Spanning the isogeny class of a power of an elliptic curve.

Markus Kirschmer, Fabien Narbonne, Christophe Ritzenthaler, Damien Robert

SPANNING THE ISOGENY CLASS OF A POWER OF AN ELLIPTIC CURVE

MARKUS KIRSCHMER, FABIEN NARBONNE, CHRISTOPHE RITZENTHALER, AND DAMIEN ROBERT

Abstract. Let E be an ordinary elliptic curve over a finite field and g be a positive integer. Under some technical assumptions, we give an algorithm to span the isomorphism classes of principally polarized abelian varieties in the isogeny class of E^g. The varieties are first described as hermitian lattices over (not necessarily maximal) quadratic orders and then geometrically in terms of their algebraic theta null point. We also show how to algebraically compute Siegel modular forms of even weight given as polynomials in the theta constants by a careful choice of an affine lift of the theta null point. We then use these results to give an algebraic computation of Serre's obstruction for principally polarized abelian threefolds isogenous to E^3 and of the Igusa modular form in dimension 4. We illustrate our algorithms with examples of curves with many rational points over finite fields.

Contents

1. Introduction 1
2. Hermitian lattices 5
2.1. Basic definitions and notations 5
2.2. Enumeration of positive definite unimodular hermitian lattices 7
2.3. Orthogonal families inside a lattice 11
3. The description of polarized abelian varieties in terms of lattices 15
3.1. The equivalence of categories 15
3.2. Polarizations 16
3.3. Description of the abelian variety as a quotient of E^g 18
4. Theta structures and a modular interpretation of the isogeny formula 20
4.1. Input for the isogeny formula over k 20
4.2. The isogeny formula on the universal abelian scheme 21
4.3. Modular interpretation 23
4.4. An algebraic version of Thomae's formula 26
4.5. Computing a Siegel modular form on the isogenous variety 29
5. Application to defect-0 curves of genus at most 4 30
5.1. Curves of genus 2 31
5.2. Curves of genus 3 32
5.3. Curves of genus 4 33
References 34

1. Introduction

Let $g, m \geq 1$ be integers, p be a prime, $q = p^m$ and $\mathscr{W}$ be the isogeny class of a given dimension-g abelian variety A over $\mathbb{F}_q$. The elements of $\mathscr{W}$ will be the $\mathbb{F}_q$-isomorphism classes of abelian varieties over $\mathbb{F}_q$ which are $\mathbb{F}_q$-isogenous to A. Thanks to the work of Tate [Tat66] and Honda [Hon68], one knows that the Weil polynomial W is an invariant on $\mathscr{W}$. One can also characterize the finite list $S(q, g)$ of possible

Date: April 2020.
2010 *Mathematics Subject Classification.* 14H42,14G15, 14H45, 16H20.
Key words and phrases. hermitian lattice, order in quadratic field, isogeny class, polarization, curves with many points over finite fields, Siegel modular form, theta constant, theta null point, algorithm, Igusa modular form, Serre's obstruction, Schottky locus.

Weil polynomials for given q and g. These finite lists have been made explicit up to genus 5 [Hal10; HS12; Hay19]. Representing now an isogeny class $\mathscr{W}$ by a polynomial $W \in S(q,g)$, a harder task is to describe the finite set of elements (i.e. $\mathbb{F}_q$-isomorphism classes of abelian varieties) inside $\mathscr{W}$. Currently, there is no unified nor complete way to achieve this task. To our best knowledge, one can get a full abstract description

(1) for $g = 1$ [Wat69];
(2) for ordinary abelian varieties [Del69; Ser85; How95; Mar19; JKP+18];
(3) for abelian varieties $A \sim E^g$ where E is a supersingular elliptic curve either over $\mathbb{F}_p$ or over $\mathbb{F}_{p^2}$ with trace $\pm 2p$; [JKP+18];
(4) when $q = p$ and W has no real root [CS15];
(5) for p-rank $g-1$ simple abelian varieties over fields of odd characteristics [OS19].

Roughly speaking, the above descriptions functorially relate $\mathbb{F}_q$-isomorphism classes of (non-polarized) abelian varieties in $\mathscr{W}$ and certain finitely generated modules over orders in products of number fields or quaternion algebras. Notice that even for $g = 2$, the situation is still incomplete as far as we know: there are only partial results for supersingular and superspecial abelian surfaces [IKO86; XYY19; HNR09] and p-rank 1 split isogeny classes seem untouched.

The situation is even more critical if one is interested in $\mathbb{F}_q$-isomorphism classes of *polarized* abelian varieties in $\mathscr{W}$. Since the distinction is important for one of our goal (identifying Jacobians in the isogeny class), we denote the $\mathbb{F}_q$-isomorphism classes of principally polarized abelian varieties isogenous to A by $\mathscr{W}_1$. Notice that there is no inclusion between the elements of $\mathscr{W}$ and $\mathscr{W}_1$ since the notions of isomorphism classes are distinct. When the abelian varieties in $\mathscr{W}$ are isogenous to products of non-isogenous ordinary simple abelian varieties, there are algorithms to enumerate the elements of $\mathscr{W}$ or $\mathscr{W}_1$ (see [Mar19]). The LMFDB database is currently keeping track of the cardinality of these sets for small values of g and q [DKR+20].

In the present article, we consider a different case, namely $\mathscr{W}$ is the isogeny class of the g-th power of an ordinary elliptic curve $E/\mathbb{F}_q$. Let π be the Frobenius endomorphism of E and $R = \mathbb{Z}[\pi, q/\pi] = \mathbb{Z}[\pi]$. The set S_E of $\mathbb{F}_q$-isomorphism classes of elliptic curves $\{E_1, \dots, E_r\}$ isogenous to E is in bijection with the ideal class monoid $\mathrm{ICM}(R)$ of R and equations for the E_i can be computed. Moreover it is always possible to identify one elliptic curve isogenous to E with minimal endomorphism ring, i.e. equal to R. We will assume from now on that this is our curve E. The functor given in [JKP+18] which associates to any $A \in \mathscr{W}$ the finitely generated torsion-free R-module (or in short R-lattice) $\mathrm{Hom}(A, E)$ of rank g is an equivalence of categories and provides an inverse denoted $\mathscr{F}_E$. Note that this functor is distinct from the one used for instance in [Mar19] (it is contravariant and exact) and there is no easy way to compare them away from projective R-modules. But both functors lead to the conclusion that the elements in $\mathscr{W}$ are represented by products of elliptic curves $E_1, \dots, E_g$ in S_E corresponding to a sequence of orders $R \subset \mathrm{End}(E_1) \subset \dots \subset \mathrm{End}(E_g)$ and invertible $\mathrm{End}(E_i)$-ideal classes I_i with a given fixed product $I_1 \cdots I_g$ in $\mathrm{ICM}(R)$ (see [Kan11, Th.1], [Mar19], [JKP+18, Th.3.2]).

If we are interested in $\mathbb{F}_q$-isomorphisms classes of polarized abelian varieties, we need to translate the notion of polarization in the category of R-lattices through the functor $\mathrm{Hom}(A, E)$. We show in Theorem 3.3 and Corollary 3.6 that this can indeed be done: the elements in $\mathscr{W}_1$ are in correspondence with the unimodular positive definite hermitian R-lattice (L, h) of rank g (see Section 2.1 for a review on these notions for lattices). This result is no surprise to the specialists as it generalizes a similar result of Serre [Lau18, Appendix] when R is the maximal order in $\mathbb{Q}(\pi)$ and is analogue of the result of [How95; Mar19] using a different functor.

How to enumerate the lattices (L, h)? This is part of a broader and beautiful theory which has been developed for general orders in number fields or quaternion algebras. However, even in the case of imaginary quadratic orders, the algorithms have been mainly implemented in the case where R is a maximal order, cf. [Sch98; Kir19]. In Section 2.2, we recall some elements of this theory restricted to imaginary quadratic orders and show how to adapt our algorithms when R is not maximal. This generalization comes at the price of much slower algorithms which can be sped up if one restricts to lattices which are projective R-modules (or equivalently to abelian varieties which are products of elliptic curves with endomorphism rings isomorphic to R). While our method for enumerating projective R-modules is quite efficient, we believe that there is still lot of room for improvements in the general case.

Such descriptions, though powerful, do not allow to get a real grasp on a given polarized variety $(A, \mathscr{L})$. In particular, given an abstract description of an element in $\mathscr{W}_1$, one would like for instance to see if it is the Jacobian of a curve and if so, to give an equation of the curve. For this, we have to jump back to the algebraic geometry side and associate to the abstract description some data describing the embedding $\phi_{\mathscr{L}^i}$, $i \geq 3$, of A into a projective space $\mathbb{P}^N$. When $p \neq 2$, Mumford showed how to extend the classical theory over $\mathbb{C}$ by using an algebraic version of the theta constants, called a *theta null point*. These constants are projectively the image by $\phi_{\mathscr{L}^i}$ of $0 \in A$ for a careful choice of basis of $\mathbb{P}^N$. However, if this data is not available before hand for at least one principally polarized abelian variety in $\mathscr{W}_1$, the only known method to compute it is to work with a lift of A and its polarization to $\mathbb{C}$, perform analytic computations with enough precision, hopefully recognize algebraic numbers and eventually reduce the result over the finite field. When A is simple, this is the classical setting of the Complex Multiplication methods (see for instance [CFA+06, Chap.18]) but the output is heuristic when $g > 2$ [Sut11; Str14].

In our case, we will take advantage that it is easy to compute the theta null point on $A_0 = E^g \in \mathscr{W}_1$ with the product polarization $\mathscr{L}_0$. It boils down to computing the (projective) thetanull point on E. The formula for their fourth power is a particular case of Thomae's formula. We will give an elementary proof of this result and show that one can take arbitrary fourth roots (see Lemma 4.6 and Corollary 4.8). Doing so, we will also prepare for a 'modular version' of the thetanull point that we will need later and take great care of the constant involved.

We also show how to deduce from the lattice description (L, h) of $(A, \mathscr{L}) \in \mathscr{W}_1$ an isogeny $f : A_0 \to A$ such that $f^*\mathscr{L} = \mathscr{L}_0^\ell$ for a certain $\ell \geq 1$. This is achieved by looking for g orthogonal vectors of norm ℓ in $L^\#$ (a certain dual of L for h), see Section 2.3. We can then give f through an explicit maximal isotropic kernel K in $A_0[\ell]$, see Section 3.3. The explicit *isogeny formula* developed in [CR15] allows then to transport the thetanull point on $(A_0, \mathscr{L}_0)$ to the one on $(A, \mathscr{L})$. This leads to the following overview of our algorithm.

Algorithm 1 Overview of the full algorithm

Input: An integer $g > 1$ and the Weil polynomial W of an ordinary elliptic curve over $\mathbb{F}_q$ (with some technical restrictions, see the discussion below).

Output: The theta null points of all indecomposable principally polarized abelian varieties with Weil polynomial W^g.

1: Let $R = \mathbb{Z}[x]/(W)$ and compute an elliptic curve $E/\mathbb{F}_q$ such that $\mathrm{End}(E) = \mathbb{Z}[\pi] \simeq R$ (see Section 3.3).
2: Use Algorithm 2 (resp. 3) to get a list of all (resp. all projective) indecomposable unimodular positive definite hermitian R-lattices (L, h) up to isometry.
3: Apply Algorithm 6 to compute a maximal isotropic kernel K of an isogeny $f : E^g \to \mathscr{F}_E(L)$ for each (L, h).
4: **return** the output of Algorithm 7 on each $((E)_{i=1,\dots,g}, K)$.

In practice, there are restrictions on the W for which this algorithm is going to work because the current implementation of the isogeny formula imposes several constraints on the kernel K of f. We list them below from what would require the most work to the least to remove them. This should be taken with a grain of salt as it is of course impossible to predict possible obstacles without an actual study.

(1) it imposes p to be odd since the algorithm uses theta structures of even level;
(2) it imposes to look for f such that $f^*\mathscr{L} = \mathscr{L}_0^\ell$ for an integer $\ell > 0$, whereas the strategy would work with $f^*\mathscr{L}$ any completely decomposable polarization. Because of this, f does not always exist (see example 2.24). We give necessary and sufficient conditions for its existence in Theorem 2.16 (for instance, it does always exist is g is odd);
(3) it imposes ℓ to be coprime to $2p$, see remark 4.1. We work out in Section 2.3 a thorough local analysis of the lattices which gives a refinement of Theorem 2.16. For instance, when g is odd it is sufficient that the conductor of R is odd;
(4) even when ℓ is coprime to $2p$, we have to discard it when K is not isomorphic as a group to $(\mathbb{Z}/\ell\mathbb{Z})^g$. This does not happen when ℓ is square free. We did not try to get a proof of the existence of such a good ℓ and we pragmatically chose to test the group structure of a given kernel K until we get exactly this one.

The full cost of the algorithm is hard to estimate: it heavily depends on the smallest good ℓ one can find (when it exists) and it is an open question to find an upper bound in terms of R and g for the maximum of the minimal ℓ for a given $\mathscr{W}_1$. Once ℓ is given, a lower bound for the complexity is given by the one of Algorithm 7 which is $O(\ell^g)$. Be aware that this hides a large constant, since the computations have to be performed on the extension of $\mathbb{F}_q$ where all ℓ-torsion points of E are defined. Typically, the algorithm works for a given element of $\mathscr{W}_1$ in reasonable time when ℓ is smaller than 41 (resp. 19, resp. 7) for $g = 2$ (resp. 3, resp. 4). Then the full cost depends also on the cardinality of $\mathscr{W}_1$ which can be computed by [HK89b] for $g = 2$ and 3. When $R = \mathrm{End}(E)$ is maximal, a lower bound for this cardinality grows linearly in $(\mathrm{disc}(R))^{g^2/4}$ for fixed g.

The restrictions above artificially increase the smallest ℓ we would like to consider. We therefore urge the reader to consider Algorithm 1 as a proof of concept, allowing computations which were completely out of reach before for various classes $\mathscr{W}_1$ in dimension $2, 3$ and 4 with R maximal or not (see Section 5).

We finally move to one last new algorithmic result. In Section 4.3, we show how to evaluate a Siegel modular form χ of level $\mathrm{Sp}_{2g}(\mathbb{Z})$ and even weight[1] at a principally polarized abelian variety $(A, \mathscr{L})/\mathbb{F}_q$ when χ is defined as a homogeneous polynomial P in the theta constants with coefficients in $\mathbb{F}_q$. A Siegel modular form is a section of a power of the Hodge bundle on the universal abelian variety, so to give it a value only makes sense once a $\mathbb{F}_q$-rational basis of regular differentials on A is fixed. We show that choosing such a basis yields a particular affine lift of the theta null point on $(A, \mathscr{L})$ which we call a *modular lift* (see Definition 4.3). The coordinates of a modular lift are characterized, up to a common sign, by considering all products of two theta coordinates as Siegel modular forms of weight 1. Evaluating χ is then computing the value of P in the coordinates of the modular lift. We show that our affine version of the isogeny formula preserves the modular lift property (see Theorem 4.5). Since in our Thomae's formula for elliptic curves we took care of having such a modular lift, we can therefore carry it to $(A, \mathscr{L})$ through the isogeny (see Algorithm 8) and perform the computation of the modular form on $(A, \mathscr{L})$.

As an application and in order to illustrate our algorithms, we consider curves over $\mathbb{F}_q$ with many points. A curve C of genus $g \geq 1$ over $\mathbb{F}_q$ has at most $1 + q + g\lfloor 2\sqrt{q} \rfloor$ and when this bound is reached, we say that C is a *defect-0 curve*. The best upper bounds are known only for $g \leq 2$ and sparse families of g, q. If C is a defect-0 curve, then its Jacobian $\mathrm{Jac}\, C$ is isogenous to E^g where E has trace $-\lfloor 2\sqrt{q} \rfloor$. If E is ordinary (which is always the case for instance when $q = p^m$ with $m = 1$ or 3 and $q \neq 2, 3$ [Ser85, p. II.6.4]), we can try to find $\mathrm{Jac}\, C$ among the indecomposable principally polarized abelian varieties $(A, \mathscr{L})$ in the isogeny class of E^g.

When $g = 2$, each such $(A, \mathscr{L})$ is automatically the Jacobian of a defect-0 curve. It is therefore enough to know that an indecomposable principally polarized abelian surface isogenous to E^2 exists which can already be obtained on the lattice side of the picture using [Hof91] and [Ser85, Th.3.9.1]. Now, if one wants an equation of the curve, it can be provided using Algorithm 1.

When $g = 3$, although each $(A, \mathscr{L})$ is geometrically the Jacobian of a unique curve $C/\mathbb{F}_q$, there may be an obstruction, called *Serre's obstruction*, for C to have defect-0. Fortunately, the modular form χ_{18} which is a Siegel modular form of weight 18 defined as the product of the 36 even theta constants determines this obstruction as we shall recall in Section 5. Since we can compute algebraically the values of χ_{18} at all $(A, \mathscr{L})$ in the isogeny class of E^3, we can compute the obstruction for each of them and check if a defect-0 genus-3 curve exists over $\mathbb{F}_q$. This gives the first *provable* computation of this obstruction as, so far, one had only a heuristic method using lifting and approximations over $\mathbb{C}$ [Rit10].

We conclude with an example in genus 4. We show that Igusa modular form cuts the locus of Jacobians and decomposable principally polarized abelian varieties over any algebraically closed field of characteristic different 2 (see Theorem 5.8) and use this to show that a certain class of isogeny does not contain Jacobians (see example 5.9).

The code and examples of our algorithms are available at Inria's gitlab. In the future, we hope to improve the overall speed of the algorithm (for instance by working with A_0 products of distinct elliptic curves E_i

[1] when g is odd, all of them have even weight.

instead of E^g) and waive the technical limitations above. Notice that the method presented here may be adapted to other cases: one could replace E ordinary with E supersingular over $\mathbb{F}_p$ or over $\mathbb{F}_{p^2}$ with trace $\pm 2p$; one could also replace E by a principally polarized abelian variety B for which a thetanull point is known (with some restrictions, see [AK18] and [JKP+18, Sec.8]).

Acknowledgements. We would like to thank Andrew Sutherland who kindly provided us a fast `Magma` code to check when an ordinary elliptic curve has minimal endomorphism ring and Jeroen Sijsling for helping us using his `Magma` packages. We also thank Valentijn Karemaker and Stefano Marseglia for discussions about the references in the introduction.

2. Hermitian lattices

2.1. **Basic definitions and notations.** Let $F = \mathbb{Q}(\sqrt{d})$, where $d < 0$ is a squarefree negative integer. The discriminant d_F of F equals d if $d \equiv 1 \pmod 4$ and $4d$ otherwise. The non-trivial Galois involution of $F/\mathbb{Q}$ will be denoted by $\bar{\cdot}$. Further, let

$$\mathrm{Nr}\colon F \to \mathbb{Q},\ x \mapsto x\overline{x} \quad \text{and} \quad \mathrm{Tr}\colon F \to \mathbb{Q},\ x \mapsto x + \overline{x}$$

be the usual norm and trace of $F/\mathbb{Q}$.

Definition 2.1. A *hermitian space* (V, h) over F is a finite dimensional vector space V over F equipped with a sesqui-linear map $h\colon V \times V \to F$ such that

(1) $h(\alpha v + \beta v', w) = \alpha h(v, w) + \beta h(v', w)$ for all $\alpha, \beta \in F$ and all $v, v', w \in V$.
(2) $h(v, w) = \overline{h(w, v)}$ for all $v, w \in V$.

The *rank* of a hermitian space (V, h) is the dimension of V over F. For a tuple $b = (b_1, \dots, b_r) \in V^r$ we define its *Gram matrix* by

$$\mathrm{Gram}(b) = (h(b_i, b_j)) \in F^{r \times r}\,.$$

Every hermitian space (V, h) in this paper is assumed to be *non-degenerate*, i.e. if $v \in V$ with $h(v, w) = 0$ for all $w \in V$ then $v = 0$. This is equivalent to say that the *Gram matrix* of any basis b of V is invertible.

Definition 2.2. Let b be a basis of a hermitian space (V, h). Then

$$\det(V, h) := \det(\mathrm{Gram}(b))$$

is called the *determinant* of (V, h). It is well defined when viewed as an element of $\mathbb{Q}^*/\mathrm{Nr}(F^*)$.

Definition 2.3. Two hermitian spaces (V, h) and (V', h') over F are called *isometric* if there is an isomorphism $\varphi\colon V \to V'$ such that $h'(\varphi(v), \varphi(w)) = h(v, w)$ for all $v, w \in V$. The map φ is then called an *isometry* between (V, h) and (V', h'). Moreover,

$$\mathrm{U}(V, h) = \{\varphi\colon V \to V \mid \varphi \text{ is an isometry}\} \quad \text{and} \quad \mathrm{SU}(V, h) = \{\varphi \in \mathrm{U}(V, h) \mid \det(\varphi) = 1\}\,.$$

are the *unitary* and *special unitary groups* of (V, h) respectively.

Let $\mathscr{P}$ denote the set of prime numbers. For $p \in \mathscr{P} \cup \{\infty\}$ let $F_p := \mathbb{Q}_p \otimes_{\mathbb{Q}} F$ be the completion of F at p. Let (V, h) be a hermitian space over F. The map h extends to $V_p := F_p \otimes_F V$ by linearity. This yields a hermitian space (V_p, h) over F_p. If $p = \infty$, then $\mathbb{Q}_\infty = \mathbb{R}$ and (V_∞, h) is a hermitian space over $F_\infty = \mathbb{C}$. The signature of this complex hermitian space is called the signature of (V, h).

The following local-global principle is well known.

Theorem 2.4 (Landherr)**.** *Two hermitian spaces over F are isometric if and only if they are isometric over every place of $\mathbb{Q}$.*

Hermitian spaces over $\mathbb{C}$ are parameterized by their signatures while hermitian spaces over $\mathbb{Q}_p$ are parameterized by their ranks and determinants (viewed as elements of $\mathbb{Q}_p^*/\mathrm{Nr}(F_p^*)$). We will only deal with positive definite spaces, i.e. spaces with $h(v, v) > 0$ for all non-zero $v \in V$. For these spaces, we can make Landherr's theorem more explicit.

Remark 2.5. Let g be a positive integer and let $\mathscr{P}_{\mathrm{ns}}$ be the set of primes which do not split in F.

(1) Let (V,h) be a positive definite hermitian space of rank g. Since $\mathbb{Q}_p^*/\operatorname{Nr}(F_p^*)$ has at most two elements, the isometry type of (V,h) is uniquely determined by

$$I := \{p \in \mathscr{P} \mid \det(V,h) \notin \operatorname{Nr}(F_p^*)\} \subseteq \mathscr{P}_{\text{ns}} .$$

The product formula for Hasse's norm residue symbols shows that I is a finite set of even cardinality.

(2) Let $I \subseteq \mathscr{P}_{\text{ns}}$ be a finite subset of even cardinality. There exists a positive definite hermitian space (V,h) of rank g such that

$$I = \{p \in \mathscr{P} \mid \det(V,h) \notin \operatorname{Nr}(F_p^*)\} .$$

Moreover, this space admits the Gram matrix

$$\operatorname{diag}(1,\dots,1,a)$$

with some positive integer a whose prime divisor are in $I \cup \{q\}$ for some prime q. This gives a method to construct a positive definite hermitian space of rank g with given determinant, see [Kir16, Section 3.4] for details.

For the remainder of this section, let (V,h) be a hermitian space over F of rank g. Further let R be an *order* in F, that is a subring of F which is a free $\mathbb{Z}$-module of rank 2. The ring of integers $\mathscr{O}$ of F is an order and it contains every other order R of F. Thus the index $f := [\mathscr{O} : R]$ is finite and it is called the *conductor* of R in F. Note that R is the unique quadratic order of discriminant $\operatorname{Disc}(R) = f^2 d_F$. Moreover,

$$\mathscr{O} = \mathbb{Z}[\omega] \quad \text{and} \quad R = \mathbb{Z}[f\omega] \quad \text{where } \omega = \frac{d_F + \sqrt{d_F}}{2} .$$

A *fractional R-ideal* $\mathfrak{a}$ is an R-submodule of F which has rank 2 over $\mathbb{Z}$. It is said to be an *invertible* R-ideal if there exists a fractional R-ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = R$. Given two fractional R-ideals $\mathfrak{a}, \mathfrak{b}$ we can define the fractional R-ideal $(\mathfrak{a} : \mathfrak{b}) = \{x \in F, x\mathfrak{b} \subseteq \mathfrak{a}\}$ called the *colon-quotient* of $\mathfrak{a}$ and $\mathfrak{b}$. The particular case $(\mathfrak{a} : \mathfrak{a})$ is called the *multiplicator ring* of $\mathfrak{a}$. It is the unique order in F for which $\mathfrak{a}$ is invertible.

Definition 2.6. An *R-lattice* of rank r is a finitely generated R-submodule of V such that $FL := L \otimes_R F$ has dimension r. If $r = g$ we call L a *full* R-lattice in V.

The following result is due to Borevich and Faddeev [BF60].

Proposition 2.7. *Let L be a full R-lattice in V. Then there exist a basis $(x_1,\dots,x_g)$ of V, some fractional ideals $\mathfrak{a}_1,\dots,\mathfrak{a}_g$ of R and a chain of orders $R \subseteq R_1 \subseteq \cdots \subseteq R_g$ such that $\mathfrak{a}_i$ is an invertible R_i-ideal and*

$$L = \mathfrak{a}_1 x_1 \oplus \cdots \oplus \mathfrak{a}_g x_g .$$

The list of pairs $(\mathfrak{a}_i, x_i)_{i=1,\dots,g}$ is called a pseudo-basis *of L.*

In the implementation of our algorithms we represent an R-lattice either via a pseudo basis or a $\mathbb{Z}$-basis and we use the results of [BF60] to switch between these two types of representations.

