Splitting of Abelian Varieties

by

Vijay M. Patankar

A thesis submitted in conformity with the requirements
for the degree of Doctor of Philosophy
Graduate Department of Mathematics
University of Toronto

Abstract

Given an Abelian variety A defined over a number field K, and a finite place v of K of good reduction for A, let A_v denote the reduction of A modulo v. It is defined over the (finite) residue field associated with v. We say that an Abelian variety splits if it is isogenous to a product of smaller dimensional Abelian varieties. Given such an A over K, we study the phenomenon of splitting of A_v. This is a new *local-global problem* in the context of *splitting* of Abelian varieties.

We prove the following results. Firstly, if A is an Abelian surface with a quuaternion division algebra as the algebra of endomorphisms, then it is a square at all finite places of good reduction. Secondly, if A is an absolutely simple Abelian variety of dimension d over a number field with multiplication by a C.M. field of degree $2d$ then, A remains absolutely simple over a set of places of density 1. Thirdly, if f is a newform of weight 2 of square-free level N and trivial nebentypus so that the associated Abelian variety A_f is absolutely simple then, it remains absolutely simple at a set of places of density 1. Fourthly, if A is an absolutely simple Abelian variety with trivial ring of endomorphisms (i.e. $\mathbb{Z}$), then it remains absolutely simple for a set of places of density 1.

Finally, we formulate a conjecture. Let A be an absolutely simple Abelian variety over a number field K. We conjecture that A splits over a set of places of K of positive upper density if and only if its endomorphism algebra is non-commutative. All of the above results provide evidence for the conjecture.

Our arguments are mainly based on Tate's theorem on the classification of endomorphisms of an Abelian variety defined over a finite field.

Dedication

To my late grandfather G. G. Patankar and late Swami Pramathananda.

Acknowledgements

I sincerely thank my advisor, Professor V. K. Murty, for his guidance, encouragement and mentorship during the last few years. I also thank him for introducing me to the problem studied in this thesis.

My sincere thanks to the Department of Mathematics, University of Toronto, for providing the financial assistance through various scholarships, research assistantships, and teaching duties. I also wish to thank all the faculty and the staff at the Department of Mathematics, University of Toronto. I specially thank Pat Broughton, Ida Bulat, Marco De La Cruz, and Ian Graham.

I have greatly benefited by being a visitor to the Harish Chandra Research Institute (HRI), Allahabad, India and to the Institute for Advanced Studies, Princeton. I wish to extend my thanks to them. Also, special thanks to Dipendra Prasad for funding my visits to HRI, Allahabad and for his warm and welcoming hospitality.

I thank all my friends. Notably, my special thanks to Shashikant Acharya, Amir Akbary, Indranil Biswas, Hemant Bokil, Milind Ghaisas, Kedaar Ghanekar, Cyril Guyot, Ajay and Manjusha Joon, Chandrashekhar Khare, Uday Oak, Eric Parker, Krishna Ramdayal, Jaya Sagade, Pramathanath Sastry, and Eric Schippers.

I am grateful to all my past teachers and my special thanks to Madhumalati Apte, M. Prakash, and Dipendra Prasad.

Finally, I wish to express my deep gratitude toward my entire family, especially my father and mother.

Contents

Chapter 1

Introduction:

A splitting problem for Abelian varieties

In this thesis, we wish to study a local-global principle in the context of Abelian varieties.

1.1 Local-global principle

The local-global principle is a well-studied principle in various number theoretical contexts. The following are a few illustrative examples.

1. *Irreducible monic polynomials over* $\mathbb{Z}$: Let f be a monic polynomial with integer coefficients. Suppose p is a prime such that $f \mod p$ is irreducible, then f is irreducible over $\mathbb{Z}$. The converse is *not* true. It is well-known that there are examples of irreducible monic polynomials over $\mathbb{Q}$, hence over $\mathbb{Z}$, which become reducible modulo almost all primes p (more precisely, at all the primes except perhaps those that divide the discriminant of the polynomial).

The following is a way to construct them: Let E be a Galois extension of $\mathbb{Q}$ with non-cyclic Galois group $Gal(E/\mathbb{Q})$. Let θ be an algebraic integer such that $E = \mathbb{Q}(\theta)$. Let $f(x)$ be the irreducible monic polynomial of θ over $\mathbb{Z}$. Then, for all (unramified) primes p, $f(x)$ is reducible modulo p. For example: $E = \mathbb{Q}(\zeta_8)$, where $\zeta_8 := e^{2\pi i/8}$, an 8^{th} root of unity, with $f(x) = x^4 + 1$, the monic minimal polynomial of ζ_8. Then, we have the following factorization:

$$\begin{aligned}
f(x) &\equiv (x+1)^4 \pmod 2 \\
f(x) &\equiv (x^- \sqrt{-1})(x^2 + \sqrt{-1}) \pmod p,\ p \equiv 1 \pmod 4 \\
f(x) &\equiv (x^2 + \sqrt{2}\,x + 1)(x^2 - \sqrt{2}\,x + 1) \pmod p,\ p \equiv 7 \pmod 8 \\
f(x) &\equiv (x^2 + \sqrt{-2}\,x - 1)(x^2 - \sqrt{-2}\,x - 1) \pmod p,\ p \equiv 3 \pmod 8
\end{aligned}$$

This factorization follows from the law of Quadratic Reciprocity. Thus, the factorization depends on the *Frobenius automorphism* ($Frob_p$) attached to p.

Conversely, let f be a monic irreducible polynomial over $\mathbb{Z}$ such that it generates a cyclic extension of $\mathbb{Q}$ with Galois group G. Then, by the Chebotarev density theorem it follows that the set of primes p with $Frob_p$ equals a generator σ of G, has density $\frac{\phi(|G|)}{|G|}$, where $|G|$ is the cardinality of G and ϕ is Euler's totient function. Thus, for all such primes p, f remains irreducible mod p.

2. *Hilbert's irreducibility theorem*(HIT): For now, let us assume that $K = \mathbb{Q}$. Let $f \in K[X_1, \cdots, X_n][t]$ with $\deg_t(f) = n$ (degree of f in t. Let $G \subset S_n$ be the Galois group of f over $K(X_1, \cdots, X_n)$. Then, there is a *thin set*, a subset of K^n that depends on f, such that for $\underline{x} = (x_1, \cdots, x_n) \in K^n$ that is outside the thin set, the specialization of f, $f(x_1, \cdots, x_n, t)$ has Galois group G over K.

   If the above statement, with the associated definition of *thin set*, holds for a field, then that field is called a *Hilbertian* field. It is a theorem of Hilbert that all number fields are Hilbertian. Here a *thin set*, roughly speaking, is a hypersurface in K^n (for

exact definitions, see section (2) of Bilu & Luca [B-L], and section (9.1) of Serre [Se3]).

3. *Hasse principle for quadratic forms*: Let Q be a quadratic form over the field of rational numbers in n variables. Then, the well-known theorem of Hasse and Minkowski states that Q has a solution over the rationals if and only if it has a solution over the p-adic numbers $\mathbb{Q}_p$ for all p, including the prime (place) at *infinity* ($\mathbb{R}$). By Hensel's lemma, to check whether the form Q has a solution over $\mathbb{Q}_p$, it is most of the time enough to check that it has a solution over $\mathbb{F}_p$ (or at the most over $\mathbb{Z}/p^n\mathbb{Z}$ for a large enough n, depending only on Q).

4. *Brauer group of a field and splitting of division algebras*: Let D be a central simple algebra with centre a fixed global field K. We say that D is *totally split* over K if $D \simeq M(n, K)$, the $n \times n$ matrix algebra of degree n over K. If it is *non-split* then, it is isomorphic to a matrix algebra of a division algebra over K. It is a theorem that, D is totally split over K if and only if it is totally split over K_v for all places v of K, including the places at infinity.

   This statement follows from Galois cohomology of global fields, and can be considered as the injectivity on the left in the following short exact sequence:

$$0 \to H^2(Gal(\bar{K}/K), \bar{K}) \to \sum_v H^2(Gal(\bar{K_v}/K_v), \overline{K_v}) \to \mathbb{Q}/\mathbb{Z} \to 0$$

   Local class field theory implies that $H^2(Gal(\bar{K_v}/K_v), \overline{K_v}) \simeq \mathbb{Q}/\mathbb{Z}$. Also, since there are no division algebras over $\mathbb{C}$, $H^2(Gal(\bar{K_v}/K_v), \overline{K_v}) \simeq \{0\}$ for a complex place v of K, and $H^2(Gal(\bar{K_v}/K_v), \overline{K_v}) \simeq Z/2\mathbb{Z}$ for a real place v of K.

   In Weil's Basic Number Theory [We], there is another proof of this theorem using the theory of zeta functions of central simple algebras. This proof uses the properties of local and global zeta functions, more precisely, the properties of the order

of their poles. For the sake of illustration, we now state the main results that go into this proof, modulo a set of definitions and details.

The following proposition computes the local zeta function of a matrix algebra over a local field (the identity element of the Brauer group of the field). The result below is for finite places.

Proposition 1.1.1. *Let $d \geq 1$ be an integer. Let $D_v := M_d(K_v)$, where K_v is the local field at a place v of a global field K. Let $\mathcal{O}_{D_v}$ be a maximal order in D_v, and ϕ its characteristic function. Let ν be the determinant (the reduced norm) on D_v, and let μ be the Haar measure on D_v^* such that $\mu(\mathcal{O}_{D_v}^*) = 1$. Then, the integral*

$$I(s) := \int_{D_v^*} \phi(x)|\nu(x)|_v^s d\mu(x),$$

where $s \in \mathbb{C}$, is absolutely convergent for $Re(s) > d-1$ and has then the value

$$Z_{D_v}(s) := I(s) = \prod_{i=1}^{d-1}(1 - q_v^{i-s})^{-1}$$

Proof. This is special case of the general result: Proposition 7 (page 197), chapter X, Section 3 from Weil's book [We] (The general result computes the local zeta function of any central simple algebra over a local field). Here, $\mathcal{O}_{D_v}$ can be taken to be $M_d(\mathcal{O}_v)$, where $\mathcal{O}_v := \{x \in K_v : |x|_v \leq 1\}$. □

A similar result computes the local zeta function of a central simple algebra over $\mathbb{R}$ and $\mathbb{C}$. Once again, we need to know these functions for matrix algebras over $\mathbb{R}$ and $\mathbb{C}$. In this case, the local zeta functions are made up of the Γ-functions. The details can be found in Proposition 8 (page 200), Chapter X, section 3 of [We]. We do not state it here.

The next proposition computes the global zeta function of the 'Adélic algebra' associated with a central simple algebra over a number field K. This computation expresses this global zeta function in terms of the local zeta functions of the central

simple algebras defined over the completions K_v of the number field K at the places v of K.

Proposition 1.1.2. *Let D be a central simple division algebra over a number field K of degree d, i.e. $[D : K] = d^2$. Let $\mathbb{A}_D$, $\mathbb{J}_D$, respectively, denote the adélic algebra, and the group of ideles (the group of invertible elements of $\mathbb{A}_D$). Let μ be a* well-chosen *Haar measure on $\mathbb{J}_A$. Let $|\nu(-)|_{\mathbb{J}_A}$ be the* modulus of the reduced norm ν *on $\mathbb{J}_A$. Let $\Phi = \prod_v \Phi_v$ be the* standard *function on $\mathbb{A}_D$. Then, the integral*

$$Z_D(s) := \int_{\mathbb{J}_D^*} \Phi(x)|\nu(x)|^s d\mu(x)$$

is absolutely convergent for $Re(s) > d$ and is given by the formula

$$Z_D(s) = C \prod_{i=0}^{d-1} Z_K(s-i) \cdot \prod_v \left(\prod_{\substack{0<h<d \\ h \not\equiv 0 (d(v))}} (1 - q_v^{h-s}) \right) \cdot \left(\prod_{\substack{0<h<d \\ h \not\equiv 0 (2)}} (s-h) \right)^{\rho},$$

where Z_K is the global zeta function of the number field K (global means it includes the Γ associated to the places at infinity), and ρ is the number of real places v of K for which $D_v := D \otimes \mathbb{R} = \mathbb{H}$, and C is a constant > 0.

Proof. This is Proposition 1, page 203, chapter XI, section 1 of [We]. □

On the other hand, there is the following proposition that tells us about the poles of the global zeta function of a division algebra.

Proposition 1.1.3. *Let D be a division algebra of dimension d^2 over a number field K. Let $Z_D(s)$ be its global zeta-function as defined earlier. Then, $Z_D(s)$ has no poles other than $s = 0$ and $s = d$.*

Proof. This is Proposition 2, page 206, chapter XI, section 2 of [We]. The case $d = 1$ is the well-known statement for the Dedekind zeta function of a number field K. □

The comparison between the above two propositions gives us the following theorem (Theorem 2, page 206 of [We]).

Theorem 1.1.1. *A simple algebra A over a global field K is trivial if and only if it is everywhere unramified, i.e. if and only if A_v is trivial over K_v for every place v over K.*

Proof. It is enough to prove this theorem for a division algebra D over K. If D_v is trivial for all v, then its zeta-function $Z_D(s)$, up to a constant factor, is given by

$$Z_D(s) = \prod_{i=1}^{d-1} Z_K(s-i),$$

where $Z_K(s)$ is the completed zeta function of the number field K. If $d > 1$ then, this has poles of order 2 at $s = 1, 2, \cdots, d-1$. This can't be by proposition (1.1.3) above. Therefore $d = 1$, and $D = K$. □

Remark. Actually, with a more careful analysis of these propositions one can conclude that, if $d > 1$, then D must be ramified at least at two places of K.

Remark. We use a similar idea in the proof of theorem (3.2.1) of section (3.1). In this theorem, we use the properties of poles of L-functions to prove a result for Abelian varieties with complex multiplication.

1.2 Splitting of Abelian Varieties

Similar to the "local-global" examples of the previous section, we wish to study the phenomenon of the splitting of an Abelian variety (defined over a number field), modulo various places of good reduction.

1.2.1 Preliminaries, Notations and definitions

We begin with notations, definitions and a few important background results.

