Murty, V. K., and Vijay M. Patankar. (2008) "Splitting of Abelian Varieties,"
International Mathematics Research Notices, Vol. 2008, Article ID rnn033, 27 pages.
doi:10.1093/imrn/rnn033

Splitting of Abelian Varieties

V. Kumar Murty[1] and Vijay M. Patankar[2]

[1]Department of Mathematics, University of Toronto, 40 St. George Street, Toronto, Canada M5S 2E4 and [2]Microsoft Research Lab India, "Scientia", 196/36 2nd Main Road, Sadashivanagar, Bangalore, India - 560080

Correspondence to be sent to: vij@microsoft.com

We study a new local–global problem in the context of Abelian varieties: Given an absolutely simple Abelian variety over a number field K, find a necessary and sufficient condition for the existence of a place v of K (or infinitely many places, or a set of places of positive density) such that A remains absolutely simple modulo v. It is well known that for absolutely simple Abelian surfaces with multiplication by an indefinite quaternion algebra, A modulo v, denoted by A_v, is always isogenous to the square of some elliptic curve. For absolutely simple Abelian varieties of complex multiplication type, we show that A_v stays simple for a set of places of density 1. On the other hand, for absolutely simple Abelian varieties associated by Shimura to cusp forms of weight 2, if A_v splits at a set of places of positive density, then the *absolute* endomorphism algebra is noncommutative. Based on these results, we then formulate a conjecture: An absolutely simple Abelian variety defined over a number field splits at a set of places of positive density if and only if its absolute endomorphism algebra is noncommutative.

1 Introduction

The local–global principle in number theory is a basic theme in the study of arithmetical questions, by which a global arithmetical object and its structure is examined by

Received August 8, 2007; Revised March 15, 2008; Accepted March 22, 2008
Communicated by Prof. Freydoon Shahidi

means of and in comparison with its local behavior at various primes ([6]). In this paper, we introduce and study a new local–global problem in the context of the splitting (or factoring) of Abelian varieties. The *splitting* problem that we pose is as follows.

Given an absolutely simple Abelian variety over a number field K, provide a necessary and sufficient condition for the existence of a place v of K (or infinitely many places, or a set of places of positive density) such that A remains absolutely simple modulo v.

In Section 2, we discuss some results on the relationship between the splitting behavior and the endomorphism algebra.

In Section 3, we discuss Abelian varieties with complex multiplication. The main result of this section is the following theorem.

Theorem 3.1. Let A be an absolutely simple Abelian variety of *complex multiplication* type defined over a number field K such that

$$\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q} = \mathrm{End}_{\overline{K}}(A) \otimes_{\mathbb{Z}} \mathbb{Q} \simeq F,$$

where F is a totally imaginary quadratic extension of a totally real number field and $[F : \mathbb{Q}] = 2\dim(A)$. Then, for a set of places v of K of density 1, the reduction A_v is also absolutely simple over k_v, the residue field of K at v. □

In Section 4, we discuss the Abelian varieties that are associated (by Shimura) to normalized eigenforms of weight 2 for a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. The main result here is Theorem 4.1.

Theorem 4.1. Let f be a newform of weight 2 and level N with nebentypus character 1. Let $A_f/\mathbb{Q}$ (defined up to isogeny over $\mathbb{Q}$) be the Abelian variety attached to f by Shimura. Suppose that A_f is absolutely simple over $\mathbb{Q}$. Let S be the set of primes p at which $\tilde{A}_f$, the reduction of A_f modulo p, is split over $\mathbb{F}_p$. If S has positive density, then $\mathrm{End}^0_{\overline{\mathbb{Q}}}(A_f)$ is noncommutative. □

It seems to be well known that an absolutely simple Abelian surface with multiplication by an indefinite quaternion algebra defined over a number field has the property that at any prime of good reduction, it is isogenous to the square of an elliptic curve over an extension of the corresponding residue field. See, for example, [2].

Based on the above results, we briefly discuss, in Section 5, a general conjectural answer to the splitting problem.

Conjecture 5.1. 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 $A_v := A \bmod v$ splits (up to isogeny) over k_v, the residue field of K at v. Then, S has positive density if and only if $\mathrm{End}_{\bar{K}}(A)$ is noncommutative.