Definition 2.8. Let L be an R-lattice in V.

(1) The *dual lattice* of L is

$$L^{\#} = \{x \in V, h(x,L) \subseteq R\} .$$

(2) The lattice L is called *integral* if $L \subseteq L^{\#}$ and *unimodular* if $L = L^{\#}$.

(3) An integral R-lattice L is called even, if $h(x,x) \in 2\mathbb{Z}$ for all $x \in L$; otherwise it is called odd.

(4) The lattice L is called *decomposable* if there exists two non-trivial R-submodules L_1, L_2 of L such that $L = L_1 \oplus L_2$ and $h(x_1,x_2) = 0$ for all $x_i \in L_i$. If this is the case, we write $L = L_1 \perp L_2$.

(5) If L is a free R-lattice with basis b, then $\det(L) := \det(\operatorname{Gram}(b))$ is the *determinant* of L. It is a well defined element in $\mathbb{Q}^*/\operatorname{Nr}(R^*)$.

(6) Given $a_1,\dots,a_g \in \mathbb{Q}^*$, we denote by

$$\langle a_1,\dots,a_g \rangle$$

the free hermitian R-lattice (L',h') of rank g having an orthogonal basis $(b_1,\dots,b_g)$ such that $h'(b_i,b_i) = a_i$ for all $1 \le i \le g$.

Let L be an R-lattice with pseudo-basis $(\mathfrak{a}_i, x_i)$. Denote by $(x_i^\#)$ the dual basis (x_i), i.e. the basis of V such that $h(x_i, x_i^\#) = \delta_{i,j}$ for all $1 \le i, j \le g$. Then

$$L^\# = \bigoplus_{i=1}^{g} \overline{(R : \mathfrak{a}_i)} x_i^\# .$$

From this fact and the relation $(R : (R : \mathfrak{a})) = \mathfrak{a}$ it is easy to see that $(L^\#)^\# = L$.

Lemma 2.9. *Let L be an R-lattice in (V, h) and let $L_1, \dots, L_n$ be $\mathbb{Z}$-submodules of L. For $a \in F$ let*

$$f_a \colon V \times V \to \mathbb{Q},\ (x, y) \mapsto \mathrm{Tr}(ah(x, y)) .$$

The following are equivalent:

(1) *$L = L_1 \perp \dots \perp L_n$ is an orthogonal decomposition into R-lattices.*
(2) *$L = \bigoplus_i L_i$ and $f_1(L_i, L_j) = f_{\sqrt{d}}(L_i, L_j) = \{0\}$ for all $i \neq j$.*

Proof. We only need to prove that (2) implies (1). Let $x \in L_i$ and $y \in \bigoplus_{j \neq i} L_j$. Then $f_1(x, y) = f_{\sqrt{d}(x,y)} = 0$ and thus $\mathrm{Tr}(ah(x, y)) = 0$ for all $a \in F$. Since $F/\mathbb{Q}$ is separable, it follows that $h(x, y) = 0$. Let $r \in R$. Then $h(rx, y) = 0$ and thus $f_a(rx, y) = 0$ for all $a \in F$. Hence $rx \in \mathbb{Q}L_i \cap L = L_i$. So L_i is indeed an R-module. □

If (V, h) is positive definite, then so is the rational bilinear map f_1 from above. In this case, a well known result of Kneser shows that there exists a unique decomposition of L as in Lemma 2.9 (2) into minimal $\mathbb{Z}$-submodules. It can be computed as in [HV98, Algorithm 4.5]. Hence the previous lemma shows that any positive definite hermitian R-lattice L has a unique decomposition into indecomposable sublattices and it yields a method to compute these sublattices.

For a prime $p \in \mathscr{P}$ let $R_p := \mathbb{Z}_p \otimes_{\mathbb{Z}} R$ and $L_p := R_p \otimes_R L$ be the completions of R and L at p. Then L_p is an R_p-lattice in (V_p, h). The introduced notion for R-lattices carries over to R_p-lattices. For example we call an R_2-lattice L even, if $h(x, x) \in 2\mathbb{Z}_2$ for all $x \in L$.

2.2. **Enumeration of positive definite unimodular hermitian lattices.** Let $R = \mathbb{Z}[\omega f]$ be the order of conductor f in F. In this section, we present an algorithm to enumerate all positive definite unimodular R-lattices of a given rank.

Definition 2.10. Let L and L' be full R-lattices in the hermitian spaces (V, h) and (V', h'). The lattices L and L' are said to be isometric, if there exists an isometry φ from (V, h) to (V', h') such that $\varphi(L) = L'$. In this case, we write $L \cong L'$. Further let

$$\mathrm{cls}(L) = \{\varphi(L) \mid \varphi \in \mathrm{U}(V, h)\} \quad \text{and} \quad \mathrm{Aut}(L) = \{\varphi \in \mathrm{U}(V, h) \mid \varphi(L) = L\}$$

be the *isometry class* and the *automorphism group* of L. Similarly one defines isometries between the completions L_p and L'_p at a prime p. The *genus* of L is

$$\mathrm{gen}(L) := \{L' \subset V \mid L' \text{ is an } R\text{-lattice such that } L_p \cong L'_p \text{ for all } p \in \mathscr{P}\} .$$

In the case that $R = O$ is maximal, the following remark shows how to find a lattice in a given genus.

Remark 2.11. The classification of hermitian $\mathscr{O}_p$-lattices by Jacobowitz [Jac62] yields a classification of the genera of hermitian $\mathscr{O}$-lattices in terms of local invariants. Given such a set of invariants, one can construct a lattice L in the genus as follows.

(1) Since the local invariants include the determinants of the completions L_p, we can construct a hermitian space (V, h) over F that contains this genus using Remark 2.5.
(2) Fix any $\mathscr{O}$-lattice L in V. Then the set of all primes p where L_p has the wrong invariants is finite.
(3) If L_p has the wrong invariants, let X be any $\mathscr{O}$-lattice in some hermitian space (V', h') over F such that X_p has the correct invariants. Approximate an isometry between (V'_p, h') and (V_p, h) by some F-linear map $\varphi \colon V' \to V$. If the approximation is good enough, then $\varphi(X)_p$ has the same invariants as X_p. Then there exists $a, b \in \mathbb{Z}$ such that

$$p^a L_p \subseteq \varphi(X)_p \subseteq p^b L_p .$$

Now the lattice $(\varphi(X) + p^a L) \cap p^b L$ coincides with L at all places different from p and it has the correct invariants at p. So if we iterate this step, we end up with an $\mathscr{O}$-lattice in the described genus.

A different approach is suggested in [Kir16, Section 3.5].

Let L be an R-lattice in a positive definite hermitian space over F. The analogue of Landherr's theorem does not hold for hermitian R-lattices, i.e. the genus of L does not necessarily consist of a single isometry class. However, the genus of L is a disjoint union of finitely many isometry classes

$$\operatorname{gen}(L) = \biguplus_{i=1}^{h(L)} \operatorname{cls}(L_i)\,. \tag{1}$$

The number of classes $h(L)$ is called the *class number* of L or $\operatorname{gen}(L)$. There are only very few partial results like [HK89a; HK89b] on how to deduce the class number from local invariants and these only deal with $\mathscr{O}$-lattices.

Thus an important problem is to work out the class number $h(L)$ or more generally to make the decomposition in Equation (1) explicit. This can be done by Kneser's neighbour method. It is explained in great detail in [Sch98] for $\mathscr{O}$-lattices. Note that this is all we need, since we will reduce the case that R is non-maximal to this special case in Algorithm 2.

The basic idea of Kneser's method the following: Let $\mathfrak{p}$ be a prime ideal of $\mathscr{O}$ over $p > 2$ such that L_p is unimodular. An $\mathscr{O}$-lattice L' in V is called a $\mathfrak{p}$-neighbour of L if $L/(L\cap L') \cong \mathscr{O}/\mathfrak{p}$ and $L'/(L\cap L') \cong \mathscr{O}/\overline{\mathfrak{p}}$. Any $\mathfrak{p}$-neighbour of L lies in $\operatorname{gen}(L)$ and the $\mathfrak{p}$-neighbours of L can be enumerated quickly. Strong approximation yields a finite set S of unramified prime ideals of $\mathscr{O}$ such that given $L' \in \operatorname{gen}(L)$, there exists a sequence of $\mathscr{O}$-lattices $L = L_0, L_1, \ldots, L_r \cong L'$ such that L_i is a $\mathfrak{p}_i$-neighbour of L_{i-1} for some $\mathfrak{p}_i \in S$. In fact, Shimura [Shi64, Theorem 5.24 and its proof 5.28] shows how to choose such a set S. Note that if g is even, his description makes use of the groups $\{\det(g) : g \in \operatorname{Aut}(L_p)\}$ at primes p that ramify in F. These groups have recently been worked out in [Kir19]. So the isometry classes in $\operatorname{gen}(L)$ are found by repeatedly computing $\mathfrak{p}$-neighbours for some $\mathfrak{p} \in S$.

Note that this procedure can be sped up considerably by using Siegel's mass formula as a stopping condition: Since isometric lattices have isomorphic automorphism groups, the *mass* of L

$$\operatorname{Mass}(L) := \operatorname{Mass}(\operatorname{gen}(L)) = \sum_{i=1}^{h(L)} \frac{1}{\#\operatorname{Aut}(L_i)}$$

is a well-defined positive rational number, which only depends on the genus of L. It can be computed a priori using Siegel's mass formula, which expresses $\operatorname{Mass}(L)$ in terms of special values of L-series and local factors that depend on the genus of L. The local factors have been worked out by Gan and Yu [GY00] for all primes p, except if $p = 2$ ramifies in F. In this exceptional case the local factors can be worked out as explained in [Kir16, Sections 4.3 and 4.5].

So if $R = \mathscr{O}$ is maximal, we can construct lattices in a given genus and enumerate the isometry classes in this genus. We will now extend these methods to enumerate the isometry classes of (unimodular) R-lattices in positive definite hermitian spaces.

Lemma 2.12. *Let L be a unimodular hermitian R-lattice. Then $M := \mathscr{O}L$ is an integral $\mathscr{O}$-lattice and*

$$fM^{\#,\mathscr{O}} \subseteq L \subseteq M\,.$$

Proof. The fact that M is integral and the inclusion $L \subseteq M$ are clear. Suppose now $z \in fM^{\#,\mathscr{O}}$. Hence $h(z/f, M) \subseteq \mathscr{O}$. This implies $h(z, L) \subseteq f\mathscr{O} \subseteq R$. So $z \in L^{\#,R} = L$. □

Algorithm 2 Enumeration of unimodular positive definite hermitian R-lattices of rank g.

Input: An order R of conductor f in an imaginary quadratic number field F and an integer $g \geq 1$.
Output: A set of R-lattices representing the isometry classes of positive definite, unimodular hermitian R-lattices of rank g.

1: $\mathscr{L} \leftarrow \emptyset$.
2: Let $p_1, \ldots, p_s$ be the prime divisors of fd_F that do not split in F.
3: **for all** subsets $I \subseteq \{p_1, \ldots, p_s\}$ of even cardinality **do**
4: Using Remark 2.5 construct some positive definite hermitian form $h\colon F^g \times F^g \to F$ such that
$$\{p \in \mathscr{P} \mid \det(F^g, h) \notin \mathrm{Nr}(F_p^*)\} = I\,.$$
5: Using Remark 2.11 find $\mathscr{O}$-lattices $G_1, \ldots, G_r$ representing the genera of all integral $\mathscr{O}$-lattices M in (F^g, h) such that $fM^{\#,\mathscr{O}} \subseteq M$.
6: **for** $1 \leq i \leq r$ **do**
7: Let $M_1, \ldots, M_s$ represent the isometry classes of $\mathscr{O}$-lattices in $\mathrm{gen}(G_i)$ using Kneser's method.
8: **if** $R = \mathscr{O}$ **then**
9: $\mathscr{L} \leftarrow \mathscr{L} \cup \{M_1, \ldots, M_s\}$.
10: **else**
11: **for** $1 \leq j \leq s$ **do**
12: Let $L_1, \ldots, L_t$ be orbit representatives of the action of $\mathrm{Aut}(M_j)$ on
$$\{L \subseteq M_j \mid L \text{ a unimodular } R\text{-lattice containing } fM_j^{\#,\mathscr{O}} \text{ with } \mathscr{O}L = M_j\}\,.$$
13: $\mathscr{L} \leftarrow \mathscr{L} \cup \{L_1, \ldots, L_t\}$.
14: **end for**
15: **end if**
16: **end for**
17: **end for**
18: **return** $\mathscr{L}$.

Proposition 2.13. *Algorithm 2 which takes as input an order R of conductor f in an imaginary quadratic field and an integer $g \geq 1$ outputs the list of R-lattices representing the isometry classes of positive definite, unimodular hermitian R-lattices of rank g.*

Proof. Let L be a unimodular, full R-lattice in a positive definite hermitian space (V, h') of rank g. We first show that $\mathscr{L}$ contains a lattice isometric to L. Let p be a prime not dividing fd_F. Then L_p is a unimodular $\mathscr{O}_p$-lattice. If p splits in F, then $\det(V_p, h') \in \mathbb{Q}_p^* = \mathrm{Nr}(F_p^*)$. Suppose now p is non-split. By [Jac62, Proposition 4.4] L_p admits an orthogonal basis. Hence $\det(V_p, h')$ has a representative in $\mathbb{Z}_p^* \subseteq \mathrm{Nr}(F_p^*)$ So Landherr's theorem implies that (V, h') is isometric to one the spaces (F^g, h) the algorithm considers. After replacing L by an isometric copy, we may therefore assume that $M := \mathscr{O}L$ is one of the lattices M_j in line 7. Proposition 2.12 shows $fM_j^{\#,\mathscr{O}} \subseteq L \subseteq M_j$. Thus $\mathscr{L}$ contains an R-lattice isometric to L.
Next we show that $\mathscr{L}$ does not represent any isometry class twice. Suppose $L_1, L_2 \in \mathscr{L}$ are isometric. This isometry extends to an isometry between $\mathscr{O}L_1$ and $\mathscr{O}L_2$. By construction, this implies $\mathscr{O}L_1 = \mathscr{O}L_2$. Hence L_1 and L_2 are in the same orbit under $\mathrm{Aut}(\mathscr{O}L_1)$. This shows $L_1 = L_2$. □

If we restrict ourselfs to projective unimodular R-lattices, we can speed up Algorithm 2 considerably. To this end, let L be a full, projective R-lattice in a positive definite hermitian space (V, h) over F and set $M = \mathscr{O}L$. The R-lattice L has a pseudo-basis
$$L = \bigoplus_{i=1}^{g} \mathfrak{a}_i x_i$$
with invertible fractional ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_g$ of R since L is a projective R-module. Let $(x_1^\#, \ldots, x_g^\#)$ denote the dual basis of $(x_1, \ldots, x_g)$. Then
$$M = \bigoplus_{i=1}^{g} \mathscr{O}\mathfrak{a}_i x_i, \quad L^{\#,R} = \bigoplus_{i=1}^{g} \overline{(R : \mathfrak{a}_i)} x_i^\# \quad \text{and} \quad M^{\#,\mathscr{O}} = \bigoplus_{i=1}^{g} \overline{(\mathscr{O} : \mathscr{O}\mathfrak{a}_i)} x_i^\# = \mathscr{O}L^{\#,R}\,.$$

Since $(R : \mathfrak{a}_i)$ is an invertible R-ideal, we see that $L^{\#,R}$ is projective as well.

Proposition 2.14. *Let L and M be as above. Let Φ be the bilinear map defined by*

$$\Phi\colon M/fM \times M/fM \to \mathscr{O}/R \cong \mathbb{Z}/f\mathbb{Z},\ (x,y) \mapsto h(x,y) + R\,. \tag{2}$$

Then the following hold.

(1) *If L is a unimodular R-lattice, then M is a unimodular $\mathscr{O}$-lattice.*
(2) *If M is a unimodular $\mathscr{O}$-lattice, then the following are equivalent:*
   (a) *L is a unimodular R-lattice.*
   (b) *L is an integral R-lattice.*
   (c) *L/fM is an isotropic subspace of $(M/fM, \Phi)$, i.e. $\Phi(x,y) = 0$ for all $x, y \in L/fM$.*

Proof. (1) The discussion before the proposition shows that $L = L^{\#,R}$ implies $M = M^{\#,\mathscr{O}}$. (2b) $\implies$ (2a): We have $L \subseteq L^{\#,R}$ by assumption. Equality follows from the fact that the projective R-modules L and $L^{\#,R}$ both have index f^g in $M = M^{\#,\mathscr{O}} = \mathscr{O}L^{\#,R}$. The implications (2a) $\implies$ (2b) $\iff$ (2c) are clear. □

Algorithm 3 Enumeration of projective unimodular R-lattices of rank g.

Input: An integer $g \geq 2$ and an order R in F.
Output: A set of representatives of the isometry classes of projective, positive definite, unimodular hermitian R-lattices of rank g.

1: Fix a chain of minimal overorders $R = \mathscr{O}^{(0)} \subsetneq \mathscr{O}^{(1)} \subsetneq \ldots \subsetneq \mathscr{O}^{(r)} = \mathscr{O}$.
2: Using Algorithm 2 compute a set $\mathscr{S}$ of representatives of isometry classes of unimodular hermitian $\mathscr{O}$-lattices of rank g.
3: **for** $i = r, \ldots, 1$ **do**
4: Let p be the index of $\mathscr{O}^{(i-1)}$ in $\mathscr{O}^{(i)}$.
5: $\mathscr{T} \leftarrow \emptyset$.
6: **for** $M \in \mathscr{S}$ **do**
7: Let $\mathscr{V}$ represent the orbits of all g-dimensional isotropic subspaces of $(M/pM, \Phi)$ under the action of $\mathrm{Aut}(M)$ where Φ is chosen as in Equation (2).
8: **for** $V \in \mathscr{V}$ **do**
9: Let L be the full preimage of V under the canonical epimorphism $M \to M/pM$.
10: If L is an integral $\mathscr{O}^{(i-1)}$-lattice with $\mathscr{O}^{(i)}L = M$ then include L to the set $\mathscr{T}$.
11: **end for**
12: **end for**
13: $\mathscr{S} \leftarrow \mathscr{T}$.
14: **end for**
15: **return** $\mathscr{S}$.

Proposition 2.15. *Algorithm 3 which takes as input an order R in an imaginary quadratic field and an integer $g \geq 2$ outputs the list of R-lattices representing the isometry classes of positive definite, unimodular, projective hermitian R-lattices of rank g.*

Proof. After line 2, $\mathscr{S}$ is a set of representatives of the isometry classes of projective, unimodular hermitian $\mathscr{O}^{(r)}$-lattices. Let L be a projective unimodular hermitian $\mathscr{O}^{(r-1)}$-lattice. Then $M := \mathscr{O}^{(r)}L$ is a projective unimodular hermitian $\mathscr{O}^{(r)}$-lattice. So without loss of generality $M \in \mathscr{S}$. Thus Proposition 2.14 shows that the set $\mathscr{T}$ in line 13 contains an $\mathscr{O}^{(r-1)}$-lattice isometric to L. Suppose it contains two such lattices L_1 and L_2. Then there is an isometry $\sigma\colon L_1 \to L_2$ which induces an isometry $\mathscr{O}^{(r)}L_1 \to \mathscr{O}^{(r)}L_2$. But then $\mathscr{O}^{(r)}L_1 = M = \mathscr{O}^{(r)}L_2$ and $\sigma \in \mathrm{Aut}(M)$. Hence L_1 and L_2 are in the same $\mathrm{Aut}(M)$-orbit. This shows that $L_1 = L_2$. Hence after line 13, $\mathscr{S}$ is a set of representatives of the isometry classes of projective, unimodular hermitian $\mathscr{O}^{(r-1)}$-lattices. By induction it follows that after r iterations, $\mathscr{S}$ represents the isometry classes of projective, unimodular hermitian R-lattices. □

Note that Algorithm 3 calls Algorithm 2. But if $R = \mathscr{O}$ is maximal, the expensive steps 11–14 of Algorithm 2 are skipped. They are replaced by a much more refined descent in lines 3–13 of Algorithm 3, which is based on Proposition 2.14.

Also note that in Algorithm 3 it would be possible to go from $\mathcal{O}$-lattices to R-lattices directly. But then it would be much more difficult to find the desired (projective) R-lattices between fM and M.

2.3. **Orthogonal families inside a lattice.** Let (V, h) be a positive definite hermitian space over F of rank g. Let R be the order in F of conductor f.

In this section, we give necessary and sufficient conditions for a unimodular hermitian R-lattice to contain a free R-sublattice isometric to $\langle \ell, \dots, \ell \rangle$ for some $\ell \in \mathbb{N}$, which we may require to be odd. This section is to prepare the search in Section 3.3 for a good isogeny from our target principally polarized abelian variety to a totally decomposable one. But we also think that this problem is natural and should deserve more investigations around the smallest values of ℓ that can be obtained.

We will prove the following result.

Theorem 2.16. *Let L be a full R-lattice in (V, h) and let $a \in \mathbb{Z} \setminus \{0\}$. Then the following hold:*

1. *There exists an orthogonal basis $(b_1, \dots, b_g) \in L^g$ of V.*
2. *There exists an integer ℓ and a free R-sublattice L' of L such that $L' \cong \langle \ell, \dots, \ell \rangle$ if and only if g is odd or $\det(V, h) \in \mathrm{Nr}(F^*)$.*
3. *Let L be unimodular and suppose g is odd or $\det(V, h) \in \mathrm{Nr}(F^*)$. There exists some positive integer ℓ coprime to a and a free R-sublattice L' of L such that $L' \cong \langle \ell, \dots, \ell \rangle$ if and only if the following conditions hold.*
   (a) *For all primes $p \mid a$ the module L_p is free over R_p.*
   (b) *If a is even then there exists some $\ell_2 \in \mathbb{Z}_2^*$ such that $L_2 \cong \langle \ell_2, \dots, \ell_2 \rangle$.*
   (c) *If g is even, then $\det(L_p, h) \in \mathrm{Nr}(R_p^*)$ for all odd primes p such that $p \mid \gcd(a, f)$.*

Lemma 2.19 and Remark 2.23 below show how to check the conditions of Theorem 2.16. Suppose an R-lattice L in V satisfies these conditions. Then we can find an orthogonal basis of V in L as follows. For any positive rational number ℓ the map

$$q_\ell \colon V \to \mathbb{Q},\ v \mapsto \mathrm{Tr}(h(v, v)/\ell)$$

is a positive definite quadratic form on the $\mathbb{Q}$-space V and

$$\{v \in L \mid h(v, v) = \ell\} \subseteq \{v \in L \mid q_\ell(v) = 2\}\,.$$

Note that the right hand side is finite and it can be enumerated using the Fincke-Pohst algorithm [FP85]. This allows us to compute the set of vectors in (L, h) of norm ℓ.

It is now clear how to find an orthogonal basis as in Theorem 2.16. For part (1), we use Algorithm 4. For parts (2) and (3), we apply Algorithm 5 to $\ell = 1, 2, 3, \dots$ until we find a suitable basis. As all our algorithms, its complexity is at least exponential in the rank g. We could not find in the literature any result about a possible upper bound on ℓ when it exists.

Algorithm 4 Computation of an orthogonal family of g vectors of L

Input: A full R-lattice L in V of rank g.
Output: An orthogonal basis of V consisting of vectors in L.

```
Let L_1 = L; S = ∅.
for i = 1 to g do
    Pick a vector v_1 ∈ L_1 \ {0} with minimal norm.
    S = S ∪ {v_1}.
    L_1 = {v ∈ L_1 | h(v, v_1) = 0}.
end for
return S.
```

Algorithm 5 Computation of an orthogonal family of g vectors of norm ℓ

Input: A full R-lattice L in V and a rational number $\ell > 0$.
Output: An orthogonal basis of V consisting of vectors in L of norm ℓ if possible; otherwise $\emptyset$.

function BACKTRACK(F, S)
  if $\#F = g$ **then return** F **end if**
  if $\#F + \dim\langle S\rangle < g$ **then return** $\emptyset$ **end if**
  Pick some $v \in S$.
  if $h(v, f) = 0$ for all $f \in F$ **then**
    $T \leftarrow$ BACKTRACK($F \cup \{v\}$, $\{w \in S \mid h(v, w) = 0\}$)).
    if $T \neq \emptyset$ **then return** T **end if**
  end if
  return BACKTRACK(F, $S \setminus \{v\}$).
end function
if $\ell^g \cdot \det(V, h) \notin \mathrm{Nr}(F^*)$ **then return** $\emptyset$ **end if**
$S \leftarrow \{v \in L \mid h(v, v) = \ell\}$.
return BACKTRACK($\emptyset$, S).

The remainder of this section gives a proof of Theorem 2.16. We start by giving a classification of all free unimodular hermitian R_p-lattices which admit an orthogonal basis. If R is maximal, this follows from Jacobowitz classification of local hermitian lattices [Jac62].

Proposition 2.17. *Let L be a free, unimodular hermitian R_p-lattice or rank g. Then*

$$L = L_1 \perp \ldots \perp L_r$$

for some free unimodular hermitian R_p-sublattices L_i of rank at most 2. If one of p, g or L is odd, then all L_i can be chosen to have rank 1.

