Leiden University Mathematics

Using heuristics on local matrix groups to count Abelian surfaces.

Extending a heuristic model to where K is non-Galois to obtain an already proven formula for counting ordinary principally polarized Abelian surfaces over a finite field with CM by K.

Name: Job Rauch
Date: 2017-08-21
Supervisor: Marco Streng

MASTER'S THESIS

Mathematical Institute
Leiden University
Niels Bohrweg 1
2333 CA Leiden
The Netherlands

Contents

1 Introduction

The prime topic in this thesis is counting in an isogeny class the isomorphism classes of principally polarized, ordinary Abelian surfaces over a finite field. An answer to this problem can be found in terms of class numbers, however there is also another approach to this problem. The basic principle behind this other approach was introduced by Gekeler in the case of elliptic curves over a finite field $\mathbb{F}_q$ of characteristic p [Gek03]. Gekeler based the approach on the failure of the following uniformity assumption.

> *For $k >> 0$, the number of matrices in $\mathrm{Mat}_{2\times 2}(\mathbb{Z}/l^k\mathbb{Z})$ with the given characteristic polynomial f equals the average $l^{2(k-1)}(l-1)$.*

For every prime l, to measure this failure he defined the heuristic factor $v_l(f)$ as the number of matrices in $\mathrm{Mat}_{2\times 2}(\mathbb{Z}/l^k\mathbb{Z})$ with the given characteristic polynomial f divided by the average $l^{2(k-1)}(l-1)$. At infinity he introduced a factor that was based upon the same assumption but then for large coprime to p integers $l \in \mathbb{Z} \setminus p\mathbb{Z}$. He showed also that the product

$$v_\infty(f) \prod_{l \text{ prime}} v_l(f)$$

converges and agrees with the number of isomorphism classes of elliptic curves E over $\mathbb{F}_p$ such that the characteristic polynomial is f. Therefore, giving a method for counting the isomorphism classes of elliptic curves with a given number of rational points.

Achter and Williams [AW15, Wil12] gave an extension of this heuristic model to the case of certain Abelian surfaces. Again, the heuristics result in a factor for every place and their product is a priori a possibly transcendental number, which they prove to be equal to a quotient of class numbers. This quotient happens to be exactly the cardinality of the set of isomorphism classes we are counting. In this thesis we will give an argument for only including cyclic matrices in the heuristics at the finite places l as we could not find this in [AW15, Wil12].

Our main contribution is the proof of that one of the restrictions that Achter and Williams impose upon the isogeny class, namely that it had to be determined by a polynomial f such that $K := \mathbb{Q}(X)/(f(X))$ is a Galois extension of $\mathbb{Q}$, can be dropped.

In Section 2 we will start with some necessary background on Abelian varieties and schemes that benefits the understanding of the principles behind the heuristics. This background includes the structure of Abelian schemes and Abelian varieties, as well as isogenies, Tate modules, the Frobenius morphisms, and the Verschiebung. Equipped with the acquired theory, we will also look at the theory of lifting ordinary Abelian varieties over finite fields to characteristic 0. We discuss this theory in Section 3.3 and demonstrate that by restricting to certain Abelian surfaces, as we do in this thesis, the size of the isogeny class can be calculated using class numbers. To be precise, we will count Abelian surfaces that are principally polarized, ordinary and contained in an isogeny class that is

determined by a irreducible quartic polynomial $f = X^4 - \alpha X^3 + \beta X^2 - \alpha q X + q^2$, where $\alpha, \beta \in \mathbb{Z}$ and $q = \#k$, such that $K := \mathbb{Q}[X]/(f(X))$ is not a Galois extension of $\mathbb{Q}$ and in which the prime $p = \mathrm{char}(k)$ is unramified. Some consequences of these restrictions are discussed in Section 3.1, like that K is a CM field and thus has a maximal totally real subfield $K_0 = \mathbb{Q}[X]/(f_0(X))$ with $f_0 = X^2 - \alpha X + (\beta - 2q)$. In Section 3.2 we discuss for a commutative ring R the group $\mathrm{GSp}_4(R)$ of elements $\alpha \in \mathrm{GL}(R)$ that satisfy the relation $\alpha^t J \alpha = m_\alpha J$ for a fixed matrix J and a multiplier $m_\alpha \in R^\times$. The subset $\mathrm{GSp}_4(R)^{(i)}$ of matrices $\alpha \in \mathrm{GSp}(R)$ with multiplier $m_\alpha = i$ is instrumental for defining the factors of our local heuristics. Then in Section 4, using the insight we obtained about the heuristics in the aforementioned sections, we define the factors of the heuristic model for primes $l \neq p, 2$ as

$$v_l(f) := \frac{\#\{\text{cyclic } \gamma \in \mathrm{GSp}_4(\mathbb{F}_l)^{(q)} | f_\gamma \equiv f_A \bmod l\}}{\#\,\mathrm{GSp}_4(\mathbb{F}_l)^{(q)}/l^2}.$$

Using the heuristics of Achter and Williams [AW15], we follow the definition for their factors of the heuristic model at ∞, p for which we let $\mathrm{cond}(f)$ be the index of $\mathbb{Z}[\pi]$ in $\mathbb{Z}[\pi, \overline{\pi}]$, where π is an complex root of f, so we define the factors as

$$v_p(f) := \frac{\#\{\text{semisimple } \gamma \in \mathrm{GSp}_4(\mathbb{F}_p)^{(\beta^2)} | f_\gamma \equiv (X^2 + \alpha X - \beta)^2 \bmod p\}}{\#\,\mathrm{GSp}_4(\mathbb{F}_p)^{(\beta^2)}/p^2}$$

$$v_\infty := \frac{\sqrt{|\Delta_f|}}{(2\pi)^2 \,\mathrm{cond}(f) \sqrt{|\Delta_{f_0}|}}.$$

We have not defined a factor at 2 based upon the heuristic, but up to that factor we will show, using the analytic class number formula, that the product of the heuristic factors is exactly $\frac{h_k}{h_{K_0}}$, where K_0 is the totally real maximal subfield of $K = \mathbb{Q}[X]/(f(X))$. For this proof, we define the rational factors $v_l(K)$ for all finite primes l based upon the Euler product of the Dedekind zeta function and the real number $v_\infty(K)$ based upon the factors in the analytic class number formula other then the zeta function.

We determine the factors $v_l(K)$ and $v_l(f)$ in Section 6 and thereby demonstrate the equality of these for each place $l \neq 2$. For the product $\prod v_l(K)$ we know that it equals $\frac{h_k}{h_{K_0}}$. In Section 3.3 we show that $\frac{h_k}{h_{K_0}}$ equals the number of isomorphism classes of Abelian varieties in the isogeny class of Abelian varieties that have f as characteristic polynomial for the Frobenius. Therefore, we conclude that the combination of the heuristics provides a method to counting the isomorphism classes up to a rational factor

$$v_2(K) := \frac{\prod_{\mathfrak{l}|(2);\mathfrak{l}\subset\mathcal{O}_K}(1 - N_{K/\mathbb{Q}}(\mathfrak{l})^{-1})}{\prod_{\mathfrak{l}|(2);\mathfrak{l}\subset\mathcal{O}_{K_+}}(1 - N_{K_+/\mathbb{Q}}(\mathfrak{l})^{-1})}$$

for which there are finitely many possibilities.

2 Background on Abelian varieties

In this Section we will summarise part of the theory of Abelian varieties and Abelian schemes. More definitions and details are given in Appendix A. We start with demonstrating that Abelian schemes over fields are Abelian varieties. Followed by a description of multiple results about Abelian varieties that can also be found in Moonen en van der Geer [MvdG11] or Milne [Mil08].

2.1 Definition and basic structure

Definition 2.1. An *Abelian scheme over a scheme* S is an S-group scheme A such that the structure morphism $\sigma : A \to S$ is smooth and proper and the geometric fibres are connected. △

Definition 2.2. An *Abelian variety over a field* k is a geometrically integral $\mathrm{Spec}(k)$-group scheme A such that the structure morphism $\sigma : A \to \mathrm{Spec}(k)$ is proper. △

Notation 2.3. Any group scheme G comes with a *multiplication map* m_G, an *inverse map* i_G and a distinguished *identity element* e_G. △

An intuitive way of thinking about Abelian schemes is to see them as group schemes of which the fibres are Abelian varieties. To justify this picture we will show that Abelian schemes over fields are Abelian varieties.

Proposition 2.4. Let k be a field and $S = \mathrm{Spec}(k)$. Every Abelian scheme over S is an Abelian variety over k. Conversely, every Abelian variety is an Abelian scheme. △

Proof. Let k be a field, $S = \mathrm{Spec}(k)$ and A be an Abelian scheme over S. The properness of the structure morphism is included in both the definition of Abelian scheme and Abelian variety, hence we only have to demonstrate that A is geometrically integral. From the Stack Project [Sta, Tag 038K] it follows that that A is geometrically integral if and only if it is both geometrically irreducible and geometrically reduced. By assumption $A \to \mathrm{Spec}(k)$ is a smooth morphism where k is a field and therefore X is geometrically regular and geometrically reduced over k [Sta, Tag 056T]. Thus it remains to show that A is geometrically irreducible.

The geometrically regularity of A implies that the local rings of $A_{\overline{k}}$ are regular. Therefore, we find that the local rings are integral domains and thus have a unique minimal prime. Notice that k is Noetherian and that the structure morphism is proper, thus of finite type and thus A is Noetherian [Sta, Tag 01T6]. From this we can deduce that our scheme has only finitely many irreducible components [Sta, Tag 0BA8]. From Lemma A.19 follows that the connected components of $A_{\overline{k}}$ are irreducible. We know that the geometric fibres are connected, hence $A_{\overline{k}}$ is connected. Thus we can conclude that $A_{\overline{k}}$ is irreducible, i.e. that A is geometrically irreducible.

For the converse, let A be an Abelian variety. The smooth points of A form an open and dense set that is stable under all translations, hence A is smooth

[MvdG11, Proposition 1.5]. Since Abelian varieties are geometrically integral, they are geometrically irreducible and thus also geometrically connected. So all Abelian varieties are Abelian schemes. □

From this point on we will focus on Abelian varieties and all results can be found in Milne [Mil08], Oort[Oor08] or Moonen and van de Geer[MvdG11]. In Section 3.1 The first proposition is more of a corollary of the Rigidity Lemma, which can be found in Appendix A.

Proposition 2.5. The group structure of an Abelian variety is commutative. △

Proof. Let A be an Abelian variety. Then by Corollary A.21 the map i_A is a homomorphism as $i_A(e_A) = e_A$. □

From now on, we will use an additive notation for the group structure on an Abelian variety A, i.e. use $+, -$ and 0 instead of m_A, i_A and e_A. Moreover, given two homomorphism $f, g : A \to B$ of Abelian varieties A, B over k we define their sum $(f + g)$ as $+ \circ (f \times g)$. This makes $\mathrm{Hom}(A, B)$ into an Abelian group.

Definition 2.6. Let $n \in \mathbb{Z}$ and A be an Abelian variety over a field k. We define the *multiplication-by-n map* $[n]_A$ as the homomorphism

$$A(k) \to A(k), a \mapsto n \cdot a = \begin{cases} 0_A & \text{if } n = 0, \\ \mathrm{sign}(n) \cdot (\overbrace{a + \cdots + a}^{|n|}) & \text{if } n \neq 0. \end{cases}$$ △

We denote the kernel in terms of group schemes of $[n]_A$ as $A[n]$.

Let $n \in \mathbb{Z}$ and $f \in \mathrm{Hom}(A, B)$, then $n \cdot f = [n]_B \circ f = f \circ [n]_A$ and we will see in the next section (Theorem 2.12) for $n \neq 0$ that $[n]_A$ is surjective. Therefore, the group $\mathrm{Hom}(A, B)$ is torsion free. The $\mathbb{Q}$-algebras $\mathbb{Q} \otimes \mathrm{Hom}(A, B)$ and $\mathbb{Q} \otimes \mathrm{End}(A)$ we denote as $\mathrm{Hom}^0(A, B)$ and $\mathrm{End}^0(A)$.

Before further discussing homomorphism, we introduce two special finite group schemes.

Definition 2.7. Let G be a finite group scheme over a field k. If the structure morphism $G \to \mathrm{Spec}(k)$ is étale, then we refer to G as *étale*. On the other hand, if G is connected we refer to G as *local*. △

Lemma 2.8. Let G be a finite group scheme over a field k and let G^0 be the connected component of the identity. Then there is an étale group scheme $G_{\text{ét}}$ such that the following sequence of group schemes is exact.

$$1 \longrightarrow G^0 \longrightarrow G \longrightarrow G_{\text{ét}} \longrightarrow 1.$$

Moreover, if k is perfect and G commutative, then the exact sequence splits, i.e. $G \cong G^0 \times G_{\text{ét}}$. △

Proof. See [MvdG11, Chapter 3, Proposition 4.45]. □

2.2 Morphisms and isogenies

Definition 2.9. A homomorphism $f : A \to B$ is called an *isogeny* if it satisfies the following equivalent conditions:

(1) The morphism f is surjective and $\dim(A) = \dim(B)$,

(2) The kernel $\ker(f)$ is a finite group scheme and $\dim(A) = \dim(B)$,

(3) The morphism f is flat, finite and surjective.

We define the *degree* of an isogeny as the degree $[k(A) : k(B)]$ of the extension of the function fields. △

Proof. See [MvdG11, Proposition 5.2] for the equivalence of (1), (2) and (3). □

Remark 2.10. *The composition of two isogenies f, g is again an isogeny of degree* $\deg(f) \cdot \deg(g)$. △

Proposition 2.11. Let $f : A \to B$ be an isogeny of Abelian varieties over k. Then the following two equivalences hold

(1) The isogeny f is an étale morphism if and only if the group scheme $\ker(f)$ is étale,

(2) The isogeny f is a purely inseparable morphism if and only if $\ker(f)$ is local.

An isogeny satisfying (1) we refer to as a *separable* isogeny and an isogeny satisfying (2) we refer to as a *purely inseparable* isogeny. For an isogeny $f : A \to B$ there is a decomposition into a purely inseparable isogeny $f_i : A \to C$ and a separable isogeny $f_s : C \to B$. △

Proof. See [MvdG11, Proposition 5.6] for the equivalences. In the proof of the second equivalence the following sequence is introduced.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \ker(f)/\ker(f)^0 & \longrightarrow & A/\ker(f)^0 & \xrightarrow{f_s} & B & \longrightarrow & 1 \\ & & & & \uparrow{\scriptstyle f_i} & \nearrow_{f} & & & \\ & & & & A & & & & \end{array} .$$

The horizontal arrows form an exact sequence and so the kernel of f_s is isomorphic to $\ker(f)/\ker(f)^0$. It follows from Lemma 2.8 that $\ker(f)/\ker(f)^0$ is étale and thus f_s is separable. Clearly the kernel of f_i is $\ker(f)^0$, a connected scheme, making f_i purely inseparable. □

A classic example of an étale morphism is that of multiplication by an integer.

