Abelian surfaces over finite fields containing no curves of genus 3 or less

Elena Berardini, Alejandro Giangreco Maidana, Stefano Marseglia

ABELIAN SURFACES OVER FINITE FIELDS CONTAINING NO CURVES OF GENUS 3 OR LESS

ELENA BERARDINI, ALEJANDRO GIANGRECO MAIDANA, AND STEFANO MARSEGLIA

Abstract. We characterise abelian surfaces defined over finite fields containing no curves of genus less than or equal to 3. Firstly, we complete and expand the characterisation of isogeny classes of abelian surfaces with no curves of genus up to 2 initiated by the first author *et al.* in previous work. Secondly, we show that, for simple abelian surfaces, containing a curve of genus 3 is equivalent to admitting a polarisation of degree 4. Thanks to this result, we can use existing algorithms to check which isomorphism classes in the isogeny classes containing no genus 2 curves have a polarisation of degree 4. Thirdly, we characterise isogeny classes of abelian surfaces with no curves of genus ≤ 2, containing no abelian surface with a polarisation of degree 4. Finally, we describe absolutely irreducible genus 3 curves lying on abelian surfaces containing no curves of genus less than or equal to 2, and show that their number of rational points is far from the Serre–Weil bound.

Introduction

Studying the minimal genus of algebraic curves lying on an abelian variety is a classical question [1, 8, 4]. In this paper we focus our attention on abelian surfaces. Over an algebraically closed field, every abelian surface is isogenous to a principally polarised one [20, Cor. 1, p. 234], that is, to the Jacobian of a genus 2 curve or to the product of two elliptic curves. A well-known consequence of this fact is that every abelian surface over an algebraically closed field contains a (possibly singular) absolutely irreducible curve of geometric genus 2 or 1; see also Lemma 1.1 below. On another note, one can also study when an abelian surface contains curves of a fixed genus. Over the complex numbers, this question has been treated in [5] for genus 3 curves and in [7] for hyperelliptic curves of genus 4. Over non-algebraically closed fields, the situation is more complicated. For example, it is no longer true that any abelian surface is isogenous to a principally polarised one.

From now on, we direct our attention to the case of finite fields. Isogeny classes in which no abelian surface admits a principal polarisation are classified in [14]. Furthermore, even if an isogeny class is principally polarisable, it might not contain a Jacobian surface nor the product of two elliptic curves [15]. Indeed, by a theorem of Weil [15, Thm. 1.3], we have one more option among principally polarisable abelian surfaces, that is, Weil restrictions of elliptic curves defined over a quadratic extension of the finite field. To sum up, studying the minimal genus of algebraic curves lying over an abelian surface defined over a finite field is a hard question, and it is in fact open in its full generality. Besides the intrinsic theoretical interest, this question was raised in the context of algebraic geometry coding theory. Indeed, the first author and her co-authors showed in [2] that so called algebraic geometry codes constructed from abelian surfaces defined over a finite field and containing no curves of small genus respect a better bound on their minimum distance.

2020 *Mathematics Subject Classification.* Primary: 14K15, 11G20. Secondary: 14G15, 11G10 .
Key words and phrases. abelian varieties, algebraic curves, finite fields, polarisations.

Our contributions. Let $\mathbb{F}_q$ be a finite field of cardinality q the power of a prime p. We recall that an isogeny class of abelian surfaces over $\mathbb{F}_q$ corresponds via the Honda–Tate theory to a polynomial of the form $f(t) = t^4 + at^3 + bt^2 + aqt + q^2$, called Weil polynomial.

Previous work by the first author and coauthors showed that abelian surfaces defined over $\mathbb{F}_q$ which are not isogenous to a principally polarised abelian surface or which are isogenous to Weil restrictions of some elliptic curves defined over $\mathbb{F}_{q^2}$ do not contain absolutely irreducible curves of arithmetic genus up to 2; see [2, Prop. 4.2 and 4.3]. We denote the set of Weil polynomials corresponding to the former by $\mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}}$ while the latter splits into $\{(t^2-2)^2, (t^2-3)^2\} \sqcup \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$. As the notation suggests, the Weil polynomials of the aforementioned isogeny classes are all irreducible except for $(t^2-2)^2$ and $(t^2-3)^2$. We expand the previous result in Theorem 1.2, by showing that these abelian surfaces do not contain absolutely irreducible curves of *geometric* genus up to 2, and that this is an equivalence. In Remark 1.3 we show that restricting to absolutely irreducible curves of arithmetic genus up to 2 does not provide an equivalence.

The main goal of the present paper is to determine when an abelian surface A does not contain curves of genus ≤ 3. Our first main result is the following, which can be found later in the text as Theorem 2.3.

Main Theorem 1. *Let A be a simple abelian surface defined over $\mathbb{F}_q$. Then, the following are equivalent:*

(1) A has a polarisation of degree 4,
(2) A contains an $\mathbb{F}_q$-irreducible curve of arithmetic genus 3.

The isogeny classes determined by $(t^2-2)^2$ and $(t^2-3)^2$ are dealt in Proposition 2.1. So we now assume that $f(t)$ is irreducible, that is $f(t) \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}} \sqcup \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$. When the corresponding isogeny class $\mathcal{C}$ is ordinary, the third author designed an algorithm in [18] to compute the isomorphism classes of abelian surface in $\mathcal{C}$ admitting a polarisation of degree 4. See Section 6 for an overview and examples.

Our second main result gives a complete classification of the isogeny classes determined by $f(t) \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}} \sqcup \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$ that contain an abelian surface with a polarisation of degree 4. The proof of this classification builds on Howe's seminal work [12, 13] on kernels of polarisations of abelian varieties over finite fields. An expanded statement appears later in the paper as Theorem 5.7.

Main Theorem 2. *Assume that $f(t) \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}} \sqcup \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$ and let $\mathcal{C}$ be the corresponding isogeny class. Set $K = \mathbb{Q}[t]/(f(t))$, which is a CM field with totally real subfield K^+. Consider the statement:*

(★) *There is no A in $\mathcal{C}$ admitting a polarisation of degree 4.*

Then, the following statements hold.

(i) Assume $\mathcal{C}$ is ordinary. Then (★) holds if and only if there is no A in $\mathcal{C}$ with maximal $\mathbb{F}_q$-endomorphism ring admitting a polarisation of degree 4.
(ii) Assume that $f(t) \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}}$. Then (★) holds if and only if 2 is inert in K^+.
(iii) Assume that $f(t) \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$, so that $f(t) = t^4 + bt^2 + q^2$. Then (★) is equivalent to
- *$b = 1 - 2q$ and q is odd, if $\mathcal{C}$ is ordinary,*
- *q is even, if $\mathcal{C}$ is non-ordinary.*

Organisation of the paper. In Section 1 we recall and complete the characterisation given in [2] of isogeny classes of abelian surfaces containing no absolutely irreducible curves of genus smaller than or equal to 2, and describe some properties of their Weil polynomials. In Section 2, we start the characterisation of abelian surfaces containing no curves of genus 3 among

those containing no curves of genus up to 2. In particular, in Theorem 2.3, we prove the key equivalence between containing a curve of arithmetic genus 3 and having a polarisation of degree 4 stated above as Main Theorem 1. In Section 3 we collect technical results on the factorisation of 2 in the extension $K/\mathbb{Q}$, that we shall use throughout the paper. Section 4 is devoted to results on kernels of polarisations of abelian varieties, based on the work of Howe [12, 13]. In Section 5, we prove an expanded version of Main Theorem 2, namely Theorem 5.7, in which we give necessary and sufficient conditions on an isogeny class to not contain surfaces admitting a polarisation of degree 4, hence containing no curves of arithmetic genus up to 3. Section 6 describes the algorithm proposed by the third author [18] to compute the isomorphism classes of abelian surface in an isogeny class admitting a polarisation of degree 4, and provides examples for our Theorem 5.7. Finally, in Section 7, we characterise curves of genus 3 lying on abelian surfaces containing no curves of genus less than 2, and give bounds for their number of rational points, showing that those genus 3 curves are far from being maximal.

1. Abelian surfaces containing no curves of genus ≤ 2

Let A be a g-dimensional abelian variety defined over the finite field $\mathbb{F}_q$ of characteristic p. The characteristic polynomial $f(t)$ of its Frobenius endomorphism acting on the ℓ-Tate module (for any prime $\ell \neq p$) is a monic polynomial of degree $2g$ with integer coefficients. All the complex roots of $f(t)$ have absolute value $\sqrt{q}$. We call such a polynomial a Weil polynomial. Honda and Tate showed in [25, 11, 26] that $f(t)$ completely determines the isogeny class $\mathcal{C}$ of A. Recall that an abelian variety A over $\mathbb{F}_q$ of dimension g is called ordinary if the coefficient of t^g in $f(t)$ is coprime with q. In particular, being ordinary is a property of the isogeny class $\mathcal{C}$ of A. We will say that $\mathcal{C}$ and $f(t)$ are ordinary if A is so.

In the rest of the paper, whenever we talk about a morphism, we always mean an $\mathbb{F}_q$-morphism. In particular, we will say simple for $\mathbb{F}_q$-simple, isogeny for $\mathbb{F}_q$-isogeny, etc.

By a *curve* C we mean a possibly singular one-dimensional $\mathbb{F}_q$-irreducible projective variety always defined over $\mathbb{F}_q$. We say that a curve is absolutely irreducible if it is irreducible over the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$. Nevertheless, later in the paper, when we want to emphasise that a curve C is not necessarily absolutely irreducible, we will say that C is $\mathbb{F}_q$-irreducible. We say that a curve C lies on an abelian surface A or that A contains C, if C is a closed subvariety of A, or, equivalently, if there is an embedding of C in A. We recall here some well-known definitions and results, following [23, Ch. 4, Sec. 2]. The arithmetic genus p_a of a curve is defined as $1-\chi(C)$, $\chi(C)$ being the Euler-Poincaré characteristic of C. The geometric genus g of C is by definition the genus of its normalisation $\tilde{C}$. The geometric genus of a curve is always smaller than or equal to its arithmetic genus, and equality holds if and only if the curve is smooth. A *divisor* of A is a formal sum, with integer coefficients, of $\mathbb{F}_q$-irreducible curves lying on A. It is called effective if all its coefficients are non-negative. By the adjunction formula [23, Ch. 4, Sec. 2, Prop. 5], since the class of canonical divisor of an abelian surface is trivial, for any $\mathbb{F}_q$-irreducible curve C of arithmetic genus p_a on A we have $C^2 = 2p_a - 2$.

The goal of this section is to prove some characterisations and properties of Weil polynomials of abelian surfaces which do not contain absolutely irreducible curves of geometric genus 0, 1 or 2. We start with the following well-known lemma.

Lemma 1.1. *Let $f : A \to B$ be an isogeny of abelian varieties defined over a field k. Let C be a curve of geometric genus g defined over k, lying on A. Then, $f(C)$ is a curve of geometric genus g on B. Moreover, if C is absolutely irreducible then $f(C)$ is absolutely irreducible as well.*

Proof. It follows from the fact that $f(C)$ is birationally equivalent to C. □

Some of the implications of the next theorem are proved in [2]. However, as we will discuss in Remark 1.3, there were some gaps that we fill in.

Theorem 1.2. *Let A be an abelian surface defined over $\mathbb{F}_q$ with Weil polynomial*

$$f(t) = t^4 + at^3 + bt^2 + qat + q^2.$$

Then, the following statements are equivalent:

1. *A does not contain absolutely irreducible curves of geometric genus $0, 1$ or 2;*
2. *A is simple and not isogenous to the Jacobian of an absolutely irreducible smooth genus 2 curve;*
3. *exactly one of the following statements hold:*
   - (a) *A is not isogenous to a principally polarised abelian surface, which is equivalent to have $a^2 - b = q$, $b < 0$ and all prime divisors of b are congruent to $1 \bmod 3$;*
   - (b) *A is isogenous to a Weil restriction of an elliptic curve defined over the quadratic extension of $\mathbb{F}_q$ (hence $a = 0$), which is equivalent to having $A \otimes_{\mathbb{F}_q} \mathbb{F}_{q^2}$ not simple, and one of the following conditions hold:*
     - *$b = 1 - 2q$;*
     - *$p > 2$ and $b = 2 - 2q$;*
     - *$p \equiv 11 \bmod 12$, q is a square and $b = -q$;*
     - *$p = 3$, q is a square and $b = -q$;*
     - *$p = 2$, q is nonsquare and $b = -q$;*
     - *$q = 2$ and $b = -4$;*
     - *$q = 3$ and $b = -6$.*

Proof. We start by proving (1) $\Rightarrow$ (2). By assumption, A does not contain an elliptic curve, hence it is simple. Assume that A is isogenous to the Jacobian of a smooth absolutely irreducible genus 2 curve C. Since C is canonically embedded into its Jacobian, Lemma 1.1 would imply that A contains an absolutely irreducible curve of geometric genus 2, in contradiction with (1).

Now we show that (2) $\Rightarrow$ (1). First note that A cannot contain a curve D of geometric genus 0. Indeed, the normalisation $\tilde{D}$ of D is birationally equivalent to $\mathbb{P}^1$ and, by [19, Cor. 3.8], the only rational maps from $\mathbb{P}^1$ to A are the constant maps. The abelian variety A cannot contain a curve of geometric genus 1 as well. Indeed, such a curve would be an elliptic curve and hence an isogeny factor of A by [9, Prop. 1]. Similarly, A cannot contain a curve D of geometric genus 2 because the induced map $\tilde{D} \to A$ would give a morphism $\mathrm{Jac}(\tilde{D}) \to A$, which is an isogeny since A is simple.