An exposition of some of our results is given in [10]. We also mention results of Chai-Oort, Serre, and Chavadarov that support this conjecture. □

1.1 Notations, definitions, and preliminaries

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

Throughout, K will denote a number 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 a separable 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 $\sum_{\text{fin}}$, we will, respectively, mean the set of *Archimedean* (or *infinite*) 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, $\wp$, 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 a central simple algebra with center a number field. This notational scheme, whenever appropriate, also applies to $L_v, L_w, l_v, l_w, F_v, f_v, E_v, e_v$, etc. We mostly use letters A, B for Abelian varieties, and d or g for their dimensions.

Given a number field K and a subset S of the set of finite primes of K, we use the following notion of *density* of S throughout this paper.

Definition 1.1. Let S be a set of primes v in Σ_{fin}. The upper natural density or in short, upper density of S, to be denoted by $ud(S)$ is defined by

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

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

Let A be an Abelian variety defined over a field k. We denote by $\mathrm{End}_k(A)$ the ring of endomorphisms of A which are defined over k. We also consider the corresponding algebra over $\mathbb{Q}$ denoted by $\mathrm{End}^0_k(A) := \mathrm{End}_k(A) \otimes \mathbb{Q}$. We write $\mathrm{End}(A)$ for $\mathrm{End}_{\bar{k}}(A)$—the ring of *absolute* endomorphisms of A. By $\mathrm{End}^0(A)$, we will denote the corresponding algebra of absolute endomorphisms [1]. If A and B are two Abelian varieties defined over a field k, we write $A \sim_l B$, if they are *isogenous* over an extension l of k.

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

Definition 1.2. An Abelian variety A defined over a field K is said to be split—or factor—over an extension $L \subset \overline{K}$ of K, if

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

that is, 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_1 and B_2 are strictly smaller than the dimension of A.

Similarly, and with notation as above, A is said to be strictly split—or strictly factor—over L, if

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

that is, if A is isomorphic to $B_1 \times B_2$ over L. □

In what follows, we may not mention the field L if it is clear from the context.

Given an Abelian variety defined over a number field or a local field k, the reduction of A at a place v is the special fiber at v of a Néron minimal model of A (Serre–Tate [21]).

Definition 1.3. Let A be an Abelian variety over a number field K. Let v be a finite place of K of good reduction for A. Then, A is said to be *s*plit (respectively, strictly split) at v if A_v, the reduction of A modulo v, splits over a finite extension of k_v (respectively over k_v), where k_v is the residue field at v. When A_v is strictly split at v, we also say that A_v splits over k_v. □

1.2 Tate's theorem

The theorem that is used often in this work is the fundamental result of Tate about the endomorphism algebras of Abelian varieties over finite fields [9, Theorem 3, p. 256]. (See also [25, Theorem 3, p. 140] and [27].) For ease of reference, we state it below.

Theorem 1.1. Let A be an abelian variety of dimension g 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 center of the semisimple algebra $E = \mathrm{End}^0_{k_0}(A)$;

(b) $\mathrm{End}^0_{k_0}(A)$ contains a semisimple $\mathbb{Q}$-subalgebra M of rank $2g$ which is maximal commutative;

(c) the following statements are equivalent:

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

(c_2) P has no multiple roots,

(c_3) $E = F$,

(c_4) E is commutative;

(d) the following statements are equivalent:

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

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

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

(d_4) E is isomorphic to the algebra of g by g matrices over the unique quaternion division algebra D_p over $\mathbb{Q}$ (p = characteristic of k_0) which splits at all primes $l \neq p$, ∞,

(d_5) A is k_0 isogenous to the gth 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 primes v of F not dividing p, but does not split at any real prime of F. □

2 Abelian Varieties with Real and Complex Multiplication

Lemma 2.1. Let A be an Abelian variety defined over a field k (k is any field). Let $E = \mathrm{End}^0_k(A)$ be its endomorphism algebra over k. Suppose $F := Z(E)$ (the center 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 such that B_1 and B_2 do not share a simple Abelian variety as a factor. This means that $Hom_k(B_1, B_2) = \{0\}$. Thus, we have

$$E = \mathrm{End}_k^0(A) \simeq \mathrm{End}_k^0(B_1) \oplus \mathrm{End}_k^0(B_2).$$

This gives,

$$F = Z(E) = Z(\mathrm{End}_k^0(B_1)) \oplus Z(\mathrm{End}_k^0(B_2)).$$

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

We now state a lemma that relates the endomorphism ring of an Abelian variety and the splitting behavior of A. The proof is left to the reader.