Throughout, K will denote a global field. At times, when the situation is more general and applies to any field, we denote such fields by the letter k. By $\bar{k}$, or $\bar{K}$, we will denote an algebraic closure of k and K, respectively. By v we mean a valuation or a place or a prime of a global field K. The words valuation, place or prime will be used interchangeably. By $\sum_\infty$ and $\sum_{fin}$, we will, respectively, mean the set of Archimedean places of K and the set of all finite places of K. Here the K will be clear from the context and will mostly be suppressed. Occasionally, we also use the letters p or w to denote a place of a global field. By K_v we mean the completion of K at v, and k_v means the residue field of K_v at v, or by abuse of notation, we sometimes call it, the residue field of K at v. We also use L, F, and E to denote global fields, mostly number fields. The letter E is also used to denote central simple algebra with centre a number field. This notational scheme, whenever appropriate, also applies to $L_v, L_w, l_v, l_w, F_v, f_v, E_v, e_v$ et cetera. We mostly use letters A, B for Abelian varieties, and d or g for their dimensions.

We now present a few definitions related to *density of primes*. Let K be a number field. Let Σ_{fin} denote the set of finite places of K. Let S be a subset of Σ_{fin}. To S one associates various 'density' measures. Below we define two such basic densities: natural density and Dirichlet (or analytic) density.

Definition 1.2.1. *The* upper natural density *or in short,* upper density *of S, to be denoted by $ud(S)$ is defined by*

$$ud(S) \;:=\; \limsup_{x\to\infty} \frac{\#\{v \in \Sigma_{fin} \mid Nv \leq x,\, v \in S\}}{\#\{v \in \Sigma_{fin} \mid Nv \leq x\}},$$

where Nv, the norm of v, is the cardinality of the finite field k_v, the residue field at v.

Similarly, one defines the *lower natural density* or in short the *lower density* of S. It is defined using $\liminf$ instead of $\limsup$ in the above. When the lower density of S

equals the upper density of S, it also equals the natural density of S. It is then denoted by $d(S)$ and is defined as follows.

$$d(S) = \lim_{x \to \infty} \frac{\#\{v \in \Sigma_{fin} \,\|\, Nv \leq x,\, v \in S\}}{\#\{v \in \Sigma_{fin} \,\|\, Nv \leq x\}},$$

There is also the notion of analytic density or Dirichlet density associated to $S \subset \Sigma_{fin}$. There is firstly the upper Dirichlet density.

Definition 1.2.2. *The upper Dirichlet density of S, denoted by $uDd(S)$, is defined by*

$$uDd(S) := \limsup_{s \to 1^+} -\frac{\sum_{v \in S} Nv^{-s}}{\log(s-1)}.$$

Here one can assume that s is real > 1.

Similarly, the *lower Dirichlet density* or *lower analytic density* of S is defined by replacing lim sup by lim inf. One says that S has *Dirichlet density*, denoted by $Dd(S)$, when the upper and lower Dirichlet densities are equal. It then equals the following limit.

$$Dd(S) \;\; := \;\; \lim_{s \to 1^+} -\frac{\sum_{v \in S} Nv^{-s}}{\log(s-1)}.$$

One can prove that, if S has natural density δ, then the analytic or Dirichlet density of S exists and is equal to δ. On the other hand, there exists sets having an analytic density but *no* natural density. The details can be found in chapter VI, section (4.5) of Serre's [Se].

Remark. In this thesis, we mostly use the notion of upper density. We now state some definitions related to Abelian varieties:

Definition 1.2.3. *An Abelian variety over a field k is a complete variety with a group morphism, both defined over k.*

We can then talk about morphisms between two Abelian varieties that respect the group structure.

Definition 1.2.4. *Let k be any field. Let A and B be Abelian varieties defined over k. Then, we say that A is* isogenous *to B over k, and write*

$$A \sim_k B,$$

provided, there is a homomorphism (a group morphism), say ϕ from A to B with finite kernel and co-kernel. i.e. the following is a short exact sequence with both Ker *and* Coker *finite Abelian groups.*

$$0 \to Ker \to A \xrightarrow{\phi} B \to Coker \to 0.$$

When this is so, the homomorphism ϕ is called an isogeny*.*

The definition changes appropriately when one has an isogeny defined over an extension of k, or over $\bar{k}$. It follows that, *isogeny* (relative to a field k) defines an equivalence relation, and that the dimension of an Abelian variety is an isogeny-invariant.

If there exists an isomorphism between A and B over k, then we write $A \simeq_k B$.

Definition 1.2.5. *Let A be an Abelian variety defined over a field k. Then A is said to be* simple *over k, if A does not have a proper Abelian subvariety of non-zero dimension defined over k.*

The above definition is *field-sensitive*. Related to the above, we also have the notion of absolutely simple Abelian variety over k.

Definition 1.2.6. *Let A be an Abelian variety over k. Then, A is said to be* absolutely simple*, if A is simple over $\bar{k}$, a separable algebraic closure of k.*

The following proposition can be considered as the *unique factorization theorem* for Abelian varieties up to isogeny.

Proposition 1.2.1. (Poincaré) *Let A be an Abelian variety over k. Then, we can write:*

$$A \sim_k B_1^{n_1} \times \cdots \times B_r^{n_r}$$

where B_is are pair-wise non-isogenous simple Abelian varieties over k and $n_i \geq 1$. Moreover, up to isogeny, the factorization of an Abelian variety as a product of powers of simple Abelian varieties (as above) is unique up to the ordering of the B_i.

Proof. This is the Poincare-Weil complete reducibility theorem. This can be found in Mumford's book [Mu], Theorem 1, Corollary 1 and Corollary 2 (pages 173-174). □

For an Abelian variety A defined over a field k, by $End_k(A)$ we mean the ring of endomorphisms of A defined over k. By tensoring by $\mathbb{Q}$, we consider it as an algebra over $\mathbb{Q}$, and we denote it by $End_k^0(A) := End_k(A) \otimes \mathbb{Q}$.

Corollary 1.2.1. *For an Abelian variety A over k, together with its factorization as above, we have:*

$$End_k^0(A) \simeq \oplus_{i=1}^r M_{n_i}\left(End_k^0(B_i)\right).$$

Proof. Firstly, $End_k^0(A) \simeq End_k^0(B_1^{n_1} \times \cdots \times B_r^{n_r})$, because they are isogenous. Now notice that an endomorphism, when restricted to any of the components $B_i^{n_i}$, leaves it invariant, and thus, we can write it as a sum of elements of $End_k(B_i^{n_i})$, and that proves the corollary, as

$$End_k^0(B_i^{n_i}) = M_{n_i}(End_k^0(B_i).$$

□

With the above definitions, and the proposition in place, we now make the following basic definition.

Definition 1.2.7. Split relative to L: *An Abelian Variety A defined over a field K is said to be* split *over an extension $L \subset \bar{K}$ of K, if*

$$A \sim_L B_1 \times B_2,$$

i.e., A is isogenous to $B_1 \times B_2$ over L , where B_1 and B_2 are Abelian varieties defined over L, and such that dimensions of B_i, $i = 1, 2$ are strictly smaller than the dimension of A. Here A is considered as an Abelian variety defined over L.

At times, we use the "$\sim$" notation rather than the "$\sim_L$", whenever L, the field of definition, is clear from the context.

Definition 1.2.8. Strictly-split relative to L: *An Abelian variety A defined over a field K is said to be* strictly-split *over an extension $L \subset \bar{K}$ of K, if*

$$A \simeq_L B_1 \times B_2,$$

i.e., A is isomorphic to $B_1 \times B_2$ over L , where B_1 and B_2 are Abelian varieties defined over L, and such that dimensions of B_i, $i = 1, 2$ are strictly smaller than the dimension of A. Here A is considered as an Abelian variety defined over L.

At times, we use the "$\simeq$" notation when the field L is clear from the context.

Remark. In the above definitions, the questions that we ask are basically of two kinds.

- Splitting (or strict-spltting) of an Abelian variety over its field of definition and over the residue field corresponding to various finite places.
- Splitting (or strict-splitting) of the Abelian variety over the algebraic closure of the field of definition, and over algebraic closures of its various associated residue fields.

The aim of this thesis is to study these and related questions. Along the way, we will try to point out the subtle effect the above definitions have on the approach to the questions and the answers thereof.

1.3 Summary of our results

Here is a brief summary of our results:

1. We begin our study with the well-known example that belongs to the family of Abelian surfaces with quaternionic multiplication. It turns out that any absolutely

simple Abelian surface with quaternionic multiplication (more precisely, multiplication by a quaternion division algebra over $\mathbb{Q}$ that splits at $\mathbb{R}$) is split at all its places of good reduction provided the full endomorphism ring is defined over the field of definition of the given Abelian surface. (*It is a fact that such an Abelian surface has potential good reduction everywhere and follows from Oort's proposition (2.1.3) stated later.*)

Remark. Even though this is the starting point of our work, this example seems to be well-known to experts. Since we did not find a good reference that included all the relevant details, we decided to include it here. Furthermore, we improve our argument to prove that such an Abelian surface with quaternionic multiplication is *strictly-split* at all its places of good reduction. This was not noticed before. We also believe that there is more to this example than has been studied so far, and we wish to investigate this further in a future work.

Remark. Examples of such Abelian surfaces can be found in the paper of Hashimoto and Murabayanishi [HM]. We state them in chapter 2, section (2.3).

2. We then prove a result for Abelian varieties with *complex multiplication*. We prove that an absolutely simple Abelian variety with complex multiplication defined over a number field K remains absolutely simple for a set of places of density 1. (This is a joint work with K. Murty.)

3. We then consider Abelian varieties A_f associated to cusp forms f of weight 2 for $\Gamma_0(N)$. In this case we show that, if A_f splits over a positive density of places then its endomorphism algebra is non-commutative. As a consequence we prove that if the level N is square-free, then A_f remains absolutely simple at a set of primes of density 1. (This is a joint work with K. Murty.)

   Remark. In both the above cases, our proofs actually show that they remain absolutely simple over the corresponding finite fields as well.

4. We cover the "phenomenon of splitting" for all the absolutely simple Abelian surfaces classified according to their endomorphism algebras, except the general case of absolutely simple Abelian surfaces with multiplication by a real quadratic field. One of the cases (with trivial multiplication) is covered by a theorem of Chai and Oort [CO], and [Cha].

5. These results lead us to make the following conjecture:

   Conjecture 1.3.1. *Let A be an absolutely simple Abelian variety over a number field K. Let S be the set of places v of K of good reduction for A such that $A_v := A \mod v$ splits (up to isogeny) over k_v, the residue field of K at v. Then, S has positive upper density if and only if $End_K^0(A)$ is non-commutative.*

   Remark. In the above conjecture, we believe that the upper density may be related to the invariants associated to $End_K^0(A)$.

Chapter 2

Abelian surfaces with quaternionic multiplication

2.1 Background results and preliminaries

We begin with the following lemma which says that the splitting property is respected under extension of fields.

Lemma 2.1.1. *Let A be an Abelian variety defined over a number field (or a global field) K. Let v be a finite place of K such that A has good reduction at v, and that $A_v := A \mod v$ splits over the residue field k_v of K at v. Let L be a finite extension of K and w a finite place of L lying over v. Then, A considered as a variety over L has good reduction at w and splits over the residue field l_w of L at w.*

Proof. We have:

$$A_v \sim_{k_v} B_{1,v} \times B_{2,v},$$

where $B_{1,v}$ and $B_{2,v}$ are both defined over k_v. Base changing l_w, it follows that A_w splits as $B_{1,w} \times B_{2,w}$, where $B_{i,w}$ are obtained by considering $B_{i,v}$ over l_w. In short, $B_{i,w} \simeq B_{i,v} \times_{k_v} l_w$, $i = 1, 2$. □

We now record a few well-known results on Abelian varieties and the structure of their endomorphism rings and algebras.

We begin by recalling the following basic result by Albert on classification of possible endomorphism algebras of a simple Abelian variety.

Theorem 2.1.1. (Albert) *Let A be a simple Abelian variety over a field k, with $g = \dim(A)$. Let $R := End_k(A)$, and $D := End_k^0(A) := R \otimes_{\mathbb{Z}} \mathbb{Q}$ be the endomorphism algebra of A. Let τ be the related Rosati involution defined on the division algebra D. Let $F := Z(D)$, the centre of D, $F_0 := \{a \in F \mid a^\tau = a\}$. Also, let us define the following numerical invariants: $d^2 = [D : F]$, $e := [F : \mathbb{Q}]$, $e_0 := [F_0 : \mathbb{Q}]$, and $m := \frac{2g}{[D:\mathbb{Q}]} = \frac{2g}{d^2 e}$. Then, with above notation, $D := End_K^0(A)$ is one of the following four types:*

- *I(e_0): $d = 1$, $e = e_0$. $D = F = F_0$ is a totally real field.*
- *II(e_0): $d = 2$, $e = e_0$. D is a quaternion division algebra over the centre F with $inv_v(D) = 0$, for all $v \in \Sigma_{F,\infty}$, and $F = F_0$ is a totally real field. This means that D is an* indefinite *division algebra, i.e. splits at all the real places of F.*
- *III(e_0): $d = 2$, $e = e_0$. D is quaternion division algebra with centre F such that $inv_v(D) \neq 0$, for all $v \in \Sigma_{F,\infty}$. This means that D is* definite *division algebra, i.e. it does not split at any of the real places of F.*
- *IV(e_0, d): $\mathbb{Q} \subset F_0 \subset F$ is a complex multiplication field with $[F : \mathbb{Q}] = e = 2e_0$, and $[F : F_0] = 2$ with F_0 a totally real field. Here, D is a division algebra of degree d^2 over its centre F and $[D : \mathbb{Q}] = d^2 e$.*

  Here, $inv_v(D)$ denotes the invariant *associated to $D_v := D \otimes_{\mathbb{Q}} F_v$ and is an element of $\mathbb{Q}/\mathbb{Z}$.*

Proof. This is well-quoted, and is proved in Mumford's book [Mu][thm. 2, pg. 201], as well as the original paper of Albert [Alb]. □

Let it be noted that the above list provides *necessary conditions* for an algebra to occur as an endomorphism algebra of a simple Abelian variety over a general field. Henceforth, we will call these algebras *Albert algebras*. If we restrict ourselves to fields of characteristic zero, say number fields, then not all Albert-algebras as above can be realised as endomorphism algebras of Abelian varieties. One of the restrictions in characteristic zero is: $m = \frac{2\dim(A)}{[End_K^0(A):\mathbb{Q}]}$ be an integer. Further restrictions exist when the characteristic is positive, and we will state these as and when needed.