Proof. Let $(b_1, \ldots, b_g)$ be a basis of L. Suppose first that $h(b_i, b_i) \in \mathbb{Z}_p^*$ for some i. Then $L = R_p b_i \perp \sum_{j \neq i} R_p(b_j - \frac{h(b_j,b_i)}{h(b_i,b_i)} b_i)$. Suppose now that such an index i does not exist. Since L is free and unimodular, there exist $1 \leq i < j \leq g$ such that $h(b_i, b_j) \in R_p^*$. If $p \neq 2$, we can replace b_i with $b_i' := b_i + 1/(2h(b_j, b_i))b_j$. Then $h(b_i', b_i') \in \mathbb{Z}_p^*$ and we obtain a splitting $L = Rb_i' \perp L'$ as before. If $p = 2$, we may assume that $h(b_i, b_j) = 1$. Then $L = (R_p b_i \oplus R_p b_j) \perp L'$ where

$$L' = \bigoplus_{k \neq i,j} R_p(b_k - \frac{h(b_j, b_j)h(b_k, b_i) - h(b_k, b_j)}{h(b_i, b_i)h(b_j, b_j) - 1} b_i - \frac{h(b_i, b_i)h(b_k, b_j) - h(b_k, b_i)}{h(b_i, b_i)h(b_j, b_j) - 1} b_j) \,.$$

So in any case, we obtain a decomposition $L = L_1 \perp L'$ with free, unimodular lattices L_1 and L' such that the rank of L_1 is at most 2. The first assertion now follows by induction on the rank g and we have also seen that we can choose all L_i of rank 1 when p is odd.
Suppose now $p = 2$ and also suppose that g or L is odd. If L is odd, we can choose the vector b_1 in our original basis such that $h(b_1, b_1) \in \mathbb{Z}_2^*$. If g is odd, then one of the L_i must have rank 1. So in both cases, there exists a summand $L_i = R_2 x_1$ of rank 1. Suppose $L_j = R_2 x_2 \oplus R_2 x_3$ is binary. If $h(x_2, x_2) \in \mathbb{Z}_2^*$ or $h(x_3, x_3) \in \mathbb{Z}_2^*$, we can split L_j just as before. So suppose $h(x_2, x_2), h(x_3, x_3) \in 2\mathbb{Z}_2$. Let $x_2' := x_2 + x_1$. Then as before $L_i \oplus L_j = (R_2 x_2' \oplus R_2 x_3) \perp R_2 x_1'$ for some $x_1' \in L_i \oplus L_j$. But now $h(x_2', x_2') \in \mathbb{Z}_2^*$ and thus $L_i \oplus L_j$ has an orthogonal basis. Iterating this argument shows that L has an orthogonal basis. □

Corollary 2.18. *Let L be a free unimodular hermitian R_p-lattice.*

(1) *If $p = 2$ and the rank of L is odd, then L is odd.*
(2) *L has an orthogonal basis if and only if $p > 2$ or L is odd.*

The classification of all free unimodular hermitian R_p-lattices which have an orthogonal basis more or less boils down to a description of the norm group $\mathrm{Nr}(R_p^*)$. To this end, let

$$\mathbb{Z}_p^{*2} = \{u^2 \mid u \in \mathbb{Z}_p^*\} = \{\mathrm{Nr}(u) \mid u \in \mathbb{Z}_p^*\}$$

be group of squares in $\mathbb{Z}_p^*$.

Lemma 2.19. *If p is odd, then*

$$\mathrm{Nr}(R_p^*) = \begin{cases} \mathbb{Z}_p^* & \text{if } p \nmid f d_F, \\ \mathbb{Z}_p^{*2} & \text{if } p \mid f d_F \end{cases}$$

and

$$\mathrm{Nr}(R_2^*) = \begin{cases} \mathbb{Z}_2^* & \text{if } 2 \nmid d_F \text{ and } 4 \nmid f, \\ \mathbb{Z}_2^{*2} \uplus (1 - \frac{d_F}{4})\mathbb{Z}_2^{*2} & \text{if } 8 \mid d_F \text{ and } 2 \nmid f, \\ \mathbb{Z}_2^{*2} & \text{if } 2^5 \mid f^2 d_F, \\ \mathbb{Z}_2^{*2} \uplus 5\mathbb{Z}_2^{*2} & \text{otherwise.} \end{cases}$$

Proof. We have $\mathbb{Z}_p^{*2} \subseteq \mathrm{Nr}(R_p^*) \subseteq \mathbb{Z}_p^*$ and the structure of $\mathbb{Z}_p^*/\mathbb{Z}_p^{*2}$ is well known. In particular, the square classes can be distinguished modulo $4p$. Any unit $u \in R_p = \mathbb{Z}_p[f\omega]$ is of the form $u = x + yf\omega$ with $x, y \in \mathbb{Z}_p$ and

$$\mathrm{Nr}(u) = (x + yf\omega)\overline{(x + yf\omega)} = x^2 + xyfd_F + y^2 f^2 \frac{d_F^2 - d_F}{4} \in \mathbb{Z}_p^* .$$

The result now follows by a case by case discussion of the possible p-adic valuations of f and d_F. □

Corollary 2.20. *Let L be a free unimodular hermitian R_p-lattice of rank g. Let $u \in \mathbb{Z}_p^*$ be a representative of $\det(L) \in \mathbb{Z}_p^*/\mathrm{Nr}(R_p^*)$. If $p > 2$, then $L \cong \langle 1, \dots, 1, u\rangle$.*

Proof. Let $\varepsilon \in \mathbb{Z}_p^*$ be a non-square. Proposition 2.17 shows that $L \cong \langle u_1, \dots, u_g\rangle$ with $u_i \in \{1, \varepsilon\}$. It is well known that there exists some $U \in \mathrm{GL}_2(\mathbb{Z}_p)$ such that ${}^tU \operatorname{diag}(1,1)U = \operatorname{diag}(\varepsilon, \varepsilon)$. Hence $\langle 1, 1\rangle \cong \langle \varepsilon, \varepsilon\rangle$ and thus we can assume that $u_1 = \ldots = u_{g-1} = 1$. □

Proposition 2.21. *Let L be a free, odd, unimodular hermitian R_2-lattice of rank $g \geq 2$. Let $u \in \mathbb{Z}_2^*$ be a representative of $\det(L) \in \mathbb{Z}_2^*/\mathrm{Nr}(R_2^*)$.*

1. *If R_2 is maximal or $3 \in \mathrm{Nr}(R_2^*)$ or $7 \in \mathrm{Nr}(R_2^*)$, then $L \cong \langle 1, \dots, 1, u\rangle$.*
2. *If $g > 2$ and the conditions in (1) are not satisfied then either*

$$L \cong \langle 1, \dots, 1, u\rangle \quad \text{or} \quad L \cong \langle 1, \dots, 1, 3, 3, u\rangle$$

   but not both.
3. *If $g = 2$ and the conditions in (1) are not satisfied then either $L \cong \langle 1, u\rangle$ or $u \equiv 1, 5 \pmod{\mathrm{Nr}(R_2^*)}$ and $L \cong \langle 3, 3u\rangle$.*

Proof. If R_2 is maximal, the result follows from [Jac62, Theorem 7.1 and Proposition 10.4]. Suppose now R_2 is not maximal. Proposition 2.17 shows that $L \cong \langle u_1, \dots, u_g\rangle$ with $u_i \in \mathbb{Z}_2^*$. If $3 \in \mathrm{Nr}(R_2^*)$ or $7 \in \mathrm{Nr}(R_2^*)$ we may assume that $u_i \in \{1, 5\}$ for all i. As in the proof of Corollary 2.20 we conclude that $u_1 = \cdots = u_{g-1} = 1$. The first assertion follows.
Suppose now $3, 7 \notin \mathrm{Nr}(R_2^*)$ and $g \geq 3$. [O'M63, Theorem 93:16] yields some $T \in \mathrm{GL}_g(\mathbb{Z}_2)$ and $e \in \{1, 3\}$ such that

$${}^tT \operatorname{diag}(u_1, \dots, u_g)T = \operatorname{diag}(1, \dots, 1, e, e, \prod_i u_i) .$$

Hence $L \cong \langle 1, \dots, 1, e, e, u\rangle$. It remains to show that $M := \langle 1, \dots, 1, 1, 1, u\rangle$ and $N := \langle 1, \dots, 1, 3, 3, u\rangle$ are not isometric. Let V be the ambient hermitian space of M and N. Let X and Y be the $\mathbb{Z}_2$-lattices M and N equipped with the bilinear form $V \times V \to \mathbb{Q}_2, (x, y) \mapsto \mathrm{Tr}(h(x, y)/2)$. Lemma 2.19 shows that $R_2 = \mathbb{Z}_2 \oplus \alpha\mathbb{Z}_2$ for some $\alpha \in R_2$ with $\mathrm{Tr}(\alpha) = 0$ and $n := \mathrm{Nr}(\alpha) \in 4\mathbb{Z}_2$. Hence $X = X_0 \perp X_1$ where X_0 and X_1 are free with Gram matrices $\operatorname{diag}(1, \dots, 1, u)$ and $\operatorname{diag}(n, \dots, n, un)$. Similarly $Y = Y_0 \perp Y_1$ where Y_0 and Y_1 are free with Gram matrices $\operatorname{diag}(1, \dots, 1, 3, 3, u)$ and $\operatorname{diag}(n, \dots, n, 3n, 3n, un)$. Suppose M and N are isometric hermitian R_2-lattices. Then X and Y are isometric bilinear $\mathbb{Z}_2$-lattices. By [O'M63, Theorem 93:29 (ii)], this implies that X_0 is isometric to Y_0, which is impossible since the two ambient quadratic spaces have different Hasse-Witt invariants. The case $g = 2$ follows along the same lines. □

The above proof shows that the possible cases in part (2) and (3) of Proposition 2.21 can be distinguished as follows.

Remark 2.22. Let $L \cong \langle u_1, \dots, u_g \rangle$ where $u_i \in \mathbb{Z}_2^*$ and $g \geq 2$. Write $u = \prod_i u_i$. Suppose that R_2 is not maximal and that $3, 7 \notin \mathrm{Nr}(R_2^*)$. Then $L \cong \langle 1, \dots, 1, u \rangle$ if and only if $\prod_{i<j}(u_i, u_j)_2 = 1$ where $(\_, \_)_2$ denotes the Hilbert-Symbol of $\mathbb{Q}_2$.

We are now ready to prove the main result of this section.

Proof of Theorem 2.16. The first assertion is the Gram-Schmidt process. For the remainder let $\mu \in \mathbb{N}$ be a representative of $\det(V,h) \in \mathbb{Q}^*/\mathrm{Nr}(F^*)$. Let (V', h') be a hermitian space over F with Gram matrix $\mu \cdot I_g$. If g is odd or $\det(V,h) \in \mathrm{Nr}(F^*)$, then (V,h) and (V',h') have the same rank, the same determinant and the same signature. Hence they are isometric by Landherr's Theorem. Thus (V,h) contains a free R-lattice $M \cong \langle \mu, \dots, \mu \rangle$. Let $m \in \mathbb{N}$ such that $L' := mM \subseteq L$. Then $L' \cong \langle \ell, \dots, \ell \rangle$ where $\ell = m^2\mu$. Conversely, if such a lattice L' exists and g is even, then $\det(V,h) = \ell^g \in \mathrm{Nr}(F^*)$. This proves the second assertion.
Suppose now L has a sublattice L' as in (3). For any prime divisor p of a, we have

$$L'_p \subseteq L_p \subseteq L_p^{\#} \subseteq (L'_p)^{\#} = L'_p \,.$$

Hence $L_p = L'_p \cong \langle \ell, \dots, \ell \rangle$ and if g is even, then $\det(L_p, h) = \ell^g \in \mathrm{Nr}(R_p^*)$. Finally suppose that the three conditions of part (3) hold. If g is even and a is odd, set $r = 1$. If g and a are both even let $r \in \mathbb{N}$ such that $r/\ell_2 \in \mathrm{Nr}(R_2^*)$. If g is odd, we also choose some integer r, but much more carefully. For all $p \mid a$ the assumption that L_p is free and unimodular implies $\det(L_p, h) \in \mathbb{Z}_p^*$. Hence we may assume that the representative $\mu \in \mathbb{N}$ of $\det(V,h)$ from above is coprime to a. Dirichlet's theorem on primes in arithmetic progressions yields some prime r such that

$$\begin{aligned} r &\equiv \ell_2 \pmod{\mathrm{Nr}(R_2^*)} \text{ if } 2 \mid a, \\ r &\equiv \mu \pmod{\mathrm{Nr}(R_p^*)} \text{ for all } 2 \neq p \mid a, \\ r &\equiv \mu \pmod{\mathrm{Nr}(F_p^*)} \text{ for all } p \mid \mu d_F \text{ and } p \nmid a. \end{aligned}$$

Notice that if $2 \mid a$, then $\ell_2 \equiv \ell_2^g \equiv \mu \pmod{\mathrm{Nr}(F_2^*)}$ and for $p \nmid ra\mu d_F$ we have $r/\mu \in \mathbb{Z}_p^* \subseteq \mathrm{Nr}(F_p^*)$. Hence $r/\mu \in \mathrm{Nr}(F_p^*)$ for all primes $p \neq r$. The product formula for norm symbols and Hasse's norm theorem imply that $r/\mu \in \mathrm{Nr}(F^*)$.
So whether g is even or odd, we have $r^g/\mu \in \mathrm{Nr}(F^*)$. As in part (2) it follows that (V,h) has a Gram matrix $r \cdot I_g$. Thus (V,h) contains a full R-lattice $M \cong \langle r, \dots, r \rangle$. Corollary 2.20, condition (3c) and the choice of r show that for $p \mid a$ there exists some local isometry $\sigma_p \colon M_p \to L_p$. Since M has an orthogonal basis, we may assume that $\det(\sigma_p) = 1$. Strong approximation yields some $\sigma \in \mathrm{SU}(V,h)$ such that $\sigma(M)_p = L_p$ for all $p \mid a$, cf. [Kne66]. Hence there exists an integer b coprime to a such that $b\sigma(M) \subseteq L$. Then $L' := b\sigma(M) \cong \langle \ell, \dots, \ell \rangle$ with $\ell = b^2 r$. This proves the third assertion. □

Remark 2.23. Let L be a unimodular R-lattice in (V,h) given by a pseudo basis $L = \bigoplus_{i=1}^g \mathfrak{a}_i x_i$. Then the conditions in part (3) of Theorem 2.16 can be checked as follows.

(1) The R_p-module L_p is free if and only $\mathfrak{a}_i R_p$ is principal for all i. Since R is Gorenstein, the latter condition holds if and only if the conductor of R and the conductors of the multiplicator rings of all $\mathfrak{a}_i$ have the same p-adic valuation. In particular, this holds if R_p is maximal.
(2) Let $p > 2$ be a prime such that $p \mid \gcd(a, f)$ and suppose L_p is free. For $1 \leq i \leq g$ pick some $a_i \in \mathfrak{a}_i$ such that $a_i R_p = \mathfrak{a}_i R_p$. Then $L_p = \bigoplus_i R_p b_i$ with $b_i = a_i x_i$ and thus $\det(L_p, h) = \det(\mathrm{Gram}(b))$. This can be used to check the condition (3c) as the norm group $\mathrm{Nr}(R_p^*)$ has been worked out in Lemma 2.19.
(3) Suppose $2 \mid a$, L_2 is free and g is odd. The existence of ℓ_2 is guaranteed whenever R_2 is maximal or $3 \in \mathrm{Nr}(R_2^*)$ or $7 \in \mathrm{Nr}(R_2^*)$ since in these cases all free unimodular R_2-lattices in (V_p, h) of determinant $\det(L_p, h)$ are isometric, cf. Proposition 2.21. So suppose we are not in this case. Since the square classes of $\mathbb{Z}_2^*$ are represented by $\{1, 3, 5, 7\}$, there are at most 4 possibilities for ℓ_2. As before we obtain an R_2-basis of L_2. The proof of Proposition 2.17 yields an orthogonal basis of L_2 and thus $u_1, \dots, u_g \in \{1, 3, 5, 7\}$ such that $L_2 \cong \langle u_1, \dots, u_g \rangle$. By Remark 2.22 we have $L_2 \cong \langle \ell_2, \dots, \ell_2 \rangle$ if and only if $\ell_2 \equiv \prod_i u_i \pmod{\mathrm{Nr}(R_2^*)}$ and $\prod_{i<j}(u_i, u_j)_2 = (\ell_2, \ell_2)_2^{(g-1)/2}$. This gives an effective method to find the element ℓ_2 or to show that it does not exist.

(4) Suppose $2 \mid a$, L_2 is free and g is even. If $2 \nmid fd_F$ then $L_2 \cong \langle 1, \dots, 1 \rangle$ by [Jac62, Proposition 10.4]. So we may assume that $2 \mid fd_F$ and we compute a Gram matrix G of L_2. The existence of ℓ_2 implies that $\det(G) \in \mathrm{Nr}(R_2^*)$ and L_2 is odd. The first condition is readily checked and the second holds if and only if some diagonal entry of G lies in $\mathbb{Z}_2^*$. Suppose these conditions both hold. As in in the case of odd ranks, the existence of ℓ_2 is now guaranteed whenever R_2 is maximal or $3 \in \mathrm{Nr}(R_2^*)$ or $7 \in \mathrm{Nr}(R_2^*)$. In the other cases, the proof of Proposition 2.17 shows how to compute $u_1, \dots, u_g \in \{1, 3, 5, 7\}$ such that $L_2 \cong \langle u_1, \dots, u_g \rangle$. Then $L_2 \cong \langle \ell_2, \dots, \ell_2 \rangle$ if and only if $\prod_{i<j}(u_i, u_j)_2 = (\ell_2, \ell_2)_2^{g/2}$. This again yields an effective method to decide if $\ell_2 \in \{1, 3, 5, 7\}$ exists.

Example 2.24. Let $F = \mathbb{Q}(\sqrt{-10})$ and let $\mathfrak{p}$ be the (non-principal) prime ideal of $\mathscr{O}$ over 2. Equip F^2 with the hermitian form h induced by $\mathrm{diag}(1, 2)$. Then

$$L := \mathfrak{p} \cdot (2, 0) \oplus \frac{1}{4}\mathscr{O} \cdot (\sqrt{-10} + 2, 1)$$

is a unimodular (and projective) $\mathscr{O}$-lattice in (F^2, h) but $\det(F^2, h) = 2$ is not a norm in F.

Example 2.25. Let $R = \mathbb{Z}[2i]$ be the order of conductor 2 in $\mathbb{Q}(i)$. Let L be the free hermitian R-lattice with Gram matrix

$$G = \begin{pmatrix} 3 & 2i & 2i-1 \\ -2i & 3 & 2i+1 \\ -2i-1 & -2i+1 & 3 \end{pmatrix} \in R^{3\times 3}.$$

The determinant of G is 1, so L is unimodular. We find that $L_2 \cong \langle 1, 3, 3 \rangle$ and $\mathrm{Nr}(R^*) = \mathbb{Z}_2^{*2} \uplus 5\mathbb{Z}_2^{*2}$. Now $(1, 3)_2^2 \cdot (3, 3)_2 = -1$ but $(1, 1)_2^3 = (5, 5)_2^3 = +1$. Hence $L_2 \ncong \langle \ell_2, \ell_2, \ell_2 \rangle$ for any $\ell_2 \in \mathbb{Z}_2^*$. In particular, L does not contain a free R-sublattice $L' \cong \langle \ell, \ell, \ell \rangle$ for any odd integer ℓ.

3. The description of polarized abelian varieties in terms of lattices

We set the essential tools up to introduce the equivalence of categories which allows us to interpret certain polarized abelian varieties as hermitian lattices.

3.1. **The equivalence of categories.** Let $\mathscr{C}$ be an abelian category, let E be an object of $\mathscr{C}$ and let R be a ring. Fix a morphism $\rho\colon R \to \mathrm{End}(E)$. Let L be a finitely presented left R-module and let

$$R^m \xrightarrow{\varphi} R^n \to L \to 0$$

be a finite presentation. We identity the map $\varphi \in M_{n,m}(R)$ with its image in $M_{n,m}(\mathrm{End}(E))$ by the map induced by ρ, where $M_{n,m}(R)$ denotes the ring of matrices with n rows and m columns with coefficients in R. It defines a morphism

$$E^n \xrightarrow{{}^t\varphi} E^m.$$

The object $\ker({}^t\varphi)$ does not depend on the presentation of L and [Ser85, III.Sec.8.1] uses this to define the functor $\mathscr{F}_E$ as $\mathscr{F}_E(L) = \ker({}^t\varphi)$ on objects. Let us look now on what $\mathscr{F}_E$ does on arrows. Let $f : L_1 \to L_2$ be a morphism of R-modules. Given finite presentations $R^{m_i} \xrightarrow{\varphi_i} R^{n_i} \to L_i \to 0$ of L_i we can lift f to a commutative diagram of R-modules as follows.

$$\begin{array}{ccccccc} R^{m_1} & \xrightarrow{\varphi_1} & R^{n_1} & \longrightarrow & L_1 & \longrightarrow & 0 \\ \downarrow{\scriptstyle G} & & \downarrow{\scriptstyle F} & & \downarrow{\scriptstyle f} & & \\ R^{m_2} & \xrightarrow{\varphi_2} & R^{n_2} & \longrightarrow & L_2 & \longrightarrow & 0. \end{array}$$

We can define $\mathscr{F}_E(f)$ as the map induced by ${}^tF$ by restriction to $\ker({}^t\varphi_2) \to \ker({}^t\varphi_1)$

$$\begin{array}{ccccccc} E^{m_2} & \xleftarrow{{}^t\varphi_2} & E^{n_2} & \longleftarrow & \ker({}^t\varphi_2) & \longleftarrow & 0 \\ \downarrow{\scriptstyle {}^tG} & & \downarrow{\scriptstyle {}^tF} & & \downarrow{\scriptstyle \mathscr{F}_E(f)} & & \\ E^{m_1} & \xleftarrow{{}^t\varphi_1} & E^{n_1} & \longleftarrow & \ker({}^t\varphi_1) & \longleftarrow & 0. \end{array}$$

We now focus on the case where $\mathscr{C}$ is the category of group schemes over $\mathbb{F}_q$ (with $\mathbb{F}_q$-morphisms), $E/\mathbb{F}_q$ is an ordinary elliptic curve and $R = \mathrm{End}(E)$. The ring R is an order in an imaginary quadratic field $F = \mathrm{Frac}\, R$. Denote by $\pi \in R$ the Frobenius endomorphism of E. Let $R - \mathrm{Mod}_{\mathrm{f.p}}$ be the category of finitely presented torsion-free left R-modules (this is the category of R-lattices from Section 2) and Ab_E be the sub-category of $\mathscr{C}$ of abelian varieties $\mathbb{F}_q$-isogenous to a power of E.

Theorem 3.1. *Let E be an ordinary elliptic curve over $\mathbb{F}_q$. Then $\mathscr{F}_E$ defines an equivalence of categories between $(R - Mod_{f.p})^{opp}$, the opposite category of $R - Mod_{f.p}$, and Ab_E if, and only if, $R = \mathbb{Z}[\pi]$. Moreover the functor $\mathscr{F}_E$ is exact.*

The reader can refer to [JKP+18, Theorem 7.6] and [JKP+18, Theorem 4.4] for proofs.

Remark 3.2. Serre also introduces another functor $M \mapsto M \otimes E := \mathrm{Coker}\, \varphi$ which is further studied in [Lau18, Appendice], [JKP+18, section 8] or [AK18]. This functor is covariant but not exact. We also prefer to use $\mathscr{F}_E$ since the theory is settled for an arbitrary order R whereas Serre only develops it for the maximal order. In general there is no easy way to compare the two functors if the R-module is not projective. Notice that the image of a projective R-module $L \in (R - \mathrm{Mod}_{\mathrm{f.p}})^{\mathrm{opp}}$ by $\mathscr{F}_E$ is an abelian variety A isomorphic to a product of elliptic curves $E_i \sim E$ such that $\mathrm{End}(E_i) = R$ for all $1 \leq i \leq g$. Indeed, for an R-ideal I_i such that $E_i = \mathscr{F}_E(I_i)$, $\mathrm{End}(E_i) \simeq (I_i : I_i)$ and since R is Gorenstein, I_i is invertible if and only if $(I_i : I_i) = R$ [Mar19, Prop.2.1].

Notice that if E is such that $R = \mathrm{End}(E) \supset \mathbb{Z}[\pi]$ then the image of $\mathscr{F}_E$ consists of the abelian varieties isomorphic to products of elliptic curves E_i such that the conductor of $\mathrm{End}(E_i)$ divides the conductor of $\mathrm{End}(E)$, as subrings of the maximal order of $F = \mathrm{Frac}(R)$ (see [JKP+18, Theorem 7.5]). However, if $R \neq \mathrm{End}(E)$, it may occur that $\mathscr{F}_E(L)$ is not even an abelian variety (see [JKP+18, Remark 4.6]).

Notice that, given an ordinary elliptic curve $E/\mathbb{F}_q$ with Frobenius endomorphism π, for each order R containing $\mathbb{Z}[\pi]$, there exists an elliptic curve over $\mathbb{F}_q$, isogenous to E, with endomorphism ring isomorphic to R (see [Wat69, Theorem 4.2]). Hence, in what follows, we will always assume that the assumption $R = \mathbb{Z}[\pi] = \mathrm{End}(E)$ is satisfied. Also notice that the main result of [JKP+18] is more general and can also deal with certain supersingular elliptic curves.

3.2. **Polarizations.** Let A be an abelian variety over $\mathbb{F}_q$ isogenous to a power of an elliptic curve E such that $R = \mathrm{End}(E) = \mathbb{Z}[\pi]$. Let us recall that a polarization is an isogeny $\phi_{\mathscr{L}} : A \to \widehat{A}$ with $\mathscr{L}$ an ample line bundle. Let L be a R-lattice. As in [JKP+18, Sec.4.3], we denote L^* the R-lattice $\mathrm{Hom}_R(L, R)$ with the action of $r \in R$ on $\alpha \in L^*$ given by $r.\alpha(x) = \alpha(\bar{r}x)$. We want to translate polarizations in the category of R-lattices.