Lemma 2.2. 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

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

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

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

induces an injection

$$Pr_i : \mathrm{End}_K^0(A) \hookrightarrow M_{n_i}\big(\mathrm{End}_{k_v}^0(B_i)\big),$$

for $1 \leq i \leq r$. □

The next proposition is crucial for our results.

Proposition 2.1. Let A be a simple Abelian variety defined over a number field K with multiplication by a field F, where $[F:\mathbb{Q}] = 2g$, where $g = \dim(A)$. Suppose, for a finite place v of K, $A_v := A \bmod v$ 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. The proposition would follow from Lemma 2.1 if we prove that the center of the endomorphism algebra $\mathrm{End}^0_{k_v}(A_v)$ is a field.

By Tate's classification theorem (1.1), we know that a maximal commutative subalgebra of $\mathrm{End}^0_{k_v}(A_v)$ has dimension $2\dim(A_v) = 2g$ over $\mathbb{Q}$. But F injects into $\mathrm{End}^0_{k_v}(A_v)$, and is indeed a commutative semisimple subalgebra of $\mathrm{End}^0_{k_v}(A_v)$ with $[F:\mathbb{Q}] = 2g$. Hence, F is a maximal commutative semisimple subalgebra of $\mathrm{End}^0_{k_v}(A_v)$. Since, the center of $\mathrm{End}^0_{k_v}(A_v)$ is contained in any maximal commutative semisimple subalgebra of $\mathrm{End}^0_{k_v}(A_v)$, we get

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

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

Remark 2.1. Note that the above proposition is true over any global field with the same proof as above. □

Next, we consider Abelian varieties with real multiplication.

Proposition 2.2. Let A be an Abelian variety of dimension d defined over a number field K such that

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

where F is a totally real field with $[F:\mathbb{Q}] = d = \dim(A)$. Further, assume that the $1 \in F$ acts on A as the identity element of $\mathrm{End}^0_K(A)$. Let v be a prime of good reduction of A. Also assume that v is of degree 1 and that the underlying rational prime p does not ramify in F. Suppose $A_v := A \bmod v$ is not simple over k_v, the residue field of K at v. Then, the characteristic polynomial of A_v has repeated roots. □

Proof. Note that since v is a place of degree 1, $k_v \simeq \mathbb{F}_p$. By assumption, A_v splits over k_v, so we may write

$$A_v \sim_{\mathbb{F}_p} B_1^{n_1} \times \cdots \times B_r^{n_r},$$

where the B_i are pairwise nonisogenous simple Abelian varieties over $\mathbb{F}_p$ of a strictly smaller dimension than $d = \dim(A)$.

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

$$A_v \sim_{\mathbb{F}_p} B_1 \times \cdots \times B_r,\ r \geq 2.$$

Let $E_i := \mathrm{End}^0_{\mathbb{F}_p}(B_i)$. Then, we have

$$F \hookrightarrow \mathrm{End}^0_K(A) \hookrightarrow \mathrm{End}^0_{\mathbb{F}_p}(A_v) \simeq \oplus_i E_i.$$

By our assumption that the $1 \in F$ acts on A_v as the identity, it follows that the map that takes F to $\mathrm{End}^0_{\mathbb{F}_p}(A_v)$ followed by the natural *projection* to E_i, is an injection for all $i = 1$ to r. Thus under these maps,

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

Let us set $F_i = Z(E_i) = \mathrm{center}(E_i)$. By Tate's theorem (1.1), it follows that

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

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 (1.1(c)), it then follows that E_i is commutative for all i, and

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

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

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

Note that $\deg(P_i) \geq 2$ for all i. Let $P(t)$ be the characteristic polynomial of the Frobenius at v acting on A_v. Then, $P_1(t)|P(t)$. Let α be a root of $P_1(t)$. By construction, $\alpha \in F$. Then $\beta = \frac{\mathbb{N}v}{\alpha} = \frac{p}{\alpha}$ is another root of $P(t)$, and $\beta \in F$. Being a root of $P(t)$, we have $|\alpha| = |\beta| = \sqrt{p}$. On the other hand, both are totally real as elements of F, and satisfy the quadratic polynomial

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

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 satisfies

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

Thus, it follows that $\alpha, \beta \in F$ are totally real if and only if

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

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

The next result applies to Abelian varieties of odd dimension.