Given an Abelian variety defined over a number field or a local field, there is a well-defined way of reducing it modulo a place of so called good reduction. This is part of the theory that was initially developed by Shimura-Taniyama in their work [ShTa] and we take it for granted. Furthermore, it makes sense to talk about the reduction of morphisms between two such Abelian varieties modulo a finite place, provided the reduction of the Abelian varieties modulo the given finite place is also well-defined. The next theorem is about such reductions.

Theorem 2.1.2. *Let A and B be two Abelian varieties defined over a local field K. Let $\mathcal{O}_K$ be the ring of integers of K, and let v be the valuation of K. Let A and B both have good reduction at v. Let A_v and B_v be the reductions of A and B modulo the maximal ideal m_v of $\mathcal{O}_K$. Let $k_v := \mathcal{O}_K/m_v$ be the residue field of K at v. Then, the natural map:*

$$i_v : Hom_K(A, B) \to Hom_{k_v}(A_v, B_v)$$

is well-defined and is an injection.

Proof. This is a well-known fact proved in Shimura's book [Sh2][prop. 12, pg. 83] and in Shimura-Taniyama [ShTa][prop. 12, pg. 95]. Their proof uses the concept of generic points. This fact can also be proved by other means, as in Lang [La1][theorem 3.2, pg. 45] using properties of torsion points under reduction. We sketch a proof that is along the lines of Lang's proof, and uses the following two well-known facts:

1. Let X be an Abelian variety over a field k. Let m be a positive integer prime to the characteristic of k. Then $\#X[m] = m^{2\dim(X)}$, where $X[m] := X[m](\bar{k})$ denotes the group of m-torsion points of X over $\bar{k}$, an algebraic closure of k.

2. Suppose X is an Abelian variety over a local ring $\mathcal{O}_v$ with valuation v and having good reduction at v. Let X_v denote the reducion of the Abelian variety modulo v and defined over the corresponding residue field $k_v := \mathcal{O}_v/m_v$. Then, the reduction mod v is an isomorphism between $X[m]$ and $X_v[m]$. This follows from the fact that the reduction mod v respects the multiplication by m-map, and from (1) above.

We now return to the proof of the lemma. Let ϕ be a non-zero homomorphism $\phi : A \to B$. Let $\phi_v : A_v \to B_v$, be its reduction modulo v. Consider $X := im(\phi) \subset B$. Then, X is an Abelian subvariety of B of non-zero dimension. Granted that the reduction mod v respects the usual algebraic operations, we have $X_v = X \bmod v = im(\phi_v)$. Then, for an integer m prime to v,

$$\#X[m] = \#X_v[m] = m^{2\dim(X)} = m^{2\dim(X_v)}.$$

Thus, $\dim(X) = \dim(X_v)$. This implies that ϕ_v is non-zero. □

Then, we have:

Lemma 2.1.2. *Let A and B be two isogenous Abelian varieties over k. Then,*

$$End_k^0(A) \simeq End_k^0(B)$$

Proof. Let $\phi : A \to B$ be an isogeny. Then, there is a dual isogeny, $\hat{\phi} : \hat{A} \to \hat{B}$ on the dual Abelian varieties. We also have isogenies: $\hat{A} \to A$ and $B \to \hat{B}$. Composing these, gives an isogeny

$$\tilde{\phi} : B \to \hat{B} \to \hat{A} \to A,$$

with the property that

$$\tilde{\phi} \circ \phi = \phi \circ \tilde{\phi} = [m],$$

for some positive integer m. Now given an $\alpha \in End_k(A)$, we see that $\phi \circ \alpha \circ \tilde{\phi} \in End_k(B)$. This defines a map

$$i_\phi : End_k(A) \to End_k(B),$$

attached to ϕ. By a similar construction, we can also define a map

$$i_\psi : End_k(B) \to End_k(A),$$

for any isogeny $\psi : B \to A$. By tensoring with $\mathbb{Q}$, it is easy to see that these are isomorphisms as algebras over $\mathbb{Q}$. Note that tensoring by $\mathbb{Q}$ is necessary. Otherwise, under i_ϕ, the $1 \in End_k(A)$ may be sent to a non-one scalar of $End_k(B)$, and it will then not be a ring map. □

Remark. In fact, from the proof, it follows that the map i_ϕ is an isomorphism between $End_k(A)$ and $End_k(B)$ if and only if the corresponding map ϕ is an isomorphism between A and B.

The following is important and we use it often.

Corollary 2.1.1. *Let A be an Abelian variety defined over a number field K, and v a finite prime of K of good reduction for A. Let*

$$i_v : End_K(A) \to End_{k_v}(A_v)$$

be the natural map induced by the reduction modulo v. Then, i_v is injective. Thus, $End^0_K(A)$ is a sub-algebra of $End^0_{k_v}(A_v)$ over $\mathbb{Q}$.

Proof. Suppose ϕ is a non-trivial endomorphism of A defined over $\bar{K}$, then it is also defined over the local field K_v, the completion of K at v. The rest follows from the above theorem. □

We now state a simple general lemma about the endomorphism ring of an Abelian variety and its relation to the splitting property of A.

Lemma 2.1.3. *Suppose A is a simple Abelian variety over a number field K. Let v be a finite place of K of good reduction for A. Suppose that:*

$$A_v \sim_k B_1^{n_1} \times \cdots \times B_r^{n_r},$$

where the B_is are simple and pairwise non-isogenous Abelian varieties over k_v and $n_i \geq 1$ are integers. Then, the reduction map followed by the projection to the i-th factor given by

$$A \to A_v \to B_i^{n_i},$$

induces an injection

$$Pr_i : End_k^0(A) \hookrightarrow M_{n_i}(End_k^0(B_i)),$$

for $1 \leq i \leq r$.

Proof. By corollary (1.2.1), we can write:

$$End_{k_v}^0(A) \simeq \oplus_{i=1}^r M_{n_i}(End_{k_v}^0(B_i)).$$

Now note that under the Pr_i's, the *identity* $\in D$ goes to the *identity* endomorphism of $B_i^{n_i}$, for all i.

Let $D := End_k(A)$. As A is simple, this is a division ring. Suppose that for some i, Pr_i is not an injection. Let $\phi \neq 0$ be an element of D such that $Pr_i(\phi)$ acts as *zero* map on $B_i^{n_i}$. Since ϕ is non-zero, there exists another element $\hat{\phi} \in D$ such that $\hat{\phi} \circ \phi = [m]$, where m is a positive integer, and $[m]$ denotes the endomorphism given by *multiplication by m*. Since i_v is a ring map, so is Pr_i, this implies that $Pr_i(\hat{\phi} \circ \phi) = Pr_i([m]) = [0]$. This contradicts the fact that $Pr_i([1]) = [1]$, as stated at the beginning of the proof. This proves the lemma. □

Let us now recall a result from Oort [Oo][Proposition 6.1, page 494] regarding the realization of Albert-algebras (theorem 2.1.1) as endomorphism algebras of Abelian surfaces.

Proposition 2.1.1. (Oort) *Let k be an algebraically closed field, and X a simple Abelian surface over k. Then, $End_k^0(X)$ is one of the following four types, and all the four types do occur in any given characteristic of the field k.*

- *I(1):* $\mathbb{Q}$
- *I(2):* $\mathbb{Q}(\sqrt{d})$ *= A real quadratic extension of* $\mathbb{Q}$
- *II(1):* D *= Quaternion division algebra over* $\mathbb{Q}$ *split at the real place of* $\mathbb{Q}$*, that means* $D \otimes_{\mathbb{Q}} \mathbb{R} = M_2(\mathbb{R})$*. Also known as indefinite quaternion division algebra.*
- *IV(2,1): A CM (Complex Multiplication) field of degree 4 over* $\mathbb{Q}$*. In this case, it is an imaginary quadratic extension of a real quadratic extension of* $\mathbb{Q}$*.*

Proof. By Albert's classification Theorem (2.1.1) on endomorphism algebras of simple Abelian varieties ([Mu][Thm. 2, page 202]), we know that the above four types are the only possibilities for a simple Abelian surface. The existence of simple Abelian surfaces having the above endomorphism algebras (over algebraically closed fields of characteristic zero) follows from analytic constructions due to Shimura [Sh1][thm. 5]. The corresponding moduli spaces are algebraic curves, and are defined over $\bar{\mathbb{Q}}$. Thus, generic points on these curves provide us with examples of an absolutely simple Abelian surface defined over a number field with any of the above prescribed endomorphism algebras. □

The following is a basic theorem of Tate's about the endomorphism algebras of Abelian varieties over finite fields. This is Theorem 3, page 256 of Mumford's 'Abelian varieties' [Mu].

Theorem 2.1.3. (*Tate*) *Let A be an Abelian variety of dimension d defined over a finite field k_0. Let π be the Frobenius endomorphism of A relative to k_0 and P its characteristic polynomial. We then have the following:*

- *(a) The algebra $F = \mathbb{Q}[\pi]$ is the centre of the semi-simple algebra $E = End^0_{k_0}(A)$;*
- *(b) $End^0_{k_0}(A)$ contains a semi-simple $\mathbb{Q}$-subalgebra M of rank $2d$ which is maximal commutative;*
- *(c) the following statements are equivalent:*

  (c_1) $[E : \mathbb{Q}] = 2d$,

  (c_2) P has no multiple roots,

  (c_3) $E = F$,

  (c_4) E is commutative;

- *(d) the following statements are equivalent:*

  (d_1) $[E : \mathbb{Q}] = (2d)^2$,

  (d_2) P is a power of a linear polynomial,

  (d_3) $F = \mathbb{Q}$,

  (d_4) E is isomoprhic to the algebra of d by d matrices over the unique quaternion division algebra D_p over $\mathbb{Q}$ (p is the characteristic of k_0), which splits at all primes l away from p and ∞,

  (d_5) A is k_0 isogenous to the d-th power of a supersingular elliptic curve, all of whose endomorphisms are defined over k_0;

- *(e) A is k_0-isogenous to a power of a k_0-simple Abelian variety if and only if P is a power of a $\mathbb{Q}$-irreducible polynomial. When this is the case, E is a central simple algebra over F which splits at all finite places v of F not dividing p, but does not split at any real prime of F.*

Proof. This is proved in Mumford's "Abelian varieties" [Mu][Thm. 3, page 256] □

We now state a few important consequences of Tate's theorem (or more precisely, conseqeunces of it's proof):

Proposition 2.1.2. *Let A be an Abelian variety defined over a finite field k. Let $P(T)$ be the characteristic polynomial of the Frobenius relative to k, and let $Q(T)$ be the minimal polynomial of the Frobenius acting on A. Then,*

1. *$P(T)$ is irreducible over $\mathbb{Q}$ implies that A is simple over k with $End_k^0(A)$ a commutative field.*

2. *A is simple over k implies that $P(T)$ is a power of $Q(T)$.*

3. *A is simple over k and $End_k^0(A)$ is non-commutative implies that $P(T) = Q(T)^r$, with $r \geq 2$.*

Proof. By π, we denote the Frobenius endomorphism of A relative to k. If the polynomial $P(T)$ is irreducible over $\mathbb{Q}$, then it has distinct roots. By part (b) of Tate's theorem (2.1.3), this implies that

$$E = F = \mathbb{Q}[\pi] = \frac{\mathbb{Q}[T]}{(P(T))},$$

which is a field, and that proves that A is simple over k and that $End_k^0(A)$ is commutative.

Conversely, if A is simple over k, then

$$F = \mathbb{Q}[\pi] \hookrightarrow E := End_k^0(A),$$

and therefore F is a field. This implies that $Q(T)$ is irreducible. Since $P(T)$ is the characteristic polynomial of π and $Q(T)$ is the minimal polynomial of π, it follows that $Q(T)$ divides $P(T)$, and moreover, every root of $P(T)$ is a root of $Q(T)$. From the irreducibility of $Q(T)$, it then follows that $P(T) = Q(T)^r$ for some integer $r \geq 1$. This proves (2).

By (2) above, we have $P(T) = Q(T)^r$, with $r \geq 1$. Since E is a non-commutative central simple division algebra over F, it follows that $P(T)$ has to have repeated roots. otherwise, it would contradict part(c) of Tate's theorem (2.1.3). Therefore, $r > 1$. This proves (3). □

Corollary 2.1.2. *Let A be a simple Abelian variety defined over a finite field k. Let $P(T)$ and $Q(T)$ be as in the above proposition. Then, $P(T) = Q(T)^r$ with $r \geq 2$ if and only if $End_k^0(A)$ is non-commutative.*

Proof. This is somewhat of a restatement of the proposition above. It is stated as above due to its relation with our conjecture.

The following is related to the above Proposition (2.1.2), but is also of independent interest.

Theorem 2.1.4. *Let A be a simple Abelian variety over a finite field k with $\dim(A) > 1$. Suppose that $E := End_k^0(A)$ is non-commutative. Then, $F = \mathbb{Q}[\pi]$ does not have any real embeddings. Furthermore, E is ramified only at those places λ of F that lie above p, the characteristic of the finite field k. Hence, the number places λ of F that lie above p is strictly greater than 1.*

Proof. By the Proposition (2.1.2), we have $P(T) = Q(T)^r$, with $r > 1$. If F has a real embedding, then π can be considered as a real root of $Q(T)$ such that $\pi\bar{\pi} = \pi^2 = q$. Thus, $Q(T)$, the minimal polynomial of the Frobenius endomorphism, is either a linear polynomial $(T - \sqrt{q})$ or the irreducible quadratic polynomial $(T^2 - q)$. But, it can not be linear, for otherwise, part(d) of theorem (2.1.3) would then imply that A is the g-th power of a supersingular elliptic curve over k, and the same follows when $P(T) = (T^2 - q)^g$. By the part(e) of theorem (2.1.3), we know that E is unramified at all places of F that are away from p. This then proves the last assertion of the proposition. □

The proposition below says that if an Abelian variety has enough endomorphisms then it has *potential-good* reduction everywhere. This is from Oort's paper [Oo].

Proposition 2.1.3. (Oort) *Let A be a simple Abelian variety defined over a field k. Let $D := End_k^0(A)$. Suppose that $[D : \mathbb{Q}] > g = \dim(A)$. Then, A has potential-good reduction at all places of k.*

Proof. This is proved in Oort's article [Oo], Lemma (3.9), page 484. □

2.2 Abelian surfaces with Quaternionic Multiplication

We begin this section with the following easy but important result.