Theorem 3.3. *Let $E/\mathbb{F}_q$ be an ordinary elliptic curve with $R = End(E) = \mathbb{Z}[\pi]$ where π is the Frobenius endomorphism of E. Let $F = \mathrm{Frac}(R)$. The functor $\mathscr{F}_E$ defines an equivalence of categories between polarized abelian varieties A which are isogenous to E^g and positive definite hermitian R-lattices (L, h) of rank g where $h(x, y) = \Lambda(x)(y)$ with $\Lambda : L \otimes F = V \to V^*$ a linear map such that $\Lambda^{-1}(L^*) \subset L$. Moreover the degree of the polarization is equal to $[L : \Lambda^{-1}(L^*)]$.*

Notice also that, since $\mathscr{F}_E$ is exact, a hermitian lattice (L, h) is indecomposable (see Definition 2.8) if and only if the corresponding polarized abelian variety (A, a) is indecomposable (i.e. (A, a) is not the product of two non-trivial polarized abelian sub-varieties).

Remark 3.4. In [Ser85, Chap.III.Sec.8], Serre uses the functor $M \to M \otimes E$ to get Theorem 3.3 under the hypothesis that R is the maximal order. In another direction, [AK18, Th.A] gets a similar result for arbitrary R (not necessarily quadratic) but only for projective modules.

Before giving various lemmas which will culminate in the proof of Theorem 3.3, in order to stick with the terminology of Section 2 and to lead to an algorithmic version of the theorem, we now give its translation in terms of the dual lattice $L^{\#} = \{x \in V, h(x, L) \subseteq R\}$.

Lemma 3.5. *With the notation above, $\lambda := \Lambda^{-1}$ is an isomorphism between the R-modules $L^{\#}$ and L^*.*

Proof. Notice that $x \in V$ belongs to $\mathrm{Im}\lambda$ if and only if $\Lambda(x) \in L^*$ which is the case if and only if $\forall y \in L, h(x,y) = (\Lambda(x))(y) \in R$. This means, by definition, $x \in L^\#$. Hence, $L^\# = \mathrm{Im}\lambda$. □

Under this isomorphism, one obtains a more natural functor as follows.

Corollary 3.6. *Let $E/\mathbb{F}_q$ be an ordinary elliptic curve with $R = End(E) = \mathbb{Z}[\pi]$ where π is the Frobenius endomorphism of E. There is an equivalence of categories between polarized abelian varieties A which are isogenous to E^g and positive definite hermitian R-lattices (L,h) of rank g such that $L^\#$ is integral. Moreover, the degree of the polarization is equal to $[L : L^\#]$.*

Hence, the isomorphism classes of principally polarized abelian varieties in the isogeny class E^g correspond to the isometry classes of unimodular positive definite hermitian R-lattices.

The rest of the section is devoted to the proof of Theorem 3.3, which will use several lemmas.

In [JKP+18, Th.4.7], it is shown that the dual of $A = \mathscr{F}_E(L)$ is functorially isomorphic to $\mathscr{F}_E(L^*)$. Hence we can relate polarizations and injective morphisms from $L^* \to L$. Now, a morphism $\lambda\colon L^* \to L$ also induces a sesquilinear form

$$H_\lambda\colon L^* \times L^* \to R, (\alpha,\beta) \mapsto \alpha\lambda\beta.$$

We first prove the following lemma.

Lemma 3.7. *The form H_λ is hermitian if and only if there exists a line bundle $\mathscr{L}$ on $A = \mathscr{F}_E(L)$ such that $\mathscr{F}_E(\lambda) = \phi_{\mathscr{L}}$.*

Proof. Let $f : E^g \to A$ be an isogeny induced by an inclusion $\iota : L \to N \simeq R^g$. Observe that the isogeny $a = \mathscr{F}_E(\lambda)$ is of the form $\phi_{\mathscr{L}}$ if and only if $a' = \hat{f}af$ is of the form $\phi_{\mathscr{L}'}$ for a line bundle $\mathscr{L}'$ on E^g. The direct implication is obvious since $\hat{f}af = \phi_{f^*\mathscr{L}}$. As for the other direction, let ℓ be any prime distinct from the characteristic of $\mathbb{F}_q$. By [Mum08, Th.2, p.188], the form $e_\ell(x, a'y)$ is skew-symmetric and therefore the form $e_\ell(x, ay)$ is as well. Still using [Mum08, Th.2], we then have that there exists a line bundle $\mathscr{M}$ such that $2a = \phi_{\mathscr{M}}$ and [Mum08, Th.3, p.231] shows that there exists $\mathscr{L}$ such that $\mathscr{M} \simeq \mathscr{L}^2$ hence $a = \phi_{\mathscr{L}}$.

Now, denote $\lambda' = \iota\lambda\iota^*$ so that $\mathscr{F}_E(\lambda') = a'$. Similarly, the form H_λ is hermitian if and only if the form $H_{\lambda'}$ is. This equivalence can be checked on the F-vector spaces FL and FN where ι is an isomorphism. There we have that $H_{\lambda'}(\alpha',\beta') = \alpha'(\iota\lambda\iota^*)\beta' = H_\lambda(\alpha'\iota, \beta'\iota)$, so it is only a change of basis and the equivalence is clear.

We can therefore assume that $A = \mathscr{F}_E(R^g) = E^g$. Let $\lambda_0 : R^* \to R$ be the isomorphism defined by $\alpha \mapsto \alpha(1)$. Since the dual of E is only defined up to isomorphisms, we can assume by composing with an isomorphism that $\mathscr{F}_E(\lambda_0) : E \to \hat{E}$ is the unique principal polarization $P \mapsto \mathscr{O}([O] - [P])$ on E. Then the product polarization $a_0 = \mathscr{F}_E(\Lambda_0)$ where $\Lambda_0 : (R^g)^* \to R^g$ is defined by $(\alpha_1, \dots, \alpha_g) \mapsto (\alpha_1(1), \dots, \alpha_g(1))$. Now let $M = \lambda\Lambda_0^{-1} \in \mathrm{End}(R^g) = M_g(R)$. Since $\Lambda_0 M^* \Lambda_0^{-1} = {}^t\bar{M}$, the Rosati involution $\dagger$ induced by a_0 on $\mathrm{End}(E^g) = M_g(R)$ is $M \mapsto {}^t\bar{M}$. Hence, ${}^t\bar{M} = M$ if and only if $(a_0^{-1}a)^\dagger = (a_0^{-1}a)$ i.e. $a = \phi_{\mathscr{L}}$ by [Mil86, Prop.17.2]. On the other hand, the form H_λ is hermitian if and only if ${}^t\bar{M} = M$. □

Lemma 3.8. *Let L be a R-lattice of rank g and $\lambda\colon L^* \to L$ injective such that H_λ is hermitian. Then there exists a free over-lattice $L \overset{\iota}{\hookrightarrow} N = \bigoplus_{i=1}^g Re_i$ and integers $(\ell_i)_{1\le i\le g}$ such that if $\lambda' = \iota\lambda\iota^*$, then $H_{\lambda'} : N^* \times N^* \to R$ satisfies $H_{\lambda'}(e_i^*, e_j^*) = \ell_i\delta_{ij}$.*

Proof. Since λ is injective, the hermitian form H_λ is non-degenerate. As in Theorem 2.16(1), we can find a basis (α_i) of $V^* = FL^*$ of vectors of L^* which is orthogonal for H_λ, i.e., $\alpha_i\lambda\alpha_j = \ell_i\delta_{ij}$ with $\ell_i \in \mathbb{Z}$. Consider $N' = \bigoplus_{i=1}^g R\alpha_i \subseteq L^*$ and then $N = N'^* \supseteq L^{**} \simeq L$, the last isomorphism being the evaluation map $ev : L \to L^{**}$. Denote by $\iota\colon L \to N$ the injection and (e_i) the dual basis of (α_i). Noticing that $\alpha_i^{**} = \alpha_i \circ ev^{-1}$, we get that

$$H_{\lambda'}(e_i^*, e_j^*) = \alpha_i^{**}(\iota\lambda\iota^*)\alpha_j^{**} = \alpha_i\lambda\alpha_j = \ell_i\delta_{ij}.$$

□

Lemma 3.9. *Let $f\colon A \to B$ be an isogeny and $\mathscr{L}$ be an invertible line bundle on B. Then $\mathscr{L}$ is ample if and only if $f^*\mathscr{L}$ is ample.*

Proof. An isogeny is a finite faithfully flat morphism. So ampleness ascends along the isogeny, since it is finite, by [GD64, p. II.5.1.12], and descends since it is faithfully flat [GD64, p. IV.2.7.2] (the proof holds for relative ampleness but it is easy to adapt it for ampleness, see also [Liu02, Exercise 5.1.29]). □

Lemma 3.10. *Let L be a R-lattice and $A = \mathscr{F}_E(L)$ be the corresponding abelian variety. Let $\lambda : L \to L^*$ be such that H_λ is hermitian and $a = \mathscr{F}_E(\lambda)\colon A \to \widehat{A}$ be the corresponding isogeny. Then there exists an isogeny $f\colon E^g \to A$, integers $(\ell_i)_{1\le i\le g}$, a map $D \in End(E^g) : (x_1, \dots, x_g) \mapsto (\ell_1 x_1, \dots, \ell_g x_g)$ and a commutative diagram*

$$\begin{array}{ccc} A & \xrightarrow{a} & \widehat{A} \\ {\scriptstyle f}\uparrow & & \downarrow{\scriptstyle \widehat{f}} \\ E^g & \xrightarrow{a_0 \circ D} & \widehat{E^g} \end{array}$$

FIGURE 1. Fundamental diagram

where a_0 is the product polarization on E^g. Moreover a is a polarization if and only if $\ell_i > 0$ for all i, or equivalently if and only if H_λ is positive definite on FL^*.

Proof. Let $\iota : L \hookrightarrow N = \bigoplus_{i=1}^g Re_i$ and $\lambda' = \iota\lambda\iota^*$ be as in Lemma 3.8. Consider the isomorphism $u\colon N \xrightarrow{\sim} R^g$ given by the basis (e_i) of N. Hence we have

$$\begin{array}{ccccccccc} & & & & L^* & \xrightarrow{\lambda} & L & & \\ & & & & {\scriptstyle \iota^*}\uparrow & & \downarrow{\scriptstyle \iota} & & \\ (R^g)^* & \xrightarrow[\Lambda_0]{\sim} & R^g & \xrightarrow[u^*]{\sim} & N^* & \xrightarrow{\lambda'} & N & \xrightarrow[u]{\sim} & R^g. \end{array}$$

We obtain the desired diagram by composing this diagram by $\mathscr{F}_E$ and taking $f = \mathscr{F}_E(u\iota)$.
Since H_λ is hermitian, there exists a line bundle $\mathscr{L}$ on A such that $a = \phi_{\mathscr{L}}$. Since $a_0 D$ is the pullback of a by f the isogeny a is a polarization if and only $a_0 D$ is a polarization by Lemma 3.9 below. Moreover, $a_0 D$ is a polarization of E^g if and only if $\ell_i > 0$ for all i. As in the first part of Lemma 3.7, we can conclude that H_λ is positive definite if and only if $H_{\lambda'} = \mathrm{diag}(\ell_1, \dots, \ell_g)$ is, and we have the final equivalence of the lemma. □

Remark 3.11. The fact that H_λ is a hermitian form on L^* and not on L is a bit cumbersome. Since λ is injective, it induces an isomorphism $\Lambda := (\lambda \otimes_R \mathrm{Id}_F)^{-1}\colon L \otimes F = V \to V^*$. This defines a hermitian form on V given by

$$h\colon V \times V \to F, (x, y) \mapsto \Lambda(x)(y)$$

which makes (L, h) a hermitian R-lattice.

Proof of Theorem 3.3. Simply combine Lemmas 3.7 and 3.10 with remark 3.11 to get h on $L \times L$ instead of H_λ on $L^* \times L^*$. The final statement about the degree of the polarization is easily obtained using [JKP+18, Theorem 4.4] which computes the degree of an isogeny corresponding to an inclusion of lattices with equal rank $\iota\colon L \to M$ by $\deg \mathscr{F}_E(\iota) = [M\colon \iota(L)]$. □

3.3. **Description of the abelian variety as a quotient of E^g.** Let (L, h) be a hermitian lattice with $L^\#$ integral. The goal of this section is to compute the kernel of the isogeny $f\colon E^g \to A = \mathscr{F}_E(L)$ of Corollary 3.10 obtained by the inclusion $L \hookrightarrow R^g$ induced by ι in Lemma 3.8 after identification of $N = \bigoplus Re_i$ with R^g.

As a first step, to apply Corollary 3.6, we need to start with an explicit elliptic curve $E/\mathbb{F}_q$ with ring of endomorphism $\mathbb{Z}[\pi]$. There are several algorithms in the literature to determine the endomorphism ring of an ordinary elliptic curve [EL10] or [BS11]. We use a version of the latter kindly provided by Sutherland and apply it to the list of elliptic curves with a given trace (which can be naively obtained from the list of all elliptic curves computing the trace on each of them).

Given an inclusion of equal rank g R-lattices $\iota\colon L_1 \to L_2$ and surjective morphisms $T_i\colon R^{m_i} \to L_i$ we can lift ι to $P \in M_{m_2,m_1}(R)$

$$\begin{array}{ccc} R^{m_1} & \xrightarrow{T_1} & L_1 \\ {\scriptstyle P}\downarrow & & \downarrow{\scriptstyle \iota} \\ R^{m_2} & \xrightarrow{T_2} & L_2 \end{array}$$

by computing the image of the canonical basis of R^{m_1} by $\iota \circ T_1$ and taking any preimages by T_2. Since the morphisms T_i are surjective, $\mathscr{F}_E(T_i)$ are injective and the kernel of the corresponding isogeny $\mathscr{F}_E(\iota) = f\colon \mathscr{F}_E(L_2) \to \mathscr{F}_E(L_1)$ can be computed by $\ker f = \mathscr{F}_E(T_2)^{-1} \ker {}^tP$.

In the present situation, $L_1 = L, L_2 = N = \bigoplus Re_i, m_2 = g$ and $T_2 = \mathrm{Id}$. It remains to make T_1 and the (e_i) explicit. Consider a pseudo-basis $L = \mathfrak{a}_1 x_1 \oplus \cdots \oplus \mathfrak{a}_g x_g$. Since the $\mathfrak{a}_i$ are fractional R-ideals they have at most 2 generators. Hence, L is generated by $g \leq r \leq 2g$ generators. So, T_1 is the surjective morphism $R^r \twoheadrightarrow L$ sending the canonical basis of R^r on the generators of L. Applying the functor $\mathscr{F}_E$ to the composition leads to the commutative diagram

$$\begin{array}{ccc} E^r & \xleftarrow{\mathscr{F}_E(T_1)} & A \\ {\scriptstyle {}^tP}\uparrow & \nearrow_{f} & \\ E^g & & \end{array}$$

and $\ker f = \ker(\mathscr{F}_E(T_1) \circ f) = \ker {}^tP$. By Figure 1, one sees that $\ker f \subseteq \ker D = \prod_{i=1}^g E[\ell_i] \subseteq E[\ell]^g$ with $\ell = \mathrm{lcm}(\ell_i)$ and D the map of Lemma 3.10. Thus, it is enough to compute the action of ${}^tP$ on a basis of the ℓ-torsion of E^g to have the whole kernel. To go on, we will assume that ℓ is prime to $\mathrm{char}\, \mathbb{F}_q$ so $E[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$ is étale and we can work with geometric points.

Let clarify how to compute the family $(e_i)_{1\leq i\leq g}$. Let us recall that we defined it as the dual basis of an orthogonal family of L^* so they satisfy $e_i^* \lambda' e_j^* = \ell_i \delta_{ij}$. This means that $\lambda'(e_i^*) = \ell_i e_i$ and then $h(e_i, e_i) = \frac{1}{\ell_i}$ (see proof of Lemma 3.5). Consider an orthogonal family $(u_i)_{1\leq i\leq g}$ of vectors of $L^\#$ of norm $(\ell_i)_{1\leq i\leq g}$ and let $e_i = \frac{1}{\ell_i} u_i$. By the inclusion $\bigoplus_{i=1}^g Ru_i \subseteq L^\#$ we have

$$L \subseteq \left(\perp\!\!\!\perp_{1\leq i\leq g} Ru_i \right)^\# = \perp\!\!\!\perp_{1\leq i\leq g} (Ru_i)^\# = \perp\!\!\!\perp_{1\leq i\leq g} Re_i.$$

Hence, if we find an orthogonal family $(u_i)_{1\leq i\leq g}$ of $L^\#$ with norm $(\ell_i)_{1\leq i\leq g}$ then $(e_i)_{1\leq i\leq g} = (1/\ell_i \cdot u_i)_{1\leq i\leq g}$ is an orthogonal family of norm $(1/\ell_i)_{1\leq i\leq g}$ suited for the inclusion $\iota\colon L \to \bigoplus_{i=1}^g Re_i$.

We summarize these computations in Algorithm 6.

Algorithm 6 Computation of the kernel of an isogeny $E^g \to A$

Input: A R-lattice (L, h) and E an elliptic curve over $\mathbb{F}_q$ with $\mathrm{End}(E) = \mathbb{Z}[\pi] \simeq R$.

Output: A basis of the kernel of an isogeny $f : E^g \to \mathscr{F}_E(L)$ such that the polarization a on L induced by h satisfies $\hat{f} a f$ is a completely decomposable polarization.

1: Compute an orthogonal family $(u_i)_{1\leq i\leq g}$ of $L^\#$ of norms $\ell_i \in \mathbb{Z}$ using Algorithm 4. Define $e_i = u_i/\ell_i$ and $\ell = \mathrm{lcm}(\ell_i)$.
2: Compute a pseudo-basis $L = \mathfrak{a}_1 x_1 \oplus \cdots \oplus \mathfrak{a}_g x_g$ given by $1 \leq r \leq 2g$ generators.
3: Let P be the matrix defined by the morphism $\iota \circ T_1 : R^r \to N$ in the canonical basis of R^r and the basis (e_i) of N.
4: Compute a basis (b_0, b_1) of $E[\ell]$. This fixes an identification of $E[\ell]$ with $(\mathbb{Z}/\ell\mathbb{Z})^2$;
5: Compute the action of the Frobenius π on $\mathscr{B}$ as a matrix $\Pi \in M_2(\mathbb{Z}/\ell\mathbb{Z})$.
6: Create a matrix $Q \in M_{2r,2g}(\mathbb{Z}/\ell\mathbb{Z})$ by replacing each entry $a + b\pi$ of ${}^tP$ by $aI_2 + b\Pi$.
7: Compute a basis $\mathscr{B}$ of $\ker Q \in M_{2r,2g}(\mathbb{Z}/\ell\mathbb{Z})$.
8: **return** $\mu^{-1}(\mathscr{B})$.

We will use this algorithm with the additional condition $\ell_1 = \ldots = \ell_g$. Hence, for Step 1 of Algorithm 6 one can use Algorithm 5. Indeed, in Section 4, we need more specific properties about the kernel K of the

isogeny in order to be able to compute the theta null point on A using the current algorithms. We first require that $\ell = \ell_1 = \ldots = \ell_g$ is odd and prime to q (see Remark 4.1 for the condition ℓ odd). We have discussed in Theorem 2.16, when this can be achieved. By [Mil86, Prop.16.8], K is a maximal isotropic subgroup of $E[\ell]^g$ for the Weil pairing on E^g induced by the product polarization. However for the algorithms we also need K to be of rank g, that is isomorphic as a group to $(\mathbb{Z}/\ell\mathbb{Z})^g$. We call such a K a *totally isotropic* subgroup. Equivalently, for an abelian variety A_0, $K \subset A_0[\ell]$ is a *totally isotropic* subgroup of level ℓ if it is isotropic, and one can find a symplectic decomposition $A_0[\ell] = K \oplus K'$. If K is maximal isotropic, it is always totally isotropic when ℓ is square free, but this can fail if ℓ has a square factor (for instance $A_0[\ell]$ is maximal isotropic in $A_0[\ell^2]$). In every computation we made, when an odd ℓ exists, we always found one for which K was totally isotropic.

4. Theta structures and a modular interpretation of the isogeny formula

In this section, k is any field of characteristic $p \neq 2$. We will first recall in Section 4.1 how to use the so-called isogeny formula to derive the theta null point on a target abelian variety from a (well-chosen) isogenous one. Then, in Section 4.2, we will show that the isogeny formula is actually valid over the universal abelian scheme. Although the proof basically follows the same lines as the proof over a field, this result, and the notation introduced there, will be useful in Section 4.3, where we will derive a precise affine version of the isogeny formula. More precisely, we introduce a particular choice of affine lifts of the theta null points which we call *modular*, since they are derived from interpreting the theta constants as modular forms, and we show in Theorem 4.5 that the isogeny formula respects the modular lifts. In Section 4.4, we explain how to compute k-rational modular lifts for a product of elliptic curves with a product polarization. Combining the 'modular' isogeny formula and these initial modular lifts allow us in Section 4.5 to compute values of Siegel modular forms of even weight given as polynomials in the theta constants with coefficients in k on the span of the isogeny class (see Theorem 4.9 and Algorithm 8).

4.1. Input for the isogeny formula over k.

Let $(A, \mathscr{L}, \Theta_{\mathscr{L}})/k$ be a principally polarized abelian variety of dimension g with a totally symmetric theta structure $\Theta_{\mathscr{L}}$ of level n on $\mathscr{L}$. This implies that n is even which we assume from now on (until the end of this section). Let K be a k-rational totally isotropic subgroup for the Weil pairing of $\mathscr{L}^\ell$, with ℓ prime to np or to n if $p = 0$.

In [CR15; LR15], an algorithm (which we call the *isogeny formula* and implemented in the package `Avisogenies` [BCR10]) is given to compute the isogeny $f : (A, \mathscr{L}, \Theta_{\mathscr{L}}) \to (B, \mathscr{M}, \Theta_{\mathscr{M}})$ where $B = A/K$, $f^*\mathscr{M} = \mathscr{L}^\ell$ and $\Theta_{\mathscr{M}}$ is the unique symmetric theta structure of level n on $\mathscr{M}$ compatible with $\Theta_{\mathscr{L}}$ (the unicity comes from the fact that ℓ is prime to n). More precisely the algorithm takes as input the (projective) theta null point $\theta^A(0) := \left(\theta^A_{i\in Z(\overline{n})}(0)\right) \in \mathbb{P}(\bar{k})^{n^g-1}$ of A, where $Z(\overline{n}) = (\mathbb{Z}/n\mathbb{Z})^g$, along with the theta coordinates of the geometric points of K (or suitable equations giving the kernel K) and outputs the theta null point $\theta^B(0) := \left(\theta^B_{i\in Z(\overline{n})}(0)\right)$ of B along with the equations for the isogeny f. We usually take $n = 4$ (since this is the smallest even n which gives an embedding of the variety into projective space) and the theta null point completely characterizes $(B, \mathscr{M})$ up to $\bar{k}$-isomorphism. We will describe in more details (a generalisation of) this algorithm in Section 4.2. In this section we explain how to compute the inputs for the isogeny formula in our situation.

Let E/k be an elliptic curve. If $(B, \mathscr{M})$ is isogenous to E^g, we show how to compute $\theta^B(0)$ of level 4 by applying the algorithm with $A = \prod_{i=1}^g E_i$ where E_i are elliptic curves over k isogenous to E and $\mathscr{L}$ the principal product polarization on A. For this, we need three elements as inputs for the algorithm:

- compute a totally isotropic kernel K such that $B = A/K$. When k is a finite field and $E = E_1 = \ldots = E_g$ is ordinary, we have seen in Section 3.3 how to do this effectively;
- compute the theta null point $\theta^A(0)$ of level 4 on $(A, \mathscr{L})$. As we deal with the product polarization, the coordinate $\theta^A_{i_1,\ldots,i_g}(0)$ of $\theta^A(0)$ is equal to $\prod_{1\leq j\leq g} \theta^{E_j}_{i_j}(0)$. Getting the theta null point on an elliptic curve (over a field of odd characteristic) is a classical result. In Corollary 4.8, we give an even more precise version of this to which we refer now and that we use in Step 1 and 2 of Algorithm 7.

- compute the theta coordinates of the points in the kernel K. Likewise since we have a product polarization, $\theta^A_{i_1,\dots,i_g}(x_1,\dots,x_g) = \prod_{1\le j\le g}\theta^{E_j}_{i_j}(x_j)$. Computing the theta coordinates $\left(\theta^{E_i}_j(x_i)\right)_{j\in\mathbb{Z}/4\mathbb{Z}}$ is also classical [Mum07b], [Cos11, Chapter 5], and is implemented in `Avisogenies` [BCR10].

We therefore get the following algorithm 7.

Algorithm 7 Computation of the theta null point of level 4 on the quotient variety

Input: Elliptic curves E_i/k with equation $y^2 = (x-e_{1i})(x-e_{2i})(x-e_{3i})$ where k is of characteristic p different from 2, a k-rational totally isotropic subgroup K of $A = \prod_i E_i$ of order prime to $2p$ (or just prime to 2 if $p=0$).

Output: The theta null point $\theta^B(0)$ of level 4 on $B = A/K$ with $\mathscr{M}$ the polarization induced by the product polarization on A.

1: For all $1\le i\le g$, define $\theta'^{E_i}_0 = \sqrt[4]{e_{1i}-e_{3i}}, \theta'^{E_i}_1 = \sqrt[4]{e_{1i}-e_{2i}}, \theta'^{E_i}_2 = \sqrt[4]{e_{2i}-e_{3i}}$ for arbitrary choices of the roots.