Theorem 2.12. Let A be an Abelian variety over a field k and $g := \dim(A)$. For $n \neq 0$, the homomorphism $[n]_A$ is an isogeny of degree n^{2g} and if $\mathrm{char}(k) \nmid n$ or $\mathrm{char}(k) = 0$ the kernel $A[n] := \ker([n]_A)$ is an étale group scheme. △

Proof. See [MvdG11, Proposition 5.9]. □

Corollary 2.13. Set $p = \operatorname{char} k$ and let $n \in \mathbb{Z}$ such that $p \nmid n$. Then the group of n-torsion point over the separable closure $A[n](k^{sep})$ of k is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{2g}$, where g is the dimension of A. △

Our work until now was mainly for this result, as for a prime l we can now look at the l^r torsion points for any $r \in \mathbb{Z}_{\geq 1}$.

Definition 2.14. Let A be an Abelian variety over a field k, with $\operatorname{char} k = p$ and let $l \neq p$ be a prime. The *l-Tate module* $T_l(A)$ we define as the projective limit of the system $\{A[l^n](k^{sep})\}_{n\in\mathbb{Z}_{\geq 1}}$ with the maps $A[l^n](k^{sep}) \to A[l^{n-1}](k^{sep})$. △

From Corollary 2.13 we obtain that $T_l(A)$ is a free $\mathbb{Z}_l$-module of rank $2g$, since it is (non-canonically) isomorphic as $\mathbb{Z}_l$-module to $\mathbb{Z}_l^{2g} = \varprojlim_r (\mathbb{Z}/l^r\mathbb{Z})^{2g}$. Therefore, we define

$$V_l(A) := T_l(A) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$$

which is a $\mathbb{Q}_l$-vector space of dimension $2g$. Observe that structure of $T_l(A)$ is not restricted to being a free $\mathbb{Z}_l$-module, for example there is an action of $\operatorname{Gal}(k^{sep}/k)$ on $T_l(A)$ induced via the natural action of $\operatorname{Gal}(k^{sep}/k)$ on $A[l^r](k^{sep})$. This example gives rise to an integral l-adic representation $\rho_l : \operatorname{Gal}(k^{sep}/k) \to \operatorname{GL}(T_l(A))$.

For any $r \in \mathbb{Z}_{\geq 1}$ and prime l, a homomorphism $f : A \to B$ of Abelian varieties over k can be restricted to a homomorphism $A[l^r](k^{sep}) \to B[l^r](k^{sep})$ and $A[l^r](\overline{k}) \to B[l^r](\overline{k})$. Therefore, f induces an unique $\mathbb{Z}_l$-linear map $T_l(f) : T_l(A) \to T_l(B)$ sending a point $(a_i)_{i=0}^{\infty}$ to $(f(a_i))_{i=0}^{\infty}$. Likewise, we have an induced linear map $V_l(f) : V_l(A) \to V_l(B)$.

Lemma 2.15. Let $f : A \to B$ be an isogeny of Abelian varieties over a field k and set $d := \deg f$. There is an isogeny $g : B \to A$ such that $g \circ f = [d]_A$ and $f \circ g = [d]_B$. △

Proof. See [MvdG11, Proposition 5.12] □

Corollary 2.16. The existence of an isogeny between Abelian varieties A and B is an equivalence relation. △

Corollary 2.17. For an isogeny $f : A \to B$, the induced linear map $V_l(f) : V_l(A) \to V_l(B)$ is an isomorphism. △

Proof. By Lemma 2.15, there is an isogeny g such that $f \circ g = g \circ f = [\deg(f)]$. The linear map induced by $[\deg(f)]$ is an automorphism of $V_l(A)$, so the map $V_l(f)$ is an isomorphism. □

When f is an endomorphism, we have for $V_l(f)$ a definition of its characteristic polynomial, namely $P_{l,f}(X) := \det(X \cdot \mathrm{id} - V_l(f))$.

Proposition 2.18. Let A be an Abelian variety over k and $f \in \operatorname{End}^0(A) = \operatorname{End}(A) \otimes \mathbb{Q}$. There exists a unique monic polynomial $P_f \in \mathbb{Q}[X]$ of degree $2g$ defined for $n \in \mathbb{Z}$ as $P_f(n) = \deg([n]_A - f)$. The polynomial P_f we refer to as the *characteristic polynomial of f*. △

Proof. By Proposition 12.15 of [MvdG11] the map deg : $\mathrm{End}^0(A) \to \mathbb{Q}$ is a homogeneous polynomial map of degree $2g$. In other words, given a $\mathbb{Q}$-basis $\{[1]_A, e_1, e_2, \cdots, e_r\}$ of $\mathrm{End}^0(A)$ there is a homogeneous polynomial $D \in \mathbb{Q}[X_0, \cdots, X_r]$ of degree $2g$ such that for all $c_0, \cdots, c_r \in \mathbb{Q}$ we have

$$\deg(c_0 \cdot [1]_A + \Sigma_{i=1}^r c_i \cdot e_i) = D(c_0, c_1, \cdots, c_r).$$

As $\{[1]_A, e_1, e_2, \cdots, e_r\}$ is a basis, there are unique rational numbers $z_i \in \mathbb{Q}$ such that $f = [z_i]_A + \sum_{i=1}^r z_i \cdot e_i$. Defining the polynomial $P_f(X)$ as $D(X - z_0, -z_1, -z_2, \cdots, -z_r)$ establishes that $P_f(n) = \deg([n]_A - f)$. As the degree of $[1]_A$ is $2g$ it follows that $P_f(X)$ is a polynomial of degree $2g$. □

Example 2.19. For any $m, n \in \mathbb{Z}$ we have that $P_{[m]_A}(n) = \deg([n-m]_A) = (n-m)^{2g}$ and thus $P_{[m]_A}(X) = (X-m)^{2g}$. △

Theorem 2.20. Let A be an Abelian variety over a field k. For any prime number $l \neq \mathrm{char}(k)$ the characteristic polynomial $P_{l,f}$ of $V_l(f) \in \mathrm{End}_{\mathbb{Q}_l}(V_l(A))$ equals the characteristic polynomial P_f of f. △

Proof. See [MvdG11, Proposition 12.18]. □

Corollary 2.21. Let $f \in \mathrm{End}^0(A)$. It is a root of its own characteristic polynomial, i.e. $P_f(f) = 0$. △

Proof. Any $f \in \mathrm{End}^0(A)$ can be written as $f = z \times g$ for $z \in \mathbb{Q}$ and $g \in \mathrm{End}(A)$. By [MvdG11, 12.14] we have the equality $\deg(f) = z^{2g} \cdot \deg g$ and thus we only have to show that the result holds for an $g \in \mathrm{End}(A)$. For a prime $l \neq p$, the result holds for g on the l-Tate module, hence it holds on $\cup_{r=1}^\infty A[l^r]$. By [MvdG11, Theorem 5.30] the set $\cup_{r=1}^\infty A[l^r]$ is topologically dense in A, hence the result holds on A. □

Corollary 2.22. For an $f \in \mathrm{End}(A)$ the polynomial P_f has integer coefficients. △

Proof. See [MvdG11, Proposition 12.20]. □

There is another important isogeny, namely the Frobenius. We conclude this section with discussing the geometric Frobenius morphism. There are other Frobenii and those will give more insight in the p-torsion of an Abelian variety, however the heuristic for the factor at p given by Achter and Williams can be used in our case without adjustments, therefore we do not discuss these definitions. For (more) details on Frobenii morphisms we refer to the "Notation and conventions" Chapter of Moonen and van der Geer [MvdG11, Chapter 0] and for the relation with the p-torsion see Section 5.2 of the same reference.

For the remainder of the section, we let the number q be a power of the prime p.

Definition 2.23. Let A be an Abelian variety over a finite field $\mathbb{F}_q$. We define the *geometric Frobenius* $\mathrm{Frob}_A : A \to A$ of A as the morphism that is the identity on the topological space and the endomorphism $\mathrm{Frob}_A^\#$ of the sheaf $\mathcal{O}_A$ is defined by $f \mapsto f^q$. △

Lemma 2.24. Let A be a g-dimensional Abelian variety over the finite field $\mathbb{F}_q$. Then the geometric Frobenius homomorphism $\mathrm{Frob}_A : A \to A$ is a purely inseparable isogeny of degree q^g. △

Proof. Proposition 5.15 of [MvdG11] tells us that relative Frobenius F is an isogeny of degree q^g. Moreover, in [MvdG11, Chapter 0] the relation $F^m = \mathrm{Frob}_A$ is given, for $m \in \mathbb{Z}$ such that $p^m = q$. □

In Lemma 2.15 we demonstrated that an isogeny of degree d gives rise to a factorisation of the multiplication-by-d map. So the geometric Frobenius gives rise to a factorisation of the map $[q^g]$. This result can be improved to a factorisation of the map $[q]$.

Lemma 2.25. Let A be an Abelian variety over the finite field $\mathbb{F}_q$. There is a map $\mathrm{Ver}_A : A \to A$ such that the multiplication-by-q on A factors as

$$[q]_A = \mathrm{Ver}_A \circ \mathrm{Frob}_A = \mathrm{Frob}_A \circ \mathrm{Ver}_A \,.$$

We refer to the map Ver_A as the *geometric Verschiebung*. Moreover, the geometric Verschiebung Ver_A is an isogeny of degree q^g. △

Proof. See Proposition 5.20 of [MvdG11]. □

3 Setting up for the Heuristic

3.1 Main objects of study

For the remainder of the thesis, let A be an Abelian surface over the finite field $\mathbb{F}_q$ with $q = p^n$ elements. Let f_A be the characteristic polynomial of the geometric Frobenius endomorphism π_A of A. By a theorem of Tate [Tat66, Theorem 1(c)], for any Abelian variety B over the field $\mathbb{F}_q$ there is an isogeny from B to A if and only if $f_B = f_A$. Under the assumption that A is simple follows that the geometric Frobenius π_A is an q-Weil number, i.e. it is an algebraic number and for every embedding $\phi : \mathbb{Q}(\pi_A) \to \mathbb{C}$ we have the equality $|\phi(\pi_A)| = \sqrt{q}$. For more details on this see for example [Oor08, Theorem 3.2]. If we also assume A to be ordinary, then from a proposition of Howe [How95, Theorem 1.2] we have that f_A is irreducible and of the form $X^4 - \alpha X^3 + \beta X^2 - \alpha q X + q^2$, with $\alpha \in \mathbb{Z}$ and $\beta \in \mathbb{Z} \setminus p\mathbb{Z}$.

We can also start with an irreducible q-Weil polynomial and wonder if it gives rise to an isogeny class of Abelian surfaces. Theorem 1 of Honda [Hon68] tells us that every irreducible q-Weil polynomial corresponds to an isogeny class of simple Abelian varities. If we combine the results of Weil, Tate and Honda we get a new bijection, namely the main theorem of Honda-Tate theory.

Theorem 3.1. The set of simple Abelian varieties over $\mathbb{F}_q$ up to isogeny is in bijection with the set of irreducible q-Weil polynomials via the map $A \mapsto f_A$. △

Proof. For a more detailed description and proof see [Oor08]. □

In this thesis we will look at a special kind of Abelian surface A and corresponding Weil polynomial f. The Abelian surfaces we consider in this thesis, satisfy the following four assumption.

A.1 The polynomial f is *ordinary* and of degree 4, therefore $f(X)$ is of the form $X^4 - \alpha X^3 + \beta X^2 - \alpha q X + q^2$ with $\alpha, \beta \in \mathbb{Z}$ and β coprime to q.

A.2 The polynomial f is *principally polarizable*, i.e. there exists a principally polarized Abelian variety with characteristic polynomial f.

A.3 The polynomial f is *irreducible* and the field $K_f = \mathbb{Q}[X]/(f(X))$ is *unramified* at p and $\mathrm{Gal}(K/\mathbb{Q}) \cong D_4$.

A.4 For a complex root π_f of f and its complex conjugate $\overline{\pi}_f$, the order $\mathbb{Z}[\pi_f, \overline{\pi}_f]$ in K_f is maximal. This implies that $\mathrm{End}(A)$ is maximal.

The assumptions **A.1** and **A.2** give some extra restrictions on α and β, for more information see [How95, Theorem 1.2].

Remark 3.2. *The reading commission pointed out that it might be possible in our case that* **A.2** *is automatic based upon the other assumptions.* △

Notation 3.3. For an irreducible q-Weil polynomial f, write $\mathcal{A}(\mathbb{F}_q; f)$ for the set of isomorphism classes of principally polarized Abelian varities A such that $f_A = f$. △

Definition 3.4. A field K is said to be a CM-field if K is a number field and that has a subfield $K_0 \subset K$ such that K_0 is totally real and K is totally imaginary and is quadratic over K_0. △

Remark 3.5. *The field K_f is a CM-field, since the automorphism $\pi_f \mapsto \frac{q}{\pi_f}$ of K_f corresponds with complex conjugation and is not the identity as $K_f \ncong \mathbb{Q}(\sqrt{q})$. Thus K_f has a maximal totally real subfield $K_+ = \mathbb{Q}(\pi_f + \frac{q}{\pi_f})$ and this subfield is determined by $f_0(X) = X^2 - \alpha X + (\beta - 2q)$, where α, β are the same as in **A.1**.* △

We saw in Section 2 that the Frobenius induces a morphism on the Tate-module $T_l(A)$, with $l \neq p$ prime, and we will show in Section 4 that the Frobenius can be identified with an element of a certain subgroup of $\mathrm{GL}_4(\mathbb{Z}_l)$. In the next section we will discuss this subgroup.

3.2 General symplectic group

For the remainder of the thesis we set

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

Let R be a commutative ring and assume that $\alpha, \beta \in \mathrm{GL}_4(R)$ are such that $\alpha^t J \alpha = m_\alpha J$ and $\beta^t J \beta = m_\beta J$ for $m_\alpha, m_\beta \in R^\times$. Then $(\alpha\beta)^t J \alpha\beta = m_\alpha m_\beta J$ and also for the matrix

$$\mathbf{1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

we have $\mathbf{1}J\mathbf{1} = J$. This allows us to define a subgroup of $\mathrm{GL}_4(R)$.

Definition 3.6. Let R be a commutative ring. Then the *general symplectic group* $\mathrm{GSp}_4(R)$ *of dimension* 4 *with elements in* R is the subgroup of $\mathrm{GL}_4(R)$ consisting of the elements $\alpha \in \mathrm{GL}_4(R)$ such that $\alpha^t J \alpha = mJ$ for a unit $m \in R^\times$. The *special symplectic group* $\mathrm{Sp}_4(R)$ *of dimension* 4 *with elements in* R is the subgroup of $\mathrm{GSp}_4(R)$ such that $m = 1$. △

We can now define the map $m : \mathrm{GSp}_4(R) \to R^\times$ that sends a matrix α to the multiplier m_α in the relation $\alpha^t J \alpha = m_\alpha J$. For $i \in R^\times$, define $\mathrm{GSp}_4(R)^{(i)}$ as the inverse image $m^{-1}(\{i\})$. Note that the sequence

$$1 \longrightarrow \mathrm{Sp}_4(R) \longrightarrow \mathrm{GSp}_4(R) \xrightarrow{m} R^\times \longrightarrow 1$$

is exact. This sequence helps us with the cardinality of $\mathrm{GSp}_4(R)$.