Lemma 2.2.1. *Let A be an absolutely simple Abelian surface defined over a finite field k. Then, $End^0_{\bar{k}}(A)$ is commutative.*

Proof. Let k' be a finite extension of k, such that all the endomorphisms of A over $\bar{k}$ are defined over k'. Thus, $End^0_{\bar{k}}(A) = End^0_{k'}(A)$ is a division algebra over $\mathbb{Q}$. Suppose D is non-commutative. Then, by Oort's Proposition (2.1.1) stated earlier, D is a quaternion division algebra over $\mathbb{Q}$ that splits at $\mathbb{R}$. Thus,

$$[End^0_{k'}(A) : \mathbb{Q}] = [D : \mathbb{Q}] = 4.$$

On the other hand, Tate's Theorem (2.1.3(c)) implies that $End^0_{k'}(A)$ is commutative. A contradiction, which proves the lemma. □

Remark. We believe that it is perhaps possible to prove this using Tate's theorem (2.1.3) alone, i.e. without the use of Oort's proposition. We have not explored this as yet.

Theorem 2.2.1. *Let A be an absolutely simple Abelian surface over a number field K such that A has good reduction at all finite places v of K and*

$$End^0_K(A) = D,$$

where D a quaternion division algebra over $\mathbb{Q}$ that splits at $\mathbb{R}$. Then, at all primes v of K of good reduction, A_v is isogenous to the square of an elliptic curve E_v defined over $\overline{k_v}$.

Proof. We will first prove that A_v splits over $\overline{k_v}$. Assume the contrary. Suppose A_v is simple over $\overline{k_v}$, for some finite place v of K. Then by the Lemma (2.2.1) above, $End^0_{k_v}(A_v)$ is commutative. On the other hand, by Corollary (2.1.1), it follows that

$$D := End^0_K(A) \hookrightarrow End^0_{\overline{k_v}}(A_v).$$

Thus, $[End^0_{k_v}(A_v) : \mathbb{Q}]$ is at least 4. Hence, by Oort's Proposition (2.1.1), $End^0_{\overline{k_v}}(A_v) \simeq D$. This contradicts the above Lemma (2.2.1), as D is non-commutative, proving that A_v splits over $\overline{k_v}$.

Thus, A_v is isogenous to a product of two elliptic curves, say E_1 and E_2 over $\overline{k_v}$. Suppose E_1 and E_2 are non-isogenous over $\overline{k_v}$, then

$$End_{\overline{k_v}}(A_v) \simeq End_{\overline{k_v}}(E_1) \oplus End_{\overline{k_v}}(E_2).$$

Also, we have:

$$D \hookrightarrow End^0_{\overline{k_v}}(E_1) \oplus End^0_{\overline{k_v}}(E_2),$$

under the reduction map. By Lemma (2.1.3), D sits injectively into both $End^0_{\overline{k_v}}(E_1)$ and $End^0_{\overline{k_v}}(E_2)$. It is well-known, and does follow from Theorem (2.1.3), that, for an elliptic curve E over $\overline{k_v}$, the dimension of $End^0_{\overline{k_v}}(E)$ over $\mathbb{Q}$ can be at the most 4. It also follows that when it is achieved, the endomorphism algebra is a *definite* quaternion division algebra over $\mathbb{Q}$, i.e. it is non-split at $\mathbb{R}$. This contradicts the fact that D splits at $\mathbb{R}$. Thus, E_1 and E_2 are isogenous over $\overline{k_v}$. Let E_v be an elliptic curve over $\overline{k_v}$ be such that $E_v \sim E_1 \sim E_2$ over $\overline{k_v}$. We can now write:

$$A_v \sim E_v^2$$

over $\overline{k_v}$. Proving the theorem. □

In the above theorem, one can further ask:

Question. Can we find an E_v defined over k_v itself so that A_v and E_v^2 are isogenous over k_v?

With a bit more work, we answer this question affirmatively.

Theorem 2.2.2. *Let A be as in the theorem above. Let v be a place of K of good reduction for A. Then, A_v is isogenous to the square of an elliptic curve E_v defined over the residue field k_v of K.*

Proof. We will follow the notation as in the theorem above. Then, for a place v of K of good reduction for A, we have:

$$D \hookrightarrow End^0_{k_v}(A_v) \hookrightarrow End^0_{\overline{k_v}}(A_v),$$

Let $M := End^0_{\overline{k_v}}(A_v)$, and $\tilde{D} := End^0_{k_v}(A_v)$. By the theorem above, if A_v is *ordinary*, then $M = M_2(F)$, where F is a quadratic field extension of $\mathbb{Q}$, and if A_v is *supersingular*, then $M = M_2(D_p)$, where D_p is the unique quaternion division algebra over $\mathbb{Q}$ that is split at p and at ∞ (i.e. at $\mathbb{R}$).

We want to prove that A_v is split over k_v, and hence is isogenous to the square of an elliptic curve over k_v. This is equivalent to proving that $\tilde{D}$ is not a division algebra. We will show this by using the classification theorem of Tate.

Note that $\tilde{D}$ is non-commutative as it contains D. So, by part (c) of Tate's theorem (2.1.3), $[\tilde{D} : \mathbb{Q}] \neq 4$. Thus, $[\tilde{D} : \mathbb{Q}]$ is either 8 or 16.

By part (d) of the same theorem, if $[\tilde{D} : \mathbb{Q}] = 16$, then it is isomorphic to the algebra of 2 by 2 matrices over the unique quaternion division algebra D_p over $\mathbb{Q}$ which splits at all primes $l \neq p, \infty$. Thus, A_v is isogenous over k_v to the square of a supersingular elliptic curve E_v, all whose endomorphisms are also defined over k_v. This takes care of the supersingular case.

Let us now consider the case of $[\tilde{D} : \mathbb{Q}] = 8$. Then, $\tilde{D}$ is a semi-simple algebra over its centre $F = \mathbb{Q}[\pi]$, where π is the Frobenius endomorphism of A_v relative to k_v. By the proof of the previous Theorem (2.2.1), it follows that if A_v is split over k_v, then it is isogenous to the square of an elliptic curve over k_v. From the dimension of $\tilde{D}$ it then follows that, $\tilde{D} = M_2(F)$, where $F = \mathbb{Q}[\pi]$ is a quadratic field. Thus, in this case, A_v is isogenous over k_v to the square of an ordinary elliptic curve. So let us now assume that

A_v is non-split over k_v. Thus, $F = \mathbb{Q}[\pi]$ is a field. By parts (c) and (d) of Tate's Theorem (2.1.3), the degree of F over $\mathbb{Q}$ can not be 1 or 4. Thus, the minimal polynomial of π is an irreducible quadratic polynomial over $\mathbb{Q}$. Let us denote it by $Q(t) := min(\pi, t)$. Since, we also know that $P(t)$, the characteristic polynomial of π, has to have repeated roots, we conclude that $P(t) = Q(t)^2$. This, by part (e) of Tate's Theorem (2.1.3), implies that $\tilde{D} = M_2(F)$, and that A_v is isogenous to the square of an elliptic curve over k_v. This is a contradiction, and that proves our theorem. □

We recall a definition before we state the next corollary.

Definition 2.2.1. *Let X be a smooth projective variety over a finite field k. Then, by $L(X/k, s)$, we will mean the H^1 L-function of X over k.*

Corollary 2.2.1. *Let A be an absolutely simple Abelian surface with quaternionic multiplication by D defined over a number field K. Assume that K is large enough so that A has everywhere good reduction over K and that all its endomorphisms are defined over K itself. Then, for all v of K, we have:*

$$L(A_v/k_v, s) = L(E_v/k_v, s)^2$$

Proof. This follows from the fact that isogenous Abelian varieties have the same L-function (or that, the characteristic polynomial of the Frobenius endomorphism relative to a fixed finite field depends only on the isogeny class of a given Abelian variety). □

2.3 Examples of absolutely simple Abelian surfaces with quaternionic multiplication

In this brief section, we state a couple of examples of Jacobians of genus 2 hyperelliptic curves as produced by Hashimoto and Murabayanishi [HM]. In their work, they

produce families of curves of genus 2, whose Jacobians have multiplication by an indefinite quaternion division algebra over $\mathbb{Q}$. They call such curves QM-curves. The following are a couple of examples from Example (1.6), page 275 of [HM].

$$C^{(6)}_{1/4,\sqrt{11}/2} \;:\; Y^2 = X\left(X^4 + \frac{1+2\sqrt{11}}{2}X^3 + \frac{99}{20}X62 + \frac{-1+2\sqrt{11}}{2}X + 1\right)$$

$$C^{(6)}_{5/2,\sqrt{-228}} \;:\; Y^2 = X\left(X^4 + \frac{20+\sqrt{-22}}{4}X^3 + \frac{297}{56}X^2 + \frac{-20+\sqrt{-22}}{4}X + 1\right)$$

For these examples, Hashimoto-Murabayanishi prove that the Jacobians of these curves are absolutely simple. This is proved using computations that involve the *Congruence Zeta-functions* of these curves. (The Congruence Zeta-functions are related to Hasse-Weil L-functions and are defined in chapter 2 of Koblitz's book [Ko]).

2.4 Picard numbers of Abelian varieties and Tate's conjectures

In this section we recall some definitions and state some facts and conjectures related to Tate's conjectures about order of poles of L-functions associated with Abelian varieties over number fields.

Let A be an Abelian surface over K. Suppose it is not simple, then it is isogenous to the product of two elliptic curves. The Picard numbers of such surfaces are tabulated below.

Proposition 2.4.1. *Let E_1, E_2 be two elliptic curves over a number field K. Then, the Picard numbers ρ of Abelian surfaces that are isogenous to $E_1 \times E_2$, where E_1 and E_2 are elliptic curves are as follows:*

(a) $\rho = 2$ if $E_1 \not\sim E_2$, i.e. they are non $-$ isogenous.

(b) $\rho = 3$ if $E_1 \sim E_2$, E_1 does not have C.M.

(c) $\rho = 4$ if $E_1 \sim E_2$, isogenous and both have C.M.

Proof. (Sketch) We explain in brief the main ingredients of a line of proof. Firstly notice that, $E_1 \times \{0\}$ and $\{0\} \times E_2$ contribute two cycles in all the above cases. In (b), the extra cycle comes from the graph of an isogeny between E_1 and E_2. In (c), the added extra cycle comes from the graph of the *twisted-isogeny* between E_1 and E_2. (The twisted isogeny is the isogeny between E_1 and E_2, twisted by an extra non-trivial endomorphism that comes from complex multiplication). It then remains to prove that these cycles are *independent* and *generate* the Picard group. □

The next proposition tabulates the Picard numbers based on the endomorphism algebra of a (given) simple Abelian surface.

Proposition 2.4.2. *Let A be a simple Abelian surface over a number field K. Then, the Picard number of A depends on the endomorphism algebra of A as follows:*

$\rho(A) = 1$ if $End_K^0(A) \simeq \mathbb{Q}$, A of type I(1)

$\rho(A) = 2$ if A has multiplication by a real quadratic field, A of type I(2)

$\rho(A) = 3$ if A has quaternionic mulitplication, A of type II(1)

$\rho(A) = 2$ if A has complex multiplication by a field of degree 4, A of type IV$(2,1)$

Proof. This follows from Lemma (3.3) from a paper by Murty [MK], which we state below (as a proposition) for easy reference. □

Proposition 2.4.3. (Murty) *Let A be a simple Abelian variety over a field k of characteristic zero such that $D := End_{\bar{k}}(A) = End_k(A)$. Let $d^2 := [D : F]$ and $e := [F : \mathbb{Q}]$, where $F := Z(D)$ is the centre of D. Then, the Picard number of $\rho(A^r)$ for a positive*

integer r, is given by:

$$\begin{aligned} \textit{type } I(e_0): &\quad \frac{1}{2}er(r+1) \\ \textit{type } II(e_0): &\quad er(2r+1) \\ \textit{type } III(e_0): &\quad er(2r-1) \\ \textit{type } IV(e_0,d): &\quad \frac{1}{2}d^2er^2 \end{aligned}$$

Proof. (*Sketch*) The main idea is to use the fact that the Neron-Severi group of A, denoted by $NS(A)$, injects into $End_k^0(A)$, and that the image is precisely the sub-algebra of $End_k^0(A)$ that is fixed by the Rosati-involution. This identification of $NS(A)$, as a sub-algebra of $End_k^0(A)$, is described in Mumford's [Mu]. □

For easy reference, we now state the above result for $r = 1$.

Corollary 2.4.1. *Let A be a simple Abelian variety defined over a field k of characteristic 0 such that $D := End_{\bar{k}}^0(A) = End_k^0(A)$. Then, with above notation, the Picard numbers $\rho(A)$ of A, are as follows:*

$$\begin{aligned} \textit{type } I(e_0): &\quad e \\ \textit{type } II(e_0): &\quad 3e \\ \textit{type } III(e_0): &\quad e \\ \textit{type } IV(e_0,d): &\quad \frac{1}{2}d^2e \end{aligned}$$

From the above calculations, we deduce the following proposition.

Proposition 2.4.4. *Let A be a simple Abelian surface over a number field K so that $End_K(A) = End_{\bar{K}}(A)$. Then, $\rho(A) = 3$ if and only if $End_K(A) \otimes \mathbb{Q}$ is non-commutative. Moreover, if $\rho(A) = 3$ then for all but finitely many primes v, we have that A_v is reducible.*

This result can be interpreted in terms of lifting of cycles to characteristic zero. Indeed, the fact that A_v is reducible implies the existence of "extra" algebraic cycles, say

C_v, on A_v. The question is whether there is a global cycle C on A which specializes to C_v for every v. The above proposition suggests that there is a cycle. To prove this, we need to prove the converse of the last statement of the above proposition.

Lemma 2.4.1. *Let A be a simple Abelian surface over a number field K as above. Suppose that for a finite place v of K of good reduction for A, we have $A_v \sim_{k_v} E_1 \times E_2$, where E_1 and E_2 are ordinary non-isogenous elliptic curves over k_v. Here k_v is the finite residue field at v. Then, A is of type $I(1)$, that is $End_K(A) \otimes \mathbb{Q} = \mathbb{Q}$.*

Proof. We see that $End_{k_v}(E_1) \otimes \mathbb{Q}$ and $End_{k_v}(E_2) \otimes \mathbb{Q}$ are imaginary quadratic fields. But $End_K(A) \otimes \mathbb{Q}$ injects into each of them. The result follows by the Albert-Oort classification. □

Chapter 3

Main Results

3.1 Abelian varieties with C.M.

We begin with a theorem by Rajan [Ra], which we need to prove the main theorem of this section. This is a qualitative form of the strong multiplicity one theorem for $GL(1)$. It is noted in [Ra] that the result is essentially due to Hecke.