2: Compute $\theta^{E_i}_0(0) = \theta'^{E_i}_0 + \theta'^{E_i}_1$, $\theta^{E_i}_2(0) = \theta'^{E_i}_0 - \theta'^{E_i}_1$ and $\theta^{E_i}_1(0) = \theta^{E_i}_3(0) = \theta'^{E_i}_2$ for all $1\le i\le g$.

3: Compute $\theta^A_{(i_1,\dots,i_g)}(0) = \theta^{E_1}_{i_1}(0)\cdots\theta^{E_g}_{i_g}(0)$ for all $(i_1,\dots,i_g)\in Z(\overline{4})$.

4: For all $1\le i\le g$ and for all $x=(x_1,\dots,x_g)\in K\setminus\{0\}$, compute the theta coordinates $\left(\theta^{E_i}_j(x_i)\right)_{j\in\mathbb{Z}/4\mathbb{Z}}$, using [Cos11, Chapter 5],

5: Compute for all $j=(j_1,\dots,j_g)\in Z(\overline{4})$ and for all $x=(x_1,\dots,x_g)\in K\setminus\{0\}$ $\theta^A_j(x) = \theta^{E_1}_{j_1}(x_1)\cdots\theta^{E_g}_{j_g}(x_g)$.

6: Use [CR15]taking as input $\theta^A(0)$ and the theta coordinates of the points of K and output $\theta^B(0)$.

7: **return** $\theta^B(0)\in\mathbb{P}(\bar{k})^{4^g-1}$.

Remark 4.1. Some remarks on the code:

- The original version of `Avisogenies` assumed ℓ to be a prime. The only modification to the code we had to make is on how to construct a matrix $F\in \mathrm{Mat}_r(\mathbb{Z})$ such that ${}^tFF = \ell\mathrm{Id}$ used by Koizumi's formula Eq. (6). The integer r depends on ℓ being a square (hence $r=1$), ℓ being a sum of two positive squares (hence $r=2$) or a sum of four positive square (hence $r=4$). Adapting the construction of F to ℓ odd non prime is straightforward by multiplicativity of the complex norm (if $r=2$) or of the quaternionic norm (if $r=4$).
- The restriction ℓ odd is not necessary in theory if some great care is taken. First the lift from level n to level ℓn is more complicated since we cannot work only on the points in the kernel K. We first need to compute a basis of points P_i such that nP_i is a basis of K (this was given to us for free before by the CRT). Furthermore this basis has to be compatible with the level n structure on A, so this may require first to act by an automorphism of the theta structure to make the level n structure on A compatible with $K[n]$. Secondly, if ℓ is not odd, then there may be several symmetric theta structures on B compatible with the one on A. So the isogeny formula in this case yields several solutions. This has not yet been implemented in [BCR10].

4.2. **The isogeny formula on the universal abelian scheme.** In this section we reformulate the isogeny formulae from [CR15] to show that the formulae are polynomials with coefficients in $\mathbb{Z}[\frac{1}{\ell n}]$ in the coordinates of the points of K. Since the fine moduli scheme (or stack if $n\le 2$) $\mathscr{A}_{g,n}$ of abelian varieties with a symmetric theta structure of level n is smooth (or by rigidity [MFK94, § 6]), the isogeny formula is thus valid on the universal abelian variety defined over $\mathbb{Z}[\frac{1}{\ell n}]$. Though well known to experts, this is not completely obvious in the formulation of [CR15] since the authors only work with fields and implicitly use divisions in their equations.

We first give some motivations for this result. In Section 4.3 we give an algebraic modular interpretation of the isogeny formula by first considering the analytic modular interpretation over $\mathbb{C}$. It is then possible, by standard lifting arguments to extend this result to ordinary abelian varieties over a finite field. But, while possible, this is a bit painful to do properly since we want to control the lifts of the endomorphisms along with the differentials, and then give an algebraic meaning to the reduction of the period matrix modulo p. By contrast, showing that the isogeny formula is actually defined over $\mathbb{Z}[\frac{1}{\ell}]$ yields a much simpler proof that the

analytic interpretation holds algebraically. Indeed, by smoothness, the modular interpretation is ultimately a statement about the equality of two multivariate polynomials defined over $\mathbb{Z}[\frac{1}{\ell}]$. But this equality holds when it holds over $\mathbb{C}$. In addition, this proof holds for all abelian varieties rather than just the ordinary ones. The notations introduced in this section will also be useful in Section 4.3 where we keep track of each modular factor at each step of the algorithm.

In order to avoid heavy notation, we will often let the theta structure $\Theta_{\mathscr{L}}$ (and eventually the polarization $\mathscr{L}$) be implicit, along with the coordinate group $Z(\overline{n})$.

Assume from now on that n is (even and) greater or equal to 4 and ℓ prime to n. Mumford constructs in [Mum67] the universal abelian variety $\mathscr{X}_{g,n} \to \mathscr{A}_{g,n}$ with a totally symmetric normalized relatively ample line bundle[2] and a symmetric theta structure of level n over $\mathbb{Z}[1/n]$ [3] as a quasi-projective scheme. Moreover Mumford uses Riemann's relations [Mum67, p. 83] to define a projective scheme $\overline{\mathscr{X}}_{g,n} \to \overline{\mathscr{A}}_{g,n}$ (where the equations of $\overline{\mathscr{A}}_{g,n}$ are given by evaluating the Riemann's relations on the zero section, together with the symmetry relations $\theta_i(0) = \theta_{-i}(0)$) and an embedding of $\mathscr{X}_{g,n} \to \mathscr{A}_{g,n}$ into $\overline{\mathscr{X}}_{g,n} \to \overline{\mathscr{A}}_{g,n}$ (so that $\mathscr{X}_{g,n}$ is the pullback of $\overline{\mathscr{X}}_{g,n}$ to $\mathscr{A}_{g,n}$). We denote $(\theta_i)_{i\in Z(\overline{n})}$ the theta coordinates on either $\mathscr{X}_{g,n}$ or $\overline{\mathscr{X}}_{g,n}$ and $(\theta_i(0))_{i\in Z(\overline{n})}$ the theta null point coordinates on either $\mathscr{A}_{g,n}$ or $\overline{\mathscr{A}}_{g,n}$ coming from the section $s : \overline{\mathscr{A}}_{g,n} \to \overline{\mathscr{X}}_{g,n}$ (which restricted to $\mathscr{A}_{g,n}$ corresponds to the zero section).

On $\overline{\mathscr{X}}_{g,n}$, we have an explicit action λ of the Heisenberg group $\mathcal{H}(\overline{n})$ on $\mathscr{L}_{\overline{\mathscr{X}}_{g,n}}$ [Mum67, Step 1, p. 84]. Writing $\mathcal{H}(\overline{n}) = \mathbb{G}_m \times Z(\overline{n}) \times \hat{Z}(\overline{n})$ where $\hat{Z}(\overline{n}) \simeq \oplus_{i=1}^{g}\mu_n$ is the Cartier dual of $Z(\overline{n})$, this canonical action is given by $\lambda(i).\theta_j = \theta_{i+j}$ for $i \in Z(\overline{n})$ and $\lambda(i).\theta_j =< i, j > \theta_j$ for $i \in \hat{Z}(\overline{n})$ where $< i, j >$ is the canonical pairing between $Z(\overline{n})$ and its Cartier dual $\hat{Z}(\overline{n})$. Acting on the zero section s gives a canonical basis of n-torsion.

Mumford's isogeny theorem [Mum66] then describes the universal isogeny (with a descent of level of the theta structure)

$$\pi_1 : \mathscr{X}_{g,\ell n} \to \mathscr{X}_{g,n}, (\theta_i)_{i\in Z(\overline{\ell n})} \mapsto (\theta_i)_{i\in Z(\overline{n})\subset Z(\overline{\ell n})}. \tag{3}$$

On $\mathscr{X}_{g,\ell n}$ the level ℓn theta structure induces a symplectic basis of the ℓn-torsion, and in particular a symplectic decomposition $K_1 \oplus K_2$ of the ℓ-torsion. Concretely over a field k, $K_1 = \{(< i, j > \theta_j(0))_{j\in Z(\overline{\ell n})}\}_{i\in\hat{Z}(\overline{\ell})}$ is the kernel of π_1, while $K_2 = \{(\theta_{i+j}(0))_{j\in Z(\overline{\ell n})}\}_{i\in Z(\overline{\ell})}$ is such that $\pi_1(K_2) = \{(\theta_{i+j}(0))_{j\in Z(\overline{n})}\}_{i\in Z(\overline{\ell})}$ is the kernel of the contragredient isogeny $\tilde{\pi}_1$.

Using π_1, we can now describe the isogeny formula in three steps.

Step 1. Denote $\Pi_1 : \mathscr{X}_{g,\ell n} \to \mathscr{X}_{g,n}^{\ell^g}, (\theta_i)_{i\in Z(\overline{\ell n})} \mapsto \left(\pi_1(\lambda(i)(\theta_j))_{j\in Z(\overline{\ell n})}\right)_{i\in Z(l)}$, where λ is the action of the Heisenberg group $\mathcal{H}(\overline{\ell n})$ described above. For $j \in Z(\overline{\ell})$ the component Π_1^j of Π_1 is given by

$$\Pi_1^{j*}(\theta_i^{\mathscr{X}_{g,n}}) = \theta_{i+j}^{\mathscr{X}_{g,\ell n}}, \quad i \in Z(\overline{n}). \tag{4}$$

The image of the restriction of Π_1 to $\mathscr{A}_{g,\ell n}$ (seen as the zero section of $\mathscr{X}_{g,\ell n}$) then describes the moduli scheme $\mathscr{T}_{g,n,\ell}$ of abelian varieties with a level n symmetric theta structure together with the points of an isotropic kernel of the ℓ-torsion.

It is easy to see that π_1 extends to a morphism $\overline{\pi}_1 : \overline{\mathscr{X}}_{g,\ell n} \to \overline{\mathscr{X}}_{g,n}$. Since the action λ is defined on $\overline{\mathscr{X}}_{g,\ell n}$, we can also extend Π_1 to a morphism $\overline{\Pi}_1 : \overline{\mathscr{X}}_{g,\ell n} \to \overline{\mathscr{X}}_{g,n}^{\ell^g}$. Let $\overline{T}$ be the image of $\overline{\mathscr{A}}_{g,\ell n}$. By construction $\mathscr{T}_{g,n,\ell}$ embeds into $\overline{T}$ and since we have explicit equations for $\overline{\mathscr{A}}_{g,\ell n}$ we have equations for $\overline{T}$.

By construction, given a k-point (A_0, K_0) of $\mathscr{T}_{g,n,\ell}$, geometric points of $\Pi_1^{-1}(A_0, K_0) \to \mathscr{A}_{g,\ell n}$ corresponds to abelian varieties $B_{0,\overline{k}} \in \mathscr{A}_{g,\ell n}(\overline{k})$ with a level ℓn symmetric theta structure such that the universal isogeny π_1 restricted to B_0 is the contragredient isogeny of $A_{0,\overline{k}} \to A_{0,\overline{k}}/K_{0,\overline{k}}$. In particular, starting with our abelian variety $(A, \mathscr{L})/k$, if k' is an étale extension of k such that all points of K are defined, then fixing an isomorphism $Z(\overline{\ell}) \to K$ over k' yields a k'-point of $\mathscr{T}_{g,n,\ell}$. A k"-point in $\Pi_1^{-1}(A, K)$ then correspond to a theta structure on $(B, \mathscr{M}^{\ell})$ defined over k" such that the contragredient isogeny $\tilde{f} : B \to A$ is given by the pullback of π_1 to B.

[2] See [Mum67, Definition p.78] for the definition of these terms.

[3] The irreducible components are defined over $\mathbb{Z}[1/n, \zeta_n]$ since over this ring all points of the level n Heisenberg group $\mathcal{H}(\overline{n})$ are defined.

The discussions in [LR16, Corollary 3.6, Proposition 3.7], [Rob10, Algorithm 4.4.10]), [CR15, § 4.1], [LR12b] can then be reinterpreted as a way to use Riemann relations to give explicit equations for $\overline{\Pi}_1^{-1}(A,K)$ and $\Pi_1^{-1}(A,K)$.

Step 2. Now let $r=1$ if ℓ is a square, $r=2$ if ℓ is a sum of two squares and $r=4$ otherwise (the reason of our choice of r will appear in Step 3). On $\mathscr{A}_{g,\ell n}$ the Segre embedding yields a map $\pi_2 : \mathscr{A}_{g,1} \to \mathscr{A}_{rg,\ell n}$, which sends the universal abelian variety $\mathscr{X}_{g,\ell n}$ to $\mathscr{X}_{g,\ell n}^r$ with its product theta structure [Mum66, Lemma 1, p. 323]. Concretely,

$$\pi_2^*(\theta_{i_1,\dots,i_r}^{\mathscr{X}_{rg,\ell n}}) = \theta_{i_1}^{\mathscr{X}_{g,\ell n}} \cdot \dots \cdot \theta_{i_r}^{\mathscr{X}_{g,\ell n}} \tag{5}$$

In particular, π_2 sends the theta null point of level ℓn of $(B, \mathscr{M}^\ell)$ to the theta null point of $(B^r, \mathscr{M}^\ell \star \dots \star \mathscr{M}^\ell)$ [4].

Step 3. Let F be an $r \times r$ matrix with integral coefficients such that ${}^tFF = \ell \mathrm{Id}$ (see remark 4.1). Then the Koizumi-Kempf formula [Koi76; Kem89] yields a map $\pi_3 : \mathscr{A}_{rg,\ell n} \to \mathscr{A}_{rg,n}$ which corresponds to the isogeny $F : \mathscr{X}_{g,\ell n}^r \to \mathscr{X}_{g,\ell n}^r$ along with the descent of product theta structure from level ℓn to level n. The formula is given, for $(i_1,\dots,i_r) \in Z(\overline{n})^r$, by

$$\pi_3^*(\theta_{i_1,\dots,i_g}^{\mathscr{X}_{rg,n}}) = F^*(\theta_{i_1}^{\mathscr{X}_{g,n}} \cdot \dots \cdot \theta_{i_r}^{\mathscr{X}_{g,n}}) = \sum_{\substack{(j_1,\dots,j_r) \in Z(\overline{\ell n})^r \\ F(j_1,\dots,j_r)=(i_1,\dots,i_r)}} \theta_{j_1}^{\mathscr{X}_{g,\ell n}} \cdot \dots \cdot \theta_{j_r}^{\mathscr{X}_{g,\ell n}}. \tag{6}$$

Since Eq. (6) is homogeneous, this is well defined for projective coordinates.

In particular, π_3 uses F to send $(B^r, \mathscr{M}^\ell \star \dots \star \mathscr{M}^\ell)$ to $(B^r, \mathscr{M} \star \dots \star \mathscr{M})$, from which $(B, \mathscr{M})$ can be recovered by projecting to one of the factor.

The *isogeny formula* is then the composition $\pi_3 \circ \pi_2 \circ \Pi_1^{-1}$.

Theorem 4.2. *Let n be an even integer greater or equal to 4 and ℓ be an integer prime to n. The image of $\Pi_1 \times \pi_3 \circ \pi_2 : \mathscr{A}_{g,\ell n} \to \mathscr{T}_{g,n,\ell} \times \mathscr{A}_{g,n}$ induces a modular correspondence defined over $\mathbb{Z}[\frac{1}{\ell n}]$.*

Let k be a field of characteristic prime to ℓn. If (A,K) is a k-point of $\mathscr{T}_{g,n,\ell}$, then $\pi_3 \circ \pi_2 \circ \Pi_1^{-1}(A,K)$ only has a single $\overline{k}$-point (with multiplicity ℓ^g and which is actually defined over k), corresponding to A/K.

This point can be computed in $O(\ell^{g \max(1,r/2)})$ operations in k where, by assumption, k contains the field of definition of the geometric points of K.

Proof. The first part follows from the steps above. For the statement over a field k, by construction, each geometric point in $\Pi_1^{-1}(A,K)$ corresponds to $B = A/K$ with a level ℓn structure compatible with the level n structure on A. Descending the product level ℓn structure via F then induce the same level n structure on B.

For the complexity estimate, writing equations for Π_1^{-1} is in $O(\ell^g)$ operations, the Segre embedding only depends on n so is absorbed by the big O notation, and computing π_3 requires $O(\ell^{r/2})$ operations, hence the total complexity. We refer to [CR15] for more details. □

4.3. **Modular interpretation.** Consider again the algorithm from Theorem 4.2 but suppose now that we would like to apply it to an affine lift of a theta null point of $(A, \mathscr{L}, \Theta_{\mathscr{L}})$. Notice that the choice of an affine lift is induced by the choice of a trivialization of $\mathscr{L}$ since the θ_i^A are sections of a power of $\mathscr{L}$. Since π_1, π_2 and π_3 are well defined as affine morphisms (using the exact same equations), we can also interpret the isogeny formula $\pi_3 \circ \pi_2 \circ \Pi_1^{-1}$ as an *affine isogeny formula*, yielding an affine lift of the theta null point of $B = A/K$.

In this section, we want to achieve two goals: give the precise relation between affine lifts on A and B through the affine isogeny formula (Theorem 4.5) and also show that we can compute Siegel modular forms constructed as polynomials in the theta constants.

For both purposes, we will need modularity and we therefore start with some classical notions on Siegel modular forms (see for instance [Cha86; DM69; FC90; BGH+08]). As before, let $g \geq 1$, n even and greater or equal to 4. Let $\pi : \mathscr{X}_{g,n} \to \mathscr{A}_{g,n}$ be the universal abelian variety with a totally symmetric normalized

[4] If $\mathscr{L}_1$ is a line bundle on A_1 and $\mathscr{L}_2$ is a line bundle on A_2 we use the notation $\mathscr{L}_1 \star \mathscr{L}_2$ to denote the line bundle $p_1^*\mathscr{L}_1 \otimes p_2^*\mathscr{L}_2$ where p_i is the projection $A_1 \times A_2 \to A_i$.

relatively ample line bundle and a symmetric theta structure of level n over $\mathbb{Z}[\frac{1}{n}]$ and $s : \mathscr{A}_{g,n} \to \mathscr{X}_{g,n}$ be the zero section. We denote $\mathcal{H} = \wedge^g(s^*\Omega_{\mathscr{X}_{g,n}}) = \wedge^g(\pi_*\Omega_{\mathscr{X}_{g,n}})$ the Hodge line bundle.

Let R be a commutative ring with all residue fields k of characteristic $p = 0$ or prime to n. Recall that a (scalar) Siegel modular form χ of integral weight $\rho \geq 1$ and level n [5] over R is a section of $\mathcal{H}^\rho$ on $\mathscr{A}_{g,n} \otimes R$ [6]. For a given $(A, \mathscr{L}, \Theta_{\mathscr{L}}) \in \mathscr{A}_{g,n}(k)$ and w_A a basis of k-rational regular differentials on A, it can also be seen as a function $\chi : (A, \mathscr{L}, \Theta_{\mathscr{L}}, w_A) \mapsto k$, such that $\chi(A, \mathscr{L}, \Theta_{\mathscr{L}}, \lambda w_A) = (\det \lambda)^\rho \cdot \chi(A, \mathscr{L}, \Theta_{\mathscr{L}}, w_A)$ for any $\lambda \in \mathrm{GL}_g(\overline{k})$. Likewise, a Siegel modular form χ of weight ρ and level 1 [7] is a section of $\mathcal{H}^\rho$ on the algebraic stack $\mathscr{A}_{g,1}$ of principally polarized abelian schemes. In that case, we simply write $\chi(A, \mathscr{L}, w_A)$.

Let $\mathscr{L}_{\mathscr{X}_{g,n}}$ be the totally symmetric normalized relatively ample line bundle on $\mathscr{X}_{g,n}$ as in Section 4.2. Let $\iota : \operatorname{Spec} k \to \mathscr{A}_{g,n} \xrightarrow{s} \mathscr{X}_{g,n}$ corresponding to a closed point $(A, \mathscr{L}, \Theta_A) \in \mathscr{A}_{g,n}(k)$. We have that $\iota^*\theta^{\mathscr{X}_{g,n}}(0) = \theta^A(0)$, as projective coordinates. In the special case where $k = \mathbb{C}$, let Ω be a Riemann matrix in the Siegel upper half-space $\mathbb{H}_g$ and let us denote $\vartheta\left[\begin{smallmatrix} x_1 \\ x_2 \end{smallmatrix}\right](0, \Omega)$, the value at 0 of the classical theta function with characteristic $(x_1, x_2) \in \mathbb{Q}^{2g}$ [Mum07a, p.192]. We will refer to these complex values as *theta constants* (in contrast with the theta coordinates when speaking about the $\theta_i^A(0)$). Following [Mum07c, Prop. 5.11] (see also loc. cit. Definition. 5.8 and p. 36), if $(A, \mathscr{L}, \Theta_A) = \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$, with its associated polarization induced by $\mathrm{Im}\Omega^{-1}$ and associated canonical symmetric level structure induced by the canonical symplectic basis on the lattice, then $(\theta_i^A(0))_{i \in Z(\overline{n})}$ is projectively equal to $(\vartheta\left[\begin{smallmatrix} 0 \\ i/n \end{smallmatrix}\right](0, \Omega/n))$ for arbitrary lifts of $i \in Z(\overline{n})$ to $\mathbb{Z}^g$. In fact Mumford shows this equality for the adically defined theta functions. For the level n algebraic theta functions, it suffices to remark that both the algebraic $\theta_i(z)$ and analytic $\vartheta\left[\begin{smallmatrix} 0 \\ i/n \end{smallmatrix}\right](z, \Omega/n)$ theta functions satisfy the canonical irreducible representation of the Heisenberg group of level n [Mum66, Theorem 2 and definition p. 297].

We will use this projective equality to fix a particular choice of affine lifts over any field in the following way. Because of the transformation formula [Mum07a, Cor.5.11], if we define for any $i, j \in Z(\overline{n})$,

$$\chi_{ij}(A, \mathscr{L}, \Theta_A, (2i\pi dz_1, \ldots, 2i\pi dz_g)) = \vartheta\left[\begin{smallmatrix} 0 \\ i/n \end{smallmatrix}\right](0, \Omega/n) \cdot \vartheta\left[\begin{smallmatrix} 0 \\ j/n \end{smallmatrix}\right](0, \Omega/n) \tag{7}$$

we get Siegel modular forms of weight 1 and level n over $\mathbb{C}$. Since the Fourier coefficients of the theta constants belong to $\mathbb{Z}$, by the q-expansion principle [FC90, p.140], this definition can be extended to a section of $\mathcal{H}$ over $\mathbb{Z}[\frac{1}{n}]$ and therefore over R. Since the sections $(\chi_{ij})_{i,j \in Z(\overline{n})}$ and $(\theta_i^{\mathscr{X}_{g,n}}(0)\theta_j^{\mathscr{X}_{g,n}}(0))_{i,j \in Z(\overline{n})}$ are equal up to a constant over $\mathbb{C}$, for any $(A, \mathscr{L}, \Theta_A) \in \mathscr{X}_{g,n}(k)$ and w_A a basis of k-rational regular differentials on A, $\chi_{ij}(A, \mathscr{L}, \Theta_A, w_A)$ is an affine lift of $\theta_i^A(0) \cdot \theta_j^A(0)$. This allows the following definition.

Definition 4.3. Let $(A, \mathscr{L}, \Theta_{\mathscr{L}}) \in \mathscr{A}_{g,n}(k)$ and w_A a basis of regular differentials on A. A *modular lift*, denoted $\theta^A(0, \sqrt{w_A}) = (\theta_i^A(0, \sqrt{w_A}))_{i \in Z(\overline{n})}$, is an affine lift of $\theta^A(0)$ such that for all $i, j \in Z(\overline{n})$, $\theta_i^A(0, \sqrt{w_A}) \cdot \theta_j^A(0, \sqrt{w_A}) = \chi_{ij}(A, \mathscr{L}, \Theta_{\mathscr{L}}, w_A)$. Notice that the modular lift is unique up to a common sign.

Remark 4.4. We consider the two by two products because they give modular forms of weight one. The $\theta^A(0, \sqrt{w_A})$ themselves would be modular forms of weight one half. But the line bundle $\mathscr{L}_{\mathscr{A}_{g,n}}$ does not descend on $\mathscr{A}_{g,1}$, only to a μ_2-gerbe of $\mathscr{A}_{g,1}$ [Can16]. Since we only need to compute modular forms of integral weight, this *ad hoc* definition is sufficient and requires less abstract material. Notice also that as a consequence of [Mum67, p. 82] and [Can16, Th. 4.2.1], $\mathscr{L}^2_{\mathscr{A}_{g,n}} \simeq \mathcal{H}$, which gives another purely algebraic proof of the modularity of $s^*(\theta_i^{\mathscr{X}_{g,n}} \cdot \theta_j^{\mathscr{X}_{g,n}})$. In particular, a choice of basis of regular differentials gives a trivialization of $\mathcal{H}$, so a trivialization of $\mathscr{L}^2_{\mathscr{A}_{g,n}}$ and corresponding affine lifts for the χ_{ij}.

If we start with a principally polarized abelian variety $(A, \mathscr{L})$ over a field k with a k-rational basis of regular differentials w_A, we may need to go to an extension to build the level n structure $\Theta_{\mathscr{L}}$ on A. Hence the $\theta_i^A(0, \sqrt{w_A})$ are not necessarily defined over k. However, consider a Siegel modular form χ of level 1 and of integral weight $\rho \geq 1$, written as a homogeneous polynomial P of degree 2ρ in the theta constants of level $\Theta_{\mathscr{L}}$ and with coefficients in k. As 2ρ is even, we can express P as polynomial Q in pairs of theta

[5] Here by level n we mean the level group $\Gamma_g(n, 2n)$ of matrices $\gamma \in \mathrm{Sp}_{2g}(\mathbb{Z})$ such that $\gamma = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \equiv \mathrm{Id} \pmod{n}$ and $2n$ divides the diagonals of B and C.