Lemma 3.7. Let R be a commutative ring and $i \in R^\times$, then $\#\,\mathrm{Sp}_4(R) = \#\,\mathrm{GSp}_4(R)^{(i)}$. △

Proof. The set $\mathrm{GSp}_4(R)^{(i)}$ is the coset of $\mathrm{Sp}_4(R)$ in $\mathrm{GSp}_4(R)$ containing

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & 0 & 0 & i \end{pmatrix}.$$

□

Lemma 3.8. For a prime l, the cardinality of the group $\mathrm{Sp}_4(\mathbb{Z}/l^r\mathbb{Z})$ equals $l^{10(r-1)} \# \mathrm{Sp}_4(\mathbb{F}_l)$ for $r \in \mathbb{Z}_{\geq 1}$. △

Proof. For $r = 1$ the Lemma is trivial. For $r \geq 2$, we follow [New72, Section 36, p135] by counting the lifts for an arbitrary matrix $M' \in \mathrm{Sp}(\mathbb{Z}/l^{r-1}\mathbb{Z})$. A matrix $M \in \mathrm{Mat}_{4,4}(\mathbb{Z}/l^r\mathbb{Z})$ can be described uniquely as a summation of matrices M_i with coefficients in $\{0, 1, ..., l-1\} \subset \mathbb{Z}$ such that $M = \left(\sum_{i=1}^{r} M_i l^{i-1}\right) \bmod l^r$. Let M be a lift of M', the relation $M' = \left(\sum_{i=1}^{r-1} M_i l^{i-1}\right) \bmod l^{r-1}$ fully restricts all matrices M_i except for M_r. Set $M'_r = \sum_{i=1}^{r-1} M_i l^{i-1}$ and let $C, U \in \mathrm{Mat}_{4\times 4}(\mathbb{F}_l)$ be such that

$$\begin{aligned} C &\equiv \frac{1}{l^{r-1}}({M'_r}^T J M_r - J) \pmod{l} \\ U &\equiv {M'_r}^T J M'_r \pmod{l} \end{aligned}$$

The matrix M is an element of $\mathrm{Sp}_4(\mathbb{Z}/l^r\mathbb{Z})$ if and only if the following equivalent statements hold.

$$M^T J M \equiv J \pmod{l^r} \tag{3.1}$$

$$M_r^T J M_r - J + {M'_r}^T J M_r l^{r-1} + M_r^T J M'_r l^{r-1} \equiv 0 \pmod{l^r} \tag{3.2}$$

$$C + U - U^T \equiv 0 \pmod{l} \tag{3.3}$$

Moreover, $M'_r J$ is non-singular modulo l and thus U and M_r are completely determined by each other. Given M'_r, we count how may U satisfying (3.3). The diagonal and upper diagonal coefficients of U can be chosen free and determine the lower diagonal coefficients. Therefore, there are l^{10} possible lifts for M'. □

3.3 Lifting of Abelian varieties

In this section we will prove the following theorem.

Theorem 3.9. Let A be an Abelian surface and f the characteristic polynomial of its geometric Frobenius satisfying **A.1-A.4**. The number $\#\mathcal{A}(\mathbb{F}_q; f)$ of isomorphism classes of principally polarized Abelian surfaces that have CM by $\mathcal{O}_K$ over $\mathbb{F}_q$ with characteristic polynomial of Frobenius f is $\frac{h_K}{h_{K_0}}$. △

We use a correspondence between these Abelian varieties over finite fields and objects in characteristic 0. The basis for the correspondence comes from

Lubin, Serre and Tate, who discussed this topic during seminars at the Summer Institute on Algebraic Geometry in 1964 [LST64]. The following theorem allows us to lift Abelian varieties over finite fields to an Abelian scheme in characteristic zero.

Theorem 3.10 (Lubin-Serre-Tate)**.** Let A be an ordinary Abelian variety over $\mathbb{F}_q$ and R the ring of integers of the p-adic completion $\widehat{\mathbb{Q}_p^{ur}}$ of the maximal unramified extension of $\mathbb{Q}_p$. Then there is a projective Abelian scheme A' over R such that the reduction $A' \otimes_R \mathbb{F}_q = A$ and $\phi : \mathrm{End}(A') \to \mathrm{End}(A)$ are bijective. Such an A' we refer to as an lift of A and is upto a canonical isomorphism unique. Let $\pi \in \mathrm{End}(A)$, then we refer to the pair $(A', \phi^{-1}(\pi))$ as the *canonical lift* of A and π. △

In the original version of Lubin-Serre-Tate the scheme is defined over $W(\overline{\mathbb{F}_p})$ the ring of Witt vectors over $\overline{\mathbb{F}_p}$, which is isomorphic to R. The ring of Witt vectors over $\mathbb{F}_{p^m}$ is isomorphic to the ring of integers R_m of the unique unramified extension of degree m over $\mathbb{Q}_p$, moreover we know that the ring of Witt vectors over a perfect field of characteristic $p > 0$ is a complete discrete valuation ring [Haz09, 6.20]. For every $i \in \mathbb{Z}_{\geq 1}$, let K_i be a finite unramified extension of $K_0 := \mathbb{Q}_p$ such that $K_{i-1} \subsetneq K_i$. Note that $\mathbb{Q}_p^{ur}$ is not complete as the limit of $(\sum_{i=1}^{n} a_i p^i)_{n=1}^{\infty}$, with $a_i \in K_{i+1} \setminus K_i$, is not an element of $\mathbb{Q}_p^{ur}$. However, our ring R, the ring of integers of the completion of the field $\mathbb{Q}_p^{ur}$, is isomorphic to $W(\overline{\mathbb{F}_p})$.

Let $L = \widehat{\mathbb{Q}_p^{ur}}$ be the fraction field of R. Take an embedding $\epsilon : L \to \mathbb{C}$. Now, given a canonical lift (A', π_q') of an ordinary Abelian variety A over $\mathbb{F}_q$ and its Frobenius endomorphism π_q there is an Abelian scheme $A_{\mathbb{C}}$ over $\mathbb{C}$ that is the extension of scalars for A' via ϵ. By Proposition 2.4 is $A_{\mathbb{C}}$ an Abelian variety. Also π_q' extends via ϵ to an endomorphism of $H_1(A_{\mathbb{C}}, \mathbb{Z})$ and denote this endomorphism as $F(A, \pi_q)$. We refer to $A_{\mathbb{C}}$ as the *Serre-Tate lift* of A.

Based upon the Serre-Tate lift, Deligne introduced in his article [Del69] a category that has a correspondence with the ordinary Abelian varieties over a finite field.

Definition 3.11. Let $\mathcal{L}_q$ be the category of pairs (Λ, F) where Λ is a finitely generated free $\mathbb{Z}$-module and F is an endomorphism of Λ such that the following holds.

- The endomorphism $F \otimes \mathbb{Q}$ of $\Lambda \otimes \mathbb{Q}$ is semi-simple, and its eigenvalues in $\mathbb{C}$ have absolute value $\sqrt{q}$.
- At least half of the roots of the characteristic polynomial of F in $\overline{\mathbb{Q}_p}$, counting multiplicities, are units in $\overline{\mathbb{Z}_p}$.
- There is an endomorphism V of Λ such that $FV = q$.

We refer to the endomorphism F as the *Frobenius* and V as the *Verschiebung*. We will refer to objects of $\mathcal{L}_q$ as *Deligne pairs*. The morphisms from the pair (Λ_1, F_1) to the pair (Λ_2, F_2) are the homomorphisms $\alpha : \Lambda_1 \to \Lambda_2$ of the $\mathbb{Z}$-modules such that $\alpha \circ F_1 = F_2 \circ \alpha$. △

Deligne showed that for a pair $(\Lambda, F) \in \mathcal{L}_q$ the $\mathbb{Z}$-rank of Λ is even and that exactly half the roots if the characteristic polynomial are p-adic units. The *dimension* of a Deligne pair (Λ, F) we define as half the $\mathbb{Z}$-rank of Λ.

Theorem 3.12 (Deligne)**.** Fix an embedding $L \hookrightarrow \mathbb{C}$. There is an equivalence of categories between the category of ordinary Abelian varieties over $\mathbb{F}_q$ and the category of Deligne pairs given by the functor

$$\mathcal{D} : \underline{\mathrm{OrdVar}}_{\mathbb{F}_q} \to \mathcal{L}_q : A \mapsto (H_1(A_{\mathbb{C}}, \mathbb{Z}), F(A, \pi_q)). \qquad \triangle$$

Proof. See [Del69, **7**]. □

Corollary 3.13. The number of isomorphism classes of ordinary Abelian surfaces with CM by $\mathcal{O}_K$ over $\mathbb{F}_q$ in the isogeny class of an ordinary Abelian varieties A satisfying **A.1-A.4** with CM by $\mathcal{O}_K$ equals the class number h_K, where $K = \mathrm{End}(A) \otimes \mathbb{Q}$. $\triangle$

Sketch of Proof: The functor $\mathcal{D}$ preserves dimensions and thus given an ordinary Abelian variety $A'/\mathbb{F}_q$ of dimension g we know that the $\mathrm{End}(A')$-module $\Lambda := H_1(A'_{\mathbb{C}}, \mathbb{Z})$ as a $\mathbb{Z}$-module is free of rank $2g$. Under the isomorphism $\mathrm{End}(A') \cong \mathcal{O}_K$ Λ becomes an $\mathcal{O}_K$-module. Now notice that $\Lambda \otimes \mathbb{Q}$ is a $2g$-dimensional vector space of $\mathbb{Q}$, but that it is also a vector space over $K = \mathcal{O}_K \otimes \mathbb{Q}$. This makes Λ into an 1-dimensional K-vector space. Notice that $\Lambda \subset K$ and thus Λ is a finitely-generated $\mathcal{O}_K$-submodule of K, in other words a fractional ideal of $\mathcal{O}_K$.

Using that isomorphisms of Abelian varieties $A_1 \to A_2$ correspond via the functor to the isomorphisms $\Lambda_1 \to (\lambda)\Lambda_2$ where $\Lambda_i = H_1(A_{i_{\mathbb{C}}}, \mathbb{Z})$ and $\lambda \in \mathrm{End}(A_1) \otimes \mathbb{Q} = \mathrm{End}(A_2) \otimes \mathbb{Q}$. Then counting Abelian varieties upto isomorphism is the same as counting fractional ideals upto principal ideals. $\triangle$

We make a step towards counting principally polarizable ordinary Abelian varieties with CM by $\mathcal{O}_K$. Howe refines in [How95] the correspondence of Deligne. He shows that we can extend isogenies, duals and polarisations from the category of ordinary Abelian varieties to Deligne pairs.

Definition 3.14. Let $(\Lambda_1, F_1), (\Lambda_2, F_2) \in \mathcal{L}_q$. A morphism $\alpha : (\Lambda_1, F_1) \to (\Lambda_2, F_2)$ is an *isogeny* if $\alpha \otimes \mathbb{Q} : \Lambda_1 \otimes \mathbb{Q} \to \Lambda_2 \otimes \mathbb{Q}$ is an isomorphism. $\triangle$

Definition 3.15. Let $(\Lambda, F) \in \mathcal{L}_q$. The *dual* is the pair $(\widehat{\Lambda}, \widehat{F})$ such that $\widehat{\Lambda}$ is the $\mathbb{Z}$-module $\mathrm{Hom}(\Lambda, \mathbb{Z})$ and $\widehat{F}$ is the endomorphism of $\widehat{\Lambda}$ such that for all $\phi \in \widehat{\Lambda}$ and all $x \in \Lambda$ we have $\widehat{F}(\phi(x)) = \phi(V(x))$, where V is the verschiebung of F. $\triangle$

We made a choice for an embedding $\epsilon : L \to \mathbb{C}$ and this induces a p-adic valuation on $\overline{\mathbb{Q}}$ as $\mathbb{Q}$ lies in $\overline{L}$ and thus also $\overline{\mathbb{Q}} \subset \overline{L}$. This valuation gives us a CM-type $\Phi = \{\phi : K \to \mathbb{C} | v(\phi(F)) > 0\}$ on K. Now let $\mathfrak{i} \in K$ be such that for all $\phi \in \Phi$ the image $\phi(\mathfrak{i})$ is positive imaginary. Observe that an isogeny $\lambda : (\Lambda, F) \to (\widehat{\Lambda}, \widehat{F})$ to the dual gives rise to a pairing $P : \Lambda \times \Lambda \to \mathbb{Z}$.

Definition 3.16. An isogeny $\lambda : (\Lambda, F) \to (\widehat{\Lambda}, \widehat{F})$ is a *polarization* if the induced pairing P is alternating and the pairing $(x, y) \mapsto P(\mathfrak{i}x, y)$ is symmetric and positive definite. △

Proposition 3.17 (Howe)**.** Let A be an ordinary Abelian variety over $\mathbb{F}_q$ with corresponding pair (Λ, F). Let γ be a morphism of ordinary Abelian varieties over $\mathbb{F}_q$. Then

(a) the morphism γ is an isogeny if and only if the corresponding morphism Γ in $\mathcal{L}_q$ is an isogeny,

(b) the dual variety $\widehat{A}$ corresponds via Deligne's equivalence to $(\widehat{\Lambda}, \widehat{F})$,

(c) under the assumption that γ is a morphism from A to $\widehat{A}$, the morphism γ is a polarization if and only if the morphism $\Gamma : (\Lambda, F) \to (\widehat{\Lambda}, \widehat{F})$ is a polarization. △

Proof. See [How95, Proposition 4.9], but be aware that the proof refers to a known fact, while the reference does not contain a proof. For details see [Mar17, Corollary 1.4.26]. □

Now we know that we can lift Abelian varieties to characteristic 0 and that the condition principally polarized is unaffected by lifting. Therefore, we are in a situation to give a proof for Theorem 3.9.

Proof of Theorem 3.9. In [Str10, Proposition I.5.3] (we advise the reader who will look up this reference to also read the accompanying Errata) Streng shows for the set $\mathbf{S}$ of pairs (Φ, A) of a CM-type Φ and a principally polarized Abelian Surfaces with CM by $\mathcal{O}_K$ and CM-type Φ the equality

$$\#\mathbf{S} = \frac{h_K}{h_{K_0}} \cdot \#(\mathcal{O}_{K_+})^\times / N_{K/K_+}(\mathcal{O}_K^\times).$$

Moreover, Streng gives also the the equality $\#(\mathcal{O}_{K_+})^\times / N_{K/K_+}(\mathcal{O}_K^\times) = 4$ [Str10, Corollary II.3.5.]. However, every Abelian surface with CM by $\mathcal{O}_K$ is found twice in $\mathbf{S}$ and the number of principally polarized ordinary Abelian varieties over $\mathbb{C}$ with CM by $\mathcal{O}_K$ is $2\frac{h_K}{h_{K_+}}$. By [Str10, Lemma III.2.1.] we know that there are two equivalence classes of CM-types and they are disjoint and Galois conjugate and thus of the same cardinality. Also remember that we made a choice for an embedding j when lifting, which gave us a CM-type. Therefore we have

$$\#\mathcal{A}(\mathbb{F}_q; f) = \frac{h_K}{h_{K_+}}.$$

□

4 The heuristics and the factors of our model

In this section we will discuss the heuristics introduced by Achter and Williams [AW15] and expand arguments for the heuristic factors at primes $l \neq p$. For the heuristic factors at ∞ and p we follow Achter and Williams.

In this section, let A satisfy **A.1-A.4** and let the polynomial $f_a(X) = X^4 + \alpha X^3 - \beta X^2 + \alpha q X + q^2$ be the characteristic polynomial of its (geometric) Frobenius endomorphism Frob_A.