We now focus on (2) $\Rightarrow$ (3). We distinguish two cases. Assume first that A is not isogenous to a principally polarised abelian surface. This corresponds to (3a). The equivalence in terms of the coefficients of the Weil polynomial follows from [14, Thm. 1]. Assume now that A is isogenous to a principally polarised abelian surface. By a classification theorem due to Weil (see for instance [15, Thm. 1.3]), a principally polarised abelian surface defined over $\mathbb{F}_q$ is exactly one of the following: a product of two elliptic curves defined over $\mathbb{F}_q$ with the product polarisation; the Jacobian of a genus 2 curve defined over $\mathbb{F}_q$ with the canonical polarisation; the Weil restriction of an elliptic curve defined over the quadratic extension of $\mathbb{F}_q$ with the induced polarisation. Since we are assuming (2), we exclude the first two cases. So, A is the Weil restriction of an elliptic curve defined over the quadratic extension of $\mathbb{F}_q$. This is equivalent to $A \otimes_{\mathbb{F}_q} \mathbb{F}_{q^2}$ being not simple by [14, Lemma 4]. Finally, the characterisation of the coefficients of the Weil polynomial follows from [2, Prop. 4.3] and the beginning of its proof. Hence, we are in case (3b).

We conclude by showing that (3) ⇒ (2). For A satisfying (3a) the implication is clear. If A satisfies (3b) the result follows from [15, Thm. 1.2-(2), Table 1.2]. □

Remark 1.3. In [2, Lemma 4.1], it is stated that for an abelian surface A defined over $\mathbb{F}_q$ we have that the following statements are equivalent:

(i) A is simple and not isogenous to a Jacobian surface,
(ii) A does not contain absolutely irreducible curves of arithmetic genus 0, 1 or 2,
(iii) A does not contain absolutely irreducible smooth curves of genus 0, 1 or 2.

Note that the implication (2)⇒(1) of Theorem 1.2 is a stronger statement than the implication (i)⇒(ii). However, while our reverse implication (1)⇒(2) holds true, the implication (ii)⇒(i) claimed in [2, Lemma 4.1] is false. Indeed, consider a simple isogeny class containing a Jacobian surface and non-principally polarisable abelian surfaces. Then, any isomorphism class of abelian surface admitting no principal polarisation inside such an isogeny class gives an example of abelian surfaces isogenous to a Jacobian and containing no curves of arithmetic genus 2. Indeed, using the same argument in the proof of Theorem 2.3 below, such a curve would define a polarisation of degree 1, that is, a principal polarisation of the surface. An example of such a class is given in Example 6.2.

Finally, let us remark that the implication (iii)⇒(ii) of [2, Lemma 4.1] still holds true, but a new proof is necessary, that we offer here. Let us suppose that A contains a curve of arithmetic genus $p_a = 1$. Then the geometric genus is necessarily 1 as well, since g cannot be 0 and $g \leq p_a$, thus the curve is smooth, a contradiction. Suppose now that A contains a curve of arithmetic genus $p_a = 2$. If the geometric genus is 1 then we know by [9, Prop. 1] that the curve is smooth and has a structure of an elliptic curve, which leads to a contradiction. If the geometric genus is 2 then the curve is smooth of genus 2, leading again to a contradiction.

Remark 1.4. Lemma 1.1 implies that the property of an abelian surface A to contain or not curves of geometric genus ≤ 3 is an invariant of its isogeny class. In the previous remark, we stressed that this is not the case for curves of arithmetic genus ≤ 2. We are going to see below that this is also the case when considering curves of arithmetic genus ≤ 3.

Remark 1.5. From [14, p. 122], we know that an abelian surface A defined over $\mathbb{F}_q$ which is in a not principally polarisable isogeny class splits over the cubic extension of the base field, that is $A \otimes_{\mathbb{F}_q} \mathbb{F}_{q^3}$ is not simple.

The rest of the section is devoted to prove various results about the Weil polynomials from Theorem 1.2.

Lemma 1.6. *Let $f(t)$ be a Weil polynomial of an abelian surface satisfying one of the equivalent conditions of Theorem 1.2. Then either $f(t) = (t^2 - q)^2$ with $q \in \{2, 3\}$, or $f(t)$ is irreducible over $\mathbb{Q}[x]$.*

Proof. Since $f(t)$ is the Weil polynomial of a simple abelian surface then either it is irreducible or it is the square of a quadratic polynomial. Assume that $f(t)$ is reducible. Then either $f(t) = (t^2 - q)^2$ or $f(t) = (t^2 - \beta t + q)^2$ for some $\beta \in \mathbb{Z}$. If we are the in the former case, then by comparing with Theorem 1.2, we see that $q \in \{2, 3\}$, and we are done. So assume that we are in the latter case. Then $a = -2\beta$ and $b = 2q + \beta^2$. Observe that $b > 0$ which implies that $f(t)$ does not satisfy condition (3a). So we must be in case (3b). Hence $a = 0$ which implies that $\beta = 0$ and $b = 2q$, giving a contradiction with the constraints on b from (3b). Therefore $f(t)$ is irreducible. □

In view of Lemma 1.6, the set of Weil polynomials described in Theorem 1.2 can be partitioned as follows.

Definition 1.7. Let $\mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}}$ (resp. $\mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$) be the set of Weil polynomials described in Theorem 1.2.(3a) (resp. Theorem 1.2.(3b)) which are irreducible over $\mathbb{Q}[x]$. The set of Weil polynomials described in Theorem 1.2 is partitioned as follows:

$$\mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}} \sqcup \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}} \sqcup \{(t^2-2)^2, (t^2-3)^2\}.$$

Recall that if A is an abelian variety over $\mathbb{F}_q$ whose Weil polynomial $f(t)$ has complex roots $\alpha_1 \ldots, \alpha_{2g}$, then the Weil polynomial of the extension of scalars $A_{\mathbb{F}_{q^n}} = A \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}$ has complex roots $\alpha_1^n, \ldots, \alpha_{2g}^n$. This observation, combined with the next result, gives us an effective way to test whether an irreducible Weil polynomial belongs to $\mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$.

Lemma 1.8. *Let A be an abelian surface over $\mathbb{F}_q$ with Weil polynomial $f(t) = t^4 + at^3 + bt^2 + qat + q^2$. Then $f(t) \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$ if and only if $f(t)$ is irreducible, the Weil polynomial of $A_{\mathbb{F}_{q^2}}$ is not irreducible, and b is as in Theorem 1.2.(3b).*

Proof. It follows from Theorem 1.2.(3b). □

For the rest of the section we focus on Weil polynomials belonging to $\mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}} \sqcup \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$.

Lemma 1.9. *Let A be an abelian surface over $\mathbb{F}_q$ with Weil polynomial $f(t) = t^4 + at^3 + bt^2 + qat + q^2$ in $\mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}} \sqcup \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$. Then A is either ordinary or supersingular. If $f(t) \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}}$ then A is ordinary if and only if $a \neq 0$. If $f(t) \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$, then A is ordinary if and only if $b = 1 - 2q$ or, $b = 2 - 2q$ and $p > 2$.*

Proof. Assume that $f(t) \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}}$. Note that A cannot have p-rank 1 since in that case it would be principally polarisable by [17, Thm. 4.3][1]. If $a = 0$ then we have $b = a^2 - q = -q$, and therefore A is supersingular. Suppose $a \neq 0$. By [14, Thm. 2], the abelian variety A cannot be supersingular. Hence, A is ordinary. Now, assume that $f(t) \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$. Obviously if $b = 1-2q$, or $b = 2-2q$ and $p > 2$ then A is ordinary. By Theorem 1.2.(3b), those are the only possible values for b to have ordinarity. To conclude the proof, we need to show that if A is non-ordinary then it is supersingular. Say that A is the Weil restriction of an elliptic curve E over $\mathbb{F}_{q^2}$. If A is non-ordinary, then E is supersingular, and hence A is also supersingular. □

Proposition 1.10. *Let $f(t) = t^4 + at^3 + bt^2 + qat + q^2$ be a Weil polynomial in $\mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}} \sqcup \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$. Then, the number field $K = \mathbb{Q}[t]/f(t)$ is Galois.*

Proof. Let $\alpha, q/\alpha, \beta, q/\beta$ be the complex roots of $f(t)$. Then $-a = \alpha + q/\alpha + \beta + q/\beta$. If $a = 0$ then either $\alpha = -\beta$ or $\alpha = -q/\beta$. In both cases $\beta \in \mathbb{Q}(\alpha)$, so the extension is normal and K is Galois. If $a \neq 0$ then $f(t)$ is in $\mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}}$ and A is ordinary by Lemma 1.9. Hence K is Galois by [12, Lemma 12.1]. □

Lemma 1.11. *Every polynomial $f(t) \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}} \sqcup \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$ is congruent to the product of two quadratic polynomials modulo 2.*

Proof. If $f(t) \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$ then it is an easy calculation. Assume now that $f(t) \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}}$. As usual, write $f(t) = t^4 + at^3 + bt^2 + aqt + q^2$. The statement follows from two remarks. Firstly, since all prime divisors of b are $\equiv 1 \mod 3$, b must be odd. Secondly, since $b = a^2 - q$, if q is even then we must have a^2 (and thus a) odd, while if q is odd we must have a^2 (and thus a) even. Therefore, an easy calculation shows that if q is even then $f(t) \equiv t^2(t^2 + t + 1) \mod 2$, and that if q is odd then $f(t) \equiv (t^2 + t + 1)^2 \mod 2$. □

[1]The authors of [17] call the neither ordinary nor supersingular case "mixed".

2. Abelian surfaces containing genus 3 curves

The key question of the paper is characterising abelian surfaces which do not contain genus 3 curves. Our main focus will be to characterise such surfaces among those with Weil polynomial in $\mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}} \sqcup \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}} \sqcup \{(t^2-2)^2, (t^2-3)^2\}$, which we know by Theorem 1.2 do not contain curves of geometric (hence arithmetic) genus up to 2.

We start by analysing the two cases of $(t^2-2)^2$ and $(t^2-3)^2$ in Proposition 2.1. Then, in Theorem 2.3, we prove a criterion to check when a simple abelian surface contains a genus 3 curve. This criterion will be applied in the following sections to characterise which isogeny classes with Weil polynomial in $\mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}} \sqcup \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$ contain an abelian surface containing a curve of genus 3.

Proposition 2.1. *Let $\mathcal{C}$ (resp. $\mathcal{C}'$) be be the isogeny class determined by $(t^2-2)^2$ (resp. $(t^2-3)^2$). Then*

- *no abelian surface in $\mathcal{C}$ contains an absolutely irreducible curve of geometric (and thus arithmetic) genus 3.*
- *there exists an abelian surface in $\mathcal{C}'$ containing an absolutely irreducible smooth curve of genus 3.*

Proof. If an abelian surface A in $\mathcal{C}$ contains an absolutely irreducible curve C of geometric genus 3, then A is an isogeny factor of the Jacobian $\mathrm{Jac}(\tilde{C})$ of the normalisation $\tilde{C}$ of C by [9, Prop. 2][2]. Hence, the Weil polynomial of $\mathrm{Jac}(\tilde{C})$ must be of the form $(t^2-2)^2 f_E(t)$, where $f_E(t)$ is the Weil polynomial of an elliptic curve over $\mathbb{F}_2$.

Note that there are only 5 distinct isogeny classes of elliptic curves over $\mathbb{F}_2$. A search in the database of isogeny classes abelian threefolds defined over $\mathbb{F}_2$ in the LMFDB [16] returns the isogeny classes 3.2.ac_ac_i, 3.2.ab_ac_e, 3.2.a_ac_a, 3.2.b_ac_ae and 3.2.c_ac_ai. None of them contains a Jacobian, which implies that A does not contain an absolutely irreducible curve of geometric genus 3. Hence, A does not contain an absolutely irreducible curve of arithmetic genus 3, as well.

We now apply the same reasoning to $\mathcal{C}'$. By searching in the LMFDB, we find 7 isogeny classes of the form $(t^2-3)^2 f_{E'}(t)$ for some elliptic curve $E'/\mathbb{F}_3$. Moreover, 6 of these 7 isogeny classes do not contain a Jacobian. See 3.3.ad_ad_s, 3.3.ac_ad_m, 3.3.ab_ad_g, 3.3.b_ad_ag, 3.3.c_ad_am and 3.3.d_ad_as. The remaining one has label 3.3.a_ad_a and Weil polynomial $(t^2-3)^2(t^2+3)$. It contains only one Jacobian surface, of the curve $C: y^4 + xz^3 + 2x^3z$. The degree 2 map sending $(x:y:z) \mapsto (x:-y:z)$ defines a double cover of C over the elliptic curve $F\colon y^2z + 2x^3 + xz^2$. Hence, C is bielliptic. So, by [5, Prop. 1.8], C is contained in an abelian surface in $\mathcal{C}'$. □

Lemma 2.2. *Let A be a simple abelian surface defined over $\mathbb{F}_q$. Let D be an effective divisor on A such that $D^2 = 4$ Then, D is an $\mathbb{F}_q$-irreducible curve of arithmetic genus 3. More precisely, D is one of the following:*

- *an absolutely irreducible smooth curve of genus 3;*
- *an absolutely irreducible curve of geometric genus 2 with a double point;*
- *an $\mathbb{F}_q$-irreducible curve of arithmetic genus 3 which is not absolutely irreducible.*

Proof. By the adjunction formula, for an $\mathbb{F}_q$-irreducible curve C over A we have $C^2 = 2p_a - 2$. Thus, the above divisors clearly have self-intersection equal to 4. Hence, we only need to prove

[2]The author requires the curve to have a rational point on the smooth curve to guarantee the existence of an embedding into its Jacobian. However, the existence of a divisor of degree 1 is sufficient. A curve defined over a finite field always admits such a divisor.

that the list is complete. If D is a single curve then it necessarily has arithmetic genus 3. If $D = E + F$ is reducible, since it is effective, its components have genus strictly lower than 3. Since A is simple, the components of D cannot be elliptic curves. Hence they necessarily have arithmetic genus 2. Then, we get $D^2 = E^2 + F^2 + 2 \cdot E.F > 4$ as $E^2 = F^2 = 2$ and $E.F > 0$ by [5, Lemma 1.1]. □

Theorem 2.3. *Let A be a simple abelian surface defined over $\mathbb{F}_q$. Then, the following statements are equivalent:*

(1) A has a polarisation of degree 4,
(2) A contains an $\mathbb{F}_q$-irreducible curve of arithmetic genus 3.