Theorem 3.1.1. (Rajan)[Ra] *Let θ_1 and θ_2 be two idèle class characters on K. Suppose that the set of places v of K for which*

$$\theta_{1,v} = \theta_{2,v}$$

is of positive upper density. Then,

$$\theta_1 = \chi\theta_2$$

for some Dirichlet character χ of K. In particular the set of primes at which the local components of θ_1 and θ_2 coincide has a density.

Proof. The proof can be found in a paper by Rajan [Ra], and is based on an *equidistribution* result about Hecke characters. □

In our use of this theorem, we need it when the Hecke characters involved are of type A_0 (in the sense of Weil, as described in the proposition below). A proof of this result

in this special case appears in [Ha], page 95. We found out about this in the paper of Rajan mentioned above, and we reproduce it here for the sake of completeness.

Proposition 3.1.1. *Let K be a Galois extension of $\mathbb{Q}$, and let w be an unramified prime of degree 1 over $\mathbb{Q}$. Suppose θ is an algebraic character of type A_0, and $\theta_w = 1$. Then θ is of finite order.*

Proof. A character θ is said to be of type A_0, if θ restricted to the Archimedean components $\prod_{\lambda\in\sum_\infty} K_\lambda^*$, is of the form

$$\theta(\alpha_\lambda)_{\lambda\in\sum_\infty} = \prod_{\lambda\in\sum_\infty} \alpha_\lambda^{r_\lambda}\overline{\alpha_\lambda}^{s_\lambda}$$

for some integers r_λ and s_λ, and where λ runs through the Archimedean places $\sum_\infty$ of K. At each finite place v of K, $\mathcal{O}_v^*$ is a compact, profinite group. Hence the image $\theta_v(\mathcal{O}_v^*)$ is a finite subgroup of $\mathbb{C}^*$. Since θ is unramified at all but a finite number of places of K, by raising θ to a suitable power we can assume that θ is unramified at all finite places of K. Let $\wp_w$ be the prime ideal of $\mathcal{O}_K$ that corresponds to the finite place w of K. By the finiteness of class number, it follows that there exists $\alpha_w \in \mathcal{O}_K$ that generates $\wp_w^m \subset \mathcal{O}_K$ for some positive integer m, (m can be taken to be the class number $h(K)$ of K). By definition, α_w is a unit for all other finite places $w' \neq w$. Since, $\theta_w = 1$, and θ is unramified at all finite places of K, it follows that

$$\theta((\alpha_w)_{fin}) = \theta((\alpha_{w_\lambda})_{\lambda\in\sum_f in}) = 1.$$

As θ is an idèle class character, $\theta(\alpha_w) = 1$. Hence,

$$\theta((\alpha_{w_\lambda})_{\lambda\in\sum_\infty}) = \prod_{\lambda\in\sum_\infty} \alpha_{w_\lambda}^{r_\lambda}\overline{\alpha_{w_\lambda}}^{s_\lambda} = 1$$

Since, w (or $\wp_w$) is unramified and of degree 1 over $\mathbb{Q}$, the conjugates of α_w are multiplicatively independent. It thus follows from the above that $r_\lambda = s_\lambda = 0$ for all Archimedean places λ. This implies that the character θ (more correctly, θ^m) is trivial at all the

archimedean places. By the finiteness of class number of K, it now follows that the character θ has finite order. □

As a corollary of the above, we have the following 'strong multiplicity one theorem' for Hecke characters of type A_0.

Corollary 3.1.1. *Let θ_1 and θ_2 be two idèle class characters on a number field K and of type A_0. Suppose that the set of places v of K for which both*

$$\theta_{1,v} = \theta_{2,v}$$

is of positive upper density. Then,

$$\theta_1 = \chi\theta_2$$

for some Dirichlet character χ of K. In particular, the set of primes at which the local components of θ_1 and θ_2 coincide has a density and an arithmetic meaning.

Proof. This follows from applying Proposition (3.1.1) to the idèle class character $\theta = \theta_1\theta_2^{-1}$. □

We now state the following consequence of the theory of Abelian varieties with complex multiplication. This computes the H^1 L-function of such an Abelian variety.

Theorem 3.1.2. *(Shimura-Taniyama) Let A be an Abelian variety defined over a number field K and with C.M. by a number field F such that*

$$F \hookrightarrow End_K^0(A),$$

with $[F : \mathbb{Q}] = 2\dim(A) = 2g$. Then, there exist a unique continuous homomorphism

$$\psi : \mathbb{J}_K \to (F \otimes_{\mathbb{Q}} \mathbb{R})^\times$$

that is trivial on $K^\times$. For each $\sigma \in Hom(F, \mathbb{C})$, let ψ_σ be the composite defined by:

$$\psi_\sigma : \mathbb{J}_K \xrightarrow{\psi} (F \otimes_{\mathbb{Q}} \mathbb{R})^\times \xrightarrow{\sigma\otimes 1} \mathbb{C}^\times.$$

Then, each ψ_σ is trivial on $K^\times$, and thus forms an idèle class character (or grossen-character) of K, and the H^1 L-function of A over K is given by:

$$L(H^1(A), s) = \prod_{\sigma \in Hom(F,\mathbb{C})} L(\psi_\sigma, s).$$

Proof. This is the Shimura-Taniyama theory. The case of elliptic curves was treated by Deuring [De]. Our reference for this is a nice exposition by Milne [Mi], Theorem 13.1 and 13.2 (page 28). □

3.2 The Complex Multiplication Case

Let A be an Abelian variety of CM-type defined over $\mathbb{C}$. This means that there exists a commutative, semi-simple subfield F of $End^0(A)$ such that $[F : \mathbb{Q}] = 2\dim(A) = 2g$.

If A is defined over $\mathbb{C}$ and has C.M. by a number field F, then it can be shown that it has a model defined over a number field K (Shimura-Taniyama [ShTa] or Lang [La1]). Thus, we will henceforth assume that A is defined over a number field K, and by extending the field (if necessary), we will further assume that all the endomorphisms of A are defined over K as well.

Before stating the theorem, we begin with the following general lemma that we use.

Lemma 3.2.1. *Let A be an Abelian variety defined over field k. (Here k is any field.) Let $E = End_k^0(A)$ be its endomorphism algebra over k. Suppose $F := Z(E)$ (the centre of E) is a field, then A is isogenous to a power of a simple Abelian variety defined over k.*

Proof. If A is simple over k, then we are done. Suppose A is not simple over k, and is not isogenous to a power of a simple Abelian variety over k. Then, we can write:

$$A \sim_k B_1 \times B_2,$$

where B_1 and B_2 are defined over k, and that B_1 and B_2 do not share a simple Abelian variety as a factor. In other words, under the above assumption we can ensure that: $End_k(B_1, B_2) = \{0\}$. Thus, we have:

$$E = End_k^0(A) \simeq End_k^0(B_1) \oplus End_k^0(B_2).$$

This gives,

$$F = Z(E) = Z(End_k^0(B_1)) \oplus Z(End_k^0(B_2)).$$

This contradicts the fact that F is a field, and that proves the lemma. □

The next lemma is crucial for our theorem.

Lemma 3.2.2. *Let A be a simple Abelian variety defined over a number field K with C.M. by F, where $[F : \mathbb{Q}] = 2g$. Suppose, for a finite place v of K, $A_v := A \mod v$ is split over k_v, the residue field of K at v. Then,*

$$A_v \sim_{k_v} B_v^n,$$

for a simple Abelian variety B_v defined over k_v, and $n \geq 2$.

Proof. By Proposition (1.2.1) of chapter 1, we can write:

$$A_v \sim B_1^{n_1} \times \cdots \times B_r^{n_r},$$

where B_i are simple and pair-wise non-isogenous over k_v. Let

$$D_i := End_{k_v}^0(B_i),$$

with

$$K_i := Z(D_i) = \text{ Centre}(D_i),$$

for $i = 1$ to r. Thus, we have:

$$F = End_K^0(A) \hookrightarrow End_{k_v}^0(A_v) \simeq \oplus_{i=1}^r M_{n_i}(D_i),$$

and

$$\begin{aligned} Z(End^0_{k_v}(A_v)) &= Z(\oplus_{i=1}^r M_{n_i}(D_i)) = \oplus_{i=1}^r Z(M_{n_i}(D_i)) \\ &= \oplus_{i=1}^r Z(D_i) = \oplus_{i=1}^r K_i. \end{aligned}$$

The lemma would follow if we prove that $Z(End^0(A_v))$ - the centre of the endomorphism algebra $End^0_{k_v}(A_v)$ - is itself a field, as this will force $r = 1$ by Lemma (3.2.1). This is proved as follows:

By Tate's classification theorem (2.1.3), we know that a maximal commutative sub-algebra of $End^0_{k_v}(A_v)$ has dimension $2\dim(A_v) = 2g$ over $\mathbb{Q}$. But F injects into $End^0_{k_v}(A_v)$, and is indeed a commutative semi-simple sub-algebra of $End^0_{k_v}(A_v)$ with $[F : \mathbb{Q}] = 2g$. Hence, F is a maximal commutative semi-simple sub-algebra of $End^0_{k_v}(A_v)$. Since, the centre of $End^0_{k_v}(A_v)$ is contained in any maximal commutative semi-simple sub-algebra of $End^0_{k_v}(A_v)$, we get:

$$Z(End^0_{k_v}(A_v)) \hookrightarrow F.$$

This proves that $Z(End^0_{k_v}(A_v))$ is a field, and that proves the lemma. □

The next corollary states that the eigenvalues of the *Frobenius* at all finite places v of K are contained in the C.M. field F.

Corollary 3.2.1. *Let A defined over K be as above. Let v be a finite place of K of good reduction. Then, $A_v \sim B_v^n$ for a simple Abelian variety B_v over k_v with $n \geq 1$. Let $K_{B_v} := Z(End^0_{k_v}(B_v))$. Then,*

$$K_{B_v} \subset F.$$

Also, if $K_{B_v} = F$, then A remains simple modulo v.

Proof. In the lemma above, we proved that F is a maximal commutative semi-simple subalgebra of $M_n(End^0_{k_v}(B_v))$. Thus, it contains K_{B_v}.

If $K_{B_v} = F$, then $[K_{B_v} : \mathbb{Q}] = 2\dim(A_v)$. On the other hand, by Tate's classification theorem (2.1.3) $[K_{B_v} : \mathbb{Q}] \leq 2\dim(B_v)$. Thus, $2\dim(A_v) \leq 2\dim(B_v)$. Since, B_v is an Abelian subvariety of A_v, this implies that $A_v = B_v$ is simple over k_v. □

Remark. Note that, we already know this result from the Shimura-Taniyama theory. Nonetheless, the way it relates the simplicity of A_v over k_v to the generation of F (over $\mathbb{Q}$) by the eigenvalues of the Frobenius at v, is noteworthy.

Remark. The converse of the above corollary is false. Here is a counterexample. Let E be an elliptic curve defined over a number field K such that E has C.M. by a quadratic imaginary field F with C.M. defined over K. Let v be a place of K of good supersingular reduction for E. Then, $D := End^0_{k_v}(E_v)$ is a quaternion division algebra over $\mathbb{Q}$. In this case, $Z(D)$, the centre of D is $\mathbb{Q}$ and is strictly contained in F.

Corollary 3.2.2. *With above notation:*

$$L(H^1(A_v), s) = L(H^1(B_v), s)^r,$$

where L is the H^1 L-function.

Proof. This follows from the fact that the H^1 L-function of an Abelian variety is invariant under isogeny. □

From here onwards, we will assume that F acts K-rationally, and that A has everywhere good reduction over K. These assumptions are not essential, but they do simplify the proof considerably. Later, we will indicate how the theorem below would follow without any assumptions as above.

The following is the main theorem of this section:

Theorem 3.2.1. *Let A be an absolutely simple Abelian variety of CM-type defined over a number field K such that*

$$End^0_K(A) \simeq F.$$

Then, for a set of places v of K of density 1, the reduction A_v is also simple over k_v, the residue field of K at v.

Proof. Let $g := dim(A)$. By Theorem (3.1.2) as above, the L-function of A over K is given by

$$L(A,s) = \prod_{\sigma \in Hom(F,\mathbb{C})} L(\psi_\sigma, s).$$

We will re-index the ψ_σ's by $1 \leq i \leq 2g$ as follows: for $1 \leq i \leq g$, let $\psi_i := \psi_\sigma$ be the Hecke-characters of K. Here σ varies over a subset of cardinality g consisting of pairwise non-conjugate elements of $Hom(F,\mathbb{C})$. For $1+g \leq i+g \leq 2g$, we let $\psi_{i+g} := \overline{\psi_i} = \overline{\psi_\sigma} = \psi_{\bar{\sigma}}$. Then, the H^1 L-function of A can be re-written as:

$$L(A,s) = \prod_{i=1}^{2g} L(\psi_i, s).$$

In the above equation

$$\psi_i \bar{\psi}_i = \mathbb{N}_{\mathbb{J}_\mathbb{Q}}^{\mathbb{J}_K} = \mathbb{N}$$

as an equality of characters of $\mathbb{J}_K$ into $\mathbb{C}^*$. Here $\mathbb{N}_{\mathbb{J}_\mathbb{Q}}^{\mathbb{J}_K} = \mathbb{N}$ is the *norm* character of $\mathbb{J}_K$. Thus, for a finite place v of K, $\mathbb{N}v$ denotes the usual norm of v over $\mathbb{Q}$. Note that, if ψ is unramified at v, then we can write:

$$\alpha_{v,\,i} := \psi_i(\pi_v),$$

where π_v is a uniformizer of K_v. Here the value of $\psi_i(\pi_v)$ is independent of the choice of the uniformizer π_v. By the Shimura-Taniyama theory, the $\alpha_{v,i}s$ are the eigenvalues of the *Frobenius* at v acting on $T_l(A)$. Let R be the set of finite places v of K at which some character $\psi_i,\ 1 \leq i \leq g$ is ramified. Then, R is a finite set. Thus, up to a factor, say $*$, associated with the places $vinR$, we can write:

$$L(A,s) = * \prod_{v \notin R} \left(\prod_{i=1}^{2d} (1 - \frac{\alpha_{v,\,i}}{(\mathbb{N}v)^s})^{-1} \right)$$

Further more it follows that, the H^2 L-function of A is given by:

$$\begin{aligned} L(H_l^2(A), s) &= \prod_{i<j} L(\psi_i\psi_j, s) \\ &= \prod_{i<j\neq i+g} L(\psi_i\psi_j, s) \cdot \left(\prod_{1\leq i\leq g} L(\psi_i\psi_{i+g}, s) \right) \\ &= \prod_{i<j\neq i+g} L(\psi_i\psi_j, s) \cdot \left(\prod_{1\leq i\leq g} L(\mathbb{N}_{\mathbb{J}_\mathbb{Q}}^{\mathbb{J}_K}, s) \right) \end{aligned}$$

In the above, each factor $L(\mathbb{N}_{\mathbb{J}_\mathbb{Q}}^{\mathbb{J}_K}, s) = \zeta(s-1)$ contributes a simple pole at $s = 2$. By Theorem 5, page 177 of Pohlmann [Po] that verifies a conjecture of Tate's, the order of pole at $s = 2$ of the H^2 L-function equals the Picard number of A. By Proposition (2.4.3) of Chapter 2, the Picard number of A over K equals g, and thus the order of pole at $s = 2$ equals g. This then forces the holomorphy of $L(\psi_i\psi_{j+g}, s)$ at $s = 2$, whenever $i \neq j$, $1 \leq i, j \leq g$.