4.1 The heuristic locally at prime $l \neq p$

Recall from Corollary 2.13 that the l-Tate modules $T_l(A)$ for $l \neq p$ are isomorphic as $\mathbb{Z}_l$-modules to $\mathbb{Z}_l^4$. The Frobenius endomorphism Frob_A induces an endomorphism π_q on $T_l(A)$ and initially this induced endomorphism can be identified by an element of $\mathrm{GL}_4(\mathbb{Z}_l)$ after choosing a basis. Moreover, after one chooses a symplectic basis for the Tate-module, which can be done as the Weil-pairing is symplectic, the polarisation forces π_q to lie in the subset $\mathrm{GSp}_4(\mathbb{Z}_l)^{(q)}$ of the subgroup $\mathrm{GSp}_4(\mathbb{Z}_l) \subset \mathrm{GL}_4(\mathbb{Z}_l)$.

The false assumption, knowingly made by Gekeler and we discussed in the Introduction, has been extended to the case of Abelian surfaces by Achter and Williams to assumption

> *The number of matrices in* $\mathrm{GSp}_4(\mathbb{F}_l)^{(q)}$ *with the given characteristic polynomial* f_A *equals the average of matrices per* q*-Weil polynomial, namely* $l^{-2}\#\mathrm{GSp}_4(\mathbb{F}_l)^{(q)}$.

This is again a false assumption, but upon the failure we analogously define the heuristic factors. Observe that this assumption is stated for $\mathbb{F}_l$ and not $\mathbb{Z}_l$. So before defining the factors we first look at the distribution of matrices with f_A in $\mathrm{GSp}_4(\mathbb{Z}_l)^{(q)}$ compared to the expected number of matrices with f_A in our assumption (of uniform distribution).

So we look at the size of $\mathrm{GSp}_4(\mathbb{Z}_l)^{(q)}$ divided by the number of possible characteristic polynomials $N(\mathbb{Z}_l) = \#\{f \in \mathbb{Z}_l[X] | \exists \alpha \in \mathrm{GSp}_4(R)^{(q)} : \mathrm{charpol}(\alpha) = f\}$, but that is only possible if the cardinalities are finite. Therefore, the expression

$$\frac{\text{“}\#\{\gamma \in \mathrm{GSp}_4(\mathbb{Z}_l)^{(q)} | f_\gamma = f_A\}\text{”}}{\#\,\mathrm{GSp}_4(\mathbb{Z}_l)^{(q)}/N(\mathbb{Z}_l)}$$

is nonsense and will not give a factor at l that tells us how far from uniform distribution the matrices with characteristic polynomial f_A are. Using that $\mathbb{Z}_l$ is a limit of a projective system of the finite rings $\mathbb{Z}/l^r\mathbb{Z}$, we can look at finite levels where the analogue of the expression is defined and then look at the limit

$$\lim_{r\to\infty} \frac{\#\{\gamma \in \mathrm{GSp}_4(\mathbb{Z}/l^r\mathbb{Z})^{(q)} | f_\gamma \equiv f_A \bmod l^r\}}{\#\,\mathrm{GSp}_4(\mathbb{Z}/l^r\mathbb{Z})^{(q)}/l^{2r}}. \tag{4.1}$$

One might wonder if this limit converges. We start with analysing this limit for nice primes l, namely those that do not divide $p\Delta_k$, for which we use the following definition.

Definition 4.1. Let M be a finitely generated R-module. An $\alpha \in \mathrm{End}_R(M)$ is *cyclic* if there is a $\mathbf{v} \in M$ such that $\{\mathbf{v}, \alpha\mathbf{v}, \alpha^2\mathbf{v}, \alpha^3\mathbf{v}, ...\}$ generates M as an R-module. Equivalently, if M is cyclic as an $R[X]$-module, where X acts as α on V. △

Proposition 4.2. For a prime $l \nmid p\Delta_K$ the limit (4.1) is attained at $r = 1$. △

Proof. We start by proving that the conjugacy class of $\gamma \in \mathrm{GSp}_4(\mathbb{Z}/l^r\mathbb{Z})$ such that $f_\gamma = f_A \pmod{l^r}$ is the only conjugacy class with f_A as characteristic polynomial. The assumption $l \nmid p\Delta_K$ forces $l \nmid \Delta_f$ as $\Delta_f = q^2\Delta_K$ [AW15, Lemma 2.2]. Therefore, $f \pmod{l}$ has distinct roots in $\overline{\mathbb{F}_l}$ and thus an element $\gamma \in \mathrm{GSp}_4(\mathbb{Z}/l^r\mathbb{Z})^{(q)}$ such that $f_\gamma \equiv f_A \pmod{l^r}$ is always cyclic. Moreover, every element in the conjugacy class of γ is cyclic, as conjugacy is a change of basis and for $(\mathbb{Z}/l^r\mathbb{Z})[X]$-modules being cyclic is independent of a choice of $\mathbb{Z}/l^r\mathbb{Z}$-basis. The reduction modulo l of every element of the conjugacy class $\mathcal{C}(\gamma)$ in $\mathrm{GSp}_4(\mathbb{Z}/l^r\mathbb{Z})$ is an element of the conjugacy class $\mathcal{C}(\gamma \bmod l)$ in $\mathrm{GSp}_4(\mathbb{Z}/l\mathbb{Z})$ of the reduction of γ.

All conjugacy classes in $\mathrm{GSp}_4(\mathbb{Z}/l\mathbb{Z})$ are described in table 2 of [Shi82], and they are not necessarily uniquely determined by the characteristic polynomials. Even though some characteristic polynomials correspond to multiple conjugacy classes, this does not happen for characteristic polynomials that have distinct roots. So the conjugacy class $\mathcal{C}(\gamma \bmod l)$ is uniquely determined by $f_\gamma \bmod l$. This is generalised by Lemma 6.4.5 of [Wil12], which shows that any lift of charpol$(\gamma \bmod l)$ to a polynomial in $\mathbb{Z}/l^r\mathbb{Z}$, and thus also charpol(γ), also uniquely determines one conjugacy class of $\mathrm{GSp}_4(\mathbb{Z}/l^r\mathbb{Z})$. Then we apply Proposition 6.4.6 of [Wil12] which states that for a cyclic matrix $\alpha \in \mathrm{GSp}_4(\mathbb{Z}/l^r\mathbb{Z})$ that

$$\#\mathcal{C}(\alpha) = l^{8(r-1)}\#\mathcal{C}(\alpha \bmod l).$$

Recall from Lemma 3.8 that $\#\,\mathrm{Sp}_4(\mathbb{Z}/l^r\mathbb{Z}) = l^{10(r-1)}\#\,\mathrm{Sp}_4(\mathbb{F}_l)$. Thus we find the desired result

$$\begin{aligned}\frac{\#\{\gamma' \in \mathrm{GSp}_4(\mathbb{Z}/l^r\mathbb{Z})^{(q)} | f_{\gamma'} \equiv f_A \bmod l^r\}}{l^{-2r}\#\,\mathrm{GSp}_4(\mathbb{Z}/l^r\mathbb{Z})^{(q)}} &= \frac{\#\mathcal{C}(\gamma)}{l^{-2r}\#\,\mathrm{GSp}_4(\mathbb{Z}/l^r\mathbb{Z})^{(q)}} \\ &= \frac{l^{8(r-1)}\#\mathcal{C}(\gamma \bmod l)}{l^{-2r}l^{10(r-1)}\#\,\mathrm{GSp}_4(\mathbb{F}_l)^{(q)}} \\ &= \frac{\#\mathcal{C}(\gamma \bmod l)}{l^{-2}\#\,\mathrm{GSp}_4(\mathbb{F}_l)^{(q)}} \\ &= \frac{\#\{\gamma' \in \mathrm{GSp}_4(\mathbb{F}_l)^{(q)} | f_{\gamma'} \equiv f_A \bmod l\}}{l^{-2}\#\,\mathrm{GSp}_4(\mathbb{F}_l)^{(q)}}.\end{aligned}$$

□

As this limit is attained at $r = 1$ (the situation $\mathbb{F}_l$) it also fits the assumption of Achter and Williams. If we had an analogous statement of Proposition 4.2 for the case $l \nmid p\Delta_K$, we would be able to define at this point our heuristic local factors at l. In previous work on this heuristic for elliptic curves by

Gekeler [Gek03] or on Abelian surfaces by Williams [Wil12] and Achter and Williams[AW15] there are cases $l \nmid p\Delta_K$ that contain non-cyclic elements and those form an obstruction in finding the analogue statement. For example, in situations where K is the splitting field of f and thus $\mathrm{Gal}(K/\mathbb{Q}) \cong C_4$ or $\mathrm{Gal}(K/\mathbb{Q}) \cong V_4$, then [Wil12, Corollary 8.0.2] shows that the limit

$$\lim_{r\to\infty} \frac{\#\{\text{cyclic } \gamma \in \mathrm{GSp}_4(\mathbb{Z}/l^r\mathbb{Z})^{(q)} | f_\gamma \equiv f_A \bmod l^r\}}{\#\,\mathrm{GSp}_4(\mathbb{Z}/l^r\mathbb{Z})^{(q)}/l^{2r}} \tag{4.2}$$

is attained at $r = 1$ and that it equals the desired ratio for all primes $l \neq p$. In addition, Williams shows that including non-cyclic elements does not give the desired ratio and therefore they restrict to cyclic matrices for $l \mid \Delta_K$. Achter and Williams did not give an argument for the restriction to cyclic elements other than that it results in the desired ratio. The following proposition will be

Proposition 4.3. Let A be an Abelian variety satisfying **A.1-A.4** and $\alpha = V_l(\mathrm{Frob}_A)$ be the endomorphism induced by the geometric Frobenius Frob_A on the l-Tate module T_lA. The characteristic polynomial f of α is also its minimal polynomial and α is cyclic. △

Proof. We know by Theorem 2.20 that the characteristic polynomial f of α is also the characteristic polynomial of Frob_A and $f \in \mathbb{Z}[X]$. Moreover, by **A.1** we know f is of degree 4. We can use the theory of lifting on (A, Frob_A) to $\mathbb{C}$ and obtain a pair $(A_{\mathbb{C}}, \pi)$. Note that by the irreducibility over $\mathbb{Q}$, assumed in **A.3**, the polynomial f is the minimal polynomial of π over $\mathbb{Q}$. Thus, f has distinct roots in $\mathbb{C}$ or consequently $\overline{\mathbb{Q}_l}$. Therefore, f is the minimal polynomial of α. Now since T_lA is an free $\mathbb{Z}_l[\alpha]$-module of rank 1, as the lattice of $A_{\mathbb{C}}$ is locally free of rang 1 over $\mathbb{Z}[\alpha]$. Now the equality of the polynomials implies that α is cyclic. □

As a result, non-cyclic elements will not arise as induced matrices by a Frobenius of Abelian varieties satisfying **A.1-A.4**. The argumentation in the proof of Proposition 4.2 only used the condition $l \nmid p\Delta_K$ to prove that only cyclic elements arose. An analogue argument can thus be applied for $l \neq p$ to the limit (4.2) in the case of non-Galois fields K and shows that the limit is attained at $r = 1$. So, we can now define heuristic factors that measure how far from uniform distribution the matrices with characteristic polynomial f_A are as follows.

Definition 4.4. Let A be an Abelian variety and f the characteristic polynomial of its Frobenius, satisfying **A.1-A.4**. For l a prime different from p, we define the *factor* $v_l(f)$ *of the local heuristic at* l as

$$v_l(f) := \frac{\#\{\text{cyclic } \gamma \in \mathrm{GSp}_4(\mathbb{F}_l)^{(q)} | f_\gamma \equiv f \bmod l\}}{\#\,\mathrm{GSp}_4(\mathbb{F}_l)^{(q)}/l^2}.$$

△

4.2 Defining the factor at ∞ and p

The local factors that have not been discussed are those at the places ∞ and p. We follow the choice made by Achter and Williams [AW15, 4.3.] to define the factor at ∞ as

$$v_\infty(f) := \frac{\sqrt{|\Delta_f|}}{(2\pi)^2 \operatorname{cond}(f)\sqrt{|\Delta_{f_+}|}},$$

where $\operatorname{cond}(f)$ is the index of $\mathbb{Z}[\pi_f]$ in $\mathbb{Z}[\pi_f, \overline{\pi_f}]$ for π_f the complex root of f as in **A.4**. We refer the reader who is interested in the heuristic behind this factor to [Wil12, Chapter 9, Appendix B].

For the factor at p we also follow the choices made by Achter and Williams [AW15, 4.3.] and define it as

$$v_p(f) := \frac{\#\{\text{semisimple } \gamma \in \mathrm{GSp}_4(\mathbb{F}_p)^{(\beta^2)} | f_\gamma \equiv (X^2 + \alpha X - \beta)^2 \bmod p\}}{\#\,\mathrm{GSp}_4(\mathbb{F}_p)^{(\beta^2)}/p^2}.$$

For the heuristic behind this factor we refer to [AW15, 4.3] and for more details on p-torsion to [MvdG11, Chapters 5.2 & 10.2].

5 Factorising the analytic class formula

Given an Abelian variety A over $\mathbb{F}_q$ satisfying **A.1-A.4**, where $q = p^n$. Let f_A be the characteristic polynomial of the geometric Frobenius. As discussed is $K = \mathbb{Q}[X]/(f_A(X))$ a CM-field, so it has a maximal real subfield which we denote as K_+. We saw in Section 3.3 that the number of objects in the isogeny class of A is given by the quotient of class numbers $\frac{h_K}{h_{K_+}}$.

For an arbitrary number field L let Δ_L be its discriminant over $\mathbb{Q}$, $\mathrm{Reg}(L)$ be the regulator, $\omega(L) := \#\mu(L)$ be the number of roots of unity , $r_1(L)$ be the number of real embeddings of L in $\mathbb{C}$, $r_2(L)$ be half the number of complex embeddings L in $\mathbb{C}$ and $\zeta_L(s)$ the Dedekind zeta function of L. Now we get the class number of L via the analytic class number formula

$$h_L = \frac{\omega(L)\sqrt{|\Delta_L|}}{\mathrm{Reg}(L)2^{r_1(L)}(2\pi)^{r_2(L)}} \lim_{s\to 1}(s-1)\zeta_L(s). \tag{5.1}$$

Using the norm map $N_{L/\mathbb{Q}}$ of L over $\mathbb{Q}$, for $\Re(s) > 1$ the Dedekind zeta function $\zeta_L(s)$ can be written as the Euler product over the primes in $\mathcal{O}_L$ given by

$$\prod_{\mathfrak{l}\in \mathrm{Spec}(\mathcal{O}_L)} \frac{1}{1 - N_{L/\mathbb{Q}}(\mathfrak{l})^{-s}}. \tag{5.2}$$

As we are interested in $\frac{h_K}{h_{K_+}}$ we also are interested in the quotient $\frac{\zeta_K(s)}{\zeta_{K_+}(s)}$ of the Riemann zeta functions. Notice that by the class number formula the function $\frac{\zeta_K(s)}{\zeta_{K_+}(s)}$ converges for $s \to 1$. From Wintner [Win46, **6.**] we obtain the fact that

$$\prod_{l \text{ prime}} \frac{\prod_{\mathfrak{l}|l;\mathfrak{l}\subset\mathcal{O}_K}(1 - N_{K/\mathbb{Q}}(\mathfrak{l})^{-1})}{(1-l^{-1})}$$

and

$$\prod_{l \text{ prime}} \frac{\prod_{\mathfrak{l}|l;\mathfrak{l}\subset\mathcal{O}_{K_+}}(1 - N_{K_+/\mathbb{Q}}(\mathfrak{l})^{-1})}{(1-l^{-1})}$$

both converge and respectively equal $\lim_{s\to 1}\frac{\zeta_K(s)}{\zeta_{\mathbb{Q}}(s)}$ and $\lim_{s\to 1}\frac{\zeta_K(s)}{\zeta_{\mathbb{Q}}(s)}$.