Proof. We start by proving (1) ⇒ (2). Since $\mathbb{F}_q$ is finite, the existence of a polarisation guarantees the existence of an ample invertible sheaf $\mathcal{L} \in \mathrm{Pic}(A)$ such that the polarisation is given by $\lambda_{\mathcal{L}}$ [19, Remark 13.2]. From [20, p. 150] we know that, writing $\mathcal{L} = \mathcal{L}(D)$, we have $\deg \lambda_{\mathcal{L}} = \chi(D)^2 = ((D^2)/2)^2$. It follows that there exists an effective divisor D on A such that $D^2 = 4$. By Lemma 2.2 we conclude.

To prove (2) ⇒ (1), let C be an $\mathbb{F}_q$-irreducible curve of arithmetic genus 3 lying over A. Note that by the adjunction formula $C^2 = 2 \cdot 3 - 2 = 4$. By [5, Lemma 1.1] C intersects any other $\mathbb{F}_q$-irreducible curve on A positively. Hence, by the Nakai–Moishezon criterion [10, Sec. 5, Thm. 1.10], C is an ample divisor. Therefore, C defines a polarisation of degree 4 on A. □

Remark 2.4. If A does not contain an absolutely irreducible curve of geometric genus 2, then from Lemma 2.2 we entail that the genus 3 curve in the statement of Theorem 2.3 is either an absolutely irreducible smooth curve of genus 3 or an $\mathbb{F}_q$-irreducible curve of arithmetic genus 3 which is not absolutely irreducible.

Having this characterisation at hand, our new goal is to study when an isogeny class contains an abelian surface admitting a polarisation of degree 4. This question will be answered in Section 4. In light of Proposition 2.1, from now on we will focus on Weil polynomials $f(t) \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}} \sqcup \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$ only. To start with, we need some technical results concerning the factorisation of 2 in the extension $K = \mathbb{Q}[t]/f(t)$, which is the main topic of the next section.

3. Factorisation of 2

Let $f(t)$ be a polynomial from $\mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}} \sqcup \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$. For the rest of the paper, we set $K = \mathbb{Q}[t]/f(t)$. Then K is a CM-field, that is, a totally imaginary quadratic extension of a totally real field K^+. Concretely, if we denote by π the class of t in K, then $K^+ = \mathbb{Q}(\pi + q/\pi)$. Moreover, if we write

$$f(t) = t^4 + at^3 + bt^2 + aqt + q^2$$

then the minimal polynomial of $\pi + q/\pi$ is

$$f^+(t) = t^2 + at + (b - 2q).$$

We will denote by $\mathcal{O}$ (resp. $\mathcal{O}^+$) the ring of integers of K (resp. K^+).

In this section, we study the factorisation of 2 in K^+ and K. We shall use these technical results in the following sections to study when an isogeny class contains an abelian surface admitting a polarisation of degree 4.

Lemma 3.1. *Assume that $f(t) \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$. Then 2 ramifies in K^+.*

Proof. Since $f(t) \in \mathcal{P}^{\text{irr}}_{\text{Wres}}$ then $a = 0$. Hence, $\Delta_{f^+} = 4(2q - b)$. Let d be a positive squarefree integer such that $2q - b = c^2 d$ with $c \in \mathbb{Z}$. Note that if c is odd then $2q - b \equiv d \bmod 4$. Recall that 2 ramifies in $K^+ = \mathbb{Q}(\sqrt{d})$ if and only if $d = 1$ or $d \equiv 2, 3 \bmod 4$. We now analyse all the possible cases, which are described in Theorem 1.2.(3b).

- If $b = 1 - 2q$ then $2q - b = 4q - 1$. So c is odd. Hence $d \equiv 3 \bmod 4$.
- If $b = 2 - 2q$ then $2q - b = 4q - 2$. So c is odd. Hence $d \equiv 2 \bmod 4$.
- If $b = -q$ and q is a square then $d = 3$.
- If $b = -q$, $p = 2$ and q is not a square then $d = 6 \equiv 2 \bmod 4$.

□

Lemma 3.2. *Assume that $f(t) \in \mathcal{P}^{\text{irr}}_{\text{Wres}}$. Let $\mathfrak{m}$ be the unique maximal ideal of $\mathcal{O}^+$ above 2 (cf. Lemma 3.1). Then the following are equivalent:*

(i) K/K^+ is ramified.
(ii) $\mathfrak{m}$ is the unique maximal ideal of $\mathcal{O}^+$ that ramifies in K.
(iii) 2 is totally ramified in K.
(iv) $b = 2 - 2q$ with q odd.

In particular, if any of the above equivalent conditions holds then $f(t)$ is ordinary.

Proof. Clearly, (ii) ⇒ (i) and (iii) ⇒ (i). Before proving the remaining implications, we pause to prove a general claim. Set $N := N_{K^+/\mathbb{Q}}(\Delta_{K/K^+})$. We have

$$\begin{aligned} \Delta_f &= 16q^2(4q^2 - b^2)^2 = [\mathcal{O} : \mathbb{Z}[\pi]]^2 \Delta_K = [\mathcal{O} : R]^2 q^2 \Delta_K, \\ \Delta_{f^+} &= 4(2q - b) = [\mathcal{O}^+ : R^+]^2 \Delta_{K^+}, \text{ and} \\ \Delta_K &= \Delta_{K^+}^2 N. \end{aligned}$$

Combining these relations, we obtain

$$N \cdot \left(\frac{[\mathcal{O} : R]}{[\mathcal{O}^+ : R^+]^2} \right)^2 = (2q + b)^2.$$

Note that $R = R^+[\pi]$ (resp. $\mathcal{O}^+[\pi]$) is locally free of rank 2 over R^+ (resp. $\mathcal{O}^+$). Hence $[\mathcal{O}^+ : R^+]^2 = [\mathcal{O}^+[\pi] : R]$ divides $[\mathcal{O} : R]$. Therefore,

$$N \text{ divides } (2q + b)^2. \tag{1}$$

Now, we show that (i) ⇒ (iv) and (i) ⇒(ii). So we assume that $N \neq 1$.

Assume first that f is non-ordinary. Then $f(t) = t^4 - qt^2 + q^2$ by Theorem 1.2 and Lemma 1.9. Note that $\zeta_3 \mapsto -\pi^2/q$ gives an embedding of $\mathbb{Q}(\zeta_3)$ in K (cf. [14, Sec. 4]). Moreover, as we have shown in the proof of Lemma 3.1, we have that $K^+ = \mathbb{Q}(\sqrt{3})$ or $K^+ = \mathbb{Q}(\sqrt{6})$. In the first case, we have $K = \mathbb{Q}(\zeta_3, \sqrt{3})$ and one computes that $\Delta_{K^+} = 12$ and $\Delta_K = 12^2$. In the second case, we have $K = \mathbb{Q}(\zeta_3, \sqrt{6})$ and one computes that $\Delta_{K^+} = 24$ and $\Delta_K = 24^2$. In both cases K/K^+ is unramified.

Hence, $f(t)$ must be ordinary. Then, by Lemma 1.9, either $b = 1 - 2q$ or, $b = 2 - 2q$ and q is odd. In the first case, Equation (1) implies that $N = 1$, which cannot happen by assumption. So we must be in the second case, that is, (iv) holds. Equation (1) implies that if $b = 2 - 2q$ (with q odd) then $N \in \{1, 2, 4\}$, and in fact $N \in \{2, 4\}$ since we are assuming that K/K^+ is ramified. Since $\mathfrak{m}$ is the unique maximal ideal of $\mathcal{O}^+$ above 2 by Lemma 3.1, we obtain that $\mathfrak{m}$ ramifies in K, that is, (ii) holds.

To conclude, we prove that (iv) ⇒ (iii). Since $b = 2 - 2q$ with q odd, we have that $f(t) \equiv (t + 1)^4 \bmod 2$. By the Kummer-Dedekind theorem [24, Thm. 8.2], the order $\mathbb{Z}[\pi]$ in K has a unique maximal ideal above 2 which is regular since the remainder of the division of

$f(t)$ by $t+1$ is $(q-1)^2+2 \equiv 2 \bmod 2^2$, because q is odd. This implies that $\mathcal{O}$ has a unique maximal ideal above 2 with residue field $\mathbb{F}_2$, that is, 2 is totally ramified in K. □

Lemma 3.3. *Let $f(t) \in \mathcal{P}^{\text{irr}}_{\text{npp}} \sqcup \mathcal{P}^{\text{irr}}_{\text{Wres}}$. If K/K^+ is ramified, or if K/K^+ is unramified and there exists a maximal ideal of $\mathcal{O}^+$ that divides $(\pi - q/\pi)$ which stays inert in K, then $f \in \mathcal{P}^{\text{irr}}_{\text{Wres}}$. Moreover, in the latter case, $f(t)$ is non-ordinary.*

Proof. If K/K^+ is ramified or if there exists a prime in K^+ that divides $(\pi - q/\pi)$ and which stays inert in K, then, by [13, Thm. 1.1], there is a principally polarised abelian surface in the isogeny class associated to $f(t)$. Hence $f \in \mathcal{P}^{\text{irr}}_{\text{Wres}}$ by Theorem 1.2.

To show the last statement, assume that K/K^+ is unramified and that there exists a maximal ideal $\mathfrak{n}$ of $\mathcal{O}^+$ dividing $(\pi - q/\pi)$ which stays inert in $\mathcal{O}$. Write $f(t) = t^4 + bt^2 + q^2$, as usual. Since the minimal polynomial of $\pi + q/\pi$ is $f^+(t) = t^2 + b - 2q$, we have that $(\pi + q/\pi)^2 + b - 2q = 0$, which combined with $(\pi - q/\pi)^2 = \pi^2 + (q/\pi)^2 - 2q$ gives

$$(\pi - q/\pi)^2 = -b - 2q.$$

Assume by contradiction that $f(t)$ is ordinary. Then, by Lemma 1.9, either $b = 1 - 2q$, or $b = 2 - 2q$ with q odd. If $b = 1 - 2q$ then $(\pi - q/\pi)^2 = -1$ which implies that $1 \in \mathfrak{n}^2\mathcal{O}$. This is not possible since $\mathfrak{n}\mathcal{O}$ is a maximal ideal of $\mathcal{O}$ by assumption. If $b = 2 - 2q$ with q odd, then $2 \in \mathfrak{n}^2\mathcal{O}$. By Lemma 3.1, it follows that $\mathfrak{n}$ is the unique maximal ideal of $\mathcal{O}^+$ above 2. By Lemma 3.2, $\mathfrak{n}$ is ramified in K, leading to a contradiction also in this case. Therefore $f(t)$ is non-ordinary. □

Lemma 3.4. *Assume that $f(t) \in \mathcal{P}^{\text{irr}}_{\text{npp}}$. Then K contains $M = \mathbb{Q}(\zeta_3)$.*

Proof. If $f(t)$ is ordinary then [12, proof of Lemma 12.2] shows that K contains $M = \mathbb{Q}(\zeta_3)$. If $f(t)$ is not ordinary, then [14, Thm. 2] tells us that

$$f(t) = t^4 - qt^2 + q^2.$$

Then $\zeta_3 \mapsto -\pi^2/q$ gives an embedding of M in K (cf. [14, Sec. 4]). □

Proposition 3.5. *Let $f(t) \in \mathcal{P}^{\text{irr}}_{\text{npp}} \sqcup \mathcal{P}^{\text{irr}}_{\text{Wres}}$. The possible factorisations of 2 in K are as follows and all of them do occur.*

(i) if $f(t) \in \mathcal{P}^{\text{irr}}_{\text{npp}}$ then
- *if 2 is inert in K^+ then $2\mathcal{O} = \mathfrak{M}_1\mathfrak{M}_2$ with $\mathcal{O}/\mathfrak{M}_1 \simeq \mathcal{O}/\mathfrak{M}_2 \simeq \mathbb{F}_4$ and $\mathfrak{M}_1 = \overline{\mathfrak{M}}_2$;*
- *if 2 is split in K^+ then $2\mathcal{O} = \mathfrak{M}_1\mathfrak{M}_2$ with $\mathcal{O}/\mathfrak{M}_1 \simeq \mathcal{O}/\mathfrak{M}_2 \simeq \mathbb{F}_4$ and $\mathfrak{M}_1 = \overline{\mathfrak{M}}_1$ and $\mathfrak{M}_2 = \overline{\mathfrak{M}}_2$;*
- *if 2 is ramified in K^+ then $2\mathcal{O} = \mathfrak{M}^2$ with $\mathcal{O}/\mathfrak{M} \simeq \mathbb{F}_4$ and $\mathfrak{M} = \overline{\mathfrak{M}}$;*

(ii) if $f(t) \in \mathcal{P}^{\text{irr}}_{\text{Wres}}$ then there is a unique maximal ideal $\mathfrak{m}$ of $\mathcal{O}^+$ above 2 which can either ramify, split or stay inert in K.