[6] At least when $g > 1$. When $g = 1$ we also need to check that the modular form stays bounded at infinity, or algebraically that the evaluation on the Tate curve is given by a Laurent series in q with no negative terms.

[7] Meaning the full level group $\Gamma_g = Sp_{2g}(\mathbb{Z})$ and not $\Gamma_1(1, 2)$.

constants, and therefore $P(\theta^A(0,\sqrt{w_A})) = Q((\chi_{ij}(A,\mathscr{L},\Theta_{\mathscr{L}},w_A))) = \chi(A,\mathscr{L},w_A) \in k$. This is important for our application to the modular form χ_{18} in dimension $g=3$ (see Section 5.2).

Theorem 4.5. *Let $(A,\mathscr{L},\Theta_{\mathscr{L}}) \in \mathscr{A}_{g,n}(k)$. Let ℓ be an integer prime to np (or to n if $p=0$). Let K be a k-rational totally isotropic subgroup for the Weil pairing of $\mathscr{L}^\ell$. Let $f : (A,\mathscr{L},\Theta_{\mathscr{L}}) \to (B,\mathscr{M},\Theta_{\mathscr{M}})$ where $B = A/K$, $f^*\mathscr{M} = \mathscr{L}^\ell$ and $\Theta_{\mathscr{M}}$ be the unique symmetric theta structure of level n on $\mathscr{M}$ compatible with $\Theta_{\mathscr{L}}$. Let w_A be a basis of k-rational regular differentials on A and $(\theta_i^A(0,\sqrt{w_A}))_{i\in Z(\overline{n})}$ be a modular lift. Finally, let $r = 1, 2$ or 4 depending on ℓ being a square, a sum of two square or not. Then the affine isogeny formula $\pi_3\circ\pi_2\circ\Pi_1^{-1}$ yields the products $(\theta^B_{i_1}(0,\sqrt{w_B})\times\cdots\times\theta^B_{i_r}(0,\sqrt{w_B}))_{i_1,\dots,i_r\in Z(\overline{n})}$ where w_B is such that $f^*w_B = w_A$. Note that the product is uniquely defined except if $r=1$ in which case we get all constants up to a common sign.*

Proof. Using the results of Section 4.2, the statement of this theorem makes sense over $\mathbb{Z}[\frac{1}{n\ell}]$. We will thus prove this theorem for $\mathscr{X}_{g,n} \to \mathscr{A}_{g,n}$ over $\mathbb{Z}[\frac{1}{n\ell}]$, the result will then be valid for any field of characteristic prime to $n\ell$.

We note that the theta coordinates computed by the isogeny formula give sections of the very ample line bundle $\mathscr{L}_{\mathscr{A}_{rg,n}}$ of $\mathscr{A}_{rg,n}$ over B^r. Thus the s_i can also be interpreted as sections of $\mathscr{L}^r_{\mathscr{A}_{g,n}}$ over B. We are thus trying to prove the equality of two sections of $\mathscr{L}^r_{\mathscr{A}_{g,n}}$, i.e. that for any $i_1,\dots,i_r$ the corresponding theta null point of coordinates $(i_1,\dots,i_r)$ computed by the isogeny formula is equal to $(\theta^B_{i_1}(0,\sqrt{w_B})\cdots\theta^B_{i_r}(0,\sqrt{w_B}))$.

Since $\mathscr{A}_{g,n}$ is smooth, $\mathscr{L}_{\mathscr{A}_{g,n}}$ is without torsion, so we only need to check this equality over $\mathbb{C}$. The abelian variety $A/\mathbb{C}$ is isomorphic to a torus $A \simeq \mathbb{C}^g/(\mathbb{Z}^g \oplus \Omega\mathbb{Z}^g)$. First it is easy to check that if we change our affine lift by multiplying it by $\lambda \in \mathbb{C}$, then the result of the isogeny formula is multiplied by λ^r. Indeed in Step 1 (in affine coordinates), the affine lift of the points of K are normalized with respect to the affine lifts of the theta null point. Multiplying the theta null point by λ multiply the points $Q \in \Pi_1^{-1}(A,K)$ by λ. Then applying the Segre embedding multiply the theta null point by λ^r, and Koizumi's formula does not change this constant.

Changing the basis of regular differentials by a matrix $M \in \mathrm{GL}_g(\mathbb{C})$ changes the value of a modular lift by $\lambda = \sqrt{\det(M)}$ for a fixed choice of the square root, since their pair products are weight 1 modular forms. This changes both the modular forms $(\theta^B_{i_1}(0,\sqrt{w_B})\cdots\theta^B_{i_r}(0,\sqrt{w_B}))$ and the result of the isogeny formula by a factor λ^r. So we may fix the differentials on A to be $w_A = (2i\pi dz_1,\dots,2i\pi dz_g)$ of $\mathbb{C}^g$.

By Eq. (7), the corresponding modular lift of the theta null point on A is then given by the analytic theta constants $\theta_i^A = \vartheta\left[\begin{smallmatrix}0\\ i/n\end{smallmatrix}\right](0,\Omega/n)$ (where we do a slight abuse of notations in identifying $i \in Z(\overline{n})$ to a fixed lift to $\mathbb{Z}^g$).

We can then keep track of the constants in each of the three steps of the isogeny formula of Section 4.2.

Step 1: we compute an affine lift of a theta null point of level ℓn on B, such that the isogeny theorem applied to $\tilde{f}$ gives our theta null point on A. From our hypothesis, K corresponds to the subgroup $\frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g$, so $B = \mathbb{C}^g/(\mathbb{Z}^g \oplus \ell\Omega\mathbb{Z}^g)$ and $f : z \mapsto \ell z$. The contragredient isogeny $\tilde{f} : B \to A$ is then given by $\tilde{f} : B \to A, z \mapsto z$. So we see that one possible lift for the theta null point of level ℓn on B is given by $\vartheta\left[\begin{smallmatrix}0\\ \frac{i}{\ell n}\end{smallmatrix}\right](0,\frac{\ell\Omega}{\ell n})$. By plugging any i divisible by ℓ we see that the constant involved in Step 1 is 1. Indeed, the isogeny theorem (the pullback $\tilde{f}$ of π_1 to B) is simply given in terms of analytic theta coordinates by

$$\left(\vartheta\left[\begin{smallmatrix}0\\ \frac{i}{\ell n}\end{smallmatrix}\right](z,\frac{\ell\Omega}{\ell n})\right)_{i\in Z(\overline{\ell n})} \mapsto \left(\vartheta\left[\begin{smallmatrix}0\\ \frac{i}{\ell n}\end{smallmatrix}\right](z,\frac{\Omega}{n})\right)_{i\in Z(\overline{\ell n}),\ell|i} = \left(\vartheta\left[\begin{smallmatrix}0\\ \frac{i}{n}\end{smallmatrix}\right](z,\frac{\Omega}{n})\right)_{i\in Z(\overline{n})}.$$

Algebraically, this means that we are computing $(\theta_i^{B,\mathscr{M}^\ell}(0,\sqrt{w'_B}))_{i\in Z(\overline{\ell n})}$ where w'_B is such that $\tilde{f}^*w_A = w'_B$. By definition of the contragredient isogeny, we have that $w'_B = w_B/\ell$ (as seen analytically by the fact that the map f above acts by ℓ on the tangent space).

Step 2: the Segre embedding simply consists on taking the sections induced by the basis of regular differentials on B^r given by the pullbacks of the differentials w'_B by the projections on each factor. Notice that the theta constants on B^r are then easily related to the ones on B since $\vartheta\left[\begin{smallmatrix}0&0\\ b_1&b_2\end{smallmatrix}\right](0,\ell\mathrm{diag}(\Omega,\Omega)) = \vartheta\left[\begin{smallmatrix}0\\ b_1\end{smallmatrix}\right](0,\ell\Omega)\vartheta\left[\begin{smallmatrix}0\\ b_2\end{smallmatrix}\right](0,\ell\Omega)$.

Step 3: For this step, we need a version of Equation (6) taking into account the possible multiplicative constant. This is given for instance in [Cos11, Théorème 7.2.1]

$$c\cdot\vartheta\left[\begin{smallmatrix}0\\ i_1\end{smallmatrix}\right](Y_1,\ell\Omega/n)\cdots\vartheta\left[\begin{smallmatrix}0\\ i_r\end{smallmatrix}\right](Y_r,\ell\Omega/n)=\sum_{[t_1,\dots,t_r]\in \mathrm{Mat}_{r\times g}(\mathbb{Z})F^{-1}/\,\mathrm{Mat}_{r\times g}(\mathbb{Z})}\vartheta\left[\begin{smallmatrix}0\\ j_1\end{smallmatrix}\right](X_1+t_1,\Omega/n)\cdots\vartheta\left[\begin{smallmatrix}0\\ j_r\end{smallmatrix}\right](X_r+t_r,\Omega/n), \tag{8}$$

where $F\in M_r(\mathbb{Z})$ is such that ${}^tFF=\ell\mathrm{Id}$, Y in $(\mathbb{C}^g)^r$, $X=YF^{-1}\in(\mathbb{C}^g)^r$, $i\in\mathbb{Q}^r$, $j=iF^{-1}$ and

$$c=[\mathrm{Mat}_{r\times g}(\mathbb{Z})F^{-1}:\mathrm{Mat}_{r\times g}(\mathbb{Z})]=[\mathrm{Mat}_{r\times g}(\mathbb{Z}):\mathrm{Mat}_{r\times g}(\mathbb{Z})F]=\ell^{gr/2}.$$

Taking into account that $F^{-1}=\frac{1}{\ell}\,{}^tF$, that the kernel of F in $Z(\bar{\ell})^r$ is exactly the image of ${}^tF$, and taking $Y_i=0$, we can rewrite Eq. (8) in terms of modular lifts

$$c\cdot\theta^{B,\mathscr{M}}_{i_1}(0,\sqrt{w'_B})\cdots\theta^{B,\mathscr{M}}_{i_r}(0,\sqrt{w'_B})=\sum_{\substack{(j_1,\dots,j_r)\in Z(\overline{\ell n})^r\\ F(j_1,\dots,j_r)=(i_1,\dots,i_r)}}\theta^{B,\mathscr{M}^\ell}_{j_1}(0,\sqrt{w'_B})\cdots\theta^{B,\mathscr{M}^\ell}_{j_r}(0,\sqrt{w'_B}).$$

Since $w'_B=w_B/\ell$ we have $\theta^B(0,\sqrt{w'_B})=\ell^{-1/2}\cdot\theta^B(0,\sqrt{w_B})$. This kills the constant c and we get the result (up to a fixed sign if $r=1$ because there is no way to choose a canonical square root of ℓ in a field k in general). □

This theorem shows that, given a Siegel modular form χ of *even* weight as a polynomial P in the theta constants with coefficients in k, we can compute the value $\chi(B,\mathscr{M},\Theta_B,w_B)$ from the corresponding modular lift on $(A,\mathscr{L})$. In practice [BCR10] does not compute all products $(\theta^B_{i_1}(0,\sqrt{w_B})\cdot\cdots\cdot\theta^B_{i_r}(0,\sqrt{w_B}))_{i\in Z(\overline{n})}$ but only the products $t_i:=(\theta^B_i(0,\sqrt{w_B})\cdot\theta^B_0(0,\sqrt{w_B})\cdot\cdots\cdot\theta^B_0(0,\sqrt{w_B}))_{i\in Z(\overline{n})}$, since this is enough for isogenies. It is also enough in our case: the weight being even means that each monomials of P in the theta constants has a degree multiple of 4 (and hence of r). We then get

$$\chi(B,\mathscr{M},\Theta_{\mathscr{M}},w_B)=P(\theta^B_i(0,\sqrt{w_B}))=t_0^{-\frac{(r-1)\rho}{r}}\cdot P(t_i).$$

The modular forms we will consider are written as polynomials in the theta constants with half characteristics and not in the algebraic theta of level 4. However it is easy to convert one into the other: see remark 4.7

4.4. **An algebraic version of Thomae's formula.** If $E:y^2=F(x)$ is an elliptic curve defined over k, we would like to compute the modular lift of the theta null point of level 4 with respect to the k-rational differential $w=dx/y$. Over $k\subset\mathbb{C}$, the expression of the fourth powers of theta constants can be seen as an elementary case of Thomae's formula [Mum07b, p.121] for hyperelliptic curves (although a sign remains unspecified). For dimension 1, one could also use σ functions as in [Akh90, p.55], but one still only gets expression for the fourth powers of the theta constants. We will reprove these formulas in the following lemma and show that one can take arbitrary fourth roots. This will be useful for the computation of Siegel modular forms of even weight at $(B,\mathscr{M},w_B)$ in the isogeny class of E^g.

Lemma 4.6 (Analytic form of Thomae's formula)**.** *Let E be an elliptic curve with Weierstrass equation $y^2=F(x)$ defined over over $\mathbb{C}$. Let e_1,e_2,e_3 be the roots of F. Fix arbitrarily three fourth roots a_1,a_2,a_3 of e_i-e_j for $(i,j)\in((2,3),(1,2),(1,3))$. There exists a basis δ_1,δ_2 of $H_1(E,\mathbb{Z})$ such that if we denote $[\omega_1,\omega_2]=[\int_{\delta_1}dx/y,\int_{\delta_2}dx/y]$ then $\tau=\omega_2/\omega_1\in\mathbb{H}_1$ and*

$$\sqrt{c}\cdot\vartheta\left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](\tau)=a_3,\quad\sqrt{c}\cdot\vartheta\left[\begin{smallmatrix}1/2\\ 0\end{smallmatrix}\right](\tau)=a_2,\quad\sqrt{c}\cdot\vartheta\left[\begin{smallmatrix}0\\ 1/2\end{smallmatrix}\right](\tau)=a_1$$

with $c=\frac{2i\pi}{w_1}$ for an arbitrary fixed square root of c.

Proof. Let $\tau\in\mathbb{H}_1$ and denote

$$\vartheta_{00}(z)=\vartheta\left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](z,\tau),\ \vartheta_{10}(z)=\vartheta\left[\begin{smallmatrix}1/2\\ 0\end{smallmatrix}\right](z,\tau),\ \vartheta_{01}(z)=\vartheta\left[\begin{smallmatrix}0\\ 1/2\end{smallmatrix}\right](z,\tau),$$

and $\vartheta_{11}(z)=\vartheta\left[\begin{smallmatrix}1/2\\ 1/2\end{smallmatrix}\right](z,\tau)$. When z does not appear, it denotes the corresponding value at $z=0$. As in [FK01, p.125], let us consider the map $\phi:\mathbb{C}\to\mathbb{P}^2$ given by

$$(\vartheta^2_{00}(z)\vartheta_{11}(z):\vartheta_{00}(z)\vartheta_{01}(z)\vartheta_{10}(z):\vartheta^3_{11}(z)).$$

Using the divisors of these sections, one can prove that the image by ϕ of $\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z})$ is the elliptic curve

$$E_2 : Y_2^2 Z_2 = X_2(\beta X_2 - \alpha Z_2)(\alpha X_2 + \beta Z_2)$$

where $\alpha = \vartheta_{10}^2\vartheta_{00}^2$ and $\beta = \vartheta_{01}^2\vartheta_{00}^2$. Letting $Y_2 = Y_1\vartheta_{10}\vartheta_{01}/\vartheta_{00}^2, X_2 = X_1$ and $Z_2 = Z_1$, we can transform further in

$$E_1 : Y_1^2 Z_1 = X_1(X_1 - \alpha/\beta Z_1)(X_1 + \beta/\alpha Z_1).$$

Then letting $Z_1 = (\vartheta_{01}^2\vartheta_{10}^2)Z_0$ and finally $Y_1 = Y_0/(\vartheta_{01}\vartheta_{10})$ and $X_1 = X_0$ one gets

$$E_0 : Y_0^2 Z_0 = X_0(X_0 - \vartheta_{10}^4(0)Z_0)(X_0 + \vartheta_{01}^4(0)Z_0)$$

Let us study the regular differential $w_0 = d(X_0/Z_0)/(Y_0/Z_0) = \frac{1}{\vartheta_{00}^2} \cdot d(X_2/Z_2)/(Y_2/Z_2)$ on E_0. Since $w_2 = d(X_2/Z_2)/(Y_2/Z_2)$ is regular, $\phi^*(w_2)$ is a constant multiple of dz. Now

$$\begin{aligned}
\phi^* w_2 &= 2 \cdot \frac{\vartheta_{00}(z)'\vartheta_{11}(z) - \vartheta_{11}(z)'\vartheta_{00}(z)}{\vartheta_{10}(z)\vartheta_{01}(z)} \\
&= -2\frac{\vartheta_{11}'(0)\vartheta_{00}(0)}{\vartheta_{10}(0)\vartheta_{01}(0)} && \text{(evaluating at } z=0\text{)} \\
&= 2\pi\frac{\vartheta_{00}\vartheta_{10}\vartheta_{01}\vartheta_{00}}{\vartheta_{10}\vartheta_{01}} && \text{(Jacobi identity } \vartheta_{11}' = -\pi\vartheta_{00}\vartheta_{01}\vartheta_{10}\text{)} \\
&= 2\pi\vartheta_{00}^2.
\end{aligned}$$

Hence if $\psi_0 : \mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}) \to E_0$ is the isomorphism composed from ϕ and the changes of variables we get that $\psi_0^* w_0 = 2\pi dz$ (notice that this is not the natural $2i\pi dz$ we chose before but we will take care of the extra factor i when we choose the fourth root).

Now, let us start with $E : y^2 = F(x)$. If we make the change of variable $X = x - e_2$, $Y = y$, then we get $E' : Y^2 = X(X - (e_1 - e_2)Z)(X + (e_2 - e_3)Z)$. If we integrate $w = d(X/Z)/(Y/Z)$ along a basis of the homology of E', we get a torus $\mathbb{C}/(\omega_1\mathbb{Z} + \omega_2\mathbb{Z})$ and up to a change of the order in the basis, we can assume that $\tau = \omega_2/\omega_1 \in \mathbb{H}_1$ and $\psi : \mathbb{C}/(\omega_1\mathbb{Z} + \omega_2\mathbb{Z}) \to E'$ an isomorphism such that $\psi^* w = dz$. Let $s : \mathbb{C}/(\omega_1\mathbb{Z} + \omega_2\mathbb{Z}) \xrightarrow{\sim} \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ such that $z \mapsto z/\omega_1$. The composition

$$\begin{array}{ccc}
\mathbb{C}/(\omega_1\mathbb{Z} + \omega_2\mathbb{Z}) & \xleftarrow{\psi^{-1}} & E' \\
\Big\downarrow{\scriptstyle s} & & \Big\downarrow{\scriptstyle \mu} \\
\mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z}) & \xrightarrow[\psi_0]{} & E_0
\end{array}$$

defines an isomorphism $\mu : E' \to E_0$ such that $(X : Y : Z) \to (a^2X : a^3Y : Z)$ with $a \in \mathbb{C}^*$. After a possible change in the generators of the homology of E' (by a lift to $\mathrm{SL}_2(\mathbb{Z})$ of a change of basis of $E'[2]$), we can even assume that μ maps the roots 0 to 0, $e_1 - e_2$ to ϑ_{10}^4/a^2 and $e_2 - e_3$ to ϑ_{01}^4/a^2. Note that $e_1 - e_3 = (\vartheta_{10}^4 + \vartheta_{01}^4)/a^2 = \vartheta_{00}^4/a^2$. Now $\mu^* w_0 = w/a = (\psi^{-1})^* \circ s^* \circ \psi_0^* w_0 = 2\pi/\omega_1 \cdot w$. Hence $a = \omega_1/2\pi$. This means that we have the equalities

$$a_2^4 = e_1 - e_2 = -c^2\vartheta_{10}^4, \quad a_1^4 = e_2 - e_3 = -c^2\vartheta_{01}, \quad a_3^4 = e_1 - e_3 = -c^2\vartheta_{00}.$$

To conclude, we must show that we can choose the basis of homology for E in order to choose the fourth root of unity arbitrarily and get the correct result up to a common fourth root of unity. As the two-torsion points are now fixed, this boils down to find some matrices in $\mathrm{SL}_2(\mathbb{Z})$ which are congruent to the identity modulo 2. If we call $S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, let $H =< S^2, T^2, (ST)^3, (STS)^2 >$ and $(\alpha_1, \alpha_2, \alpha_3) = (i\sqrt{c}\vartheta_{01}, i\sqrt{c}\vartheta_{10}, i\sqrt{c}\vartheta_{00})$. Notice that the α_is do depend on τ but also on ω_1. The actions of S and T on the lattice induce actions on the α_i which can be computed through the classical transformation formula [Mum07a, Th.7.1]. Namely

$$\left\{\begin{array}{lcl} S.\alpha_1 &=& \alpha_3, \\ S.\alpha_2 &=& e^{i\pi/4}\alpha_2, \\ S.\alpha_3 &=& \alpha_1, \end{array}\right. \text{ and } \left\{\begin{array}{lcl} T.\alpha_1 &=& \sqrt{-i}\alpha_2, \\ T.\alpha_2 &=& \sqrt{-i}\alpha_1, \\ T.\alpha_3 &=& \sqrt{-i}\alpha_3. \end{array}\right.$$

Hence we get

$$\left\{\begin{array}{lcl} S^2.\alpha_1 &=& \alpha_1,\\ S^2.\alpha_2 &=& i\alpha_2,\\ S^2.\alpha_3 &=& \alpha_3,\end{array}\right. , \quad \left\{\begin{array}{lcl} T^2.\alpha_1 &=& -i\alpha_1,\\ T^2.\alpha_2 &=& -i\alpha_2,\\ T^2.\alpha_3 &=& -i\alpha_3,\end{array}\right.$$

and

$$\left\{\begin{array}{lcl} (ST)^3.\alpha_1 &=& i\alpha_1,\\ (ST)^3.\alpha_2 &=& i\alpha_2,\\ (ST)^3.\alpha_3 &=& i\alpha_3,\end{array}\right. , \quad \left\{\begin{array}{lcl} (STS)^2.\alpha_1 &=& -i\alpha_1,\\ (STS)^2.\alpha_2 &=& -\alpha_2,\\ (STS)^2.\alpha_3 &=& -\alpha_3.\end{array}\right.$$

The group μ_4^3 has generators $u_1 := (i,1,1), u_2 := (1,i,1), u_3 := (1,1,i)$. The expressions above show that $g_1 = (ST)^3(STS)^2$ (resp. $g_2 = S^2$, resp. $g_3 = g_1^3 g_2^3 (ST)^3$) acts on $(\alpha_1,\alpha_2,\alpha_3)$ as u_1 (resp. u_2, resp. u_3). Starting from (a_1,a_2,a_3) it is therefore possible to find a τ such that $(a_1,a_2,a_3) = (\sqrt{c}\vartheta_{01}, \sqrt{c}\vartheta_{10}, \sqrt{c}\vartheta_{00})$. □

Remark 4.7. The algebraic theta functions of level 4, $(\theta_1,\theta_2,\theta_3,\theta_4)$ analytically correspond to the theta functions $(\vartheta\left[\begin{smallmatrix}0\\ i/4\end{smallmatrix}\right](z,\Omega/4))_{i\in\mathbb{Z}/4\mathbb{Z}}$. Going to these functions from the standard level $(2,2)$ analytic theta $\vartheta\left[\begin{smallmatrix}a/2\\ b/z\end{smallmatrix}\right](2z,\Omega)$ is given by a change of variables [Mum07a], [Cos11, p. 38]

$$\begin{aligned} \theta_0(z) &= \vartheta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](z,\Omega) + \vartheta\left[\begin{smallmatrix}1/2\\0\end{smallmatrix}\right](z,\Omega), \quad \theta_1(z) = \vartheta\left[\begin{smallmatrix}0\\1/2\end{smallmatrix}\right](z,\Omega) + \vartheta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right](z,\Omega),\\ \theta_2(z) &= \vartheta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](z,\Omega) - \vartheta\left[\begin{smallmatrix}1/2\\0\end{smallmatrix}\right](z,\Omega), \quad \theta_3(z) = \vartheta\left[\begin{smallmatrix}0\\1/2\end{smallmatrix}\right](z,\Omega) - \vartheta\left[\begin{smallmatrix}1/2\\1/2\end{smallmatrix}\right](z,\Omega), \end{aligned} \tag{9}$$

where $\theta_i(z) = \vartheta\left[\begin{smallmatrix}0\\ i/4\end{smallmatrix}\right](z,\Omega/4)$.

The functions $\vartheta\left[\begin{smallmatrix}a/2\\ b/2\end{smallmatrix}\right](2z,\Omega)$ also have algebraic analogues as partial Fourier transforms over $Z(\overline{2})$ of the functions θ_i as explained in [Mum66, p. 334] and [Rob10, Exemple 4.4.9]. If θ_i is a theta function of level n, the partial Fourier transform is given for $\alpha \in \hat{Z}(\overline{2})$ by

$$\theta\left[\begin{smallmatrix}\alpha\\ i\end{smallmatrix}\right] = \sum_{j\in Z(\overline{2})} \alpha(j)\theta_{i+j}. \tag{10}$$

Analytically, $\theta\left[\begin{smallmatrix}\alpha\\ i\end{smallmatrix}\right](z) = \vartheta\left[\begin{smallmatrix}\alpha/2\\ 2i/n\end{smallmatrix}\right](2z, 2\Omega/n)$, so if $n=4$ we do recover the theta functions of level $(2,2)$.

All these expressions for the theta constants over $\mathbb{C}$ are true over k. Indeed, pairing them will give modular forms with integral Fourier expansion, so we get similar expression for the modular lift, up to a common sign which can be swallowed in the choice of the fourth root.