We use the above given factorisations into prime parts to define factors for the quotient $\frac{\zeta_K(s)}{\zeta_{K_+}(s)}\,\zeta_{\mathbb{Q}}$ which can easily be related to the factors of the heuristics.

Definition 5.1. The *local factor of the quotient of the class numbers* at a rational prime l we define as

$$v_l(K) := \frac{\prod_{\mathfrak{l}|l;\mathfrak{l}\subset\mathcal{O}_K}(1 - N_{K/\mathbb{Q}}(\mathfrak{l})^{-1})}{\prod_{\mathfrak{l}|l;\mathfrak{l}\subset\mathcal{O}_{K_+}}(1 - N_{K_+/\mathbb{Q}}(\mathfrak{l})^{-1})}.$$

The analytic class number formula (5.1) has other factors than the zeta function, those factors we collect in the definition of the *local factor of the quotient of the*

class numbers at the place ∞, which we define as

$$\begin{aligned} v_\infty(K) &:= \frac{\omega(K)2^{r_1(K_+)}(2\pi)^{r_2(K_+)}\operatorname{Reg}(K_+)\sqrt{|\Delta_K|}}{\omega(K_+)2^{r_1(K)}(2\pi)^{r_2(K)}\operatorname{Reg}(K)\sqrt{|\Delta_{K_+}|}} \\ &= \omega(K)\frac{4\operatorname{Reg}(K_+)\sqrt{|\Delta_K|}}{2(2\pi)^2\operatorname{Reg}(K)\sqrt{|\Delta_{K_+}|}}. \end{aligned}$$

△

6 Results

Recall we defined A as an Abelian surface over $\mathbb{F}_q$ satisfying **A.1-A.4**, where $q = p^n$ and f_A be the characteristic polynomial of the geometric Frobenius and K to be the CM field $\mathbb{Q}[X]/(f_A(X))$ with maximal totally real field K_+. We defined in previous sections the local factor of the quotient of the class numbers and the factor of the local heuristic. We will show that the factors $v_l(K), v_l(f_A)$ agree for any place $l \neq 2$. In order to determine the factor of the local heuristic at l, we will group the conjugacy classes of $\mathrm{GSp}_4(\mathbb{F}_l)$ as some factors $v_l(f)$ are dependent on two classes.

6.1 Classification of the conjugacy classes

The conjugacy classes in $\mathrm{GSp}_4(\mathbb{F}_l)$ are fully described in Shinoda [Shi82] and Breeding [Bre15] for odd primes l.

Definition 6.1. A *semisimple type* is a letter from the alphabet $\{\mathbf{A}, \mathbf{B}, ..., \mathbf{L}\}$. △

Let α be an element in a conjugacy class $\mathcal{C}$ of $\mathrm{GSp}_4(\mathbb{F}_l)$. We will look at the factorisation of the characteristic polynomial f_α of α and the multiplier $m_\alpha \in \mathbb{F}_l$, which is defined by the relation $m_\alpha J = \alpha^t J \alpha$. Let $a_\alpha, ..., d_\alpha \in \overline{\mathbb{F}_l}$ be such that $m_\alpha = a_\alpha d_\alpha = b_\alpha c_\alpha$ and $f_\alpha = (X - a_\alpha)(X - b_\alpha)(X - c_\alpha)(X - d_\alpha) \in \mathbb{F}_l[X]$.

Table 1: Defining the 11 semisimple types of $\mathrm{GSp}_4(\mathbb{F}_l)$.

Semisimple type	Factorisation data of f
A	$a = b = c = d \in \mathbb{F}_l^\times$
B	$a = -b = -c = d \in \mathbb{F}_l^\times$
C	$a = -b = -c = d \in \mathbb{F}_{l^2}^\times : a^{l-1} = -1$
D	$a = b, c = d \in \mathbb{F}_l^\times : a \neq c$
E	$\exists e \in \mathbb{F}_l^\times \setminus \{\pm 1\}; a = eb = ec = de^2 \in \mathbb{F}_l^\times$
F	$a = c \in \mathbb{F}_{l^2}^\times \setminus \mathbb{F}_l^\times; b = d = a^l$
G	$\exists e \in \mathbb{F}_{l^2}^\times \setminus \{\pm 1\} : e^{l+1} = 1; a = d \in \mathbb{F}_l^\times; b = ae; c = ae^{-1}$
H	$a, b, c, d \in \mathbb{F}_l^\times : ad = bc, \#\{a, b, c, d\} = 4$
I	$a \in \mathbb{F}_{l^2}^\times \setminus \mathbb{F}_l^\times; e \in \mathbb{F}_l^\times \setminus \{a^2, a^{l+1}\}; b = a^l; c = a^{-l}e; d = a^{-1}e$
J	$a \in \mathbb{F}_l^\times, b \in \mathbb{F}_{l^2}^\times \setminus \mathbb{F}_l^\times : a^2 \neq b^{l+1}; c = b^l; d = a^{-1}b^{l+1}$
K	$a^{l-1} \neq \pm 1, b \in \mathbb{F}_{l^4}^\times : b^{(l-1)(l^2+1)=1}; a = b^l; c = b^{l^2}; d = b^{l^3}$
L	$a, b \in \mathbb{F}_{l^2}^\times \setminus \mathbb{F}_l^\times : a \neq b, a \neq b^l, b \neq a^l, a^{l+1} = b^{l+1}; c = b^l; d = a^l$

Lemma 6.2. For any primes $l > 3$, we have a map from the set of conjugacy classes in $\mathrm{GSp}_4(\mathbb{F}_l)$ to semisimple types that is defined as follows. For a conjugacy class $\mathcal{C}$, let $(a_\alpha, ..., d_\alpha)$ be a 4-tuple of the roots of the characteristic polynomial f_α for an $\alpha \in \mathcal{C}$ such that $m_\alpha = a_\alpha d_\alpha = b_\alpha c_\alpha$, this tuple is sent to a semisimple type via Table 1.

For $l = 3$, there is an analogous map from the set of conjugacy classes in $\mathrm{GSp}_4(\mathbb{F}_l)$ to the set of semisimple types other then **E** and **H**. △

Proof. All elements in a conjugacy class have the same characteristic polynomial, hence the 4-tuple of roots up to reordering such that $ad = m_\alpha = bc$ is independent of the choice of α in the class. Moreover, the factorisation data in the different rows of Table 1 are chosen such that they have no overlap and cover all cases of a, b, c, d with $ad = bc$ and $f \in \mathbb{F}_l[X]$. Therefore, any permutation σ on the roots such that the product of the first and the last and the product of the second and the third root both still equal m_α, does not affects the row of the table. □

Remark 6.3. *Shinoda [Shi80, Theorem 1.18] and Breeding [Bre11] both give a method to determine the conjugacy classes. Based upon these results all possible factorisations are given in Table 1 and for every semisimple type there is a conjugacy class for primes $l > 3$. For $l = 3$ there are no classes of semisimple type* **E** *or* **H***, but for all other semisimple types there is a conjugacy class of that type. Therefore, the maps of Lemma 6.2 are surjective.* △

Definition 6.4. Let f be a polynomial such that there is a matrix $\alpha \in \mathrm{GSp}_4(\mathbb{F}_l)$ such that f is the characteristic polynomial of α and $\mathcal{C}$ the conjugacy class of α and let m_α be the multiplier of α. We say that the pair (f, m_α) (or the matrix α or the conjugacy class $\mathcal{C}$) is of *semisimple type* $\mathcal{L}$ for $\mathcal{L} \in \{\mathbf{A}, \mathbf{B}, ..., \mathbf{L}\}$ if $\mathcal{C}$ maps to $\mathcal{L}$ via the map of Lemma 6.2. △

Remark 6.5. *As discussed in section 4.1, the conjugacy classes of* $\mathrm{GSp}_4(\mathbb{F}_l)$*, are either cyclic or non-cyclic. Unfortunately, there are cyclic and non-cyclic conjugacy classes that have the same semisimple type. For example, of the two conjugacy classes with characteristic polynomial $X^4 - 2(q+1)X^3 + (4q + q^2 + 1)X^2 - 2q(q+1)X + q^2$ and multiplier q represented by*

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & q & 0 \\ 0 & 0 & 0 & q \end{pmatrix} \qquad \textit{and} \qquad \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & q & -q \\ 0 & 0 & 0 & q \end{pmatrix}.$$

The first matrix has minimal polynomial $X^2 - (q+1)X + q$ and the second matrix has minimal polynomial $X^4 - 2(q+1)X^3 + (4q + q^2 + 1)X^2 - 2q(q+1)X + q^2$, hence the first is non-cyclic and the second one is cyclic. △

Definition 6.6. A *conjugacy type* is a symbol appearing in the first column of Table 2, consisting of a semisimple type and one or two digits. △

For $\mathcal{L} \in \{\mathbf{A}, \mathbf{B}, ..., \mathbf{L}\}$, let $d_\mathcal{L}$ be the set of diagonal matrices $d_{\mathcal{L},(a,b,c,d)}$ with diagonal elements $a, b, c, d \in \overline{\mathbb{F}_l}$ such that the matrix $\mathcal{L}, (a, b, c, d)$ is an element in $\mathrm{GSp}_4(\mathbb{F}_l)$ of semisimple type $\mathcal{L}$.

We define also the upper-diagonal matrices

$$u_1(t) := \begin{pmatrix} 1 & t & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -t \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$u_2(t) := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & t & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$u_3(t) := \begin{pmatrix} 1 & 0 & t & 0 \\ 0 & 1 & 0 & t \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \text{ and}$$

$$u_4(t) := \begin{pmatrix} 1 & 0 & 0 & t \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

These matrices we will use to distinguish between some conjugacy classes of the same semisimple type.

Definition 6.7. The multiplication of a set $d_{\mathcal{L}}$ of diagonal matrices and a matrix $\alpha \in \mathrm{Sp}_4(\mathbb{F}_l)$ we define as the set $\{d \cdot \alpha | d \in d_{\mathcal{L}}\}$. Moreover, the sets in the second column of Table 2 we will refer to as the *indicator sets*. △

Lemma 6.8. For every indicator set D, there is a map ϕ_D from D to the set of conjugacy classes of $\mathrm{GSp}_4(\mathbb{F}_l)$ defined by sending α to it's conjugacy class in $\mathrm{GSp}_4(\overline{\mathbb{F}_l})$ and then intersection this class to $\mathrm{GSp}_4(\mathbb{F}_l)$. Two elements of D are sent to the same class if and only if they have the same characteristic polynomial and multiplier.

For two indicator sets D_1, D_2 the intersection $\phi_{D_1}(D_1) \cap \phi_{D_2}(D_2)$ of the images is empty or $D_1 = D_2$. Moreover, the union of the images $\phi_D(D)$ over all indicator sets D is $\mathrm{GSp}_4(\mathbb{F}_l)$. △

Proof. Both Shinoda [Shi80] and Breeding [Bre15] determined all conjugacy classes in $\mathrm{GSp}_4(\mathbb{F}_l)$ and by their classifications these maps ϕ_D are well-defined.

The if part of the equivalence is clear and for the only if part we compared number of class per conjugacy type. It turns out that this only depends on the semisimple type of the conjugacy class and we used Shinoda [Shi80, Table 1] to obtain the number of classes. The number of conjugacy class per conjugacy type is minimal in the sense that matrices conjugate only if there is an permutation $\{\sigma(a), \sigma(b), \sigma(c), \sigma(d)\}$of the (ordered) coefficients $\{a, b, c, d\}$ such that $\sigma(a)\sigma(d) = \sigma(b)\sigma(c) = ad = bc$. Thereby proving the only if part.

That the intersection of the images are empty follows as the characteristic polynomial a multiplier doesn't agree for two different conjugacy types.

Table 2: Defining the conjugacy types of $\mathrm{GSp}_4(\mathbb{F}_l)$.

Conjugacy type	Indicator set	Order of the centralizer	Cyclic?
$\mathbf{A}_0$	$d_{\mathbf{A}}$	$l^4(l-1)(l^2-1)(l^4-1)$	$\times$
$\mathbf{A}_1$	$d_{\mathbf{A}}u_4(1)$	$l^4(l-1)(l^2-1)$	$\times$
$\mathbf{A}_{21}$	$d_{\mathbf{A}}u_3(1)$	$2l^3(l-1)^2$	$\times$
$\mathbf{A}_{22}$	$d_{\mathbf{A}}u_2(1)u_4(-\tau)$	$2l^3(l^2-1)$	$\times$
$\mathbf{A}_3$	$d_{\mathbf{A}}u_1(1)u_2(1)$	$l^2(l-1)$	✓
$\mathbf{B}_0$	$d_{\mathbf{B}}$	$l^2(l-1)(l^2-1)^2$	$\times$
$\mathbf{B}_1$	$d_{\mathbf{B}}u_4(1)$	$l^2(l-1)(l^2-1)$	$\times$
$\mathbf{B}_2$	$d_{\mathbf{B}}u_2(1)$	$l^2(l-1)(l^2-1)$	$\times$
$\mathbf{B}_{31}$	$d_{\mathbf{B}}u_2(1)u_4(1)$	$2l^2(l-1)$	✓
$\mathbf{B}_{32}$	$d_{\mathbf{B}}u_2(1)u_4(\tau)$	$2l^2(l-1)$	✓
$\mathbf{C}_0$	$d_{\mathbf{C}}$	$l^2(l-1)(l^4-1)$	$\times$
$\mathbf{C}_{11}$	$d_{\mathbf{C}}u_2(1)u_4(1)$	$2l^2(l-1)$	✓
$\mathbf{C}_{12}$	$d_{\mathbf{C}}u_2(\tau_2)u_4(\tau_2^l)$	$2l^2(l-1)$	✓
$\mathbf{D}_0$	$d_{\mathbf{D}}$	$l(l-1)^2(l^2-1)$	$\times$
$\mathbf{D}_1$	$d_{\mathbf{D}}u_1(1)$	$l(l-1)^2$	✓
$\mathbf{E}_0$	$d_{\mathbf{E}}$	$l(l-1)^2(l^2-1)$	$\times$
$\mathbf{E}_1$	$d_{\mathbf{E}}u_2(1)$	$l(l-1)^2$	✓
$\mathbf{F}_0$	$d_{\mathbf{F}}$	$l(l^2-1)^2$	$\times$
$\mathbf{F}_1$	$d_{\mathbf{F}}u_3(1)$	$l(l^2-1)$	✓
$\mathbf{G}_0$	$d_{\mathbf{G}}$	$l(l^2-1)^2$	$\times$
$\mathbf{G}_1$	$d_{\mathbf{G}}u_4(1)$	$l(l^2-1)$	✓
$\mathbf{H}_0$	$d_{\mathbf{H}}$	$(l-1)^3$	✓
$\mathbf{I}_0$	$d_{\mathbf{I}}$	$(l+1)(l-1)^2$	✓
$\mathbf{J}_0$	$d_{\mathbf{J}}$	$(l+1)(l-1)^2$	✓
$\mathbf{K}_0$	$d_{\mathbf{K}}$	$(l-1)(l^2+1)$	✓
$\mathbf{L}_0$	$d_{\mathbf{L}}$	$(l-1)(l+1)^2$	✓

Note: τ (resp. τ_2) is a fixed non-square of $\mathbb{F}_l^\times$ (resp. $\mathbb{F}_{l^2}^\times$).