Proof. By Lemma 1.11, 2 is not inert in K. We now show that 2 cannot be totally split in K. If $f(t) \in \mathcal{P}^{\text{irr}}_{\text{Wres}}$ then 2 ramifies in K^+ by Lemma 3.1 and we are done. Assume then that $f(t) \in \mathcal{P}^{\text{irr}}_{\text{npp}}$. Then, by Lemma 3.4, K contains $M = \mathbb{Q}(\zeta_3)$. Note that 2 is inert in M, so 2 is not totally split in K.

Since K is Galois by Proposition 1.10, then the possible factorisations are $2\mathcal{O} = \mathfrak{M}^4$, $2\mathcal{O} = \mathfrak{M}_1^2\mathfrak{M}_2^2$, $2\mathcal{O} = \mathfrak{M}_1\mathfrak{M}_2$ and $2\mathcal{O} = \mathfrak{M}^2$.

We start by proving (i). So, assume that $f(t) \in \mathcal{P}^{\text{irr}}_{\text{npp}}$. Then $M = \mathbb{Q}(\zeta_3)$ is a subfield of K by Lemma 3.4. Since 2 is inert in M then 2 cannot be totally ramified in K. Also, K/K^+ is unramified by Lemma 3.3. If 2 is inert in K^+ then we must have $2\mathcal{O} = \mathfrak{M}_1\mathfrak{M}_2$, with $\mathfrak{M}_1 = \bar{\mathfrak{M}}_2$. If 2 splits in K^+ then $2\mathcal{O} = \mathfrak{m}_1\mathfrak{m}_2$, that is each maximal ideal of O^+ above 2 stays inert in

K. In particular, $\mathfrak{M}_1 = \overline{\mathfrak{M}}_1$ and $\mathfrak{M}_2 = \overline{\mathfrak{M}}_2$. If 2 is ramified in K^+ then $2\mathcal{O} = \mathfrak{M}^2$ must occur and $\mathfrak{M}$ is stable under conjugation. Part (ii) is Lemma 3.1. A search on the Weil polynomials shows that all listed factorisation occur; see Example 6.4. □

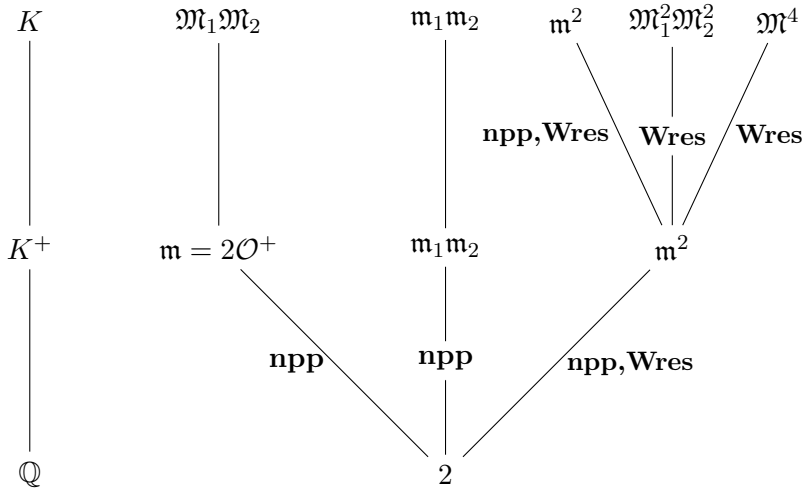

FIGURE 1. Possible factorisations of the prime 2 in $K/K^+/\mathbb{Q}$.

4. Kernels of polarisations of abelian varieties

In [12, 13], Howe studied when an isogeny class of abelian varieties contains at least one variety with a polarisation with prescribed kernel by means of Grothendieck groups of finite modules over orders associated to the isogeny class. In this section, everything is recalled from [13], but Theorem 4.5, Lemmas 4.6 and 4.7 which are novel, to the best of our knowledge.

Fix an irreducible Weil polynomial $f(t)$ determining an isogeny class $\mathcal{C}$ of abelian varieties over $\mathbb{F}_q$. We stress that in this section we do not make assumptions on the dimension. We set, as usual, $K = \mathbb{Q}[x]/f(t) = \mathbb{Q}(\pi)$ and $K^+ = \mathbb{Q}(\pi + q/\pi)$. Let $R = \mathbb{Z}[\pi, q/\pi] \subset K$ and $R^+ = \mathbb{Z}[\pi + q/\pi] \subset K^+$. In what follows, S will denote a generic order in K, possibly satisfying additional hypothesis. Denote by Mod_S the category of finite length S-modules. Since S is an order, it follows that an S-module M has finite length if and only if M is a finite set. We denote by $|M|$ the number of elements of M.

Let $G(\mathrm{Mod}_S)$ be the Grothendieck group of Mod_S which is defined as the quotient of the free abelian group on the isomorphism classes of objects in Mod_S by the subgroup generated by the expressions $M - M' - M''$ for all exact sequences $0 \to M' \to M \to M'' \to 0$ in Mod_S. For $M \in \mathrm{Mod}_S$, we denote its class in $G(\mathrm{Mod}_S)$ by $[M]_S$. The association $M \mapsto |M|$ induces a group homomorphism $G(\mathrm{Mod}_S) \to \mathbb{Q}^*$. Note that $G(\mathrm{Mod}_S)$ is a free abelian group on the simple objects of Mod_S. Every such simple object is S-linearly isomorphic to $S/\mathfrak{N}$ for a maximal S-ideal $\mathfrak{N}$. An element of $G(\mathrm{Mod}_S)$ is called *effective* if it is a sum of positive multiples of simple objects. Let $\alpha = a/b$ be an element of $K^\times$. The *principal element* generated by α is the element $\mathrm{Pr}_S(\alpha) = [S/aS]_S - [S/bS]_R$ of $G(\mathrm{Mod}_S)$. Note that Pr_S induces a group homomorphism from $K^\times$ to $G(\mathrm{Mod}_S)$.

Assume now that the order S satisfies $S = \overline{S}$. For $M \in \mathrm{Mod}_S$, define $\widehat{M} = \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ where the S-module structure is defined by $(r\psi)(m) = \psi(\overline{r}m)$ for every $\psi \in \widehat{M}$, $r \in S$ and

$m \in M$. The association $M \mapsto \widehat{M}$ induces a duality on Mod_S, which defines an involution $\bar{\cdot}$ on $G(\mathrm{Mod}_S)$ by setting $\overline{[M]}_S = [\widehat{M}]_S$. An element P of $G(\mathrm{Mod}_S)$ is *symmetric* if $P = \overline{P}$.

Lemma 4.1. *Let S be an order in K such that $S = \overline{S}$. Let $\mathfrak{M}$ a maximal ideal of S and $I \subseteq S$ be a fractional S-ideal. Then*

$$\overline{[S/\mathfrak{M}]}_S = [S/\overline{\mathfrak{M}}]_S$$

and

$$\overline{[S/I]}_S = [S/\bar{I}]_S.$$

Proof. Observe that $\overline{[S/\mathfrak{M}]}_S = [S/\overline{\mathfrak{M}}]_S$ if and only if there is an S-linear isomorphism

$$\widehat{S/\mathfrak{M}} \simeq S/\overline{\mathfrak{M}}.$$

Let $\psi : S/\mathfrak{M} \to \mathbb{Q}/\mathbb{Z}$ be a non-zero additive homomorphism. Consider the S-linear morphism $f : S \to \widehat{S/\mathfrak{M}}$ defined by $f(1) = \psi$. Note that $\overline{\mathfrak{M}} \subseteq \ker(f)$. Since $\mathfrak{M}$ is maximal and f is non-zero, we get that $\overline{\mathfrak{M}} = \ker(f)$. By Pontrjagin duality, we have that

$$|\widehat{S/\mathfrak{M}}| = |S/\overline{\mathfrak{M}}|.$$

Hence the injective S-linear morphism $S/\overline{\mathfrak{M}} \hookrightarrow \widehat{S/\mathfrak{M}}$ induced by f is an isomorphism.

For the second equality in the statement, write

$$[S/I]_S = \sum_{i=1}^{n} n_i [S/\mathfrak{M}_i]_S,$$

where the $\mathfrak{M}_i$'s are the maximal ideals of S containing I, and n_i is the length of $(S/I)_{\mathfrak{M}_i}$ as an $S_{\mathfrak{M}_i}$-module. Then

$$\overline{[S/I]}_S = \sum_{i=1}^{n} n_i \overline{[S/\mathfrak{M}_i]}_R = \sum_{i=1}^{n} n_i [S/\overline{\mathfrak{M}}_i]_S = [S/\bar{I}]_S,$$

where the central equality holds by the first part. □

Again, let S be an order in K such that $S = \overline{S}$. Set $S^+ = S \cap K^+$. By considering finite the S-modules as finite S^+-modules, we obtain the *norm* homomorphism $N_{S/S^+}([M]_S) = [M]_{S^+}$ from $G(\mathrm{Mod}_S)$ to $G(\mathrm{Mod}_{S^+})$. Define $Z(S)$ as the set of symmetric elements of

$$\ker\left(G(\mathrm{Mod}_S) \overset{N_{S/S^+} \otimes \frac{\mathbb{Z}}{2\mathbb{Z}}}{\longrightarrow} G(\mathrm{Mod}_{S^+}) \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{2\mathbb{Z}} \right).$$

Let $B(S)$ be the subgroup $\{P + \overline{P} : P \in G(\mathrm{Mod}_S)\}$ of $Z(S)$. Finally, set

$$\mathcal{B}(S) := \frac{Z(S)}{(B(S) \cdot \mathrm{Pr}_S(K^\dagger))},$$

where $K^\dagger$ is the groups of squares of totally positive elements of K^+.

Let $\mathrm{Ker}_{\mathcal{C}}$ be the category whose objects are finite commutative group schemes that can be embedded as closed subgroup-schemes in some abelian variety in the isogeny class $\mathcal{C}$. Every object of $\mathrm{Ker}_{\mathcal{C}}$ is of the form $\ker(\varphi)$ for some isogeny $\varphi : A \to B$, where A and B are elements in $\mathcal{C}$.

Definition 4.2. A finite group scheme G is *attainable* in $\mathcal{C}$ if there is a variety in $\mathcal{C}$ with a polarisation whose kernel is isomorphic to G.

Let $G(\mathrm{Ker}_{\mathcal{C}})$ be the associated Grothendieck group, which is defined analogously to the one of an order. For an element G in $\mathrm{Ker}_{\mathcal{C}}$ we denote its class in $G(\mathrm{Ker}_{\mathcal{C}})$ by $[G]_{\mathcal{C}}$. Moreover, we denote by $\widehat{G}$ its Cartier dual.

The category $\mathrm{Ker}_{\mathcal{C}}$ splits into a product of four subcategories $\mathcal{K}_{rr}$, $\mathcal{K}_{rl}$, $\mathcal{K}_{lr}$ and $\mathcal{K}_{ll}$, whose objects are respectively reduced elements of $\mathrm{Ker}_{\mathcal{C}}$ with reduced Cartier dual, reduced elements of $\mathrm{Ker}_{\mathcal{C}}$ with local Cartier dual, local elements of $\mathrm{Ker}_{\mathcal{C}}$ with reduced Cartier dual, and local elements of $\mathrm{Ker}_{\mathcal{C}}$ with local Cartier dual. For an isogeny $\varphi : A \to B$, the set of geometric points $G(\overline{\mathbb{F}_q})$ of $G = \ker\varphi$ admits a natural R-module structure by identifying π with the Frobenius of A. If $\mathcal{K}_{ll}$ is non-empty then it contains a unique simple element α_p. This occurs if and only if $\mathcal{C}$ is non-ordinary.

A crucial point of [13] is that $G(\mathrm{Ker}_{\mathcal{C}})$ and $G(\mathrm{Mod}_R)$ are isomorphic, as we now recall. Consider the association given by the following rules:

- for G in $\mathcal{K}_{rr} \times \mathcal{K}_{rl}$, set $\epsilon([G]_{\mathcal{C}}) = [G(\overline{\mathbb{F}_q})]_R$,
- for G in $\mathcal{K}_{lr}$, set $\epsilon([G]_{\mathcal{C}}) = [\widehat{G}(\overline{\mathbb{F}_q})]_R$,
- set $\epsilon([\alpha_p]_{\mathcal{C}}) = [M]_R$ where $M = \mathbb{Z}/p\mathbb{Z}$ with the R-module structure induced by letting π and q/π act as 0.

By extending ϵ by linearity to $G(\mathrm{Ker}_{\mathcal{C}})$, we obtain a group homomorphism $\epsilon : G(\mathrm{Ker}_{\mathcal{C}}) \to G(\mathrm{Mod}_R)$.

Theorem 4.3 ([13, Thm. 3.5])**.** *The group homomorphism $\epsilon : G(\mathrm{Ker}_{\mathcal{C}}) \to G(\mathrm{Mod}_R)$ is an isomorphism.*

Definition 4.4. A finite R-module M is *attainable* if $\epsilon([G]_{\mathcal{C}}) = [M]_R$ for some attainable G in $\mathcal{C}$.

By the very construction of ϵ, we can deduce the following result.