Let us now assume that the set of places v of K for which A_v splits over k_v has positive upper density. Under this assumption, we aim for a contradiction.

Let v be a place of K at which A_v is not simple. By Lemma (3.2.2),

$$A_v \sim B_v^r$$

for a simple Abelian variety B_v with $r \geq 2$. This implies that the characteristic polynomial of the Frobenius at v is a power of the characteristic polynomial of the Frobenius acting on the l-adic Tate-module of B_v. The roots of these polynomials are precisely the $\alpha_{v,i}$s and their conjugates $\alpha_{v,i+g}$s for $i = 1$ to g. We thus conclude that

$$\alpha_{v,i} = \alpha_{v,j},$$

for some $1 \leq i < j \leq g$. Here the i and j depend on v. By our assumption that A_v is not simple for a positive upper density of places v of K, it follows that there exists at

least one fixed pair $\{i_0, j_0\}$ with $1 \leq i_0 < j_0 \leq g$ and such that for a positive density of places of v of K

$$\alpha_{v,i_0} = \alpha_{v,j_0}.$$

But, by a theorem of Rajan (Theorem (3.1.1)) or by Corollary (3.1.1) applied to the Hecke characters ψ_{i_0} and ψ_{j_0}, it follows that:

$$\psi_{i_0} = \chi\psi_{j_0},$$

for some Dirichlet character χ - a Hecke character of finite order - of K. Here, by the class field theory, χ may also be considered as a character of $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$. Let L be the cyclic extension of K cut out by χ. Thus, χ becomes trivial as a Hecke character of $\mathbb{J}_L$, and we have:

$$\psi_{i_0} \;=\; \psi_{j_0},$$

where ψ_{i_0} and ψ_{j_0} are to be considered as characters of $\mathbb{J}_L$, by extension to $\mathbb{J}_L$ from $\mathbb{J}_K$, by the $\mathbb{N}_{\mathbb{J}_K}^{\mathbb{J}_L}$ (*relative norm*) map. This does not create any problems because the H^1 L-function of the Abelian variety over K also changes by the norm map, $\mathbb{N}_{\mathbb{J}_K}^{\mathbb{J}_L}$, under the base change from K to L. Note also that the splitting-property of A is preserved under the extension from K to L by Lemma (2.1.1). Thus, the factor $L(\psi_{i_0}\overline{\psi_{j_0}}, s)$ where $i_0 \neq j_0$, contributes an extra pole to $L(H_l^2(A), s)$ at $s = 2$. This contradicts the fact that $L(H_l^2(A), s)$ has a pole of exact order g at $s = 2$, and that proves the theorem. □

3.3 Abelian varieties associated with cusp forms

In this section, we wish to prove a theorem as above for Abelian varieties attached to newforms of weight 2 for congruence subgroups of $\Gamma := SL(2, \mathbb{Z})$. We begin with some standard notations, definitions and some well-known theorems.

Let N be a positive integer. Let

$$\Gamma_0(N) := \{g \in \Gamma : g \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod N\}.$$

Let $M_2(N, \mathbb{C}) := M_2(\Gamma_0(N), \mathbb{C})$ be the vector space of weight 2 modular forms for $\Gamma_0(N)$. Under the Peterson inner product, the vector space $M_2(N, \mathbb{C})$ can be turned into a Hilbert space.

It is a theorem that $M_2(N, \mathbb{C})$ has a $\mathbb{Q}$-structure enabling us to define the action of $Aut(\mathbb{C})$ on $M_2(N, \mathbb{C})$.

Remark. The converse, an exercise in Lang's Algebra [La3], is also true, and is as follows: Let V be a vector space over $\mathbb{C}$ of finite dimension, equipped with a semi-linear action of $Aut(\mathbb{C})$ on V, i.e. such that, for each $v \in V$, $\sigma \in Aut(\mathbb{C})$, and $\lambda \in \mathbb{C}$, $\sigma(\lambda v) = \sigma(\lambda)\sigma(v)$. Then, there exists a $\mathbb{Q}$-subspace of V, say $V_{\mathbb{Q}}$, such that $Aut(\mathbb{C})$ acts trivially on $V_{\mathbb{Q}}$ and such that $V = V_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{C}$.

Let f be a cusp form of weight 2 for the group $\Gamma_1(N)$ with character ϵ. We assume that f is a normalized newform, i.e. with $a_1(f) = 1$ and such that it is an eigenform of the Hecke algebra $\mathbb{T}(N)$. For such an f, it follows that $a_n(f)$ is an algebraic number for all n. Here, $a_n(f)$ is the eigenvalue of $T_n \in \mathbb{T}(N)$ for f. Since the T_ns are unitary operators with respect to the Peterson scalar product, it follows that, the $a_n(f)$s are totally real if $\epsilon = 1$. Let K_f be the field generated by $a_n(f)$s for all n and the values of the nebentypus character ϵ associated with f and N. From the fact that $M_2(\Gamma_0(N), \mathbb{C})$ has a $\mathbb{Q}$-structure, it follows that K_f is a number field. Let $\Phi := Hom(K_f, \mathbb{C})$. By the work of Shimura, to such an f, one associates an Abelian variety, say A_f, defined (up to isogeny) over $\mathbb{Q}$, as a quotient of $J := J_1(N)$, with the following main properties:

1. A_f is defined over $\mathbb{Q}$ and $\dim(A_f) = [K_f : \mathbb{Q}]$.

2. $K_f \hookrightarrow End(A_f) \otimes_{\mathbb{Z}} \mathbb{Q}$.

3. $L(A_f, s) = L(H^1_\ell(A_f), s) = \prod_{\sigma\in\Phi} L(f^\sigma, s)$.

Remark. For example, if the Fourier coefficients of f are rational integers then $K_f = \mathbb{Q}$, A_f is an elliptic curve over $\mathbb{Q}$, and $L(A_f, s) = L(f, s)$. The Shimura-Taniyama conjecture, now a theorem by Breuil-Conrad-Diamond–Taylor, says that every elliptic curve E over $\mathbb{Q}$ is isogenous to some A_f associated with an eigenform $f \in M_2(\Gamma(N), \mathbb{C})$ for a precisely predicted level $N = N(E)$.

Thus, for f as above, we can write:

$$L(A_f, s) \;=\; \prod_{\sigma}\prod_{p} (1 - a_f(p)^\sigma p^{-s} + \epsilon^\sigma(p)p^{1-2s})$$

where σ ranges over the embeddings of K_f into $\mathbb{C}$.

3.3.1 Twists and Inner Twists

Let f be a new-form of level N and let χ be a (primitive) Dirichlet character of conductor r. Then, there is a unique new-form $g = \sum_{n\geq 1} b_n q^n$ that satisfies the relation:

$$b_p = a_p\,\chi(p), \text{ for almost all } p,$$

i.e. for all but finitely many primes p. This implies $b_n = a_n\,\chi(n)$, for $(n, r) = 1$. In this case, we say that g is a *twist* of f by χ. If ϵ_f and ϵ_g are respectively the nebentypus characters of f and g, then it follows that:

$$\epsilon_g = \epsilon_f \cdot \chi^2.$$

When such a g is a conjugate $\sigma f := f^\sigma$ of f for some $\sigma \in Aut(\mathbb{C})$, we say that f^σ is an *inner twist* of f. In other words, if f is a form that is an inner-twist of itself, then

$$a_p = \chi(p)\,a_p, \text{ for almost all } p,$$

for some Dirichlet character $\chi \neq 1$. Such a form f is said to have *complex multiplication*. It turns out that if a newform f has complex multiplication, then the corresponding A_f

is of C.M. type. Since we have discussed Abelian varieties of C.M. type in the previous section, we will exclude such newforms f in this section. Thus, in what follows, we shall assume that f is a newform without C.M. This further implies that $\epsilon = 1$ and in this case, the coefficient field K_f is totally real. Even though, f is not an inner-twist of itself, it may be an inner-twist of it's conjugate. As σ varies over $Aut(\mathbb{C})$, we want to count those f^σ's that are inner-twists of f. Let $\Phi := Hom(K_f, \mathbb{C})$. It is enough to consider σ over Φ. Thus, one defines the *twisting group*, to be denoted by Γ_f, as the subset of $\sigma \in \Phi$ so that:

$$\sigma(a_p) = \chi_\sigma(p)\, a_p, \ \textit{for almost all } p,$$

for some Dirichlet character χ_σ that depends on σ. Since f does not have C.M., χ_σ is uniquely determined by $\sigma \in \Gamma_f$. This makes the notation χ_σ unambiguous. It then follows from propositions (3.1), (3.2), and (3.3) of [Ri1] that Γ_f is an Abelian subgroup of $Aut(K_f)$. Let $F_f := K_f^{\Gamma_f}$, be the fixed field of K_f under Γ_f. Then, we have the following proposition of Ribet [Ri1], that is important for us:

Proposition 3.3.1. *Let f be a newform with trivial nebentypus character. Suppose that the level N is square-free. Then, $\Gamma_f = \{1\}$.*

We now quote one of the main consequences of the work of Momose [Momose] and Ribet [Ri1]. The theorem below describes the endomorphism algebra of A_f, when f does not have C.M. and is a compilation of a few results.

Theorem 3.3.1. *Let f be a newform of level N and nebentypus ϵ_f and without C.M. Let A_f be the Abelian variety associated with f by Shimura. Let K_f, F_f and Γ_f be as defined earlier. Let $\gamma := [K_f : F_f] = |\Gamma_f|$. Let $E_f := End^0_{\mathbb{Q}}(A_f)$. Then:*

1. *E_f is central simple algebra over F_f, i.e. $[E_f : F_F] = \gamma^2$.*
2. *K_f is a maximal commutative semi-simple subalgebra of E_f.*
3. *$[E_f : \mathbb{Q}] = [K_f : F_f][K_f : \mathbb{Q}] = \gamma^2\,[F_f : \mathbb{Q}]$*

4. *The algebra E_f is a either a matrix algebra over F_f or else a matrix algebra over a quaternion division algebra with centre F_f.*

5. *E_f unramified at the Archimedean places v of F_f. It is also unramified at all places v of F_f at which A_f has ordinary reduction.*

Proof. This is Theorem (5.1) from [Ri1] and together with a few results from [Ri4]. □

As a consequence we have:

Corollary 3.3.1. *Let f be as above. Let the order of the Twisting group, $\gamma := |\Gamma_f| > 1$. Then, $End(A_f)$ is non-commutative.*

Proof. This follows from the above Theorem (3.3.1. □

We also have:

Corollary 3.3.2. *Let f be a newform with trivial nebentypus and square-free level N. Then, A_f defined over $\mathbb{Q}$ is absolutely simple with*

$$E_f := End^0_{\mathbb{Q}}(A_f) = K_f,$$

the coefficient field of f.

Proof. This follows from the above theorem with the earlier fact that $\Gamma_f = \{1\}$, when the level N is square-free. □

Remark. When the nebentypus is trivial, but N is not square-free it is not easy to tell whether the class of E_f as an element of the Brauer group of F_f is trivial or not. Though by the theorem above, we know that it has order 2.

3.3.2 Theorem on splitting

We begin with the following preliminary result.

Lemma 3.3.1. *Let A be an Abelian variety defined over $\mathbb{Q}$ such that*

$$F \hookrightarrow End^0_{\mathbb{Q}}(A)$$

where F is a totally real field with $[F : \mathbb{Q}] = g = \dim(A)$. Further, assume that the $1 \in F$ acts on A as the identity element of $End^0_{\mathbb{Q}}(A)$. Let p be a prime of good reduction of A. Also assume that p does not ramify in F. Suppose $A_p := A \mod p$ is not simple over the finite field $\mathbb{F}_p$. Then, the characteristic polynomial of A_p has repeated roots.

Proof. Since A_p splits over $\mathbb{F}_p$, let us write:

$$A_p \sim B_1^{n_1} \times \cdots \times B_r^{n_r},$$

where B_is are pairwise non-isogenous simple Abelian varieties over $\mathbb{F}_p$ of a strictly smaller dimension than $\dim(A) = g$.