That the union equals $\mathrm{GSp}_4(\mathbb{F}_l)$ can be seen also comparing the size. The combined size of the image of the indicator sets given in the second column of Table 2 can be counted by only looking at conjugacy classes of type $\mathbf{A_0}, \mathbf{B_0}, ..., \mathbf{L_0}$ as it is determined by the semisimple type. Thus we find that the combined size of the image of the indicator sets is

$$\begin{aligned}
&5 \cdot (\#\phi_{\mathbf{A_0}}(\mathbf{A_0}) + \#\phi_{\mathbf{B_0}}(\mathbf{B_0})) + 3 \cdot \#\phi_{\mathbf{C_0}}(\mathbf{C_0}) \\
&+2 \sum_{\mathcal{I} \in \{\mathbf{D_0}, \mathbf{E_0}, \mathbf{F_0}, \mathbf{G_0}\}} \#\phi_{\mathcal{I}}(\mathcal{I}) + \sum_{\mathcal{I} \in \{\mathbf{H_0}, \mathbf{I_0}, \mathbf{J_0}, \mathbf{K_0}, \mathbf{L_0}\}} \#\phi_{\mathcal{I}}(\mathcal{I}) \\
&= 5(l-1) + \frac{5(l-1)}{2} + \frac{3(l-1)}{2} \\
&+ (l-1)(l-2) + (l-1)(l-3) + l(l-1) + (l-1)^2 \\
&+ \frac{(l-1)(l-3)^2}{8} + \frac{(l-1)(l^2-2l-1)}{4} + \frac{(l-1)^3}{4} + \frac{(l-1)(l^2-1)}{4} + \frac{(l-1)^3}{8} \\
&= (l-1)(l^2+2l+4),
\end{aligned}$$

which is the total number of conjugacy classes as shown by Shinoda [Shi80, Proposition 1.5]. □

Definition 6.9. For a matrix α in $\mathrm{GSp}_4(\mathbb{F}_l)$ let D be the indicator set such that there exists a $d \in D$ for which $\phi_D(d)$ is the conjugacy class of α. We say that α (or its conjugacy class $\mathcal{C}$) is of the *conjugacy type* corresponding to D as given in Table 2 and say that d is the *conjugacy type indicator* of α. △

By checking if the minimal polynomial equals the characteristic polynomial of the conjugacy type indicator of a conjugacy class we know if the class is (non-)cyclic, as we did in Remark 6.5. Using the same method we found that the classes of conjugacy type $\mathbf{A}_0, \mathbf{A}_1, \mathbf{A}_{21}, \mathbf{A}_{22}, \mathbf{B}_0, \mathbf{B}_1, \mathbf{B}_2, \mathbf{C}_0, \mathbf{D}_0, \mathbf{E}_0, \mathbf{F}_0$ and $\mathbf{G}_0$ are all the non-cyclic classes and this information we also included in Table 2. By Proposition 4.3 we do not have to further consider the classes of these conjugacy types for our calculations of the factors at $l \notin \{2, p, \infty\}$. Among the remaining cyclic conjugacy classes, the classes of type $\mathbf{H}_0, \mathbf{I}_0, \mathbf{J}_0, \mathbf{K}_0, \mathbf{L}_0$ are regular, that is $f \bmod l$ splits in distinct irreducible polynomials. Hence, in the regular case the prime l is unramified in the extension K over $\mathbb{Q}$, contrary to expectation it can still be difficult to differentiate using (only) the characteristic polynomial between some cases as we will demonstrate in the following example.

Example 6.10. Let γ be of type $\mathbf{L}_0$. Then the characteristic polynomial f_γ of γ splits after reduction modulo l in two distinct quadratic divisors in $\mathbb{F}_l[X]$. But for δ of type $\mathbf{I}_0$ the characteristic polynomial f_δ of δ also splits after reduction modulo l in two distinct quadratic divisors in $\mathbb{F}_l[X]$.

This implies that in both cases that above l there are two distinct primes $\mathfrak{l}_1, \mathfrak{l}_2 \subset \mathcal{O}_K$ such that $l\mathcal{O}_K = \mathfrak{l}_1\mathfrak{l}_2$ and $\mathcal{O}_K/\mathfrak{l}_i \cong \mathbb{F}_{l^2}$ for $i = 1, 2$. We can make a distinction between the two types if we look at the behaviour at K_+. In the case of $\mathbf{I}_0$ we know it is of semisimple type $\mathbf{I}$ and thus $f_\delta \bmod l$ splits over $\overline{\mathbb{F}_l}$ as $(X-a)(X-a^l)(X-a^{-l}e)(X-a^{-1}e)$ with $a \in \mathbb{F}_{l^2}^\times \setminus \mathbb{F}_l^\times$ and $e =$

$m_\delta \in \mathbb{F}_l^\times \setminus \{a^2, a^{l+1}\}$. Thus $f_\delta \pmod l$ is given by $\alpha_\delta = a + a^l + a^{-1}e + a^{-l}e$, $\beta_\delta = a^{l+1} + e^2a^{-l-1} + 2e + ea^{l-1} + ea^{1-l}$ in the standard form

$$f_\delta(X) \bmod l = X^4 + \alpha_\delta X^3 + \beta_\delta X^3 + \alpha_\delta m_\delta X^2 + m_\delta^2.$$

Now we can uniquely find a polynomial $f_{\delta,+}$ such that $f_{\delta,+} \equiv f_+ \pmod l$, since the coefficients of f_+ can be obtained from coefficients of f and the multiplier m_δ of δ. As discussed in Section 3.1 we find

$$f_{\delta,+} \bmod l = X^2 + \alpha_\delta X + \beta_\delta - 2m_\delta = (X - (a + ea^{-1}))(X - (a^l + ea^{-l})).$$

Notice that if $(a + ea^{-1})^l = a + ea^{-1}$ then or the order $\mathbb{Z}[\pi, \overline{\pi}]$ would not be maximal or K_+ would ramify. By **A.4** is $\mathbb{Z}[\pi, \overline{\pi}]$ maximal and the field K is not ramified at l, as in this example f_A is the product of two distinct irreducible quadratic polynomials modulo l. Thus the assumption $(a + ea^{-1})^l = a + ea^{-1}$ gives a contradiction and thus $a + ea^{-1} \notin \mathbb{F}_l$. Therefore, $f_{\delta,+}$ does not split after reducing modulo l. With an analogous argument we find that $f_\gamma \bmod l$ is given by $\alpha_\gamma = a + a^l + b + b^l, \beta_\gamma = 2a^{l+1} + ab + (ab)^l$ and $m_\gamma = a + a^l$ for $a, b \in \mathbb{F}_{l^2}^\times \setminus \mathbb{F}_l^\times$ such that $a \neq b, a \neq b^l, b \neq a^l$ and $a^{l+1} = b^{l+1}$. Therefore, $f_{\gamma,+}(X) \bmod l = (X - (a^l + a))(X - (b^l + b))$ and thus does split in $\mathbb{F}_l[X]$, since $(a^l + a)^l = a^{l^2} + a^l = a + a^l$ and also $(b^l + b)^l = b + b^l$. △

Similar to the previous example we determined the splitting behaviour of the characteristic polynomials of the other cyclic conjugacy classes and the induced quadratic polynomials. The information is collected in Table 3.

Notation 6.11. The splitting behaviour of a polynomial f we will denote as $[m : (e_i)_{i=1}^m : (d_i)_{i=1}^m]$, where m is the number of unique irreducible factors of f, e_i the number of times the i^{th} irreducible factor appears in the factorisation of f and d_i the degree of the i^{th} irreducible factor of f. Notice that $\deg(f) = \sum_{i=1}^m e_i d_i$. △

We want to compare splitting behaviour and the size of the conjugacy classes with the decomposition of l in K and K_+ and for this we collected from Table 1 in [KS15] and Table 3.5.1 of[GL12] a classification of the splitting behaviour of degree 4 CM-fields that are not Galois extensions over $\mathbb{Q}$. These results tell us that factorisations in Table 3 are the ones that can occur for primes in non-Galois quartic field extensions K over $\mathbb{Q}$. If this was not the case the factor of the local heuristic at l would certainly be different from the local factor of the quotient of the class numbers for a field with the missing factorisation.

With the factorisation data from Table 3 and the order of the centralizer from 2 we can determine the factor of the local heuristic at l for a given $f \bmod l$ and $f_+ \bmod l$ or equivalently on $f \bmod l$ and on the multiplier $q \bmod l$. We would have some conflicted cases if we only would look at the factorisation $f \bmod l$, as discussed in Example 6.10 for classes of conjugacy type $\mathbf{I}_0$ and $\mathbf{L}_0$. Also we have a similar problem between classes of the three conjugacy types $\mathbf{B}_{31}, \mathbf{B}_{32}$ and $\mathbf{D}_1$ or classes of the three conjugacy types $\mathbf{C}_{11}, \mathbf{C}_{12}$ and $\mathbf{F}_1$.

Lemma 6.12. Let $\gamma, \delta \in \mathrm{GSp}_4(\mathbb{F}_l)^{(q)}$ be cyclic matrices such that the characteristic polynomial f_δ of δ equals the characteristic polynomial f_γ of γ.

Table 3: Behaviour of a characteristic polynomial per cyclic conjugacy type.

Conjugacy type	$f \mod l$	$f_+ \mod l$
$\mathbf{A}_3$	$[1:4:1]$	$[1:2:1]$
$\mathbf{B}_{31}$	$[2:(2,2):(1,1)]$	$[2:(1,1):(1,1)]$
$\mathbf{B}_{32}$	$[2:(2,2):(1,1)]$	$[2:(1,1):(1,1)]$
$\mathbf{C}_{11}$	$[1:2:2]$	$[1:1:2]$
$\mathbf{C}_{12}$	$[1:2:2]$	$[1:1:2]$
$\mathbf{D}_1$	$[2:(2,2):(1,1)]$	$[1:2:1]$
$\mathbf{E}_1$	$[3:(2,1,1):(1,1,1)]$	$[2:(1,1):(1,1)]$
$\mathbf{F}_1$	$[1:2:2]$	$[1:2:1]$
$\mathbf{G}_1$	$[2:(2,1):(1,2)]$	$[2:(1,1):(1,1)]$
$\mathbf{H}_0$	$[4:(1)_{i=1}^4:(1)_{i=1}^4]$	$[2:(1,1):(1,1)]$
$\mathbf{I}_0$	$[2:(1,1):(2,2)]$	$[1:1:2]$
$\mathbf{J}_0$	$[3:(1,1,1):(2,1,1)]$	$[2:(1,1):(1,1)]$
$\mathbf{K}_0$	$[1:1:4]$	$[1:1:2]$
$\mathbf{L}_0$	$[2:(1,1):(2,2)]$	$[2:(1,1):(1,1)]$

If γ is of conjugacy type $\mathbf{A}_3, \mathbf{D}_1, \mathbf{E}_1, \mathbf{F}_1, \mathbf{G}_1, \mathbf{H}_0, \mathbf{I}_0, \mathbf{J}_0, \mathbf{K}_0$ or $\mathbf{L}_0$ then δ is in the same conjugacy class as γ. If γ is of conjugacy type $\mathbf{B}_{31}$ or $\mathbf{B}_{32}$ (resp. $\mathbf{C}_{11}$ or $\mathbf{C}_{12}$), then δ is an element of possibly two conjugacy classes, namely one of conjugacy type $\mathbf{B}_{31}$ (resp. $\mathbf{C}_{11}$) and one of conjugacy type $\mathbf{B}_{32}$ (resp. $\mathbf{C}_{12}$). $\triangle$

Proof. From Lemma 6.8 we obtain for two conjugacy classes $\mathcal{C}_1, \mathcal{C}_2$ of a given conjugacy type $\mathcal{T}$ the implication if their characteristic polynomials and their multipliers agree then $\mathcal{C}_1 = \mathcal{C}_2$. The matrices γ and δ are defined such that $m_\gamma \equiv m_\delta \equiv q \bmod l$. So under the assumption that $f_\gamma = f_\delta$ and thus we know that if δ and γ are of the same conjugacy type that they are conjugate.

For the conjugacy types $\mathbf{A}_3, \mathbf{E}_1, \mathbf{G}_1, \mathbf{H}_0, \mathbf{J}_0, \mathbf{K}_0$ Table 3 shows that the factorisation of f is unique for that class among all cyclic classes and thus δ has the same conjugacy type as γ and the result follows in these cases.

In Example 6.10 we discussed that the multiplier m and the characteristic polynomial $f = X^4 + \alpha X^3 + \beta X^2 + \alpha m X + m^2$ of an arbitrary element in $\mathrm{GSp}_4(\mathbb{F}_l)$ uniquely determine a quartic polynomial $f_+ = X^2 + \alpha X + \beta - 2m$. Recall that γ and δ both have multiplier q and the same characteristic polynomial f_γ by assumption, hence the unique quartic polynomial $f_{\gamma,+}$ of both elements is also equal. Thus if γ is of conjugacy type $\mathbf{D}_1, \mathbf{F}_1, \mathbf{I}_0, \mathbf{L}_0$ the factorisation of f_γ and $f_{\gamma,+}$ is uniquely determined by that conjugacy type, as shown in Table 3, and thus δ is of the same conjugacy type as γ and the result follows in these cases.

The only cases that have not been discussed are where γ is of conjugacy type $\mathbf{B}_{31}, \mathbf{B}_{32}, \mathbf{C}_{11}$ or $\mathbf{C}_{12}$. We first assume γ is of type $\mathbf{C}_{q1}$ or $\mathbf{C}_{12}$. Then the factorisation of f_γ and $f_{\gamma,+}$ is not unique for the conjugacy type of γ, as it corresponds to precisely two conjugacy types $\mathbf{C}_{11}$ and $\mathbf{C}_{12}$. Let $a \in \{\alpha \in \mathbb{F}_{l^2} | \alpha^{l-1} = -1\}$ be the element that is unique up to sign such that the roots of

f_γ are $a, -a$, both with multiplicity 2. Then let $b \in \mathbb{F}_{l^2}^\times$ be a non-square and observe that we have two elements

$$\gamma_1 = \begin{pmatrix} a & 0 & 0 & a \\ 0 & -a & -a & 0 \\ 0 & 0 & -a & 0 \\ 0 & 0 & 0 & a \end{pmatrix} \quad \text{and} \quad \gamma_2 = \begin{pmatrix} a & 0 & 0 & ab^l \\ 0 & -a & -ab & 0 \\ 0 & 0 & -a & 0 \\ 0 & 0 & 0 & a \end{pmatrix},$$

both not in $\mathrm{GSp}_4(\mathbb{F}_l)$, but there are $\gamma_1', \gamma_2' \in \mathrm{GSp}_4(\mathbb{F}_l)$ such that over $\overline{\mathbb{F}_l}$ the matrices γ_i and γ_i' are conjugate. Note that γ_1' is of type $\mathbf{C}_{11}$ and γ_2' is of type $\mathbf{C}_{12}$. Furthermore, the characteristic polynomial $f_{\gamma_i'}$ equals f_γ, hence δ is either an element of the conjugacy class of γ_1' or of the conjugacy class of γ_2'.