Theorem 4.5. *Let $\varphi : A \to B$ be an isogeny between elements of $\mathcal{C}$. Let M be a finite R-module such that $\epsilon([\ker\phi]_{\mathcal{C}}) = [M]_R$. Then*

$$\deg(\varphi) = |M|.$$

Proof. Set $G = \ker\varphi$, so that $\deg(\varphi)$ equals the rank $\mathrm{rk}(G)$ of G as a group scheme. There exist a non-negative integer n and a group scheme $G' \in \mathcal{K}_{rr} \times \mathcal{K}_{rl} \times \mathcal{K}_{lr}$ such that

$$[G]_{\mathcal{C}} = [\alpha_p^n \times G']_{\mathcal{C}} = n[\alpha_p]_{\mathcal{C}} \oplus [G']_{\mathcal{C}}.$$

It follows that

$$\mathrm{rk}(G) = \mathrm{rk}(\alpha_p^n) \cdot \mathrm{rk}(G') = p^n \,\mathrm{rk}(G'). \tag{2}$$

Let M_p be $\mathbb{Z}/p\mathbb{Z}$ with the trivial R-module structure and M' be a finite R-module such that $\epsilon([G']_{\mathcal{C}}) = [M']_R$. By Theorem 4.3, we have

$$[M]_R = n[M_p]_R \oplus [M']_R.$$

Hence

$$|M| = |M_p|^n \cdot |M'| = p^n |M'|. \tag{3}$$

Since, by construction of M', we have that $\mathrm{rk}(G') = |M'|$, by combining Equations (2) and (3) it follows that $\mathrm{rk}(G) = |M|$. □

Since R is a locally free R^+-module, the association $M \mapsto M \otimes_{R^+} R$ induces a well defined homomorphism $t_{R/R^+} : G(\mathrm{Mod}_{R^+}) \to G(\mathrm{Mod}_R)$.

Lemma 4.6. *Let S be an order in K such that $S = \overline{S}$ and that S is locally free of rank 2 over $S^+ = S \cap K^+$. Then $Z(S) = t_{S/S^+}(G(\mathrm{Mod}_{S^+}))$. Moreover, if $M \in \mathrm{Mod}_S$ is such that $[M]_S \in Z(S)$ then $[M]_S = t_{S/S^+}(P')$ for some effective $P' \in G(\mathrm{Mod}_{S^+})$.*

Proof. Let P' be an element of $G(\mathrm{Mod}_{S^+})$. Write

$$P' = \sum_{\mathfrak{n}} n_{\mathfrak{n}}[S^+/\mathfrak{n}]_{S^+},$$

where $\mathfrak{n}$ runs over the maximal ideals of S^+. Then

$$t_{S/S^+}(P') = \sum_{\mathfrak{n}} n_{\mathfrak{n}}[S^+/\mathfrak{n} \otimes_{S^+} S]_S.$$

We have a natural S-linear isomorphism $S^+/\mathfrak{n} \otimes_{S^+} S \simeq S/\mathfrak{n}S$. So

$$N_{S/S^+}([S/\mathfrak{n}S]_S) = 2[S^+/\mathfrak{n}]_{S^+}$$

because S is locally free of rank 2 over S^+. Hence $N_{S/S^+}([S/\mathfrak{n}S]_S) \in 2G(\mathrm{Mod}_{S^+})$. Since $S = \overline{S}$ and $\mathfrak{n}S = \overline{\mathfrak{n}S}$, by Lemma 4.1, we get that $[S^+/\mathfrak{n} \otimes_{S^+} S]_S = [S/\mathfrak{n}S]_S$ is symmetric. This concludes the proof that

$$t_{S/S^+}(G(\mathrm{Mod}_{S^+})) \subseteq Z(S).$$

Now we prove the reverse inclusion. Let P be a symmetric element of $G(\mathrm{Mod}_S)$. Write

$$P = \sum_{\mathfrak{N}} n_{\mathfrak{N}}[S/\mathfrak{N}]_S,$$

where the sum is taken over all maximal ideals $\mathfrak{N}$ of S. Since P is symmetric we must have $n_{\mathfrak{N}} = n_{\overline{\mathfrak{N}}}$ for every maximal ideal $\mathfrak{N}$ of S. Write

$$P = \sum_{\mathfrak{N} \neq \overline{\mathfrak{N}}} n_{\mathfrak{N}} \left([S/\mathfrak{N} \oplus S/\overline{\mathfrak{N}}]_S \right) + \sum_{\mathfrak{N} = \overline{\mathfrak{N}}} n_{\mathfrak{N}} \left([S/\mathfrak{N}]_S \right).$$

Fix a maximal ideal $\mathfrak{N}$ of S and set $\mathfrak{n} = \mathfrak{N} \cap S^+ = \overline{\mathfrak{N}} \cap S^+$.

Assume first that $\mathfrak{N} \neq \overline{\mathfrak{N}}$. Then $\mathfrak{n}S \subseteq \mathfrak{N}\overline{\mathfrak{N}}$. Hence we have a surjective map

$$S/\mathfrak{n}S \twoheadrightarrow S/\mathfrak{N}\overline{\mathfrak{N}} \simeq S/\mathfrak{N} \times S/\overline{\mathfrak{N}}.$$

Since $S/\mathfrak{n}S$ is a 2-dimensional vector space over $S^+/\mathfrak{n}$, we get that $S/\mathfrak{N} \simeq S/\overline{\mathfrak{N}} \simeq S^+/\mathfrak{n}$. This means that $\mathfrak{n}S = \mathfrak{N}\overline{\mathfrak{N}}$. Therefore

$$[S/\mathfrak{N} \oplus S/\overline{\mathfrak{N}}]_S = [S/\mathfrak{N}\overline{\mathfrak{N}}]_S = [S/\mathfrak{n}S]_S = t_{S/S^+}([S^+/\mathfrak{n}]_{S^+}).$$

Now consider the case $\mathfrak{N} = \overline{\mathfrak{N}}$. Observe that the residue field extension $S^+/\mathfrak{n} \to S/\mathfrak{N}$ is of degree 1 or 2. Let $\mathcal{M}_1$ (resp. $\mathcal{M}_2$) be the set of maximal ideals $\mathfrak{N}$ of S such that $\mathfrak{N} = \overline{\mathfrak{N}}$ and the degree is 1 (resp. 2). If $\mathfrak{N} \in \mathcal{M}_2$ then $\mathfrak{N} = \mathfrak{n}S$, since $S/\mathfrak{n}S$ is has dimension 2 over $S^+/\mathfrak{n}$. Hence

$$[S/\mathfrak{N}]_S = [S/\mathfrak{n}S]_S = t_{S/S^+}([S^+/\mathfrak{n}]_{S^+}).$$

By the first part of the proof, we get that $P = \overline{P} \in Z(S)$ if and only if

$$\sum_{\mathfrak{N} \in \mathcal{M}_1} n_{\mathfrak{N}} \left([S/\mathfrak{N}]_S \right) = P - \sum_{\mathfrak{N} \neq \overline{\mathfrak{N}}} n_{\mathfrak{N}} \left([S/\mathfrak{N} \oplus S/\overline{\mathfrak{N}}]_S \right) - \sum_{\mathfrak{N} \in \mathcal{M}_2} n_{\mathfrak{N}} \left([S/\mathfrak{N}]_S \right)$$

is in $Z(S)$ as well. This happens precisely when $n_{\mathfrak{N}} N_{S/S^+}([S/\mathfrak{N}]_S)$ is in $2G(\mathrm{Mod}_{S^+})$ for every $\mathfrak{N} \in \mathcal{M}_1$, that is, when each $n_{\mathfrak{N}}$ is even, since $S/\mathfrak{N} \simeq S^+/\mathfrak{n}$ is a simple S^+-module. Since, for $\mathfrak{N} \in \mathcal{M}_1$, we have S-linear isomorphisms

$$t_{S/S^+}([S^+/\mathfrak{n}]_{S^+}) \simeq S/\mathfrak{n}S \simeq (S/\mathfrak{N})^2,$$

we conclude the proof that $Z(S) \subseteq t_{S/S^+}(G(\mathrm{Mod}_{S^+}))$ by additivity of t_{S/S^+}. □

Recall that the order $R = \mathbb{Z}[\pi, q/\pi]$ is locally free of rank 2 over $R^+ = \mathbb{Z}[\pi + q/\pi]$.

Lemma 4.7. *Let ℓ be a rational prime. The following statements are equivalent.*

(i) There exists a finite R-module M of order $|M| = \ell^2$ such that the class of M in $G(\mathrm{Mod}_R)$ is of the form $t_{R/R^+}(P')$ for some effective P' in $G(\mathrm{Mod}_{R^+})$.

(ii) There exists a finite R-module M of order $|M| = \ell^2$ such that $[M]_R$ is in $Z(R)$.

(iii) $f^+(t) \bmod \ell$ has a linear factor.

If any of the equivalent statements hold then $[M]_R = t_{R/R^+}([R^+/\mathfrak{l}]_{R^+})$ where $\mathfrak{l}$ is the unique maximal ideal of R^+ above ℓ corresponding to any linear factor of $f^+(t) \bmod \ell$.

Proof. The equivalence of (i) and (ii) is an immediate consequence of Lemma 4.6.

Let $P' \in G(\mathrm{Mod}_{R^+})$ be effective and non-zero. Then there are positive integers $n_1, \ldots, n_r$ and maximal R^+-ideals $\mathfrak{n}_1, \ldots, \mathfrak{n}_r$ such that

$$P' = \sum_{i=1}^{r} n_i [R^+/\mathfrak{n}_i].$$

Hence

$$t_{R/R^+}(P') = \sum_{i=1}^{r} n_i [R^+/\mathfrak{n}_i \otimes_{R^+} R].$$

Since R is locally free of rank 2 over R^+, we get that

$$|R^+/\mathfrak{n}_i \otimes_{R^+} R| = |R^+/\mathfrak{n}_i|^2.$$

If M is a finite R-module whose image in $G(\mathrm{Mod}_R)$ is $t_{R/R^+}(P')$ for P' as above then

$$|M| = \prod_{i=1}^{r} |R^+/\mathfrak{n}_i|^{2n_i}.$$

We now show that (i) implies (iii). So, assume also that M as above satisfies $|M| = \ell^2$ for a rational prime ℓ. Then $r = 1$, $n_1 = 1$ and $R^+/\mathfrak{n}_1 \simeq \mathbb{F}_\ell$. This implies that $f^+(t) \bmod \ell$ has a linear factor (cf. [24, Thm. 8.2]).

Finally, assume that (iii) holds. Let $\mathfrak{l}$ be the corresponding maximal ideal of R^+. Then we see that $R^+/\mathfrak{l} \otimes_{R^+} R$ is an R-module of order ℓ^2, as in (i). □

The following result completely describes $\mathcal{B}(\mathcal{O})$ for the maximal order $\mathcal{O}$ of K.

Proposition 4.8. *If K/K^+ is ramified at a finite prime then $\mathcal{B}(\mathcal{O}) = 0$. Otherwise, the Artin map induces an isomorphism $\mathcal{B}(\mathcal{O}) \simeq \mathrm{Gal}(K/K^+)$.*

Proof. This is part of [13, Prop. 6.2]. □

Define

$$H(R) = \frac{Z(R)}{B(R)}.$$

The group $H(R)$ is a vector space over $\mathbb{F}_2$ whose basis is given by the classes of the simple R-modules $R/\mathfrak{n}$ where $\mathfrak{n}$ is a maximal R-ideal such that $\mathfrak{n} = \overline{\mathfrak{n}}$ and the index $[R/\mathfrak{n} : R^+/(R^+ \cap \mathfrak{n})]$ of residue fields is even. Such maximal ideals are called the *generating primes* of $H(R)$.

The inclusion $i\colon R \to \mathcal{O}$ induces a group homomorphism $i^*\colon \mathcal{B}(\mathcal{O}) \to \mathcal{B}(R)$ by considering every finite $\mathcal{O}$-module as an R-module.

Let $\psi\colon H(R) \to \mathcal{B}(R)$ and $\chi\colon H(\mathcal{O}) \to \mathcal{B}(\mathcal{O})$ denote the canonical reductions. Note that i induces a norm map $G(\mathrm{Mod}_{\mathcal{O}}) \to G(\mathrm{Mod}_R)$ which in turn induces a norm $N\colon H(\mathcal{O}) \to H(R)$.

Proposition 4.9. *We have an exact sequence*

$$H(\mathcal{O}) \xrightarrow{(N,-\chi)} H(R) \oplus \mathcal{B}(\mathcal{O}) \xrightarrow{\psi \oplus i^*} \mathcal{B}(R) \to 0.$$

Proof. This is a special case of [13, Prop. 6.4]. □

We have the following:

Theorem 4.10 ([13, Thm. 1.3])**.** *There is an element $I_{\mathcal{C}}$ of $\mathcal{B}(R)$ such that the elements of $G(\mathrm{Mod}_R)$ that are attainable in $\mathcal{C}$ are precisely the effective elements of $Z(R)$ that map to $I_{\mathcal{C}}$ in $\mathcal{B}(R)$. In particular, the isogeny class $\mathcal{C}$ contains a principal polarisation if and only if $I_{\mathcal{C}} = 0$.*

Proposition 4.11. *The obstruction element $I_{\mathcal{C}}$ lies in $i^*(\mathcal{B}(\mathcal{O}))$.*

Proof. This is part of [13, Prop. 7.1]. □

5. Polarisations of degree 4 on abelian surfaces

In Section 2, we showed that an abelian surface with Weil polynomial $f \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}} \sqcup \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$ contains curve of arithmetic genus 3 if and only if it admits a polarisation with kernel of order 4. We now apply the results developed in Section 4 to characterise isogeny classes defined by a polynomial in $\mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}} \sqcup \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$ not containing abelian surfaces with a curve of genus 3 lying on.