If $n_i \geq 2$ for some i, then we are done. If not, then

$$A_p \sim B_1 \times \cdots \times B_r,\ r \geq 2,$$

Let $E_i := End^0_{\mathbb{F}_p}(B_i)$. Then, by the injectivity corollary (2.1.1), we can write:

$$F \hookrightarrow End^0_{\mathbb{Q}}(A) \hookrightarrow End^0_{\mathbb{F}_p}(A_p) \simeq \oplus_i E_i.$$

By our assumption that the $1 \in F$ acts on A_p as the identity, it follows by Lemma (2.1.3) that the image of F into $End^0_{\mathbb{F}_p}(A_p)$, followed by the projection to E_i, is also an injection for all $i = 1$ to r. Thus,

$$F \hookrightarrow E_i,\ \forall\ i = 1, \cdots, r.$$

Now, by Tate's Theorem (2.1.3) on the *endomorphism algebras of Abelian varieties defined over finite fields*, it follows that

$$F_i = Z(E_i) = \mathbb{Q}[\pi] = \frac{\mathbb{Q}[t]}{min_{B_i}(\pi, t)} = \frac{\mathbb{Q}[t]}{Q_i(t)},$$

where $Q_i(t) := min_{B_i}(\pi, t)$ is the minimal polynomial of π, the Frobenius endomorphism relative to $\mathbb{F}_p$, acting on B_i. It then follows that $P_i(t)$, the characteristic polynomial

of π with respect to B_i is a power of $Q_i(t)$ for all i, with $Q_i(t)$ irreducible over $\mathbb{Q}$. If any of these powers are greater than 2, we have a repeated root and we are done. This implies that $P_i(t) = Q_i(t)$ for all i. By Tate's Theorem (2.1.3)(c), it then follows that $E_i = End^0_{\mathbb{F}_p}(B_i)$ is commutative for all i, and

$$F \hookrightarrow E_i = F_i = \frac{\mathbb{Q}[t]}{P_i(t)}.$$

But, since $r \geq 2$, $\dim(B_i) \leq \frac{g}{2}$ for some i, and so $[F_i : \mathbb{Q}] \leq g$. Without loss of generality, let $i = 1$. Thus, we have:

$$F = F_1 = E_1 \simeq \mathbb{Q}[t]/(P_1(t))$$

(It can be assumed that $\deg(P_i) \geq 2$ for all i.) Let $P(t)$ be the characteristic polynomial of the Frobenius at p acting on A_p. Then, $P_1(t)|P(t)$. Let α be a root of $P_1(t)$. By construction, $\alpha \in F$. Then, $\beta = \frac{p}{\alpha}$ is another root of $P(t)$, and $\beta \in F$. Since both are roots of $P(t)$, they have absolute value $\sqrt{p}$. On the other hand both are totally real as elements of F , and satisfy the quadratic polynomial given by:

$$t^2 - (\alpha + \beta)t + p = t^2 - a_p t + p,$$

where $a_p = \alpha + \frac{p}{\alpha} \in F$ is totally real, and satisfies the Hasse-Weil bound

$$|a_p| \leq 2\sqrt{p}.$$

This implies that the discriminant of the quadratic polynomial:

$$a_p^2 - 4p \leq 0.$$

But, as already observed $\alpha, \beta \in F$ are totally real. By the above, this is possible if and only if

$$a_p^2 - 4p = 0,$$

implying that $\alpha = \beta = \sqrt{p} \in F$. But, by hypothesis p does not ramify in F and so this is a contradiction, and that proves the lemma. □

Remark. Note that the Lemma above generalizes to Abelian varieties that are defined over any number field K. This follows from the above proof.

We are now ready to state and prove the main theorem of this section:

Theorem 3.3.2. *Let f be a newform of weight 2 and level N with nebentypus 1. Suppose that the A_f, as defined earlier, is absolutely simple over $\mathbb{Q}$. Suppose that the set of primes p such that the reduction of A_f modulo p splits, has positive density. Then, the Twisting group Γ_f is non-trivial, i.e. $\gamma = |\Gamma_f| > 1$. Hence, $End^0_{\bar{\mathbb{Q}}}(A_f)$ is non-commutative.*

Remark. It is a fact that the A_fs are defined over $\mathbb{Q}$. It is not always the case that such an A_f is absolutely simple.

Proof. It is known that A_f has good reduction outside primes dividing N. Then, at a prime p not dividing N, the 'congruence L-function' of the reduction of A_f is given by

$$\begin{aligned} \zeta_p(A_f, T) &:= \prod_{\sigma}(T - \pi_p^{\sigma})(T - \overline{\pi_p^{\sigma}}) \\ &= \prod_{\sigma}(T^2 - a_p^{\sigma}T + p), \end{aligned}$$

where the product is over the embeddings $\sigma \in \Phi := Hom(K_f, \mathbb{C})$. Note that $\Phi = Hom(K_f, \mathbb{R})$ as K_f is a totally real field. Thus,

$$\pi_p^{\sigma} + \overline{\pi_p^{\sigma}} = a_f(p)^{\sigma}$$

and

$$\pi_p^{\sigma}\overline{\pi_p^{\sigma}} = p.$$

It is a fact that $\zeta_p(A_f, T)$ is the monic characteristic polynomial polynomial of the *Frobenius* endomorphism $A_f \mod p$ relative to the finite field $\mathbb{F}_p$. This is a consequence of Shimura theory, and is inherent in the preliminary results stated at the beginning of section (3.3).

Note that, since K_f is a number field, only finitely many primes p (as a function of the level N), ramify in K_f. In particular, for a large enough p, we see that $\sqrt{p}$

does not lie in K_f, and so $\pi_p \neq \overline{\pi_p}$. Now, by Lemma (3.3.1) it follows that, if the reduction of A_f modulo p splits over $\mathbb{F}_p$, we have a repeated root in the characteristic polynomial of the Frobenius of A_f *modulo* p. This then implies that two different factors of $\prod_\sigma (T - \pi_p^\sigma)(T - \overline{\pi_p^\sigma})$ coincide. Thus, for some pair

$$\sigma_1 \neq \sigma_2,\ \sigma_1, \sigma_2 \in \Phi,$$

we have:

$$\pi_p^{\sigma_1} = \pi_p^{\sigma_2} \text{ or } \overline{\pi_p^{\sigma_2}}. \tag{3.1}$$

This in turn implies that

$$a_f(p)^{\sigma_1} = a_f(p)^{\sigma_2}. \tag{3.2}$$

Furthermore, viewing σ_1 and σ_2 as automorphisms of $\mathbb{C}$, and setting $\sigma = \sigma_2\sigma_1^{-1}$, we deduce that:

$$a_f(p) = a_f(p)^{\sigma}. \tag{3.3}$$

Now, if A_f splits for a set of primes of positive upper density, then there exists a pair (σ_1, σ_2) such that the above relation (3.2) holds for a set of primes of positive upper density. Thus, for $\sigma = \sigma_2\sigma^{-1}$, the above relation (3.3) holds for a set of primes of positive upper density.

We now claim that there exists a Dirichlet character χ of $\mathbb{Q}$ such that

$$a_p^{\sigma_1} = a_p^{\sigma_2}\, \chi(p),\ \textit{for almost all } p.$$

Indeed this is a *direct* application of Corollary 1 of [Ra2] applied to the two modular forms f^{σ_1} and f^{σ_2}. (For easy reference, we restate this Corollary 1 of Rajan [Ra2] in simplified form. It is the Proposition (3.3.2) below.)

Remark. The claim above can also be proved using results of Ribet in [Ri2], [Ri3] and Momose [Momose] about the image of ℓ-adic Galois representations attached to modular forms. This line of proof is based on a clever use of Chebotarev density theorem and is in some sense more direct.

Thus, according to the definition of the Twisting group Γ_f,

$$\sigma := \sigma_2 \sigma_1^{-1} \neq 1 \in \Gamma_f.$$

By Corollary (3.3.1), this implies that $End^0_{\bar{\mathbb{Q}}}(A_f)$ is non-commutative and that completes the proof. □

Proposition 3.3.2. (Rajan) *Let f_i be two newforms of levels N_i, weights k_i and nebentypus characters ϵ_i for $i = 1, 2$. Also assume that f_1 is a non C.M. cusp forms of weight $k_1 \geq 2$. Suppose that the set $\{p \mid a_p(f_1) = a_p(f_2)\}$ has positive upper density. Then there exists a Dirichlet character χ of $\mathbb{Q}$ such that $f_2 \sim \mathfrak{f}_1 \otimes \chi$, i.e. f_2 is a twist of f_1 by χ.*

As a consequence, we have the following theorem.

Theorem 3.3.3. *Let f be a newform of weight 2, level N, and with trivial nebentypus. Suppose that N is square-free. Then,*

$$End^0_{\bar{\mathbb{Q}}}(A_f) \simeq K_f,$$

and A_f remains absolutely simple for a set of primes of density 1.

Proof. The first conclusion is part of Theorem (6.2) of [Ri1] and is separated out in the Corollary (3.3.2). In particular, the endomorphism algebra is a commutative field. Suppose that A_f splits modulo a positive upper density of primes p. Then, Theorem (3.3.2) above implies that the endomorphism algebra is *non-commutative*. This contradiction proves the theorem. □

Remark. The above theorem is true whenever the endomorphism algebra of A_f is commutative.

3.4 General Abelian varieties with real multiplication

We continue to study the phenomenon of splitting for general Abelian varieties with real multiplication.

3.4.1 Two interesting propositions on splitting

We begin with a proposition that applies to Abelian varieties of odd dimension with *sufficiently many endomorphisms*.

Proposition 3.4.1. *Let A be an Abelian variety of dimension d, with $d > 1$ and* odd. *Let us further assume that A has multiplication by a field F over K such that the identity of F coincides with the identity element of $End_K^0(A)$, and that $[F : \mathbb{Q}] = d$. Let v be a finite place of K at which A_v splits over k_v, the residue field of K at v. Then,*

$$A_v \sim_{k_v} B_v^n$$

for a simple Abelian variety B_v over k_v.

Proof. If not, then we can write:

$$A_v \sim_{k_v} B_1^{n_1} \times B_2^{n_2} \times \cdots B_r^{n_r},$$

where the B_is are simple Abelian varieties over k_v and are pair-wise non-isogenous. By our assumption, $r \geq 2$. Let $A_i := B_i^{n_i}$ for $i = 1, \cdots, r$. By the injectivity Corollary (2.1.1), we have:

$$F \hookrightarrow End_{k_v}^0(A_v) \simeq \oplus_{i=1}^r End_{k_v}^0(A_i).$$

Let $d_i := n_i \dim(B_i) = \dim(B_i^{n_i})$. Thus, for some i, say $i = 1$, $d_1 < \frac{d}{2}$, since d is odd and $r \geq 2$. By our assumption on F and by Lemma (2.1.3),

$$F \hookrightarrow End_{k_v}^0(B_i^{n_i})$$

for all i. Thus, F is a commutative semi-simple sub-algebra of $End^0_{k_v}(A_i)$ for all i. On the other hand, by Tate' theorem (2.1.3) on the endomorphisms of Abelian varieties over finite fields, we know that $End^0_{k_v}(A_1)$ contains a maximal commutative semi-simple $\mathbb{Q}$ sub-algebra M of dimension $2\dim(A_1)$ over $\mathbb{Q}$. Hence, the dimension of such a sub-algebra would be strictly smaller than d. But, this contradicts the fact that F is contained in $End^0_{k_v}(A_1)$, and that brings this proof to a close. □

The next corollary is a bit striking, though it is an immediate consequence of the proposition above.

Corollary 3.4.1. *Let A, F, K and v be as in the proposition above. Furthermore, let $d = \dim(A)$ be an odd prime. Let v be a finite place of K such that A_v splits over k_v. Then,*

$$A_v \sim_{k_v} E_v^p,$$

for an elliptic curve E_v over k_v. In particular, the characteristic polynomial of the Frobenius π relative to k_v as an endomorphism of A_v is the p-th power of the characteristic polynomial of E_v over k_v. In other words,

$$L_v(A, s) = L(E_v, s)^p$$

Proof. By Proposition (3.4.1, $A_i \sim B_v^{n_v}$. We therefore have $d = n\dim(B_v)$. As d is prime and $n_v > 1$, we must have $\dim(B_v) = 1$. □

Similar in spirit of the proposition (3.4.1), albeit under a bit stronger assumption, we have the following proposition for Abelian varieties of even dimension.

Proposition 3.4.2. *Let A be an Abelian variety defined over a number field K with $d := \dim(A)$ even. Let F be a number field contained in the algebra of endomorphisms of A over K, i.e.*

$$F \hookrightarrow End^0_K(A),$$

such that the $1 \in F$ acts by the identity endomorphism on A. Let $[F : \mathbb{Q}] = \dim(A)$. Let S be the set of places of K at which A has good reduction and for which A_v splits over the corresponding residue field k_v of K. Assume that S has positive upper density, say $\delta := ud(S)$. Then, the set of $v \in S$ such that

$$A_v \sim_{k_v} B_v^n,$$

where B_v is simple over k_v and $n \geq 2$, also has the same upper density as S.

Proof. Let us write:

$$A_v \sim_{k_v} B_1^{n_1} \times B_2^{n_2} \cdots \times B_r^{n_{r_v}},$$

where the B_i are simple pair-wise non-isogenous Abelian varieties over k_v, and $r_v \geq 1$, depends on v. Let v be a place at which A_v splits, so either $r_v \geq 2$ or $n_i \geq 2$. We want to prove that apart from a set of places of density zero, $r_v = 1$, forcing $n_1 \geq 2$. Suppose $r_v \geq 2$ and $n_i \geq 1$ for all i. Let $A_i := B_i^{n_i}$ for $i = 1, \cdots, r_v$. Let $d_i := \dim(A_i)$. Let $M_i := End_{k_v}^0(A_i) = M_{n_i}(End_{k_v}(B_i))$ for all i. By Corollary (2.1.1) we have:

$$\begin{aligned} F \hookrightarrow End_K^0(A) &\hookrightarrow End_{k_v}^0(A_v) \\ &\hookrightarrow \oplus_i M_i. \end{aligned}$$

Our assumption that $1 \in F$ acts as the identity endomorphism on A, and Lemma (2.1.3) implies that $F \hookrightarrow M_i$. Since F is a commutative semi-simple subalgebra of M_i, it is contained in a maximal commutative semi-simple subalgebra of M_i. By Tate's classification theorem (2.1.3), we know that a maximal commutative semi-simple subalgebra of M_i has dimension $2d_i$ over $\mathbb{Q}$. Thus,

$$d_i \geq \frac{d}{2},$$

for all i. This forces $r = 2$, and we have:

$$\dim(A_1) = \dim(A_2) = \frac{d}{2}.$$

This implies that F is a maximal commutative semi-simple subalgebra of M_i for $i = 1, 2$. Thus F contains the centers $F_i := Z(M_i) = Z(D_i)$ of $D_i := End_{k_V}(B_i)$. By Tate's Theorem (2.1.3),

$$F_i = \mathbb{Q}[\pi] = \mathbb{Q}[T]/(min_i(\pi, T)),$$

where π is the *Frobenius* endomorphism relative to k_v, and $min_i(\pi, T)$ is the minimal polynomial of π relative to k_v acting on B_i, and is a factor of the characteristic polynomial $P_i(T)$ of the *Frobenius* map π. By abuse of notation, let π be a root of $min_i(\pi, T)$ in any one of the two F_i's. Then, $\bar{\pi} = \frac{q_v}{\pi} \in F_i$ as well, where q_v is the cardinality of the residue field k_v. But F_i, being a subfield of a totally real field F, is itself totally real. Thus, $\bar{\pi} = \pi$, and we get $\pi = \sqrt{q_v}$. Thus, for all such v's in S for which A_v is not a power of a simple Abelian variety, we have:

$$\mathbb{Q}(\sqrt{q_v}) \subset F_i,\ i = 1, 2.$$

Let S_1 be the set places $v \in S$ for which q_v is not a square. Since F is a number field, S_1 is a finite set. Let S_2 be the set of places v of S for which q_v is a square. Note that $S_1 \cup S_2 \subset S$ has zero density. Thus, for $v \in SP := S \setminus S_1 \cup S_2$, we have $r = 1$ and $n_v \geq 2$. By earlier observation, $\delta(SP) = \delta(S)$ and we are done. □

3.5 General Abelian Varieties

Here we recall a result of Chai and Oort [CO], and state it as a proposition:

Proposition 3.5.1. *(Chai-Oort) Let A be an Abelian variety of dimension g over a number field K. Suppose that the Zariski closure of the image of the ℓ-adic Galois representation:*

$$\rho_\ell : \mathrm{Gal}(\bar{K}/K) \to End_{\mathbb{Z}_\ell}(T_\ell(A)),$$

is equal to GSp_{2g}. Then, there exist finite places v of K such that the reduction A_v of A at v is absolutely simple and the set of such places has a positive density.