For $\mathbf{B}_{31}$ and $\mathbf{B}_{32}$ an analogous argument, but simpler proof as $\gamma_i \in \mathrm{GSp}_4(\mathbb{F}_l)$ and getting γ_i' is not even necessary in these cases. □

With this Lemma and Table 2 we will be able to compute the factor, as they tell us how many elements there are with a certain minimal polynomial and multiplier.

6.2 Comparison of the factors at odd primes

Recall that we defined A as an Abelian surface over the finite field $\mathbb{F}_q$ with f_A the characteristic polynomial of the geometric Frobenius satisfying **A.1-A.4**, $K = \mathbb{Q}[X]/(f_A(X))$ a CM field and $K_+ = \mathbb{Q}[X]/(f_+(X))$ the maximal totally real subfield.

Proposition 6.13. Let l be an odd prime. Then $v_l(K) = v_l(f_A)$. △

Proof. First assume l is different from p. If f_A is of semisimple type $\mathbf{B}$ or $\mathbf{C}$, then there are two conjugacy classes $\mathcal{C}_1, \mathcal{C}_2$ such that $f_{\mathcal{C}_i} = f \bmod l$ and $m_{\mathcal{C}_i} = q \bmod l$, namely one of conjugacy type $\mathbf{B}_{31}$ and one of conjugacy type $\mathbf{B}_{32}$ or respectively one of conjugacy type $\mathbf{C}_{11}$ and one of conjugacy type $\mathbf{C}_{12}$. Let $\mathcal{Z}_i$ be the centralizer of $\mathcal{C}_i$. Recall that the size of a conjugacy class $\mathcal{C}$ is the order of the group divided by the order of the centralizer $\mathcal{Z}$, hence

$$\frac{\#\mathcal{C}}{\#\,\mathrm{GSp}_4(\mathbb{F}_l)^{(q)} l^{-2}} = \frac{l^2 \#\,\mathrm{GSp}_4(\mathbb{F}_l)}{\#\mathcal{Z} \#\,\mathrm{GSp}_4(\mathbb{F}_l)^{(q)}} = \frac{l^2(l-1)}{\#\mathcal{Z}}.$$

Combining this with the result that the factor of the local heuristic at l is given by the sum over both conjugacy classes we find

$$v_l(f) = \sum_{i=1}^{2} \frac{\#\mathcal{C}_i}{\#\,\mathrm{GSp}_4(\mathbb{F}_l)^{(q)} l^{-2}} = \sum_{i=1}^{2} \frac{l^2(l-1)}{\#\mathcal{Z}(\delta_i)} = 2\frac{l^2(l-1)}{2l^2(l-1)} = 1.$$

We also know how f_A and f_+ factor modulo l and thus the local factor of the quotient of the class numbers is

$$v_l(K) = \begin{cases} \frac{(1-\frac{1}{l})^2}{(1-\frac{1}{l})^2} = 1 & \text{if the semisimple type of } (f_A, q) \text{ is } \mathbf{B}, \\ \frac{(1-\frac{1}{l^2})}{(1-\frac{1}{l^2})} = 1 & \text{if the semisimple type of } (f_A, q) \text{ is } \mathbf{C}. \end{cases}$$

For the remaining cases we only have one conjugacy class to determine the factor of the local heuristic at l and thus using Table 3 we find that

$$v_l(f) = \frac{\#\mathcal{C}}{\#\,\mathrm{GSp}_4(\mathbb{F}_l)^{(q)} l^{-2}}$$
$$= \begin{cases} \frac{l^2(l-1)}{l^2(l-1)} = 1 & \text{if the semisimple type of } (f_A, q) \text{ is } \mathbf{A}, \\ \frac{l^2(l-1)}{l(l-1)^2} = \frac{l}{l-1} & \text{if the semisimple type of } (f_A, q) \text{ is } \mathbf{D} \text{ or } \mathbf{E}, \\ \frac{l^2(l-1)}{l(l^2-1)} = \frac{l}{l+1} & \text{if the semisimple type of } (f_A, q) \text{ is } \mathbf{F} \text{ or } \mathbf{G}, \\ \frac{l^2(l-1)}{(l-1)^3} = \frac{l^2}{(l-1)^2} & \text{if the semisimple type of } (f_A, q) \text{ is } \mathbf{H}, \\ \frac{l^2(l-1)}{(l+1)(l-1)^2} = \frac{l^2}{l^2-1} & \text{if the semisimple type of } (f_A, q) \text{ is } \mathbf{I} \text{ or } \mathbf{J}, \\ \frac{l^2(l-1)}{(l^2+1)(l-1)} = \frac{l^2}{l^2+1} & \text{if the semisimple type of } (f_A, q) \text{ is } \mathbf{K}, \\ \frac{l^2(l-1)}{(l+1)^2(l-1)} = \frac{l^2}{(l+1)^2} & \text{if the semisimple type of } (f_A, q) \text{ is } \mathbf{L}. \end{cases}$$

For these case, we also know how f_A and f_+ factor modulo l and thus we know the local factor of the quotient of the class numbers

$$v_l(K) = \begin{cases} \frac{1-\frac{1}{l}}{(1-\frac{1}{l})} = 1 & \text{if the type is } \mathbf{A}, \\ \frac{1-\frac{1}{l}}{(1-\frac{1}{l})^2} = \frac{1}{\frac{l-1}{l}} = \frac{l}{l-1} & \text{if the type is } \mathbf{D}, \\ \frac{(1-\frac{1}{l})^2}{(1-\frac{1}{l})^3} = \frac{1}{\frac{l-1}{l}} = \frac{l}{l-1} & \text{if the type is } \mathbf{E}, \\ \frac{1-\frac{1}{l}}{(1-\frac{1}{l^2})} = \frac{\frac{l-1}{l}}{\frac{l^2-1}{l^2}} = \frac{l}{l+1} & \text{if the type is } \mathbf{F}, \\ \frac{(1-\frac{1}{l})^2}{(1-\frac{1}{l})(1-\frac{1}{l^2})} = \frac{\frac{l-1}{l}}{\frac{l^2-1}{l^2}} = \frac{l}{l+1} & \text{if the type is } \mathbf{G}, \\ \frac{(1-\frac{1}{l})^2}{(1-\frac{1}{l})^4} = \frac{1}{\frac{(l-1)^2}{l^2}} = \frac{l^2}{(l-1)^2} & \text{if the type is } \mathbf{H}, \\ \frac{1-\frac{1}{l^2}}{(1-\frac{1}{l^2})^2} = \frac{1}{\frac{l^2-1}{l^2}} = \frac{l^2}{l^2-1} & \text{if the type is } \mathbf{I}, \\ \frac{(1-\frac{1}{l})^2}{(1-\frac{1}{l^2})(1-\frac{1}{l})^2} = \frac{1}{\frac{l^2-1}{l^2}} = \frac{l^2}{l^2-1} & \text{if the type is } \mathbf{J}, \\ \frac{1-\frac{1}{l^2}}{1-\frac{1}{l^4}} = \frac{\frac{l^2-1}{l^2}}{\frac{l^4-1}{l^4}} = \frac{l^2}{l^2+1} & \text{if the type is } \mathbf{K}, \\ \frac{(1-\frac{1}{l})^2}{(1-\frac{1}{l^2})^2} = \frac{\frac{(l-1)^2}{l^2}}{\frac{(l^2-1)^2}{l^4}} = \frac{l^2}{(l+1)^2} & \text{if the type is } \mathbf{L}. \end{cases}$$

For $l > 3$ we see that the factors agree for every conjugacy class. For the prime $l = 3$ there are no conjugacy classes of semisimple type **E** and **H** and thus f_A does not factorize this way and there for we will not have to look at the result of $v_3(K)$ for semisimple type **E** and **H**. For all other semisimple types at $l = 3$ both factors agree.

For the case $l = p$, recall from Remark 3.5 and **A.1** that $f_A(X) = X^4 - \alpha X^3 + \beta X^2 - \alpha q X + q^2$ and $f_+(X) = X^2 - \alpha X + (\beta - 2q)$ with $\alpha, \beta \in \mathbb{Z}$ and β coprime to q, hence $f_A(X) \equiv f_+(X)X^2 \pmod{p}$ and $X \nmid f_+ \pmod{p}$. By **A.3** is K unramified at p, hence the ideal (p) in K_+ is either prime or has a factorisation into two distinct prime ideals $\mathfrak{p}_1\mathfrak{p}_2$.

If we assume that the ideal (p) is prime in K_+, then we know $f_+(X) \pmod p$ is irreducible and thus $f_+(X)X^2 \pmod p$ has an irreducible factor of degree 2 and multiplicity 1. Therefore, the prime ideal (p) in K has a factor that is a prime ideal $\mathfrak{P}_1$ with norm $N_{K/\mathbb{Q}}(\mathfrak{P}_1) = 2$. Moreover, since K is unramified at p and (p) is prime in K_+ we have that $(p) = \mathfrak{P}_1\mathfrak{P}_2$, where $\mathfrak{P}_1\mathfrak{P}_2$ are distinct prime ideals in K. Therefore we find $v_p(K) = \frac{p^2}{p^2-1}$, the same as in the $l \neq p$ situation where the factorisation behaviour is like a polynomial of semisimple type **I**. Recall that for $v_p(f_A)$ we followed Achter and Williams. They say in [AW15, Lemma 6.4] that the set of semisimple elements with characteristic polynomial $(f_+(X))^2 \pmod p$ has the same cardinality as a conjugacy class of semisimple type **I**, though no calculations were given and thus we have not verified the result.

Analogously, if we assume that the ideal $(p) = \mathfrak{p}_1\mathfrak{p}_2$ is not prime in K_+, we find that (p) has at least two distinct prime ideals of norm 1 of which one lies above $\mathfrak{p}_1$ and the other above $\mathfrak{p}_2$. Recall that K is unramified at p and thus $\mathfrak{p}_1$ and $\mathfrak{p}_2$ split in K/K_+ and thus in this case (p) is a product of four prime ideals in K. Therefore, $v_p(K) = \frac{p^2}{(p-1)^2}$ and again using [AW15, Lemma 6.4] of Achter and Williams that the set of semisimple elements with characteristic polynomial $(f_+(X))^2 \pmod p$ in this case has the same cardinality as a conjugacy class of semisimple type **H**, be aware that again no calculations were given. □

Theorem 6.14. Let A be an Abelian variety over a finite field $\mathbb{F}_q$ of characteristic p satisfying **A.1-A.4**. Then, up to a factor at the prime 2, the number of isomorphism classes of principally polarized Abelian surfaces over $\mathbb{F}_q$ isogenous to A, weighted by the inverse size of the automorphism group equals the product

$$v_\infty(f) \prod_{l \text{ odd prime}} v_l(f).$$

△

Proof. Theorem 3.9 shows that $\#\mathcal{A}(\mathbb{F}_q; f) = \frac{h_k}{hk_+}$. Recall that by the analytic class number formula the quotient of class numbers and the assumption we lay on the limits (Remark 5) $\frac{h_K}{h_{K_+}}$ can be written as

$$\frac{2^2\omega(K)\sqrt{|\Delta_K|}\operatorname{Reg}(K_+)}{(2\pi)^2\omega(K_+)\sqrt{|\Delta_{K_+}|}\operatorname{Reg}(K)} \prod_{l \text{ primes}} v_l(K).$$

Lemma 6.13 shows that the factors $v_l(k)$ and $v_l(f)$ for odd primes agree.

Using the fact that $\Delta_f = q^2\Delta_K, \Delta_{f_+} = \Delta_{K_+}$, $\operatorname{cond}(f) = q$ and [AW15, Lemma 6.5 & Theorem 7.1] we obtain the relation

$$v_\infty(f) = \frac{\sqrt{|\Delta_f|}}{(2\pi)^2 \operatorname{cond}(f)\sqrt{|\Delta_{f_+}|}} = \frac{4\operatorname{Reg}(K_+)\sqrt{|\Delta_K|}}{(2\pi)^2\omega(K_+)\operatorname{Reg}(K)\sqrt{|\Delta_{K_+}|}}.$$

Combining these results we find

$$\frac{\#\mathcal{A}(\mathbb{F}_q; f)}{\omega(K)} = v_\infty(f) v_2(K) \prod_{l \text{ odd prime}} v_l(f).$$

The automorphisms of an Abelian variety are the endomorphisms of degree 1 and these are the roots of unity in $\mathcal{O}_K$ and thus every Abelian variety with CM by $\mathcal{O}_K$ is weighted by the same factor $\omega(K)$. □

Remark 6.15. *With this result we are a rational factor (determined by the prime 2) away from $\#\mathcal{A}(\mathbb{F}_q; f)$. We expect that argument of the heuristic factor $v_l(f)$ can be extendend to $v_2(f)$ and with anogulous computation one should then find the equality $v_2(f) = v_2(K)$. For this computation one can obtain the conjugacy class for this case from Enomoto[Eno72] and the tables from Kilicer and Streng [KS15] and Goren and Lauter [GL12] used in this thesis also include information of the factorisation of the prime ideal* (2). △

References

[AW15] Jeffrey Achter and Cassandra Williams. Local heuristics and an exact formula for abelian surfaces over finite fields. *Canadian Mathematical Bulletin*, 58(4):673–691, 2015.

[Bre11] Jeffery Breeding, II. *Irreducible non-cuspidal characters of* $\mathrm{GSp}(4, Fq)$. PhD thesis, 2011. Thesis (Ph.D.)–The University of Oklahoma.

[Bre15] Jeffery Breeding, II. Irreducible characters of $\mathrm{GSp}(4, q)$ and dimensions of spaces of fixed vectors. *Ramanujan Journal*, 36(3):305–354, 2015.

[Del69] Pierre Deligne. Variétés abéliennes ordinaires sur un corps fini. *Inventiones Mathematicae*, 8:238–243, 1969.

[Eno72] Hikoe Enomoto. The characters of the finite symplectic group $\mathrm{Sp}(4, q)$, $q = 2^f$. *Osaka Journal of Mathematics*, 9:75–94, 1972.

[Gek03] Ernst-Ulrich Gekeler. Frobenius distributions of elliptic curves over finite prime fields. *International Mathematics Research Notices*, 2003(37):1999–2018, 2003.

[GL12] Eyal Z. Goren and Kristin E. Lauter. Genus 2 curves with complex multiplication. *International Mathematics Research Notices*, (5):1068–1142, 2012.

[Haz09] Michiel Hazewinkel. Witt vectors. I. In *Handbook of algebra. Vol. 6*, volume 6 of *Handb. Algebr.*, pages 319–472. Elsevier/North-Holland, Amsterdam, 2009.

[Hon68] Taira Honda. Isogeny classes of abelian varieties over finite fields. *Journal of the Mathematical Society of Japan*, 20(1-2):83–95, 1968.

[How95] Everett W. Howe. Principally polarized ordinary abelian varieties over finite fields. *Transactions of the American Mathematical Society*, 347(7):2361–2401, 1995.

[KS15] Pınar Kılıçer and Marco Streng. The CM class number one problem for curves of genus 2. *arXiv preprint arXiv:1511.04869*, 2015.

[LST64] Jonathan Lubin, Jean-Pierre Serre, and John Tate. Elliptic curves and formal group, 1964. Lecture notes prepared in connection with the seminars held at the Summer Institute on Algebraic Geometry, Whitney Estate, Woods Hole, Massachusetts.