In this section, we assume that $f(t) \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}} \sqcup \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$. As before, we denote the corresponding isogeny class by $\mathcal{C}$ and set $K = \mathbb{Q}[x]/f(t) = \mathbb{Q}(\pi)$ and $K^+ = \mathbb{Q}(\pi + q/\pi)$. We fix also $R = \mathbb{Z}[\pi, q/\pi] \subset K$ and $R^+ = \mathbb{Z}[\pi + q/\pi] \subset K$.

Proposition 5.1. *Let $f(t) \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}}$. Then 2 is inert in K^+ if and only if there is no attainable R-module of order 4.*

Proof. If $f^+(t) \bmod 2$ is irreducible then 2 is inert in K^+ and there is no attainable R-module of order 4 by Lemma 4.7 and Theorem 4.10. So, we assume that $f^+(t) \bmod 2$ has a linear factor for the rest of the proof. Hence, again by Lemma 4.7 and Theorem 4.10, if there is an attainable R-module M of order 4 then we must have

$$[M]_R = [R^+/\mathfrak{l} \otimes_{R^+} R]_R = [R/\mathfrak{l}R]_R,$$

where $\mathfrak{l}$ is a maximal ideal of R^+ such that $R^+/\mathfrak{l} \simeq \mathbb{F}_2$. By Lemma 3.3, K/K^+ is unramified. So, the Artin map induces an isomorphism $\mathrm{Gal}(K/K^+) \simeq \mathcal{B}(\mathcal{O})$ by Proposition 4.8. Let α be the non-zero element of $\mathcal{B}(\mathcal{O})$, which corresponds to the Artin symbol of any maximal ideal of $\mathcal{O}^+$ that stays inert in K. By Theorem 4.10 and Proposition 4.11, $I_{\mathcal{C}}$ is non-zero and in $i^*(\mathcal{B}(\mathcal{O}))$. Hence $I_{\mathcal{C}} = i^*(\alpha)$. Let $z_{\mathfrak{l}}$ be the image of $[R/\mathfrak{l}R]_R$ in $\mathcal{B}(R)$. Note that

$$z_{\mathfrak{l}} = (\Psi \oplus i^*)((x_{\mathfrak{l}}, 0)),$$

where $x_{\mathfrak{l}}$ is the image of $[R/\mathfrak{l}R]_R$ in $H(R)$. We obtain that $z_{\mathfrak{l}} - I_{\mathcal{C}} = (\Psi \oplus i^*)((x_{\mathfrak{l}}, \alpha))$. Hence there is an R-module M of order 4 which is attainable if and only if

$$(x_{\mathfrak{l}}, \alpha) \in \ker((\Psi \oplus i^*)) = (N, -\chi)(H(\mathcal{O})),$$

where the equality holds by Proposition 4.9.

Assume that 2 is inert in K^+ and write $\mathfrak{m} = 2\mathcal{O}^+$. By Proposition 3.5, we see that $\mathfrak{m}$ splits in K, say $\mathfrak{m}\mathcal{O} = \mathfrak{M}\overline{\mathfrak{M}}$. A preimage of $x_{\mathfrak{l}}$ in $H(\mathcal{O})$ via $N : H(\mathcal{O}) \to H(R)$ must be an $\mathbb{F}_2$-linear combination of the images $y_{\mathfrak{M}}$ and $y_{\overline{\mathfrak{M}}}$ of $\mathfrak{M}$ and $\overline{\mathfrak{M}}$ in $H(\mathcal{O})$. Since $\mathfrak{m}$ is split in K, then the Artin symbols of $\mathfrak{M}$ and $\overline{\mathfrak{M}}$ are trivial in $\mathrm{Gal}(K/K^+) \simeq \mathcal{B}(\mathcal{O})$. Hence any $\mathbb{F}_2$-linear combination of the images $y_{\mathfrak{M}}$ and $y_{\overline{\mathfrak{M}}}$ won't be mapped by $\chi : H(\mathcal{O}) \to \mathcal{B}(\mathcal{O})$ to α. This

means that $(x_{\mathfrak{l}}, \alpha)$ is not in $(N, -\chi)(H(\mathcal{O}))$. Hence, there is no R-module M of order 4 which is attainable.

Assume now that 2 is not inert in K^+. Let $\mathfrak{M}$ be a maximal ideal of $\mathcal{O}$ containing $\mathfrak{l}R$. Denote the image of $[\mathcal{O}/\mathfrak{M}]_{\mathcal{O}}$ in $H(\mathcal{O})$ by $y_{\mathfrak{M}}$. By Proposition 3.5, we have that $\mathfrak{M} = \mathfrak{m}\mathcal{O}$ for a maximal ideal $\mathfrak{m}$ of $\mathcal{O}^+$. This implies that $\chi(y_{\mathfrak{M}}) = \alpha$. So, to prove that $R/\mathfrak{l}R$ is attainable, we are left to show that $N(y_{\mathfrak{M}}) = x_{\mathfrak{l}}$. We first consider the case that $\mathfrak{l}R$ is a maximal ideal of R. Note that $\mathfrak{l}R = \mathfrak{M} \cap R$ and we have an isomorphism $R/\mathfrak{l}R \simeq \mathcal{O}/\mathfrak{M}$. Hence $N(y_{\mathfrak{M}}) = x_{\mathfrak{l}}$. Therefore, $R/\mathfrak{l}R$ is attainable. Now we consider the case when $\mathfrak{l}R$ is not a maximal ideal of R. Set $\mathfrak{L} = \mathfrak{M} \cap R$. The natural surjective map $R/\mathfrak{l}R \twoheadrightarrow R/\mathfrak{L}$ is not an isomorphism. Since $\mathfrak{L} = \overline{\mathfrak{L}}$ and $[R/\mathfrak{l}R]_R \in Z(R)$ we get that

$$[R/\mathfrak{l}R]_R = 2[R/\mathfrak{L}]_R.$$

Moreover, also $[\mathcal{O}/\mathfrak{M}]_R = 2[R/\mathfrak{L}]_R$. Hence, again, $N(y_{\mathfrak{M}}) = x_{\mathfrak{l}}$. Therefore, as before, $R/\mathfrak{l}R$ is attainable. □

Proposition 5.2. *Assume that $f(t) \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$. Write $2\mathcal{O}^+ = \mathfrak{m}^2$ and let $\mathfrak{l} = \mathfrak{m} \cap R^+$ be the unique maximal ideal of R^+ above 2. Then there is an R-module M of order 4 which is attainable if and only if $\mathfrak{l}R$ is not a maximal ideal of R.*

Proof. Observe that $f(t) \bmod 2$ is a square of a linear factor. Let $\mathfrak{l}$ be the corresponding maximal ideal of R^+. By Lemma 4.7 and Theorem 4.10, if there is an attainable R-module M of order 4 then we must have

$$[M]_R = [R^+/\mathfrak{l} \otimes_{R^+} R]_R = [R/\mathfrak{l}R]_R.$$

Since $f(t) \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$, the obstruction element $I_{\mathcal{C}}$ is trivial by Theorem 4.10. Hence, there is an R-module M of order 4 which is attainable if and only if the image $z_{\mathfrak{l}}$ of $[R/\mathfrak{l}R]_R$ in $\mathcal{B}(R)$ is trivial. Note that

$$z_{\mathfrak{l}} = (\Psi \oplus i^*)((x_{\mathfrak{l}}, 0)),$$

where $x_{\mathfrak{l}}$ is the image of $[R/\mathfrak{l}R]_R$ in $H(R)$. Also, the R-module $R/\mathfrak{l}R$ has length at most 2 and that it has length 1 if and only if $\mathfrak{l}R$ is a maximal ideal of R.

If the length of $R/\mathfrak{l}R$ is 2 then $[R/\mathfrak{l}R]_R = [R/\mathfrak{n}]_R + [R/\overline{\mathfrak{n}}]_R$ for a maximal ideal $\mathfrak{n}$ of R, with possibly $\mathfrak{n} = \overline{\mathfrak{n}}$, and so, by Lemma 4.1, $[R/\mathfrak{l}R]_R$ is in $B(R)$. Hence, $x_{\mathfrak{l}}$ is trivial in $H(R)$ and so $z_{\mathfrak{l}} = I_{\mathcal{C}}$ in $\mathcal{B}(R)$. This means that $R/\mathfrak{l}R$ is an attainable R-module of order 4.

To conclude the proof, we need to show that if the length of $R/\mathfrak{l}R$ is 1, that is, $\mathfrak{l}R$ is a maximal R-ideal, then $(x_{\mathfrak{l}}, 0)$ is not in

$$\ker((\Psi \oplus i^*)) = (N, -\chi)(H(\mathcal{O})),$$

where the equality holds by Proposition 4.9. So, assume that $\mathfrak{l}R$ is a maximal ideal of R. Let $\mathfrak{M}$ be a maximal ideal of $\mathcal{O}$ above $\mathfrak{l}R$. Since we have an inclusion of residue field $R/\mathfrak{l}R \to \mathcal{O}/\mathfrak{M}$ and 2 is not inert in $\mathcal{O}$ by Proposition 3.5, then

$$R/\mathfrak{l}R \simeq \mathcal{O}/\mathfrak{M} \simeq \mathbb{F}_4.$$

This implies that $[\mathcal{O}/\mathfrak{M}]_R = [R/\mathfrak{l}R]_R$. If we denote the image of $[\mathcal{O}/\mathfrak{M}]_{\mathcal{O}}$ in $H(\mathcal{O})$ by $y_{\mathfrak{M}}$, we get $N(y_{\mathfrak{M}}) = x_{\mathfrak{l}}$. By Proposition 3.5, since $\mathcal{O}/\mathfrak{M} \simeq \mathbb{F}_4$, we get that $\mathfrak{m}$ is inert in K. This means that the Artin symbol $\left(\frac{K/K^+}{\mathfrak{m}}\right)$ is a generator of $\mathrm{Gal}(K/K^+)$. We now claim that K/K^+ is unramified. If not, then by Lemma 3.1 and Lemma 3.2, we would get that there is unique maximal ideal $\mathfrak{m}$ of $\mathcal{O}^+$ above 2 which ramifies in $\mathcal{O}$, say $\mathfrak{m}\mathcal{O} = \mathfrak{M}^2$. For such $\mathfrak{M}$ we would have $\mathcal{O}/\mathfrak{M} \simeq \mathbb{F}_2$. Since we know that every maximal ideal of $\mathcal{O}$ above $\mathfrak{l}$ has residue field isomorphic to $\mathbb{F}_4$, we deduce that K/K^+ is unramified. Then, by Proposition 4.8, we get

that $\chi(y_{\mathfrak{M}}) \neq 0$ in $\mathcal{B}(\mathcal{O})$. So $(x_{\mathfrak{l}}, 0)$ is not in the image of $(N, -\chi)$ and, therefore, there is no R-module of order 4 which is attainable. □

In Theorem 5.7, we wrap-up the discussion above. Moreover, in certain cases with $\mathcal{C}$ ordinary, we show that if there is an abelian variety with polarisation with kernel of order 4 then there is an abelian variety with polarisation with kernel of order 4 and maximal endomorphism ring. To do so, we use results from [12]. The construction of $\mathcal{B}(\mathcal{O})$ in [12] is slightly different form the one in [13] that we have presented above, but certainly equivalent in view of Proposition 4.8 and [12, Prop. 10.1].

Definition 5.3. A finite R-module M is *strongly attainable* if there exists an abelian variety B in $\mathcal{C}$ such that $\mathrm{End}(B)$ is the maximal order of K with a polarisation $\varphi : B \to B^\vee$ such that $\epsilon([\ker \varphi]_{\mathcal{C}}) = [M]_R$.

Clearly strongly attainable implies attainable, while the contrary does not hold in general. A characterisation of strongly attainable R-modules is given in [12, Prop. 5.7], repeated below as Proposition 5.5 for convenience. Such characterisation relates modules with a particular element $I_{K,\Phi}$ of $\mathcal{B}(\mathcal{O})$ which depends on a choice of a CM-type Φ of K. The definition of $I_{K,\Phi}$ is given in [12, Def. 5.2]. For our purposes, it sufficient to know whether it is trivial or not in $\mathcal{B}(\mathcal{O})$.

Lemma 5.4. *If $f \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}}$ is ordinary then $I_{K,\Phi} \neq 0$. If $f \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$ is ordinary and either*

- *K/K^+ is ramified, or*
- *K/K^+ is unramified and there is no maximal ideal of $\mathcal{O}^+$ dividing $\pi - q/\pi$ which stays inert in K/K^+,*

then $I_{K,\Phi} = 0$.

Proof. Assume that $f \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}}$ is ordinary. Then $\mathcal{C}$ does not contain a principally polarised abelian variety. The result follows from [12, Prop. 11.3] and [12, Cor. 11.4].

Assume from now that $f \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$ is ordinary. If K/K^+ is ramified then the $I_{K,\Phi} = 0$ by [12, Prop. 11.1]. If K/K^+ is unramified and there is no maximal ideal of $\mathcal{O}^+$ dividing $\pi - q/\pi$ which stays inert in K/K^+ then the result follows, again, by combining [12, Prop. 11.3] and [12, Cor. 11.4] and the observation that $\mathcal{C}$ contains a principally polarised abelian variety. □

Recall that, by Proposition 4.8, we have a natural surjective homomorphism from $G(\mathrm{Mod}_{\mathcal{O}^+})$ to $\mathcal{B}(\mathcal{O})$ defined by sending a maximal ideal to its Artin symbol.