Corollary 4.8 (Algebraic form of Thomae's formula)**.** *Let E be an elliptic curve with Weierstrass equation $y^2 = F(x)$ defined over a field k of characteristic $p \neq 2$. Let e_1,e_2,e_3 be the roots of F in $\bar{k}$. Fix arbitrarily three fourth roots a_1,a_2,a_3 of $e_i - e_j$ for $(i,j) \in ((2,3),(1,2),(1,3))$. Then there is a level 4 symmetric theta structure on E, such that a modular lift of the theta null point on E with respect to the regular differential dx/y is*

$$\begin{aligned} \theta_0^E(0_E,\sqrt{dx/y}) &= a_2+a_3, & \theta_1^E(0_E,\sqrt{dx/y}) &= a_1,\\ \theta_2^E(0_E,\sqrt{dx/y}) &= -a_2+a_3, & \theta_3^E(0_E,\sqrt{dx/y}) &= a_1. \end{aligned} \tag{11}$$

Proof. Define $\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0_E) = a_3, \theta\left[\begin{smallmatrix}1/2\\0\end{smallmatrix}\right](0_E) = a_2, \theta\left[\begin{smallmatrix}0\\1/2\end{smallmatrix}\right](0_E) = a_1$. First we note that the first part of Lemma 4.6 is valid algebraically: we just need to replace the argument involving divisors by the algebraic Riemann relations instead. Indeed it is easy to check that the theta null point defined satisfy the Riemann relation $\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0_E)^4 = \theta\left[\begin{smallmatrix}1/2\\0\end{smallmatrix}\right](0_E)^4 + \theta\left[\begin{smallmatrix}0\\1/2\end{smallmatrix}\right](0_E)^4$ (this is the standard Jacobi relation to which Riemann relations reduce to in genus 1 [Mum66, p. 353]). Since we also have that $\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0_E)\theta\left[\begin{smallmatrix}1/2\\0\end{smallmatrix}\right](0_E)\theta\left[\begin{smallmatrix}0\\1/2\end{smallmatrix}\right](0_E) = a_1a_2a_3 \neq 0$, the theta null point we compute is valid projectively by [Mum66, p. 353]. This also proves that each choice of fourth root is valid.[8]

[8]Alternatively, the affine modular action of $\Gamma/\Gamma(4,8)$ induces a projective action [Cos11, Lemme 6.2.1] which holds true algebraically, as automorphisms of the Heisenberg group of level 4. So the same generators g_1, g_2 and g_3 as in the end of Lemma 4.6 acts by fourth-root of unity projectively.

It remains to check that the affine lift given by Eq. (11) corresponds to the trivialization coming from the differential $w = dx/y$. Since the construction is valid over the universal elliptic curve with a level 4 symmetric theta structure, whose moduli space is defined over $\mathbb{Z}[1/2]$, by considering the pullback to $\mathbb{C}$ we may assume that E is defined over $\mathbb{C}$, as in the proof of Theorem 4.5. Looking at the proof of Lemma 4.6, we see that the isomorphism between E and E' does not change the differential w, while the one from E' to E_0 acts by $a = 2\pi/\omega_1$. Correcting for this last factor yields

$$\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0_E, \sqrt{dx/y}) = a_3, \quad \theta\left[\begin{smallmatrix}1/2\\0\end{smallmatrix}\right](0_E, \sqrt{dx/y}) = a_2, \quad \theta\left[\begin{smallmatrix}0\\1/2\end{smallmatrix}\right](0_E, \sqrt{dx/y}) = a_1. \tag{12}$$

Applying the linear change of variable Eq. (9) to Eq. (12) yields Eq. (11). □

4.5. **Computing a Siegel modular form on the isogenous variety.** Combining Corollary 4.8 with Theorems 4.2 and Theorem 4.5 gives the following theorem and Algorithm 8.

Theorem 4.9. *Let g be a positive integer, $(E_i/k)_{1\leq i\leq g}$ be elliptic curves, K be a k-rational totally isotropic subgroup of $\prod_i E_i$ of order ℓ^g prime to $2p$ (or just prime to 2 if $p = 0$). Let $B = (E_1 \times \cdots \times E_g)/K$ with the principal polarization induced by the product polarization on $E_1 \times \cdots \times E_g$ and let $f : \prod_i E_i \to B$ be the quotient isogeny. Finally define w_B such that $f^* w_B = (p_1^* dx_1/y_1, \ldots, p_g^* dx_g/y_g)$ where $p_i : E_1 \times \cdots \times E_g \to E_i$ is the canonical projection. Let $r = 1, 2$ or 4 depending on ℓ being a square, a sum of two squares or not. Algorithm 8 computes the products $\theta^B_{i_1}(0, \sqrt{w_B}) \cdots \theta^B_{i_r}(0, \sqrt{w_B})$ of any r modular lifts in time $O(\ell^{g \max(1, r/2)})$ operations in the field of definition of the points of K. Given a Siegel modular form χ of even weight as a polynomial P in the theta constants with coefficients in k, Algorithm 8 also computes the value $\chi(B, \mathscr{M}, w_B) \in k$.*

Remark 4.10. We can make several comments about this result.

- Note that during the execution of the algorithm, we only need to take care to compute the modular lift of the theta null point. Indeed, apart from the theta null point, we only need to compute projective coordinates for the points in the kernel, the computation of Π_1^{-1} will take care of normalizing these coordinates with respect to our choice of affine lift of the theta null point.
- We only require χ to be of even weight w if $r = 4$. Otherwise given the r-fold products

$$\theta^B_{i_1}(0, \sqrt{w_B}) \cdots \theta^B_{i_r}(0, \sqrt{w_B})$$

  we can evaluate a modular form of odd weight.
- We do not need to evaluate all the r-fold products, but only the ones of the form

$$t_i = \theta^B_i(0, \sqrt{w_B}) \cdots \theta^B_i(0, \sqrt{w_B})$$

  (provided $\theta^B_0(0, \sqrt{w_B}) \neq 0$). If χ is of weight w, it can then be evaluated as $\chi(B, \mathscr{M}, w_B) = P(t_i)/t_0^{w(r-1)/2}$.
- If the modular form χ that can be written as a polynomial with respect to the level 2 theta constants, we can do the whole isogeny computation in level 2. This gains a factor 2^g in the number of coordinates to compute.

Algorithm 8 Algebraic computation of the theta null point and a Siegel modular form of even weight

Input: Elliptic curves E_i/k with equation $y^2 = (x - e_{1i})(x - e_{2i})(x - e_{3i})$ where k is of characteristic p different from 2, a k-rational totally isotropic subgroup K of $A = \prod_i E_i$ of order ℓ^g prime to $2p$ (or just prime to 2 if $p = 0$). A Siegel modular form χ of even weight as a polynomial P in the theta constants with coefficients in k.

Output: The theta null point of level 4 and the value $\chi(B, \mathscr{M}, w_B)$ where $B = A/K$ with $\mathscr{M}$ the polarization induced by the product polarization on A and w_B such that $f^* w_B = (p_1^* dx_1/y_1, \dots, p_g^* dx_g/y_g)$ where $f : A \to B$ is the quotient isogeny and $p_i : E_1 \times \cdots \times E_g \to E_i$ is the canonical projection.

1: For all $1 \le i \le g$, define $\theta_0'^{E_i} = \sqrt[4]{e_{1i} - e_{3i}}, \theta_1'^{E_i} = \sqrt[4]{e_{1i} - e_{2i}}, \theta_2'^{E_i} = \sqrt[4]{e_{2i} - e_{3i}}$ for arbitrary choices of the roots.

2: Compute $\theta_0^{E_i}(0, \sqrt{dx_i/y_i}) = \theta_0'^{E_i} + \theta_1'^{E_i}$, $\theta_2^{E_i}(0, \sqrt{dx_i/y_i}) = \theta_0'^{E_i} - \theta_1'^{E_i}$ and $\theta_1^{E_i}(0, \sqrt{dx_i/y_i}) = \theta_3^{E_i}(0, \sqrt{dx_i/y_i}) = \theta_2'^{E_i}$ for all $1 \le i \le g$.

3: Compute all $\theta^A_{(i_1,\dots,i_g)}(0, \sqrt{w_A}) = \theta_{i_1}^{E_1}(0, \sqrt{dx_1/y_1}) \cdots \theta_{i_g}^{E_g}(0, \sqrt{dx_n/y_n})$ for all $(i_1, \dots, i_g) \in Z(\overline{4})$.

4: For all $1 \le i \le g$ and for all $x = (x_1, \dots, x_g) \in K \setminus \{0\}$, compute the theta coordinates $\left(\theta_j^{E_i}(x_i)\right)_{j \in \mathbb{Z}/4\mathbb{Z}}$.

5: Compute for all $j = (j_1, \dots, j_g) \in Z(\overline{4})$ and for all $x = (x_1, \dots, x_g) \in K \setminus \{0\}$ $\theta_j^A(x) = \theta_{j_1}^{E_1}(x_1) \cdots \theta_{j_g}^{E_g}(x_g)$.

6: Use the affine version of the isogeny formula to compute $t_i = \theta_i^B(0, \sqrt{w_B}) \cdot \theta_0^B(0, \sqrt{w_B}) \cdots \theta_0^B(0, \sqrt{w_B})$ which is a product of r factors with $r = 1$ if ℓ is a square, $r = 2$ if ℓ is the sum of two positive squares and $r = 4$ otherwise.

7: **return** $(t_i)_{i \in Z(\overline{4})}$ and $t_0^{-\frac{(r-1)\rho}{r}} \cdot P(t_i)$.

5. Application to defect-0 curves of genus at most 4

Let C be a curve of genus $g > 0$ over $\mathbb{F}_q$ with $q = p^m$. The Hasse-Weil-Serre bound asserts that $\#C(\mathbb{F}_q) \le 1 + q + gm$ where $m = \lfloor 2\sqrt{q} \rfloor$. A curve which number of rational points reaches with bound is called a *defect*-0 *curve*. When $g > 2$, it is not known in general for a given field $\mathbb{F}_q$ whether a defect-0 curve $C/\mathbb{F}_q$ of genus g exists. If it does, $\operatorname{Jac} C$ is isogenous to the g-power of an elliptic curve E with trace $-m$. In order to see if such a curve exists, we therefore start by enumerating the indecomposable principally polarized abelian varieties $(A_i, \mathscr{L}_i)$ of dimension g in the isogeny class of E^g. When m is prime to q and hence E is ordinary, we have seen in Section 3.3 how to describe all of them as a quotients of E^g by given maximal isotropic subgroups $K \subset E[\ell_1] \times \cdots \times E[\ell_g]$. When we can moreover choose $\ell = \ell_1 = \ldots = \ell_g$ odd, prime to the characteristic of $\mathbb{F}_q$ (see the condition in Theorem 2.16) and K totally isotropic, we can use Algorithm 7 to compute the theta null point of level 4 for each $(A_i, \mathscr{L}_i)$.

Now, we need to single out the ones which are Jacobians of curves of genus g over $\mathbb{F}_q$. By [OU73], we know that any indecomposable principally polarized abelian variety $(A, \mathscr{L})$ of dimension $g \le 3$ is the Jacobian of a curve C_0 of genus g over $\bar{\mathbb{F}}_q$. When $g = 4$, this is not the case, but we will be able to distinguished them computing a certain Siegel modular form using Algorithm 8, see Section 5.3. However if $(A, \mathscr{L})$ is a Jacobian of dimension 4 over $\bar{\mathbb{F}}_q$ there is currently no way to check if it is also a Jacobian over $\mathbb{F}_q$. As for $g \le 3$, notice that there is a big difference between the genus 2 and genus 3 case when dealing with the existence of C over $\mathbb{F}_q$. For the genus 2, this is automatic: the existence of an indecomposable principally polarized abelian surface over $\mathbb{F}_q$ in the class of E^2 is enough to ensure the existence of the curve C. For genus 3 curves though, there may be an arithmetic obstruction as we shall recall in Section 5.2. As we shall see this obstruction can be computed from the value of a Siegel modular form.

For $g = 2$ or 3, we can even get an equation for the curve C when it exists. In genus 2, the construction of such a curve from its theta null point is classical and we refer for instance to [CR15] ; in genus 3, the formulae depend on the curve being hyperelliptic or not, which can be distinguished by exactly one of the 36 even theta coordinates being 0 or none. In the hyperelliptic case, one can use [Wen01][9] to construct first a model C_1 over $\bar{\mathbb{F}}_q$. Then one computes Shioda invariants[10] and then reconstruct via [LR12a] when $p > 7$.

[9] [BIL+16] noticed that there are some mistakes in this article of Weng and [LSV20, Appendix] gives a correct implementation (see also this page). However, we did not try to implement the reconstruction in the genus 3 hyperelliptic case.

[10] or computes them directly from the theta constants using for instance [Lor19] and overpass the difficulties mentioned above.

In the non-hyperelliptic case, one can use Weber's formulae ([Web76, p.108], see also [Fio16]) to get first a curve C_1 over an extension $\mathbb{F}_{q^e}$ of $\mathbb{F}_q$ ($p \neq 2$). To get an equation of C_0 over $\mathbb{F}_q$, we implemented an explicit Galois descent taking advantage of the fact that C_1, being given with its full level-2 structure, has all its bitangents defined over $\mathbb{F}_{q^n}$. Hence, all isomorphisms between C_1 and its Galois conjugates over $\mathbb{F}_e$ are defined over $\mathbb{F}_{q^e}$ as well.

It may still be that $\operatorname{Jac} C_0$ is not isomorphic over $\mathbb{F}_q$ to the chosen $(A, \mathscr{L})$ as C_0 may be a twist of the right curve C. If the geometric automorphism group of C is trivial (which can be read from the automorphism group of the lattice), then the curve has no automorphism, hence no non-trivial twist and $C_0 \simeq C$. Otherwise, one has to compute the list of all twists: in the hyperelliptic case see [LR12a, Sec.4.6] (implemented in `Magma`), and in the non-hyperelliptic case see [LRR+14, Sec.4].

To conclude, it is then enough to check among the twists which ones are defect-0 curves over $\mathbb{F}_q$, which can be achieved through naive point counting algorithms. Hence for $g = 2$ and 3 our algorithms provide an explicit list of all isomorphism classes of defect-0 curves over $\mathbb{F}_q$.

Remark 5.1. A different way to do so is to pick a random $\mathbb{F}_q$-rational divisor $D \in \operatorname{Jac} C'(\mathbb{F}_q)$, and check if $(1+q-\operatorname{Trace}(E))^g D = 0$. A better way would be to select the right Galois descent directly by keeping track of the Galois action on the two torsion points of E^g through the isogeny. This could actually be achieved since a more general isogeny formula exists which can also be applied to an arbitrary torsion point of E^g. We did not implement this method yet.

5.1. **Curves of genus 2.** Let us give some examples to illustrate our algorithms. We start with a very simple one.

Example 5.2. Let $E/\mathbb{F}_{61} : y^2 = x^3 + 11x + 17$ be an elliptic curve such that $R := \mathbb{Z}[\pi] = \mathbb{Z}[w]$ with $w = \frac{1+\sqrt{-19}}{2}$. When $g = 2$, the algorithm developed in Section 2 shows that there is only one indecomposable unimodular positive definite R-lattice of rank 2, namely R^2 with the hermitian form $h = \begin{bmatrix} 2 & -\bar{w} \\ -w & 3 \end{bmatrix}$ (this can alternatively be read directly from Schiemman's tables). Hence $A = \mathscr{F}_E(R^2) = E^2$ with the polarization $\mathscr{L}$ induced by h is the only Jacobian inside the isogeny class of E^2. Using Algorithm 6 one can check that there is a polarized isogeny f from $A_0 = E^2$ with the product polarization to $(A, \mathscr{L})$ with kernel $K \subset A[\ell]$ with $\ell = 3$. Explicitly K is generated by the two affine points of E^2

$$((51a^3 + 39a^2 + 36a + 13, 59a^3 + 43a^2 + 48a + 35), (3a^3 + 31a^2 + 38a + 4, 44a^3 + 22a^2 + 19a + 11)),$$

$$((58a^3 + 30a^2 + 23a + 36, 14a^3 + 55a^2 + 47a + 45), (51a^3 + 39a^2 + 36a + 13, 2a^3 + 18a^2 + 13a + 26))$$

where $a \in \mathbb{F}_{61^4}$ has minimal polynomial $x^4 + 3x^2 + 40x + 2$. We can also compute the theta null point which we express in the classical basis of theta constants characteristics. For instance $\theta^B_{00}(0) = \vartheta\left[\begin{smallmatrix} 00 \\ 00 \end{smallmatrix}\right](0)$ is equal to

$$43b^{11} + 34b^{10} + 28b^9 + 11b^8 + 6b^7 + 19b^6 + 30b^5 + 27b^4 + 27b^3 + b^2 + 30b + 59$$

where $b \in \mathbb{F}_{61^{12}}$ with minimal polynomial $x^{12} + 2x^8 + 42x^7 + 33x^6 + 8x^5 + 38x^4 + 14x^3 + x^2 + 15x + 2$. Using the reconstruction method explained above, we find $C : y^2 = 45x^6 + 13x^5 + 25x^4 + 23x^3 + 3x^2 + 20x + 13$.

Consider the complex expression $\chi_5(\tau) = \prod_{\epsilon \text{ even}} \vartheta[\epsilon](\tau)$. Then $\chi_{10} = \chi_5^2$ is a Siegel modular form of weight 10 and level Γ_2 defined over $\mathbb{Z}$. Using Algorithm 8, we find that $\chi_{10}(A, \mathscr{L}, w_A) = 22$ where w_A is the basis of differentials constructed in Theorem 4.9. There is a well-known relation with between χ_{10} and the discriminant of $C : y^2 = f(x)$ (which is 2^8 times the discriminant of f) up to the choices of bases of regular differentials. One must have that $\chi_{10}(A, \mathscr{L}, w_A)/(2^{12} \cdot \operatorname{Disc}(C))$ is a 10th power of the determinant of the change of bases, hence a 10th power in $\mathbb{F}_q$. This is indeed the case.

Example 5.3. In a similar way, we can work out an example over $k = \mathbb{F}_{5^3}$ with a non-maximal order of discriminant -2^4. In that case there is a unique defect-0 curve of genus 2 over k, namely $C : y^2 = 3x^6 + 3x^4 + 3x^2 + 3$.

Example 5.4. Let us consider now the case $k = \mathbb{F}_{271}$ with a non-maximal order of discriminant -60. In that case, there are 9 indecomposable principally polarized abelian surfaces in the isogeny class. For only two of them, there exists an odd ℓ ($\ell = 5$) and one can write down the corresponding curves, namely $y^2 = 65x^6 + 167x^5 + 63x^4 + 49x^3 + 63x^2 + 167x + 65$ and $y^2 = 89x^6 + 224x^5 + 155x^4 + 16x^3 + 155x^2 + 224x + 89$.

For the seven other cases, such an ℓ does not exist: Theorem 2.16 shows that either there is no orthogonal basis with the same odd norm for two of them, or no orthogonal basis with the same norm for the last 5 of them.

5.2. **Curves of genus 3.** In his lectures at Harvard in 1985, Serre found that a principally polarized abelian variety $(A, \mathscr{L})$ of dimension $g > 2$ defined over a perfect field k, which is geometrically a Jacobian, is not necessarily a Jacobian over k (unlike in dimension 1 or 2). The obstruction is given by a quadratic character of $\mathrm{Gal}(\bar{k}/k)$ and is called *Serre's obstruction*. This obstruction is always trivial for hyperelliptic curves. When $k \subset \mathbb{C}$ and $g = 3$, this character can be computed in terms of the value of the modular form defined over $\mathbb{C}$ by $\chi_{18}(\tau) = -\frac{1}{2^{28}} \cdot \prod_\epsilon \vartheta[\epsilon](\tau)$, where the product is over the 36 even theta constants ([Ser85], [LR08], [Mea08], [LRZ10]). Using lifting techniques, one can thus get the obstruction for certain $(A, \mathscr{L})$ when k is a finite field of characteristic different from 2 and therefore address the question of maximal number of points of genus 3 curves (see for instance [Rit10]). However, the numerical approximations during the computation of the value of the modular form lead to heuristic results only.

The techniques developed in Section 4.3 allows us to directly work out these computations over an (extension) of the finite field. In [Igu67], it is proved that χ_{18} is a modular form of degree 18 and level 1 and therefore it induces an element of $\Gamma(\mathscr{A}_{3,1}(\mathbb{C}), \mathcal{H}^{18})$. Then [Ich96, Prop.3.4] proved that actually $\chi_{18} \in \Gamma(\mathscr{A}_{3,1}(\mathbb{Z}), \mathcal{H}^{18})$. In [LRZ10, Th.1.3.3], over a number field, and in Proposition [Rit10, Prop.2.3], over a field k of characteristic different from 2, it is proved for a principally polarized abelian threefold $(A, \mathscr{L})/k$ and any choice of k-rational basis of regular differentials w_A on A, that $\chi_{18}(A, \mathscr{L}, w_A)$ is a non-zero square in k if and only if $(A, \mathscr{L})$ is the Jacobian of a non-hyperelliptic curve of genus 3 over k. Using Algorithm 8, we can compute this value and check whether $(A, \mathscr{L})$ is the Jacobian of a non-hyperelliptic genus 3 curve over k without computing the equation of the curve. Note that as we started with $(A, \mathscr{L})/\mathbb{F}_q$ indecomposable, if $\chi_{18}(A, \mathscr{L}, w_A) = 0$, then $(A, \mathscr{L})$ is the Jacobian of a hyperelliptic genus 3 curve over $\mathbb{F}_q$.

Example 5.5 (A unique defect-0 curve without non-trivial automorphism). Let consider the question of the existence of defect-0 curve of genus 3 over $\mathbb{F}_q$ with $q = 10313$. If there is such a curve $C/\mathbb{F}_q$ then $\mathrm{Jac}\, C \sim E^3$ with E of trace $-m = -203$. The curve E has therefore complex multiplication by the maximal order $\mathscr{O} = \mathbb{Z}[\omega]$ of $\mathbb{Q}(\omega)$ where $\omega = \frac{1+\sqrt{-43}}{2}$. As $\mathscr{O}$ has class number 1, there is a unique (non-polarized) abelian variety in the class of E^3 up to isomorphism, namely E^3 itself. Moreover using Algorithm 3 (see also [Sch98]), we find 5 isomorphism classes of indecomposable positive definite unimodular hermitian $\mathscr{O}$-lattices (L, h_i) leading to 5 indecomposable principally polarized abelian threefolds (E^3, a_i). In Table 1, we give h by its Gram matrix in the canonical basis of $\mathscr{O}^3$. For each lattice (L, h_i), we also give the smallest odd ℓ determined by Algorithm 5. Recall that it determines the degree ℓ^3 of the isogeny we will compute using the Algorithm 8. We also display in Table 1 the order of the automorphism group of (L, h_i), and if $\chi := \chi_{18}(E^3, a_i, w_{E^3}) = 0$ or if it is a square in $\mathbb{F}_q$.

We see that only a_1 leads to a non-trivial obstruction and therefore to a non-hyperelliptic defect-0 curve. This result agrees with the heuristic result which can be deduced from [Rit10, Table 2]. An equation of C is

$$\begin{aligned} x^4 \;+\; & 7780x^3y + 8862x^3 + 456x^2y^2 + 2118x^2y + 1846x^2 + 5713xy^3 + 10064xy^2 + 7494xy \\ +\; & 6469x + 7559y^4 + 9490y^3 + 7458y^2 + 214y + 6746 = 0. \end{aligned}$$

Moreover by Torelli theorem [Mat58, p.790-792], since $\mathrm{Aut}(E^3, a_1) \simeq \mathrm{Aut}(L, h_1) \simeq \{\pm 1\}$ and C is non-hyperelliptic, the automorphism group of C is trivial. As far as we know, this is the first example of a finite field for which one can ensure that the defect-0 curves have no extra-automorphism. As recalled in [Rit11], most of the methods developed to find curves of genus 3 with many points use the existence of extra-automorphisms. The question of existence of a defect-0 curve over $\mathbb{F}_{10313}$ could not have been solved in this way.

Example 5.6. Let $q = 131$. As previously, the existence of a defect-0 curve of genus 3 over $\mathbb{F}_q$ leads to consider indecomposable unimodular positive definite $\mathscr{O}$-lattices L_i of rank 3, where $\mathscr{O}$ has discriminant -40. The class number of $\mathscr{O}$ is 2 and we find 12 L_i, out of which 6 are not free and the largest ℓ we have to

Case	Gram matrix of h_i	ℓ	$\#Aut(L,h_i)$	Is $\chi=0$?	Is χ a square?
1	$\begin{pmatrix} 3 & 1 & 1-\overline{\omega} \\ 1 & 4 & 2 \\ 1-w & 2 & 5 \end{pmatrix}$	11	2	no	yes
2	$\begin{pmatrix} 3 & 1+\overline{\omega} & 2-\overline{\omega} \\ 1+w & 5 & -2-\overline{\omega} \\ 2-w & -2-w & 5 \end{pmatrix}$	9	12	no	no
3	$\begin{pmatrix} 2 & -1 & 1 \\ -1 & 4 & 1-\overline{\omega} \\ 1 & 1-w & 4 \end{pmatrix}$	9	4	no	no
4	$\begin{pmatrix} 3 & 1 & -1-\overline{\omega} \\ 1 & 3 & -1 \\ -1-w & -1 & 5 \end{pmatrix}$	11	4	no	no
5	$\begin{pmatrix} 3 & -1 & -1-\overline{\omega} \\ -1 & 3 & 0 \\ -1-w & 0 & 5 \end{pmatrix}$	11	4	no	no

TABLE 1. Example 5.5.

consider is 19. We get 11 defect-0 curves of genus 3 over $\mathbb{F}_q$ up to $\mathbb{F}_q$-isomorphism, for instance

$$\begin{aligned} x^4 &+ 72x^3y + 111x^3z + 55x^2y^2 + 99x^2yz + 47x^2z^2 + 8xy^3 + 95xy^2z \\ &+ 74xyz^2 + 30xz^3 + 39y^4 + 53y^3z + 58y^2z^2 + 40yz^3 + 59z^4 = 0 \end{aligned}$$

which has an automorphism group of order 2.