Proof. Remark (5)(i) and (iv) of Chai-Oort paper [CO]. □

A related result of Serre (Theorem 3 of [Se4]) says that the conditions of the above proposition are met, provided the Abelian variety A satisfies:

1. $End^0_{\bar{K}}(A) = \mathbb{Q}$

2. The dimension g of A is either 2, or 6 or an odd integer.

In fact, under the same hypotheses as above, we have the following result of Chavdarov. This is Corollary (6.10), page 179 of [Cha].

Proposition 3.5.2. *Let A be an Abelian variety over a number field K satisfying the two conditions as above. Then, for almost all places v of K, the reduction of A at v is absolutely simple.*

As a consequence, this proposition covers the *trivial endomorphism* case of absolutely simple Abelian surfaces.

Remark. We feel that, with a bit more work we should be able to generalize this result to cover some cases of Abelian varieties A over a number field K that have a real quadratic field as its algebra of endomorphisms over $\bar{K}$.

3.6 Abelian surfaces again

By putting together the results of the previous sections, we deduce the following:

Theorem 3.6.1. *Let A be an absolutely simple Abelian surface defined over a number field K. Then we have:*

1. *If $End^0_{\bar{K}}(A) = \mathbb{Q}$, then by combining the work of Oort-Chai, Noot and Chi, we know that the set of places at which A is absolutely simple is of positive density or positive upper density. In fact, by Proposition (3.5.2) we know that such an A*

remains absolutely simple under its reduction modulo almost all finite places v of K.

2. *If $End^0_{\bar{K}}(A)$ is a C.M. field then A remains absolutely simple for a set of places of K of upper density 1.*

3. *If A has multiplication by a real quadratic field F and $K = \mathbb{Q}$, then A remains absolutely simple for a set of places of upper density 1, provided $A = A_f$, i.e. A is a modular Abelian variety.*

4. *If A has multiplication by a quaternionic division algebra D, then for all places v of good reduction, A_v splits as a square of an elliptic curve defined over k_v.*

Proof. We have all the cases covered by our results from earlier sections except when A is a general Abelian surface that is absolutely simple and has multiplication by a real quadratic field. Under the restriction that such an A is defined over $\mathbb{Q}$, the modularity conjecture states that such an A is isogenous to A_f for some f as above. Theorem (3.3.3) then implies that such Abelian surfaces remain absolutely simple for a set of places of density 1. □

Chapter 4

Conjecture

Coming back to the main focus of our study: We have a simple Abelian variety A defined over a number field K. We want to study its splitting behaviour modulo various places of good reduction of A.

4.1 Formulation of obstruction to splitting?

What types of 'splitting properties' are we considering?:

1. A remains absolutely simple at almost all places of good reduction of K.
2. A is absolutely simple at only finitely many places of good reduction.
3. A splits at almost all places of good reduction of K.
4. A splits at a set of places of K of positive density (or positive upper density).

Depending on the question, we want a recipe or a formula that predicts either of the following:

- A splits into smaller dimensional Abelian varieties at almost all the places.
- A splits at a set of places of K of positive density.

- A remains absolutely simple at a set of places of positive density (or positive upper density).

It would be interesting if we are able define *classes* of Abelian varieties (depending on the endomorphism types and perhaps something more), so that, for an Abelian variety belonging to a given class, we have a specific splitting behaviour. An *effective* way of determining this behaviour is also something to be looked into. With this in mind, we make the following remarks:

1. From table (8.1) of Oort's paper [Oo], we see that if A is a simple Abelian variety over a characteristic zero field k and of square-free odd dimension, then $End_k^0(A)$ is a commutative field. Furthermore, suppose that $End_k^0(A)$ is a field of degree $\dim(A)$ over $\mathbb{Q}$. Then, by Proposition (3.4.1), it follows that if such an A splits at a finite place v of K, then it is a power of a simple Abelian variety defined over the finite field k_v. This can be rephrased as:

$$End_{k_v}^0(A_v) \simeq M_{r_v}(D_v),$$

where $r_v \geq 2$ and D_v is the endomorphism algebra of a simple Abelian variety over k_v. Thus, for each place v at which A_v splits, $End_{k_v}^0(A_v)$ is becoming a non-commutative matrix algebra, as it acquires extra endomorphisms beyond $End_K^0(A)$ (commutative).

2. Let A be as in (1) above such that $\dim(A)$ is a prime number p. Then, A splits at a set of places of positive density implies that A is a p-power of an elliptic curve over k_v. Once again, we feel that this should not be so, unless $End_K^0(A)$ is non-commutative.

3. By Theorem (3.3.2), if A_f (as defined earlier in chapter 3) is absolutely simple and split at a set of places of positive upper density, then the endomorphism algebra is

non-commutative. We believe that the converse should also be true and perhaps may follow from the work of Ribet in [Ri1] and [Ri4].

The above facts together with the results of chapter 3 are perhaps indicative of a general statement. These suggest the following conjecture:

Conjecture 4.1.1. *Let A be an absolutely simple Abelian variety over a number field K. Let S be the set of places v of K of good reduction for A such that $A_v := A \mod v$ splits (up to isogeny) over k_v, the residue field of K at v. Then, S has positive upper density if and only if $End^0_K(A)$ is non-commutative.*

Remark. In the above conjecture, we believe that the upper density may be related to the invariants associated to $End^0_K(A)$. We have not explored this as yet.

4.2 Remarks and further questions

- Study of splitting of Abelian varieties over function fields of finite characteristic:

  The questions discussed above can be asked over function fields of curves over finite fields. The problems that one immediately faces are related to classification of endomorphism algebras of Abelian varieties over such fields. The classification as that provided by Albert (theorem 2.1.1) holds, but existence of Abelian varieties with a given endomorphism ring or algebra are not fully known.

- Abelian surfaces over function fields:

  Examples of simple (or absolutely simple) Abelian surfaces with quaternionic multiplication do exist over function fields of finite characteristic. This is part of Oort's proposition (2.1.1). We do not know if such surfaces are defined over $\overline{\mathbb{F}_q}(t)$. If this is so, then by the same arguments as in the proof of Theorem (2.2.2), it follows that such a surface splits locally at all places of $\overline{\mathbb{F}_q}(t)$ of good reduction for A.

Bibliography

[Alb] A. A. Albert, Involutorial simple algebras and real Riemann matrices, Annals of Mathematics, 36(1935), 886-994.

[B-L] Y. F. Bilu and F. Luca, Divisibility of class numbers: enumerative approach, (http://www.arxiv.org).

[B-S] Z. Borevich and I. R. Shafarevich, Number Theory, Academic Press, 1966.

[C-F] J. W. S. Cassels and A. Frölich, editors, Algebric Number Theory, Academic Press, 1967.

[Cha] N. Chavdarov, The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy, Duke Math. Journal, 87 No. 1, 1997, 151-180.

[CO] C.-L. Chai and F. Oort, A note on the existence of absolutely simple Jacobians, Journal of Pure and Applied Algebra, 155(2001), 115-120.

[De] M. Deuring, die typen der multiplikatorenringe elliptischer funktionnenkorper, Abh. Math. Sem. Hamburg 195(1941), 197-292.

[DF] R. Keith Dennis and B. Farb, Noncommutative Algebra, Graduate Texts in Mathematics (144), Springer-Verlag, 1993.

[Ha] G. Harder, Some results on the Eisenstein cohomology of arithmetic subgroups of GL_n, Cohomology of arithmetic groups and automorphic forms, eds., J.-P. Labesse and J. Schwermer, Lecture Notes in Mathematics, 1447, Springer-Verlag, 1990.

[HM] K-I Hashimoto and N. Murabayashi, Shimura curves as intersections of Humbert Surfaces and defining equations of QM-curves of genus two, Tohoku Math. J., 47 (1995), 271-296.

[Ko] N. Koblitz, Introduction to elliptic curves and modular forms, Spring-Verlag, Graduate Texts in Mathematics (97) (Second Edition), 1993.

[La] S. Lang, Algebraic Number Theory, Springer-Verlag, Graduate Texts in Mathematics (110), 1970.

[La1] S. Lang, Complex Multiplication, Springer-Verlag, Grundlehren der mathematischen Wissenschaften (Comprehensive Studies in Mathematics Series) (255), 1983.

[La2] S. Lang, Introduction to Algebraic and Abelian Functions (2nd Edition), Graduate Texts in Mathematics (89), Springer-Verlag, 1982.

[La3] S. Lang, Algebra, Addison-Wesley, Reading, MA, 1993.

[Ma] D. Marcus, Number Fields, Springer-Verlag, 1977.

[Mat] T. Matsui, Endomorphism Algebra of Jacobian Varieties attached to the field of elliptic modular functions, Osaka Journal of Mathematics, Vol. 1-2, 1964(15), 1963(249-256).

[Mi] J. S. Milne, Abelian varieties with complex multiplication (for pedestrians), www.milne.org, June 1998.

[Momose] F. Momose, On the l-adic representations attached to modular forms, J. Fac. Sci. Univ. Tokyo Sect. IA Math., 28(1981), no. 1, 89-109.

[Mu] D. Mumford, Abelian Varieties, Oxford University Press and T. I. F. R., Bombay, 1988.

[MK] V. K. Murty, Exceptional Hodge classes on certain Abelian varieties, Math. Ann., 268 (1984), pp. 197-206.

[MK1] V. K. Murty, Lectures on Complex Multiplication, Based on Lectures at the University of Vermont, February 1987 (Unpublished manuscript).

[Oo] F. Oort, Endomorphism algebras of Abelian Varieties, Algebraic Geometry and Commutative Algebra. Vol. II, 469-502, 1988.

[Og] A. Ogus, Hodge cycles and crystalline cohomology, in: (editors: P. Deligne, J. S. Milne, A. Ogus, K.-y. Shih), Hodge cycles, Motives, and Shimura Varieties, chapter VI, Lecture Notes in Mathematics, no. 900, Springer-Verlag (1982), pp. 357-414.

[OP] F. Oort and Van der Put, Construction of an Abelian variety with a given endomorphism algebra, Compositio Mathematica, 67, No. 1, 103-120, 1988.

[Po] H. Pohlmann, Algebraic cycles on Abelian varieties of complex multiplication type, Annals of Mathematics, 88(1968), 161-180.

[Ra] C. S. Rajan, Refinement of strong multiplicity one for automorphic representations of GL(n), Proc. Amer. Math. Soc., 128(2000), no. 3, 691-700.

[Ra2] C. S. Rajan, On strong multiplicity one for l-adic representations, Internat. Math. Res. Notices 1998, no. 3, 161-172.

[Ri1] K. Ribet, Twists of modular forms and endomorphisms of Abelian varieties, Math. Ann., 253(1980), 43-62.

[Ri2] K. Ribet, Galois action on division points of Abelian varieties with real multiplications, Amer. J. Math., Vol. 98, No. 3(1976), pp. 751-804.

[Ri3] K. Ribet, On ℓ-adic representations attached to modular forms, Invent. Math., 28(1975), pp. 245-275.

[Ri4] K. Ribet, Endomorphism algebras of Abelian varieties attached to newforms of weight 2, Seminaire de Theorie des Nombres, Paris 1979-80 (Seminaire Delange-Pisot-Poitou), Progress in Mathematics, Volume 12, Birkhauser, 1981.

[ST] J.-P. Serre and J. Tate, Good reduction of Abelian varieties, *Annals of Mathematics*, 88(1968), 492-517.

[Se] J.-P. Serre, A course in Arithmetic, Springer international student edition, Narosa Publishing House, New Delhi, 1979.

[Se0] J.-P. Serre, Proproeťeś conjecturrales des groupes de Galois motiviques et des repreśentations ℓ-adiques, Proc. of Symp. in Pure Mathematics, Vol. 55 (1994), Motives -Part 1, American Mathematical Society, eds. U. Jannsen, S. Kleiman, and J.-P. Serre, 1994.

[Se3] J.-P. Serre, Lectures on Mordell-Weil theorem, Third Edition, Aspects in Mathematics E 15, Vieweg, 1997.

[Se4] J.-P. Serre, Algèbre et géométrie, Ann. Collège France, 86(1985-86), 95-100.

[Sh1] G. Shimura, On analytic families of polarized Abelian varieties and automorphic functions, Annals of Mathematics, 78(1963), 149-192.

[Sh2] G. Shimura, Introduction to the arithmetic theory of automorphic functions, Princeton University Press, 1994.

[Sh3] G. Shimura, On the zeta function of an Abelian variety with complex multiplication, Annals of mathematics, 94(1971), 504-533.

[ShTa] G. Shimura and Y. Taniyama, Complex Multiplication of Abelian varieties and its applications to number theory, Publ. Math. Soc. Japan, no. 6, 1961.

[Ta] J. Tate, Endomorphisms of Abelian varieties over finite fields, Invent. Math., 2(1966), 134-144, also appendix to Mumford's book on Abelian Varieties as above.

[Ta2] J. Tate, Algebraic cycles and poles of zeta functions, Arithmetic Algebraic Geometry, edited by O. F. G. Schilling.

[We] A. Weil, Basic Number Theory, Springer-Verlag, 1971.