Proposition 5.5. [12, Prop. 5.7] *Let M be finite R-module. Then M is strongly attainable if and only if $M \simeq \mathcal{O}/\mathfrak{a}\mathcal{O}$ for some $\mathcal{O}^+$-ideal $\mathfrak{a} \subseteq \mathcal{O}^+$ such that the image in $\mathcal{B}(\mathcal{O})$ of the class of $\mathcal{O}^+/\mathfrak{a}$ in $G(\mathrm{Mod}_{\mathcal{O}^+})$ equals $I_{K,\Phi}$.*

Proposition 5.6. *Assume that $f(t) \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$ is ordinary. Write $2\mathcal{O}^+ = \mathfrak{m}^2$, Then either*

(a) K/K^+ is ramified and there is a strongly attainable R-module of order 4, or
(b) K/K^+ is unramified, there is no maximal ideal of $\mathcal{O}^+$ dividing $\pi - q/\pi$ which stays inert in K and, there is a strongly attainable R-module of order 4 if and only if $\mathfrak{m}$ splits in K.

Proof. Note that $M = \mathcal{O}/\mathfrak{m}\mathcal{O}$ has order 4. By Lemmas 3.2 and 3.3, either K/K^+ is ramified or, K/K^+ is unramified and there is no maximal ideal of $\mathcal{O}^+$ dividing $\pi - q/\pi$ which stays inert in K.

If K/K^+ is ramified then $\mathcal{B}(\mathcal{O}) = 0$ by Proposition 4.8. So $I_{K,\Phi}$ and the image in $\mathcal{B}(\mathcal{O})$ of the class of M in $G(\mathrm{Mod}_{\mathcal{O}^+})$ are equal. Hence M is a strongly attainable module of order 4 by Proposition 5.5. that is, we are in case (a).

Assume now that K/K^+ is unramified and there is no maximal ideal of $\mathcal{O}^+$ dividing $\pi - q/\pi$ which stays inert in K. By Lemma 5.4, we have that $I_{K,\Phi} = 0$. Since K/K^+ is unramified, the maximal ideal $\mathfrak{m}$ is either split or inert in K. Also, $\mathfrak{m}$ is split if and only if the Artin symbol of $\mathfrak{m}$ in $\mathrm{Gal}(K/K^+)$ is trivial. By Proposition 4.8, this happens precisely when the image in $\mathcal{B}(\mathcal{O})$ of the class of M in $G(\mathrm{Mod}_{\mathcal{O}^+})$ is trivial, that is, equal to $I_{K,\Phi}$. We conclude the proof of (b) by applying Proposition 5.5. □

Theorem 5.7. *Assume that* $f \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}} \sqcup \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$.

(i) The following are equivalent:
- *(a) There is no attainable R-module of order 4.*
- *(b) There is no A in $\mathcal{C}$ admitting a polarisation of degree 4.*

Moreover, if $\mathcal{C}$ is ordinary then (a) and (b) are also equivalent to:
- *(c) There is no strongly attainable R-module of order 4.*
- *(d) There is no A in $\mathcal{C}$ with maximal $\mathbb{F}_q$-endomorphism ring admitting a polarisation of degree 4.*

(ii) Assume that $f \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}}$. Then (a) and (b) are also equivalent to:
- *(e) 2 is inert in K^+.*

(iii) Assume that $f(t) \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$ and write $f(t) = t^4 + bt^2 + q^2$. Write $2\mathcal{O}^+ = \mathfrak{m}^2$ and let $\mathfrak{l} = \mathfrak{m} \cap R^+$ be the unique maximal ideal of R^+ above 2. Then (a) and (b) are also equivalent to each of the following statements:
- *(f) $\mathfrak{l}R$ is a maximal ideal of R.*
- *(g) $b = 1 - 2q$ and q is odd, if $\mathcal{C}$ is ordinary; q is even, if $\mathcal{C}$ is non-ordinary.*

Proof. The equivalences (a) $\iff$ (b) and (c) $\iff$ (d) follow from the definitions of attainable and strongly attainable module and Theorem 4.5. The implications (a)⇒(c) and (b)⇒(d) are clear. The reverse implications will be proven below distinguishing several cases.

We now show Part (ii). So, assume that $f(t) \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}}$. The equivalence (e) $\iff$ (a) is Proposition 5.1. We show that (c) implies (e) by contraposition, when $\mathcal{C}$ is ordinary. So, say that 2 is not inert in K^+. Then, by Proposition 3.5, there exists a maximal ideal $\mathfrak{l}$ of $\mathcal{O}^+$ above 2 such that $\mathfrak{l}$ stays inert in K. Hence, the Artin symbol of $\mathfrak{l}$ is not trivial in $\mathrm{Gal}(K/K^+)$. Since K/K^+ is unramified by Lemma 3.3, we get that the image in $\mathcal{B}(\mathcal{O})$ of the class of $\mathcal{O}^+/\mathfrak{l}$ in $G(\mathrm{Mod}_{\mathcal{O}^+})$ is non trivial by Proposition 4.8. Then by Lemma 5.4 and Proposition 5.5, the module $\mathcal{O}/\mathfrak{l}\mathcal{O}$, which has order 4, is strongly attainable. Therefore (c)⇒(a) and (d)⇒(b) for $f(t) \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}}$.

We now move to Part (iii). Assume now that $f \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$. The equivalence (f) $\iff$ (a) is Proposition 5.2. We deal with the ordinary and non-ordinary cases separately.

Assume first that $\mathcal{C}$ is ordinary. We now show (c)⇒(g). So, we assume that there are no strongly attainable R-modules of order 4. By Proposition 5.6, this is equivalent to have K/K^+ unramified and $\mathfrak{m}$ inert in K. By Theorem 1.2 and Lemma 1.9, we get that $b = 1 - 2q$. Hence $f(t) = t^4 + (1-2q)t^2 + q^2$. If q is even, then $f(t) \equiv t^2(t+1)^2 \bmod 2$. The Kummer-Dedekind Theorem [24, Thm. 8.2] implies that $\mathbb{Z}[\pi]$ has 2 distinct maximal ideals above 2. Hence the same holds for R. This cannot be the case since $\mathfrak{L} = R \cap \mathfrak{m}\mathcal{O}$ is the unique maximal ideal of R above 2. Hence, q is odd. This means that (g) holds. We now show that (g)⇒(f). Then $f(t) \equiv (t^2 + t + 1)^2 \bmod 2$. The Kummer–Dedekind Theorem [24, Thm. 8.2] implies that $\mathbb{Z}[\pi]$ has a unique maximal ideal above 2 with residue field of order 4. This implies that $\mathfrak{L}$ also has

residue field of order 4. Since $\mathfrak{l}R \subseteq \mathfrak{L}$ and $R/\mathfrak{l}R$ has also 4 elements, we must have $\mathfrak{l}R = \mathfrak{L}$, that is, (f) holds. We deduce also that (c)⇒(a) and (d)⇒(b) for $f(t) \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$ ordinary.

Assume now that $\mathcal{C}$ is non-ordinary. If q is even then $f(t) \equiv t^4 \bmod 2$. This means that R has a unique maximal ideal above 2, which must be $\mathfrak{L} = (2, \pi, q/\pi) \subset R$, since $R/\mathfrak{L} \simeq \mathbb{F}_2$. Since $R/\mathfrak{l}R$ has 4 elements, we obtain that $\mathfrak{l}R$ is not a maximal ideal of R. If q is odd then $f(t) \equiv (t^2 + t + 1)^2$. By the Kummer–Dedekind Theorem [24, Thm. 8.2], the order $\mathbb{Z}[\pi]$ has a unique maximal ideal above 2 which is regular and with residue field $\mathbb{F}_4$. It follows that the same hold for R. Hence $\mathfrak{l}R$ is maximal. This shows (g) ⟺ (f) and completes the proof of Part (iii). □

Remark 5.8. In the case when $f(t) \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$, we completely characterise when the equivalent conditions (a),(b) and (f) hold in terms of the coefficients of $f(t)$ in (g). It is easy to obtain a characterisation in terms of the coefficients of $f(t) = t^4 + at^3 + bt^2 + aqt + q^2$ also when $f(t) \in \mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}}$. Indeed, if we write $\Delta_{f^+} = a^2 - 4(b - 2q) = c^2 d$ for integers c and d with d squarefree, then it is well known that (e) holds if and only if $d \equiv 5 \bmod 8$. Moreover, if q is even (or equivalently a is odd) then $f^+(t) \equiv t^2 + t + 1 \bmod 2$ is irreducible, which implies that 2 is inert in K^+. Similarly, if a is even and $a + b \not\equiv 1 \bmod 4$ then $f^+(t) \equiv (t + 1)^2$ and the remainder of the division of $f^+(t)$ by $t + 1$ is not divisible by 4. Hence, 2 ramifies in K^+ by the Kummer–Dedekind Theorem [24, Thm. 8.2].

6. Computing isomorphism classes admitting a polarisation of degree 4

In [18], it is described how to compute the isomorphism classes of abelian varieties over $\mathbb{F}_q$ belonging to an ordinary isogeny class $\mathcal{C}$ determined by an irreducible Weil polynomial $f(t)$. We summarise here the results that are relevant for us; see [18, Cor. 4.4, Thm. 5.4].

Let $K = \mathbb{Q}[t]/(f(t)) = \mathbb{Q}[\pi]$ where π denotes the class of t in K and set $R = \mathbb{Z}[\pi, q/\pi]$. There is an equivalence between the category of abelian varieties in $\mathcal{C}$ (with $\mathbb{F}_q$-morphisms) and the category of fractional R-ideals in K (with R-linear morphisms). Hence, every overorder S of R occurs as the endomorphism ring of an abelian variety in $\mathcal{C}$. Moreover, the functor inducing the equivalence is compatible with duality and allows to describe polarizations as R-linear morphisms. For example, if $\mathrm{End}(A) = S$ then $\mathrm{End}(A^\vee) = \overline{S}$. In [18, Sec. 6], we use the equivalence to produce an algorithm to compute the abelian varieties in $\mathcal{C}$ together with their polarizations (of a fixed degree) up to polarized isomorphism. We will use this algorithm in the next examples.

Remark 6.1. An analogous description of polarisations exists also for simple almost-ordinary abelian varieties over any finite field $\mathbb{F}_q$ of odd characteristic; see [21]. This result does not apply to our case since none of the polynomials in $\mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}} \sqcup \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$ is almost-ordinary by Lemma 1.9. A similar description also exists for abelian varieties over prime fields whose Weil polynomial does not have repeated complex roots, but only for polarisations of degree 1; see [6].

Example 6.2. Consider the isogeny class of abelian surfaces over $\mathbb{F}_2$ with label 2.2.a_ab determined by the Weil polynomial $f(t) = t^4 - t^2 + 4$. According to the LMFDB, the class contains a Jacobian. Moreover, one computes that the order $\mathbb{Z}[\pi, 4/\pi]$ has 3 overorders S_1, S_2 and $\mathcal{O}$, where $\mathcal{O}$ is the maximal order of the number field $K = \mathbb{Q}[t]/(f(t))$. One observe that $S_2 = \overline{S}_1$. Hence, each abelian surface A with endomorphism ring S_1 cannot be isomorphic to its dual, which has endomorphism ring S_2. In particular, such an A does not admit a principally polarisation. Hence, such an A does not contain a curve of arithmetic genus 2, as explained in Remark 1.3, even if it is isogenous to a Jacobian.

Example 6.3. In Theorem 5.7, we see that, in the isogeny class $\mathcal{C}$ associated to an ordinary Weil polynomial in $\mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}} \sqcup \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$, there is an abelian variety A admitting a polarisation of degree 4 if and only if there is an abelian variety A' in $\mathcal{C}$ with maximal endomorphism ring admitting a polarisation of degree 4. This is not the case in general. For example, in the isogeny class with label 2.13.a_al determined by $t^4 - 11t^2 + 13^2$ there are abelian varieties admitting a polarisation of degree 4 but none of them has maximal endomorphism ring.

Example 6.4. Using the aforementioned algorithm, we count the number of polarisations of degree 4, for every isogeny class in $\mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}} \sqcup \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}}$ for a fixed range of q. For the full output, see https://raw.githubusercontent.com/stmar89/Genus3Data/main/table_output.txt. We remark that in the maximal endomorphism ring case, the ratio of isomorphism classes of abelian surfaces admitting a polarisation of degree 4 is always 0 or a power of 1/2.

7. Genus 3 curves lying on abelian surfaces

In this final section, we switch our attention from abelian surfaces to curves, and gather information on genus 3 curves lying on abelian surface with Weil polynomials in $\mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}} \sqcup \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}} \sqcup \{(t^2-2)^2, (t^2-3)^2\}$, that is, which is simple and not isogenous to a Jacobian, or equivalently, not containing curves of geometric genus 0,1 or 2. We fix an abelian surface A defined over $\mathbb{F}_q$ in such an isogeny class, and we suppose that there is an absolutely irreducible projective smooth genus 3 curve C defined over $\mathbb{F}_q$ that lies on A. The following lemma characterises the Jacobian of C.

Lemma 7.1. *Let q be the power of an odd prime. Let C be a genus 3 curve lying on an abelian surface A defined over $\mathbb{F}_q$. Then C is the double cover of an elliptic curve E and the Jacobian $\mathrm{Jac}(C)$ of C is isogenous to $E \times A$.*

Proof. By [5, Prop. 1.8], as C lies on A, it is bielliptic, that is, it is the double cover of an elliptic curve E. In particular, we know that the Jacobian of C is isogenous to $\mathrm{Jac}(E) \times P \simeq E \times P$, P being the Prym variety associated with the double cover. Hence, since by [5, Sec. 1.4] we know that P and A are isogenous, we deduce $\mathrm{Jac}(C) \sim E \times A$. □

We recall that absolutely irreducible genus 3 curves are either hyperelliptic curves or plane quartics. The next lemma shows that hyperelliptic genus 3 curves cannot lie on our abelian surfaces, at least if we work over finite fields of odd characteristic.