Example 5.7. Let $q = 97$. As previously, the existence of a defect-0 curve of genus 3 over $\mathbb{F}_q$ leads to consider indecomposable unimodular positive definite R-lattices of rank 3, where R has discriminant -27 and therefore is not the maximal order of $\mathrm{Frac}(R)$. Our algorithms finds 4 indecomposable unimodular positive definite R-lattices and there is one lattice which is not projective, namely $R^2 \oplus \mathscr{O}$. This leads to 4 indecomposable principally polarized abelian threefolds over $\mathbb{F}_q$ isogenous to E^3 where $E/\mathbb{F}_q : y^2 = x^3 + 92x + 10$. For three of them, Serre's obstruction is trivial, so we get exactly three defect-0 curves of genus 3 over $\mathbb{F}_q$ up to $\mathbb{F}_q$-isomorphism for instance

$$\begin{aligned} x^4 &+ 63x^3y + 28x^3z + 10x^2y^2 + 81x^2yz + 43x^2z^2 + 89xy^3 + 10xy^2z + 70xyz^2 + 45xz^3 \\ &+ 24y^4 + 55y^3z + 77y^2z^2 + 35yz^3 + 54z^4 = 0 \end{aligned}$$

with an automorphism group of order 6.

5.3. **Curves of genus 4.** Jacobians of curves of genus 4 are not dense in the moduli space $\mathscr{A}_{4,1}$. They form a codimension-1 variety which we shall characterize thanks to the Igusa modular form J of level 1 and weight 8. The modular form J is defined over $\mathbb{C}$ as a homogeneous polynomial of degree 16 in the theta constants with integer coefficients, see for instance [Igu81a, p.538] or in [Igu81b] (with the choice of characteristics from [CKS19]). It is therefore an element of $\Gamma(\mathscr{A}_{4,1}(\mathbb{Z}), \mathcal{H}^8)$ and its values can be computed using Algorithm 8. We will also need the following result below. In [BG92], the first term in the Fourier expansion of J is computed and its constant coefficient is -2^{16}. This means that the Siegel modular form J does not vanish identically on $\mathscr{A}_{4,1} \otimes k$ for any algebraically closed field k of characteristic different from 2.

Igusa proves that the Igusa modular form is related to the classical Schottky modular form by

$$J = \frac{1}{2^6 \cdot 3^2 \cdot 5 \cdot 7} \cdot \left(\left(\sum \vartheta[\epsilon](\tau)^8 \right)^2 - 2^4 \sum \vartheta[\epsilon](\tau)^{16} \right)$$

the sums being over all even characteristics. Hence, over $\mathbb{C}$, this form is zero precisely on the locus of principally polarized abelian varieties of dimension 4 which are decomposable or a Jacobian. Following the same lines as [Rit10, Prop.2.3], this can be extended to any field of characteristic different from 2.

Theorem 5.8. *Let $(A, \mathscr{L})$ be an indecomposable principally polarized abelian variety of dimension 4 over an algebraically closed field k of characteristic different from 2 and w_A a basis of regular differentials. Then $J(A, \mathscr{L}, w_A) = 0$ if and only if $(A, \mathscr{L})$ is the Jacobian of a curve of genus 4 over k.*

Proof. Let $\mathscr{A}_{4,1}$ be the moduli stack of principally polarized abelian schemes of relative dimension 4 and let us denote by $\mathscr{T}$ the Torelli locus (the image of the moduli stack of genus 4 curves of compact type). Following [MO13, p.554], it is a reduced and closed substack of $\mathscr{A}_{4,1}$. Moreover for any algebraically closed field k, $\mathscr{T}(k)$ coincides with the disjoint union of the set of Jacobians of genus 4 curves and the set of decomposable principally polarized abelian varieties of dimension 4 defined over k.

Over $\mathbb{C}$, $\mathscr{T}(\mathbb{C}) = (J = 0)_{red}(\mathbb{C})$. This shows that $\mathscr{T} \otimes \mathbb{Q} = (J = 0)_{red} \otimes \mathbb{Q}$. Taking the schematic closure over $\mathbb{Z}[\frac{1}{2}]$ we get $\mathscr{T} \supset \overline{\mathscr{T} \otimes \mathbb{Q}} = \overline{(J = 0)_{red} \otimes \mathbb{Q}} \subset (J = 0)_{red}$ in $\mathscr{A}_{4,1}$ We need to prove that the two inclusions are equalities, i.e. that none of the loci $\mathscr{T}$ or $(J = 0)_{red}$ has a vertical component. For $(J = 0)_{red}$ this is the case since the modular form $J \in \Gamma(\mathscr{A}_{4,1} \otimes \mathbb{Z}[\frac{1}{2}], \mathcal{H}^{\otimes 8})$ is primitive and the fibers of $\mathscr{A}_{4,1}$ are irreducible (see for instance the proof of [FC90, Lemma 3.2, p. 163]). Similarly, for $\mathscr{T}$, this is true because we can lift any genus 4 curve in a special fiber to characteristic 0.

From this we deduce that $J(A, \mathscr{L}, w_A) = 0$ if and only if $(A, \mathscr{L}) \in \mathscr{T} \otimes k$. Since we have assumed that the polarization $\mathscr{L}$ is indecomposable, this is the case if and only if $(A, \mathscr{L})$ is a Jacobian. □

As we only need to check if the value of J is zero or not, we can work with any affine lift of the theta null point. However, if it is zero and $(A, \mathscr{L})$ is therefore a Jacobian over the algebraic closure, there is currently no way to ensure that it is also a Jacobian over the ground field.

Example 5.9. Let us consider the case of defect-0 genus 4 curves C over $\mathbb{F}_{59}$. The Jacobian of C would be isogenous to E^4 with E an elliptic curve with $\mathrm{End}(E)$ of discriminant -11. There are three indecomposable principally polarized abelian varieties in the class of E^4. We can check (using for the three of them the value $\ell = 3$) that for none of them the Igusa form is 0. Hence there is no defect-0 curve of genus 4 over $\mathbb{F}_{59}$ as it is confirmed in these tables or [Zay16, Th.1.1].

It would be more interesting to look at one unknown entry of these tables, like for instance $q = 89$. However in this case the discriminant of the associated elliptic curve is 32 and our algorithms are not efficient enough to work it out yet.

References

[Akh90] N. I. Akhiezer. *Elements of the theory of elliptic functions*. Vol. 79. Translations of Mathematical Monographs. Translated from the second Russian edition by H. H. McFaden. Amer. Math. Soc., 1990 (cit. on p. 26).

[AK18] Z. Amir-Khosravi. "Serre's tensor construction and moduli of abelian schemes". In: *Manuscripta Math.* 156.3-4 (2018), pp. 409–456 (cit. on pp. 5, 16).

[BIL+16] J. S. Balakrishnan, S. Ionica, K. Lauter, and C. Vincent. "Constructing genus-3 hyperelliptic Jacobians with CM". In: *LMS J. Comput. Math.* 19.suppl. A (2016), pp. 283–300 (cit. on p. 30).

[BS11] G. Bisson and A. V. Sutherland. "Computing the endomorphism ring of an ordinary elliptic curve over a finite field". In: *J. Number Theory* 131.5 (2011), pp. 815–831 (cit. on p. 18).

[BCR10] G. Bisson, R. Cosset, and D. Robert. "AVIsogenies". Magma package devoted to the computation of isogenies between abelian varieties. 2010. URL: http://avisogenies.gforge.inria.fr. Free software (LGPLv2+), registered to APP (reference IDDN.FR.001.440011.000.R.P.2010.-000.10000). (Cit. on pp. 20, 21, 26).

[BF60] Z. I. Borevich and D. K. Faddeev. "Integral representations of quadratic rings". In: *Vestnik. Leningrad. Univ.* 15.19 (1960), pp. 52–60 (cit. on p. 6).

[BG92] B. Brinkmann and L. Gerritzen. "The lowest term of the Schottky modular form". In: *Math. Ann.* 292.2 (1992), pp. 329–335 (cit. on p. 33).

[BGH+08] J. H. Bruinier, G. van der Geer, G. Harder, and D. Zagier. *The 1-2-3 of modular forms*. Universitext. Lectures from the Summer School on Modular Forms and their Applications held in Nordfjordeid, June 2004, Edited by Kristian Ranestad. Springer, 2008 (cit. on p. 23).

[Can16] L. Candelori. *The transformation laws of algebraic theta functions*. 2016. arXiv: 1609.04486 (cit. on p. 24).

[CS15] T. G. Centeleghe and J. Stix. "Categories of abelian varieties over finite fields, I: Abelian varieties over $\mathbb{F}_p$". In: *Algebra Number Theory* 9.1 (2015), pp. 225–265 (cit. on p. 2).

[Cha86] C.-L. Chai. "Siegel moduli schemes and their compactifications over **C**". In: *Arithmetic geometry (Storrs, Conn., 1984)*. Springer, 1986, pp. 231–251 (cit. on p. 23).

[CKS19] L. Chua, M. Kummer, and B. Sturmfels. "Schottky algorithms: classical meets tropical". In: *Math. Comp.* 88.319 (2019), pp. 2541–2558 (cit. on p. 33).

[CFA+06] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, eds. *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006, pp. xxxiv+808 (cit. on p. 3).

[Cos11] R. Cosset. "Application des fonctions thêta à la cryptographie sur courbes hyperelliptiques". PhD thesis. Université Nancy-I, 2011 (cit. on pp. 21, 26, 28).

[CR15] R. Cosset and D. Robert. "An algorithm for computing (ℓ, ℓ)-isogenies in polynomial time on Jacobians of hyperelliptic curves of genus 2". In: *Math. Comp.* 84.294 (2015), pp. 1953–1975 (cit. on pp. 3, 20, 21, 23, 30).

[DM69] P. Deligne and D. Mumford. "The irreducibility of the space of curves of given genus". In: *Inst. Hautes Études Sci. Publ. Math.* 36 (1969), pp. 75–109 (cit. on p. 23).

[Del69] P. Deligne. "Variétés abéliennes ordinaires sur un corps fini". In: *Invent. Math.* 8 (1969), pp. 238–243 (cit. on p. 2).

[DKR+20] T. Dupuy, K. Kedlaya, D. Roe, and C. Vincent. *Isogeny Classes of Abelian Varieties over Finite Fields in the LMFDB*. 2020. arXiv: 2003.05380 (cit. on p. 2).

[EL10] K. Eisenträger and K. Lauter. "A CRT algorithm for constructing genus 2 curves over finite fields". In: *Arithmetics, geometry, and coding theory (AGCT 2005)*. Vol. 21. Sémin. Congr. Soc. Math. France, Paris, 2010, pp. 161–176 (cit. on p. 18).

[FC90] G. Faltings and C.-L. Chai. *Degeneration of abelian varieties*. Vol. 22. Ergebnisse der Mathematik und ihrer Grenzgebiete (3). With an appendix by David Mumford. Springer, 1990 (cit. on pp. 23, 24, 34).

[FK01] H. M. Farkas and I. Kra. *Theta constants, Riemann surfaces and the modular group*. Vol. 37. Graduate Studies in Mathematics. An introduction with applications to uniformization theorems, partition identities and combinatorial number theory. Amer. Math. Soc., 2001 (cit. on p. 26).

[FP85] U. Fincke and M. Pohst. "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis". In: *Math. Comp.* 44.170 (1985), pp. 463–471 (cit. on p. 11).

[Fio16] A. Fiorentino. *Weber's formula for the bitangents of a smooth plane quartic*. 2016. arXiv: 1612.02049 (cit. on p. 31).

[GY00] W. T. Gan and J.-K. Yu. "Group schemes and local densities". In: *Duke Math. J.* 105.3 (2000), pp. 497–524 (cit. on p. 8).

[GD64] A. Grothendieck and J. Dieudonné. "Eléments de géométrie algébrique". In: *Publ. math. IHES* 20.24 (1964), p. 1965 (cit. on p. 18).

[Hal10] S. Haloui. "The characteristic polynomials of abelian varieties of dimensions 3 over finite fields". In: *J. Number Theory* 130.12 (2010) (cit. on p. 2).

[HS12] S. Haloui and V. Singh. "The characteristic polynomials of abelian varieties of dimension 4 over finite fields". In: *Arithmetic, geometry, cryptography and coding theory*. Vol. 574. Contemp. Math. Amer. Math. Soc., 2012, pp. 59–68 (cit. on p. 2).

[HK89a] K. Hashimoto and H. Koseki. "Class numbers of definite unimodular Hermitian forms over the rings of imaginary quadratic fields". In: *Tohoku Math. J. (2)* 41.1 (1989), pp. 1–30 (cit. on p. 8).

[HK89b] K. Hashimoto and H. Koseki. "Class numbers of positive definite binary and ternary unimodular Hermitian forms". In: *Tohoku Math. J. (2)* 41.2 (1989), pp. 171–216 (cit. on pp. 4, 8).

[Hay19] D. Hayashida. "The characteristic polynomials of abelian varieties of higher dimension over finite fields". In: *J. Number Theory* 196 (2019), pp. 205–222 (cit. on p. 2).

[HV98] B. Hemkemeier and F. Vallentin. "Incremental algorithms for lattice problems". In: *Electronic Colloquium on Computational Complexity*. Vol. 52. revision 1. 1998 (cit. on p. 7).

[Hof91] D. W. Hoffmann. "On positive definite hermitian forms". In: *Manuscripta Math.* 71 (1991), pp. 399–429 (cit. on p. 4).

[Hon68] T. Honda. "Isogeny classes of abelian varieties over finite fields". In: *J. Math. Soc. Japan* 20 (1968), pp. 83–95 (cit. on p. 1).

[How95] E. W. Howe. "Principally polarized ordinary abelian varieties over finite fields". In: *Trans. Amer. Math. Soc.* 347.7 (1995), pp. 2361–2401 (cit. on p. 2).

[HNR09] E. W. Howe, E. Nart, and C. Ritzenthaler. "Jacobians in isogeny classes of abelian surfaces over finite fields". In: *Ann. Inst. Fourier (Grenoble)* 59.1 (2009), pp. 239–289 (cit. on p. 2).

[IKO86] T. Ibukiyama, T. Katsura, and F. Oort. "Supersingular curves of genus two and class numbers". In: *Compos. Math.* 57.2 (1986), pp. 127–152 (cit. on p. 2).

[Ich96] T. Ichikawa. "Theta constants and Teichmüller modular forms". In: *J. Number Theory* 61.2 (1996), pp. 409–419 (cit. on p. 32).

[Igu81a] J. Igusa. "On the irreducibility of Schottky's divisor". In: *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* 28.3 (1981), 531–545 (1982) (cit. on p. 33).

[Igu81b] J. Igusa. "Schottky's invariant and quadratic forms". In: *E. B. Christoffel.* Birkhäuser, 1981, pp. 352–362 (cit. on p. 33).

[Igu67] J. Igusa. "Modular forms and projective invariants". In: *Amer. J. Math.* 89 (1967), pp. 817–855 (cit. on p. 32).

[Jac62] R. Jacobowitz. "Hermitian forms over local fields". In: *Amer. J. Math.* 84 (1962), pp. 441–465 (cit. on pp. 7, 9, 12, 13, 15).

[JKP+18] B. W. Jordan, A. G. Keeton, B. Poonen, E. M. Rains, N. Shepherd-Barron, and J. T. Tate. "Abelian varieties isogenous to a power of an elliptic curve". In: *Compos. Math.* 154.5 (2018), pp. 934–959 (cit. on pp. 2, 5, 16–18).

[Kan11] E. Kani. "Products of CM elliptic curves". In: *Collect. Math.* 62.3 (2011), pp. 297–339 (cit. on p. 2).

[Kem89] G. Kempf. "Linear systems on abelian varieties". In: *American Journal of Mathematics* 111.1 (1989), pp. 65–94 (cit. on p. 23).

[Kir16] M. Kirschmer. "Definite quadratic and hermitian forms with small class number". Habilitation. RWTH Aachen University, 2016 (cit. on pp. 6, 8).

[Kir19] M. Kirschmer. "Determinant groups of Hermitian lattices over local fields". In: *Arch. Math.* 113.4 (2019), pp. 337–347 (cit. on pp. 2, 8).

[Kne66] M. Kneser. "Strong approximation". In: *Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965).* Amer. Math. Soc., 1966, pp. 187–196 (cit. on p. 14).

[Koi76] S. Koizumi. "Theta relations and projective normality of abelian varieties". In: *American Journal of Mathematics* (1976), pp. 865–889 (cit. on p. 23).

[LR08] G. Lachaud and C. Ritzenthaler. "On some questions of Serre on abelian threefolds". In: *Algebraic geometry and its applications.* Vol. 5. Ser. Number Theory Appl. World Sci. Publ., 2008, pp. 88–115 (cit. on p. 32).

[LRZ10] G. Lachaud, C. Ritzenthaler, and A. Zykin. "Jacobians among abelian threefolds: a formula of Klein and a question of Serre". In: *Math. Res. Lett.* 17.2 (2010) (cit. on p. 32).

[LSV20] J.-C. Lario, A. Somoza, and C. Vincent. *An inverse Jacobian algorithm for Picard curves.* 2020. arXiv: 1611.02582 [math.NT] (cit. on p. 30).

[Lau18] K. Lauter. "On maximal genus 3 curves over finite fields with an appendix by J. P. Serre." In: *Compos. Math.* 154.5 (2018), pp. 934–959 (cit. on pp. 2, 16).

[LR12a] R. Lercier and C. Ritzenthaler. "Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects". In: *J. Algebra* 372 (2012), pp. 595–636 (cit. on pp. 30, 31).

[LRR+14] R. Lercier, C. Ritzenthaler, F. Rovetta, and J. Sijsling. "Parametrizing the moduli space of curves and applications to smooth plane quartics over finite fields". In: *LMS J. Comput. Math.* 17.suppl. A (2014), pp. 128–147 (cit. on p. 31).

[Liu02] Q. Liu. *Algebraic geometry and arithmetic curves.* Vol. 6. Oxford Graduate Texts in Mathematics. Translated from the French by Reinie Erné, Oxford Science Publications. Oxford University Press, 2002 (cit. on p. 18).

[Lor19] E. Lorenzo García. *On different expressions for invariants of hyperelliptic curves of genus 3.* 2019. arXiv: 1907.05776 (cit. on p. 30).

[LR12b] D. Lubicz and D. Robert. "Computing isogenies between abelian varieties". In: *Compos. Math.* 148.5 (2012), pp. 1483–1515 (cit. on p. 23).

[LR15] D. Lubicz and D. Robert. "Computing separable isogenies in quasi-optimal time". In: *LMS J. Comput. Math.* 18 (1 2015), pp. 198–216 (cit. on p. 20).

[LR16] D. Lubicz and D. Robert. "Arithmetic on Abelian and Kummer Varieties". In: *Finite Fields and Their Applications* 39 (2016), pp. 130–158 (cit. on p. 23).

[Mar19] S. Marseglia. "Computing abelian varieties over finite fields isogenous to a power". In: *Res. Number Theory* 5.4 (2019), Paper No. 35, 17 (cit. on pp. 2, 16).

[Mat58] T. Matsusaka. "On a theorem of Torelli". In: *Amer. J. Math.* 80 (1958), pp. 784–800 (cit. on p. 32).

[Mea08] S. Meagher. "Twists of genus 3 and their Jacobians". PhD thesis. Rijksuniversiteit Groningen, 2008 (cit. on p. 32).

[Mil86] J. S. Milne. "Abelian varieties". In: *Arithmetic geometry (Storrs, Conn., 1984)*. Springer, 1986, pp. 103–150 (cit. on pp. 17, 20).

[MO13] B. Moonen and F. Oort. "The Torelli locus and special subvarieties". In: *Handbook of moduli. Vol. II*. Vol. 25. Adv. Lect. Math. (ALM). Int. Press, 2013, pp. 549–594 (cit. on p. 34).

[Mum66] D. Mumford. "On the equations defining abelian varieties. I". In: *Invent. Math.* 1 (1966), pp. 287–354 (cit. on pp. 22–24, 28).

[Mum67] D. Mumford. "On the equations defining abelian varieties. II". In: *Invent. Math.* 3 (1967), pp. 75–135 (cit. on pp. 22, 24).

[Mum07a] D. Mumford. *Tata lectures on theta. I*. Modern Birkhäuser Classics. With the collaboration of C. Musili, M. Nori, E. Previato and M. Stillman, Reprint of the 1983 edition. Birkhäuser, 2007 (cit. on pp. 24, 27, 28).

[Mum07b] D. Mumford. *Tata lectures on theta. II: Jacobian theta functions and differential equations. With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman, and H. Umemura. Reprint of the 1984 edition.* Modern Birkhäuser Classics. Birkhäuser, 2007 (cit. on pp. 21, 26).

[Mum07c] D. Mumford. *Tata lectures on theta. III*. Modern Birkhäuser Classics. With collaboration of Madhav Nori and Peter Norman, Reprint of the 1991 original. Birkhäuser, 2007 (cit. on p. 24).

[Mum08] D. Mumford. *Abelian varieties*. Vol. 5. Tata Institute of Fundamental Research Studies in Mathematics. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition. Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008 (cit. on p. 17).

[MFK94] D. Mumford, J. Fogarty, and F. Kirwan. *Geometric invariant theory*. Vol. 34. Springer, 1994 (cit. on p. 21).

[O'M63] O. T. O'Meara. *Introduction to quadratic forms*. Springer, 1963 (cit. on p. 13).

[OU73] F. Oort and K. Ueno. "Principally polarized abelian varieties of dimension two or three are Jacobian varieties". In: *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* 20 (1973), pp. 377–381 (cit. on p. 30).

[OS19] A. Oswal and A. N. Shankar. *Almost ordinary abelian varieties over finite fields*. 2019. arXiv: 1901.01589 (cit. on p. 2).

[Rit10] C. Ritzenthaler. "Explicit computations of Serre's obstruction for genus-3 curves and application to optimal curves". In: *LMS J. Comput. Math.* 13 (2010), pp. 192–207 (cit. on pp. 4, 32, 33).

[Rit11] C. Ritzenthaler. "Optimal curves of genus 1, 2 and 3". In: *Actes de la Conférence "Théorie des Nombres et Applications"*. Vol. 2011. Publ. Math. Besançon Algèbre Théorie Nr. Presses Univ. Franche-Comté, Besançon, 2011, pp. 99–117 (cit. on p. 32).

[Rob10] D. Robert. "Theta functions and cryptographic applications". PhD thesis. Université Henri-Poincarré, Nancy 1, France, 2010 (cit. on pp. 23, 28).

[Sch98] A. Schiemann. "Classification of Hermitian forms with the neighbour method". In: *J. Symbolic Comput.* 26.4 (1998), pp. 487–508 (cit. on pp. 2, 8, 32).

[Ser85] J.-P. Serre. *Rational points on curves over finite fields, Lectures given at Harvard, notes by F.Q. Gouvéa*. 1985 (cit. on pp. 2, 4, 15, 16, 32).

[Shi64] G. Shimura. "Arithmetic of the unitary group". In: *Annals of Mathematics* 79.2 (1964), pp. 369–409 (cit. on p. 8).

[Str14] M. Streng. "Computing Igusa class polynomials". In: *Math. Comp.* 83.285 (2014), pp. 275–309 (cit. on p. 3).

[Sut11] A. V. Sutherland. "Computing Hilbert class polynomials with the Chinese remainder theorem". In: *Math. Comp.* 80.273 (2011), pp. 501–538 (cit. on p. 3).

[Tat66] J. Tate. "Endomorphisms of abelian varieties over finite fields". In: *Invent. Math.* 2 (1966), pp. 134–144 (cit. on p. 1).

[Wat69] W. Waterhouse. "Abelian varieties over finite fields". In: *Annales scientifiques de l'E.N.S.* 2.4 (1969), pp. 521–560 (cit. on pp. 2, 16).

[Web76] H. Weber. *Theory of abelian functions of genus 3. (Theorie der Abelschen Functionen vom Geschlecht 3.)* 1876 (cit. on p. 31).

[Wen01] A. Weng. "A class of hyperelliptic CM-curves of genus three". In: *J. Ramanujan Math. Soc.* 16.4 (2001), pp. 339–372 (cit. on p. 30).

[XYY19] J. Xue, T.-C. Yang, and C.-F. Yu. "Supersingular abelian surfaces and Eichler class number formula". In: *Asian Journal of Mathematics* 23.4 (2019) (cit. on p. 2).

[Zay16] A. Zaytsev. "Optimal curves of low genus over finite fields". In: *Finite Fields Appl.* 37 (2016), pp. 203–224 (cit. on p. 34).

Universität Paderborn, Fakultät EIM, Institut für Mathematik, Warburger Str. 100, 33098 Paderborn, Germany
Email address: markus.kirschmer@math.upb.de

Univ Rennes, CNRS, IRMAR - UMR 6625, F-35000 Rennes, France.
Email address: fabien.narbonne@univ-rennes1.fr

Univ Rennes, CNRS, IRMAR - UMR 6625, F-35000 Rennes, France.
Email address: christophe.ritzenthaler@univ-rennes1.fr

INRIA Bordeaux–Sud-Ouest, 200 avenue de la Vieille Tour, 33405 Talence Cedex, France and Institut de Mathématiques de Bordeaux, 351 cours de la liberation, 33405 Talence cedex, France
Email address: damien.robert@inria.fr