*. Springer, 1986. ISBN: 3-540-96311-1.
- [11] Romain COSSET and Damien ROBERT. *Computing  $(\ell, \ell)$ -isogenies in polynomial time on Jacobians of genus 2 curves*. 2011. IACR ePrint: 2011/143.
- [12] Jean-Marc COUVEIGNES. “Linearizing torsion classes in the Picard group of algebraic curves over finite fields.” In: *Journal of Algebra* 321.8 (2009), pages 2085–2118. DOI: 10.1016/j.jalgebra.2008.09.032.
- [13] Kirsten EISENTRÄGER and Kristin E. LAUTER. “A CRT algorithm for constructing genus 2 curves over finite fields.” In: *Arithmetic, Geometry and Coding Theory — AGCT 2010*. Edited by François RODIER and Serge VLADUT. Volume 21. Séminaires et Congrès. Société Mathématique de France, 2009, pages 161–176.
- [14] Mireille FOUQUET and François MORAIN. “Isogeny volcanoes and the SEA algorithm.” In: *Algorithmic Number Theory — ANTS-V*. Edited by Claus FIEKER and David R. KOHEL. Volume 2369. Lecture Notes in Computer Science. Springer, 2002, pages 47–62. DOI: 10.1007/3-540-45455-1\_23.
- [15] David M. FREEMAN and Kristin E. LAUTER. “Computing endomorphism rings of Jacobians of genus 2 curves over finite fields.” In: *Algebraic Geometry and its Applications — SAGA 2007*. Edited by Jean CHAUMINE, James HIRSCHFELD, and Robert ROLLAND. Volume 5. Number Theory and Its Applications. World Scientific, 2007, pages 29–66. DOI: 10.1142/9789812793430\_0002.
- [16] Steven D. GALBRAITH. “Constructing isogenies between elliptic curves over finite fields.” In: *London Mathematical Society Journal of Computation and Mathematics* 2 (1999), pages 118–138. DOI: 10.1112/S1461157000000097.
- [17] David R. KOHEL. “Endomorphism rings of elliptic curves over finite fields.” PhD thesis. University of California at Berkeley, 1996. URL: <http://echidna.maths.usyd.edu.au/kohel/pub/thesis.pdf>.
- [18] Kristin LAUTER and Damien ROBERT. “Improved CRT algorithm for class polynomials in genus 2.” In: *Algorithmic Number Theory — ANTS-X*. Edited by Everett HOWE and Kiran KEDLAYA. Mathematical Science Publishers, 2012. Forthcoming.
- [19] Arjen K. LENSTRA and Hendrik W. LENSTRA, editors. *The Development of the Number Field Sieve*. Volume 1554. Lecture Notes in Mathematics. Springer, 1993. ISBN: 3-540-57013-4.
- [20] Hendrik W. LENSTRA and Carl POMERANCE. “A rigorous time bound for factoring integers.” In: *Journal of the American Mathematical Society* 5.3 (1992), pages 483–516. DOI: 10.1090/S0894-0347-1992-1137100-0.

- [21] Reynald LERCIER and Christophe RITZENTHALER. “Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects.” In: *Journal of Algebra* (2012). Forthcoming.
- [22] David LUBICZ and Damien ROBERT. *Computing isogenies between abelian varieties*. 2009. arXiv.org: 1001.2016.
- [23] Jean-François MESTRE. “Construction de courbes de genre 2 à partir de leurs modules.” In: *Effective methods in algebraic geometry — MEGA 1990*. Edited by Teo MORA and Carlo TRAVERSO. Volume 94. Progress in Mathematics. Birkhäuser, 1991, pages 313–334.
- [24] Jonathan PILA. “Frobenius maps of abelian varieties and finding roots of unity in finite fields.” In: *Mathematics of Computation* 55.192 (1990), pages 745–763. DOI: 10.1090/S0025-5718-1990-1035941-X.
- [25] Goro SHIMURA and Yutaka TANIYAMA. *Complex multiplication of abelian varieties and its applications to number theory*. Volume 6. Publications of the Mathematical Society of Japan. The Mathematical Society of Japan, 1961.
- [26] Marco STRENG. “Complex multiplication of abelian surfaces.” PhD thesis. Universiteit Leiden, 2010. ISBN: 90-5335-291-0. URL: <http://www.math.leidenuniv.nl/~streng/thesis.pdf>.
- [27] Andrew V. SUTHERLAND. “Computing Hilbert class polynomials with the Chinese remainder theorem.” In: *Mathematics of Computation* 80.273 (2011), pages 501–538. DOI: 10.1090/S0025-5718-2010-02373-7.
- [28] John TATE. “Endomorphisms of abelian varieties over finite fields.” In: *Inventiones mathematicae* 2.2 (1966), pages 134–144. DOI: 10.1007/BF01404549.
- [29] Markus WAGNER. “Über Korrespondenzen zwischen algebraischen Funktionenkörpern.” PhD thesis. Technische Universität Berlin, 2009. URL: <http://www.math.tu-berlin.de/~wagner/Diss.pdf>.
- [30] William C. WATERHOUSE. “Abelian varieties over finite fields.” In: *Annales Scientifiques de l’École Normale Supérieure* 2.4 (1969), pages 521–560.