Lemma 7.2. *Let q be the power of an odd prime. Let C be a genus 3 curve lying on an abelian surface A defined over $\mathbb{F}_q$ which is simple and not isogenous to a Jacobian. Then C is not hyperelliptic.*

Proof. Suppose by contradiction that C is hyperelliptic. We mainly follow the reasoning in the introduction of [22]. By Lemma 7.1, C is also bielliptic. Then, it is of the form $y^2 = x^8 + ax^6 + bx^4 + cx^2 + 1 = f(x^2)$, with $a, b, c \in \mathbb{F}_q$. Here f is a polynomial of degree 4. In this case, the double cover is given by the involution $(x, y) \mapsto (-x, y)$ and the elliptic curve is given by $y^2 = f(x)$. Furthermore, quotienting C by the hyperelliptic involution $(x, y) \mapsto (-x, -y)$ gives the genus 2 curve $F\colon y^2 = x \cdot f(x)$. Finally, we have $\mathrm{Jac}(C) \sim E \times \mathrm{Jac}(F)$, hence $\mathrm{Jac}(F) \sim A$ by Lemma 7.1. The Jacobian of F can be simple or split in the product of two elliptic curves. In both cases, this leads to a contradiction. □

Hence, we are left with the case in which C is a bielliptic plane quartic. In this case, using results from [22], we get the following result.

Proposition 7.3. *Let q be the power of an odd prime. Let C be an absolutely irreducible smooth genus 3 curve lying on an abelian surface defined over $\mathbb{F}_q$ respecting one of the equivalent conditions of Theorem 1.2. Then, C is a plane quartic of the form $y^4 - h(x,z)y^2 + r(x,z) = 0$, where h and r are homogenous polynomials of degree 2 and 4, respectively, and one of the followings holds:*

(1) the polynomial $r(x,z)$ cannot be decomposed (over $\mathbb{F}_q$) as the product of two polynomials f, g of degree 2. In particular, the polynomial r is either irreducible or it has only one root in $\mathbb{F}_q$;
(2) we have $r(x,z) = f(x,z) \cdot g(x,z)$ with $\deg f = \deg g = 2$, and the polynomial $h(x,z)$ is a linear combination of f and g.

Proof. By Lemma 7.2 we know that C cannot be hyperelliptic, and by hypothesis C is the double cover of an elliptic curve E. Then, we can assume that the involution giving the double cover is $(x : y : z) \mapsto (x : -y : z)$, and therefore that C can be written in the form $y^4 - h(x,z)y^2 + r(x,z) = 0$, where h is a homogenous degree 2 polynomial, and r is homogenous of degree 4. Let us suppose that the polynomial r has two quadratic factor f and g and that the polynomial $h(x,z)$ is not a linear combination of f and g. Then, by [22, Thm. 1.1] we can explicitly construct a genus 2 curve F such that $\mathrm{Jac}(C) \sim \mathrm{Jac}(F) \times E$. Then, the curve C cannot lie on A, since otherwise A would be isogenous to $\mathrm{Jac}(F)$ by Lemma 7.1. Finally, one of the two conditions in the proposition must hold. □

Finally, we present bounds on the number of rational points that a genus 3 curve lying on an abelian surface with Weil polynomial in $\mathcal{P}^{\mathrm{irr}}_{\mathrm{npp}} \sqcup \mathcal{P}^{\mathrm{irr}}_{\mathrm{Wres}} \sqcup \{(t^2-2)^2, (t^2-3)^2\}$ can have. To start with, we recall and extend a result from [9] on the number of rational points on curves over abelian surfaces.

Proposition 7.4. *Let A be an abelian surface defined over $\mathbb{F}_q$ with trace $-a$. Let C be an absolutely irreducible curve defined over $\mathbb{F}_q$, of arithmetic genus p_a, lying on A. Then*

$$| \#C(\mathbb{F}_q) - (q + 1 + a) | \leq |p_a - 2| \lfloor 2\sqrt{q} \rfloor.$$

Proof. The upper bound on $\#C(\mathbb{F}_q)$ is [9, Thm. 4]. The proof can be adapted to obtain also the lower bound on $\#C(\mathbb{F}_q)$. In what follows, we borrow the notation from the proof of [9, Thm. 4].

If $p_a = 1$, then we know that the curve C is elliptic, of trace say $-e$. Write $a = e + x_2$ for some integer $-\lfloor 2\sqrt{q} \rfloor \leq x_2 \leq \lfloor 2\sqrt{q} \rfloor$. Hence,

$$\#C(\mathbb{F}_q) = q + 1 + e = q + 1 + a - x_2 \geq q + 1 + a - \lfloor 2\sqrt{q} \rfloor.$$

Suppose now $p_a \geq 2$. By [3, Prop. 2.3], we know that $\#C(\mathbb{F}_q) - \#\tilde{C}(\mathbb{F}_q) \geq g - p_a$, where $\tilde{C}$ is the normalisation of C and g is its genus. Following the reasoning in the proof of [9, Thm. 4, Eq. (5)], there exist real numbers $x_3, \ldots, x_g$ such that

$$\#\tilde{C}(\mathbb{F}_q) = q + 1 + a + \sum_{i=3}^{g} x_i \quad \text{and} \quad \sum_{i=3}^{g} x_i \geq -(g-2)\lfloor 2\sqrt{q} \rfloor.$$

Using that $g - p_a \leq 0$, we get the following series of inequalities:

$$\begin{aligned}\#C(\mathbb{F}_q) &\geq q + 1 + a + \sum_{i=3}^{g} x_i + g - p_a \\ &\geq q + 1 + a - (g-2)\lfloor 2\sqrt{q} \rfloor + g - p_a \\ &\geq q + 1 + a - (g-2)\lfloor 2\sqrt{q} \rfloor + (g - p_a)\lfloor 2\sqrt{q} \rfloor \\ &= q + 1 + a - (p_a - 2)\lfloor 2\sqrt{q} \rfloor,\end{aligned}$$

and the statement follows. □

Note that in [9, Thm. 4] the author needs the hypothesis $a \geq -q$, which is however only used to prove the result for curves which are irreducible but not absolutely irreducible. For such curves, the number of rational points cannot exceed $p_a - 1$, but we cannot prove a lower bound different from the trivial one.

From Proposition 7.4, we deduce the following facts. First, recall that a Weil restriction has always zero trace. Thus, if C is an absolutely irreducible curve of arithmetic genus 3 lying on a Weil restriction, then

$$q + 1 - \lfloor 2\sqrt{q} \rfloor \leq \#C(\mathbb{F}_q) \leq q + 1 + \lfloor 2\sqrt{q} \rfloor. \tag{4}$$

Indeed, in this case, C has the same number of rational points of the elliptic curve of which it is the double cover.

Secondly, we know that the trace of an abelian surface which does not admit a principal polarisation respects $a^2 = q - b$. Then, if C is an absolutely irreducible curve of arithmetic genus 3 on such a surface, we have

$$q + 1 - \sqrt{q-b} - \lfloor 2\sqrt{q} \rfloor \leq \#C(\mathbb{F}_q) \leq q + 1 + \sqrt{q-b} + \lfloor 2\sqrt{q} \rfloor.$$

A sloppy estimation, using that $|b| \leq 2q$ and hence $\sqrt{q-b} \leq \sqrt{3q} \leq 2\sqrt{q}$, gives us

$$q + 1 - 2\lfloor 2\sqrt{q} \rfloor \leq \#C(\mathbb{F}_q) \leq q + 1 + 2\lfloor 2\sqrt{q} \rfloor. \tag{5}$$

In particular, we see that an absolutely irreducible curve of genus 3 lying on a simple abelian surface not isogenous to the Jacobian of a genus 2 curve has not many rational points and it is far from reaching the Serre–Weil bound which states $|\#C(\mathbb{F}_q) - (q+1)| \leq 3\lfloor 2\sqrt{q} \rfloor$.

Acknowledgments

The first author would like to thank Christophe Ritzenthaler for preliminary discussions about the central question of this paper back in 2019, and for putting her in contact with the third author. The first and third authors thank Qing Liu for some useful discussion during the CAVARET conference. The authors are grateful to Jonas Bergström and Gaetan Bisson for comments on a preliminary version of the paper.

The first author is supported by the grant ANR-21-CE39-0009-BARRACUDA. The third author is supported by Nederlandse Organisatie voor Wetenschappelijk Onderzoek, grant number VI.Veni.202.107, and by Agence Nationale de la Recherche under the MELODIA project, grant number ANR-20-CE40-0013.

References

[1] A. Alzati and G. Pirola, *On abelian subvarieties generated by symmetric correspondences*, Mathematische Zeitschrift, 205 (1990), pp. 333–342.

[2] Y. Aubry, E. Berardini, F. Herbaut, and M. Perret, *Algebraic geometry codes over abelian surfaces containing no absolutely irreducible curves of low genus*, Finite Fields and Their Applications, 70 (2021), p. 101791.
[3] Y. Aubry and M. Perret, *A Weil theorem for singular curves*, Contemporary mathematics, (1996), pp. 1–8.
[4] F. Bardelli, C. Ciliberto, and A. Verra, *Curves of minimal genus on a general abelian variety*, Compositio Mathematica, 96 (1995), pp. 115–147.
[5] W. Barth, *Abelian surfaces with* $(1,2)$*-polarization*, in Algebraic geometry, Sendai, 1985, vol. 10 of Adv. Stud. Pure Math., North-Holland, Amsterdam, 1987, pp. 41–84.
[6] J. Bergström, V. Karemaker, and S. Marseglia, *Polarizations of Abelian Varieties Over Finite Fields via Canonical Liftings*, International Mathematics Research Notices, 2023 (2021), pp. 3194–3248.
[7] P. Borówka and G. Sankaran, *Hyperelliptic genus 4 curves on abelian surfaces*, Proceedings of the American Mathematical Society, 145 (2017), pp. 5023–5034.
[8] O. Debarre, *Degrees of curves in abelian varieties*, Bulletin de la Société Mathématique de France, 122 (1994), pp. 343–361.
[9] S. Haloui, *Codes from Jacobian surfaces*, in Arithmetic, geometry, cryptography and coding theory, vol. 686 of Contemp. Math., Amer. Math. Soc., Providence, RI, 2017, pp. 123–135.
[10] R. Hartshorne, *Algebraic geometry*, vol. 52, Springer Science & Business Media, 2013.
[11] T. Honda, *Isogeny classes of abelian varieties over finite fields*, Journal of the Mathematical Society of Japan, 20 (1968), pp. 83–95.
[12] E. W. Howe, *Principally polarized ordinary abelian varieties over finite fields*, Trans. Amer. Math. Soc., 347 (1995), pp. 2361–2401.
[13] ———, *Kernels of polarizations of abelian varieties over finite fields*, J. Algebraic Geom., 5 (1996), pp. 583–608.
[14] E. W. Howe, D. Maisner, E. Nart, and C. Ritzenthaler, *Principally polarizable isogeny classes of abelian surfaces over finite fields*, Math. Res. Lett., 15 (2008), pp. 121–127.
[15] E. W. Howe, E. Nart, and C. Ritzenthaler, *Jacobians in isogeny classes of abelian surfaces over finite fields*, Ann. Inst. Fourier (Grenoble), 59 (2009), pp. 239–289.
[16] T. LMFDB Collaboration, *The L-functions and modular forms database*. https://www.lmfdb.org, 2023. [Online; accessed 4 October 2023].
[17] D. Maisner and E. Nart, *Abelian surfaces over finite fields as Jacobians. With an appendix by Everett W. Howe*, Experimental Mathematics, 11 (2002), pp. 321–337.
[18] S. Marseglia, *Computing square-free polarized abelian varieties over finite fields*, Math. Comp., 90 (2021), pp. 953–971.
[19] J. S. Milne, *Abelian varieties*, in Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150.
[20] D. Mumford, *Abelian varieties*, Published for the Tata Institute of Fundamental Research, Bombay Zbl0223, 14022 (1970).
[21] A. Oswal and A. N. Shankar, *Almost ordinary abelian varieties over finite fields*, J. Lond. Math. Soc. (2), 101 (2020), pp. 923–937.
[22] C. Ritzenthaler and M. Romagny, *On the Prym variety of genus 3 covers of genus 1 curves*, Épijournal Geom. Algébrique, 2 (2018), pp. Art. 2, 8.
[23] J.-P. Serre, *Algebraic groups and class fields*, vol. 117, Springer Science & Business Media, 2012.
[24] P. Stevenhagen, *The arithmetic of number rings*, in Algorithmic number theory: lattices, number fields, curves and cryptography, vol. 44 of Math. Sci. Res. Inst. Publ., Cambridge Univ. Press, Cambridge, 2008, pp. 209–266.
[25] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math., 2 (1966), pp. 134–144.
[26] J. Tate, *Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)*, in Séminaire Bourbaki vol. 1968/69 Exposés 347-363, Springer, 1971, pp. 95–110.

CNRS; IMB, Université de Bordeaux, 351 cours de la Libération, 33405 Talence, France
Email address: elena.berardini@math.u-bordeaux.fr

Facultad de Ingeniería, Universidad Nacional de Asunción
Email address: agiangreco@ing.una.py

Laboratoire GAATI, Université de la Polynésie française, BP 6570 – 98702 Faaa, Polynésie française
Email address: stefano.marseglia@upf.pf