[Mar17] Chloe Martindale. *Polarised Abelian varieties with complex multiplication.* PhD thesis, Leiden University, 2017. Draft of first chapters, retrieved from `http://pub.math.leidenuniv.nl/~martindalecr/` on 1 March 2017.

[Mil08] James S. Milne. Abelian varieties (v2.00), 2008. Retrieved from `www.jmilne.org/math/`.

[MvdG11] Ben Moonen and Gerard van der Geer. Abelian varieties. 2011.

[New72] Morris Newman. *Integral matrices*, volume 45. Academic Press, 1972.

[Oor08] Frans Oort. Abelian varieties over finite fields. In D. Kaledin and Y. Tschinkel, editors, *Higher-dimensional Geometry Over Finite Fields*, NATO Science for Peace and Security Series, chapter 5, pages 123–188. IOS Press, 2008.

[Shi80] Ken-ichi Shinoda. The characters of weil representations associated to finite fields. *Journal of Algebra*, 66(1):251–280, 1980.

[Shi82] Ken-ichi Shinoda. The characters of the finite conformal sympletctic group, $\mathrm{csp}(4, q)$. *Communications in Algebra*, 10(13):1369–1419, 1982.

[Sta] The Stacks Project Authors. *Stacks Project*. `http://stacks.math.columbia.edu` (retrieved at 2016-06-22).

[Str10] Marco Streng. *Complex multiplication of abelian surfaces*. PhD thesis, Leiden University, 2010.

[Tat66] John Tate. Endomorphisms of abelian varieties over finite fields. *Inventiones mathematicae*, 2(2):134–144, 1966.

[Wil12] Cassandra L. Williams. *Conjugacy classes of matrix groups over local rings and an application to the enumeration of abelian varieties*. PhD thesis, Colorado State University, 2012.

[Win46] Aurel Wintner. A factorization of the densities of the ideals in algebraic number fields. *American Journal of Mathematics*, 68:273–284, 1946.

A Geometry Appendix

Definition A.1. A *scheme* is a locally ringed space X such that for every point $x \in X$ there is an open neighbourhood U_x, such that U_x is isomorphic as a locally ringed space to the spectrum of a commutative ring. △

Definition A.2. Let X be a scheme. Then a scheme Y is a *closed subscheme* if the topological space $|Y|$ is a closed set of $|X|$ and the morphism $\mathcal{O}_X \to i_*\mathcal{O}_Y$ is surjective, where $i : Y \to X$ is the inclusion map. △

Definition A.3. A *group scheme over a scheme S*, or abbreviated an *S-group scheme*, is an S-scheme X with structure morphism $\sigma : X \to S$ together with S-morphisms

$$m : X \times X \to X, \qquad i : X \to X \qquad \text{and} \qquad e : S \to X,$$

such that diagrams

$$\begin{array}{ccc} X \times X \times X & \xrightarrow{\mathrm{id}\times m} & X \times X \\ \downarrow{\scriptstyle m\times\mathrm{id}} & & \downarrow{\scriptstyle m} \\ X \times X & \xrightarrow{m} & X \end{array} \quad , \quad \begin{array}{ccc} X & \xrightarrow{(\mathrm{id},e\circ\sigma)} & X \times X \\ \downarrow{\scriptstyle (e\circ\sigma,\mathrm{id})} & & \downarrow{\scriptstyle m} \\ X \times X & \xrightarrow{m} & X \end{array} \quad \text{and}$$

$$\begin{array}{ccc} X & \xrightarrow{(\mathrm{id},i)} & X \times X \\ \downarrow{\scriptstyle (i,\mathrm{id})} & \searrow^{e\circ\sigma} & \downarrow{\scriptstyle m} \\ X \times X & \xrightarrow{m} & X \end{array}$$

commute, demonstrating the associativity of the multiplication m, the existence of a neutral element and the existence of inverses. △

Definition A.4. A scheme X is called quasi-compact if the underlying topological space $|X|$ is quasi compact, i.e. if every open covering of $|X|$ has a finite subcovering. Moreover, a morphism $f : X \to Y$ of schemes is *quasi-compact* if Y can be covered by open affine subschemes V_i such that the pre-images $f^{-1}(V_i)$ are quasi-compact (as topological space). △

Definition A.5. A morphism $f : X \to Y$ of schemes is *locally of finite type* if for all $x \in X$ there exists an affine open neighbourhood $\mathrm{Spec}(R_U) = U \subset X$ of x and affine open $\mathrm{Spec}(R_V) = V \subset S$ with $f(U) \subset V$ such that the induced ring map $R_V \to R_U$ is of finite type. We say f is *of finite type* if it is locally of finite type and quasi-compact. △

Definition A.6. A scheme X is *locally Noetherian* if for every point $x \in X$ there is an affine open neighbourhood $U_x = \mathrm{Spec}\, R$ such that R is Noetherian. We say it is *Noetherian* if X is locally Noetherian and quasi-compact. △

Definition A.7. A scheme is *regular* if all local rings are regular. Moreover, we say a scheme over a field k is *geometrically regular* if for an algebraic closure $\overline{k}$ of k the scheme $X_{\overline{k}}$ is regular. △

Definition A.8. A scheme is *connected* if the underling topological structure is connected. Moreover, we say a scheme over a field k is *geometrically connected* if for an algebraic closure $\overline{k}$ of k the scheme $X_{\overline{k}}$ is connected. △

Definition A.9. A schemes X is *irreducible* if the underling topological structure is irreducible. Moreover, we say a scheme over a field k is *geometrically irreducible* if for a $k \subset \overline{k}$ algebraic closure of k the scheme $X_{\overline{k}}$ is irreducible. △

Definition A.10. A scheme X is *reduced* if for every point $x \in X$ the local ring $\mathcal{O}_{X,x}$ is reduced. Moreover, we say a scheme over a field k is *geometrically reduced* if for an algebraic closure $\overline{k}$ of k the scheme $X_{\overline{k}}$ is reduced. △

For a scheme X and a closed subspace $T \subset |X|$ there is an unique reduced closed subscheme $Y \subset X$ by [Sta, Tag 01J3].

Definition A.11. Let X be a scheme. An *irreducible component of* X is an reduced closed subschemes $Y \subset X$ such that $|Y|$ is an irreducible component of the topological space $|X|$. For a scheme X and a given irreducible component $|Z|$ of the topological space $|X|$, there is an irreducible component of X by [Sta, Tag 01J3]. △

Definition A.12. A scheme X is *integral* if it nonempty and for every nonempty affine open $\mathrm{Spec}(R) = U \subset X$ the ring is an integral domain. Moreover, we say a scheme over a field k is *geometrically integral* if for an algebraic closure $\overline{k}$ of k the scheme $X_{\overline{k}}$ is integral. △

Definition A.13. A morphism $f : X \to Y$ of schemes is *flat* if the induced ring map $\mathcal{O}_{Y,f(P)} \to \mathcal{O}_{X,P}$ for all $P \in X$ makes $\mathcal{O}_{X,P}$ a flat $\mathcal{O}_{Y,f(P)}$-module. △

Definition A.14. A morphism of schemes $f : X \to Y$ is *separated* if the diagonal map $\Delta_\phi : X \to X \times_Y X$ is a closed immersion, i.e. $|\Delta_\phi(X)|$ is closed in the topological space $|X \times_Y X|$ and $\Delta_\phi^\# : \mathcal{O}_{X \times_Y X} \to \Delta_{\phi *}\mathcal{O}_X$ is surjective. △

Definition A.15. A morphism $f : X \to S$ of schemes is *smooth* if it is locally of finite presentation, it is flat, and for every geometric point $\overline{s} \to S$ the fiber $X_{\overline{s}} = X \times_S \overline{s}$ is regular. △

Definition A.16. A morphism $f : X \to Y$ of schemes is *universally closed* if for all morphisms $g : K \to Y$ the projection map $p_2 : X \times_Y K \to K$ is closed, note that $X \times_Y K$ and p_2 come from the commuting diagram

$$\begin{array}{ccc} X \times_Y K & \xrightarrow{p_2} & K \\ {\scriptstyle p_1}\downarrow & & \downarrow{\scriptstyle g} \\ X & \xrightarrow[f]{} & Y \end{array} .$$

△

Definition A.17. A morphism of schemes is *proper* if it is separated, of finite type, and universally closed. △

Lemma A.18. Let X be a scheme. For every point $x \in X$ the irreducible components $Z \in \mathrm{Irr}(X)$ containing x correspond 1-to-1 with the minimal primes of $\mathcal{O}_{X,x}$. △

Proof. First we assume $X = \mathrm{Spec}(R)$ for some ring R. Then for a point $[P] \in X$ notice that the minimal primes of R_P correspond 1-to-1 with the minimal primes

Q of R which satisify $Q \subset P$. For the latter there is an 1-to-1 correspondence with irreducible components Z of X such that $[P] \in Z$, by [Sta, Tag 00ET].

For a general scheme X we have an affine open cover $(U_\alpha)_{\alpha \in A}$. For a point $x \in X$ there is an $\alpha \in A$ such that $x \in U_\alpha$. Let W be an irreducible component of X such that $[P] \in W$. Now we want to find a minimal prime of $\mathcal{O}_{X,x}$ such that it corresponds to W. First note that $\mathcal{O}_{U_\alpha,x} = \mathcal{O}_{X,x}$. It remains to show that the irreducible components $Z \subset X$ such that $Z \cap U_\alpha \neq \emptyset$ correspond bijectively to the irreducible components of U_α via the map $Z \to Z \cap U_\alpha$. The surjectivity of this map is clear, so we only have to show the injectivity. Suppose that $W_1, W_2 \subset X$ are irreducible components such that $W_1 \cap U_\alpha = W_2 \cap U_\alpha$. Then by looking at the closures in X of these we have, by the denseness of opens in irreducible spaces, that $W_1 = \overline{W_1 \cap U_\alpha} = \overline{W_2 \cap U_\alpha} = W_2$. So the component W corresponds uniquely to $W \cap U_\alpha$, which we saw corresponds uniquely to a prime in $\mathcal{O}_{U_\alpha,x}$ and, as remarked earlier, these correspond to primes of $\mathcal{O}_{X,x}$. □

Lemma A.19. Let X be a scheme such that every point has an open neighbourhood where only finitely many irreducible components of X pass through. Then the following are equivalent

(i) Every connected component of X is irreducible.

(ii) X is the disjoint union of its irreducible components.

(iii) For all $x \in X$, the nilradical of $\mathcal{O}_{X,x}$ is a prime ideal. △

Proof. All but one implication in the proof remains true also after one drops the assumption that every point has an open neighbourhood where only finitely many irreducible components of X pass through. It is in the proof of implication $(iii) \Rightarrow (i)$ that we use the assumption.

$(i) \Rightarrow (ii)$: Assume that every connected component of X is irreducible equivalent to saying the connected components and the irreducible components coincide.

$(ii) \Rightarrow (iii)$: Assume that the scheme X is the disjoint union of its irreducible components. Then every point $x \in X$ is contained in preciously one irreducible component and from Lemma A.18 follows that $\mathcal{O}_{X,x}$ has a unique minimal prime. This this unique minimal prime per definition is the nilradical and thus for all $x \in X$ the nilradical of $\mathcal{O}_{X,x}$ is a prime ideal.

$(iii) \Rightarrow (ii)$: Assume for all $x \in X$ the nilradical of $\mathcal{O}_{X,x}$ is a prime ideal. Thus for every point $x \in X$ the ring $\mathcal{O}_{X,x}$ has a unique minimal prime. By Lemma A.18 every point $x \in X$ is contained in precisely one irreducible component, hence no two irreducible components intersect and thus the scheme X is the disjoint union of its irreducible components.

$(iii) \implies (i)$: As discussed we need to assume that for every $x \in X$ there is an open neighbourhood U_x such that for all but finitely many $Z \in \mathrm{Irr}(X)$ we have $U_x \cap Z = \emptyset$ and that the nilradical of $\mathcal{O}_{X,x}$ is a prime ideal. So U_x has only finitely many irreducible components and they are of the

form $U_x \cap Z$ for $Z \in \mathrm{Irr}(X)$. Now let $Z_1, \cdots, Z_n \in \mathrm{Irr}(X)$ be all the irreducible components such that $U_x \cap Z_i \neq \emptyset$. By Lemma A.18 and our assumptions we know there is a unique $Z \in \mathrm{Irr}(X)$ that contains x. Since $Z \in \{Z_1, \cdots, Z_n\}$, let i_x be the integer such that $Z = Z_{i_x}$. Define $V_x := U_x \cap \left(X \setminus \left(\bigcup_{1 \leq i \leq n \wedge i \neq i_x} Z_i\right)\right)$ and observe that it is an open neighbourhood of x. Furthermore, observe that for all $Z \in \mathrm{Irr}(U_x)$ we have $Z \cap V_x \neq \emptyset$ if and only if $x \in Z$, so $\#\,\mathrm{Irr}(V_x) = 1$ and thus V_x is irreducible. As Z_{i_x} is the unique irreducible component containing x, we have $V_x \subset Z_{i_x}$. As x was arbitrary, we find that for every point in an irreducible component there is open neighbourhood that is contained in the irreducible component and thus every irreducible component is open. Irreducible components are also closed, since the closure of an irreducible set is also irreducible. Let X' be a connected component, then there is an irreducible component Z such that $X' \cap Z \neq \emptyset$. As irreducible components are also connected, we have that $X' \cup Z$ is also connected and by maximality of X' we have that $Z \subset X'$. Therefore, $Z = X' \cap Z$ and recall that Z is clopen in X, so Z is also clopen in X'. Then there is a decomposition of distinct opens $X' \setminus Z \cup Z = X'$ in a connected space and as $Z \neq \emptyset$ we find that $X' = Z$. Thus every connected component of X is irreducible.

□

Lemma A.20 (Rigidity)**.** Let X, Y, Z be varieties over a field k and assume that X is complete. Suppose a morphism $f : X \times Y \to Z$ is given with the property that there exists k-rational points $y \in Y(k)$ and $z \in Z(k)$ such that $f \circ (\mathrm{id}_X \times y) = z$. Then f factors through the projection $pr_Y : X \times Y \to Y$. That is, there exists a morphism $g : Y \to Z$ such that $f = g \circ pr_Y$. △

Proof. See [MvdG11, (1.12)]. □

Corollary A.21. Let $f : A \to B$ be a morphism of Abelian varieties and $\tau_{f(e_A)} := m_B \circ (\mathrm{id}_B, f(e_A))$ the the translation by $f(e_A)$ map. There is a homomorphism h such that $f = \tau_{f(e_A)} \circ h$ △

Proof. Define h as the map $\tau_{i_Y(f(e_A))} \circ f$, then clearly $h(e_A) \mapsto e_Y$. Also define d as the composition

$$A \times A \xrightarrow{(h \circ m_A) \times (i_B \circ m_B \circ (h \times h))} B \times B \xrightarrow{m_B} B$$

.

The map d is the difference of the diagram

$$\begin{array}{ccc} A \times A & \xrightarrow{m_A} & A \\ {\scriptstyle h \times h}\downarrow & & \downarrow{\scriptstyle h} \\ B \times B & \xrightarrow[m_B]{} & B \end{array}$$

and thus notice that $d(\{e_A\} \times A) = \{e_B\} = d(A \times \{e_A\})$. Now the Rigidity Lemma tells us that d factors through both projections $A \times A \to A$ and thus d is constant with image e_B. In other words the diagram is commutative and that is equivalent to h being a homomorphism. $\square$