Proposition 2.3. 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 $\mathrm{End}_K^0(A)$, 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

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

where the B_i are simple nonisogenous Abelian varieties over k_v, and $r \geq 2$. Let $A_i := B_i^{n_i}$ for $i = 1, \ldots, r$. We have

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

Let $d_i := \dim(A_i)$. Thus, for some i, say $i = 1$, we have $2d_1 < d$, because d is odd and $r \geq 2$. Now by Tate's theorem (1.1), a maximal commutative semisimple subalgebra of $\mathrm{End}^0_{k_v}(A_1)$ has dimension $2d_1$. But, by our assumption on F and Lemma 2.2,

$$F \hookrightarrow \mathrm{End}^0_{k_v}(A_i) \tag{1}$$

for all i, in particular for $i = 1$. This contradicts $d := [F : \mathbb{Q}] > 2d_1$. ■

The next corollary is a bit surprising, and is an immediate consequence of the proposition above.

Corollary 2.1. 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 pth power of the characteristic polynomial of E_v over k_v. □

Proof. By Proposition 2.3, $A_v \sim B_v^{n_v}$. We thus have $d = n_v \dim(B_v)$. As d is a prime number and $n_v > 1$, we must have $\dim(B_v) = 1$. ■

Similar in spirit to Proposition 2.3, albeit under a slightly stronger assumption, we have the following result for Abelian varieties of even dimension.

Proposition 2.4. Let A be an Abelian variety defined over a number field K with $d := \dim(A)$ even. Let F be a totally real number field contained in the algebra of endomorphisms of A over K, that is,

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

such that $[F : \mathbb{Q}] = \dim(A)$ and that $1 \in F$ acts as the identity endomorphism on 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. Arguing as in the proof of Proposition 2.3, and using equation (1), we see that if d is even and $r > 1$, then $r = 2$ and

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

This implies that F is a maximal commutative semisimple subalgebra of M_i for $i = 1, 2$. Thus, F contains the centeres $F_i := Z(M_i) = Z(D_i)$ of $D_i := \mathrm{End}_{k_v}(B_i)$. By Tate's theorem (1.1),

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

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. Then, $\bar{\pi} = q_v/\pi \in F_i$, 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 $\pi = \pm\sqrt{q_v}$. Thus, for all such v in S for which A_v is not a power of a simple Abelian variety, we have

$$\mathbb{Q}(\sqrt{q_v}) \subset F.$$

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 $v \in SP := S \backslash S_1 \cup S_2$, we have $r = 1$ and $n_v \geq 2$. ■

3 Abelian Varieties with Complex Multiplication

The following is the main theorem of this section.

Theorem 3.1. Let A be an absolutely simple Abelian variety of CM type defined over a number field K such that

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

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

We begin with a few results that will prepare us toward a proof of the above result.

3.1 Background results

We begin by stating the following form of the strong multiplicity one theorem for $GL(1)$.

Theorem 3.2 ([14, Theorem 2.1])**.** 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. Here, by $\theta_{i,v}$ $(i = 1, 2)$ we mean the induced characters of K_v^* obtained by restriction of θ to K_v^*. 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. This is in a paper by Rajan [14], and is based on an *equidistribution* result about Hecke characters. The result for unitary idele class characters (which is attributed to Hecke) is also found in D. Ramakrishnan's book [15, Chapter 7, p. 295, Theorem (7-33)]. ∎

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 Rajan's result in this special case appears in [5, p. 95]. We learnt about this in the paper of Rajan [14] mentioned above, and we reproduce the statement here.

Proposition 3.1. 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 a Hecke character of type A_0 (algebraic Hecke character), and $\theta_w = 1$. Then θ is of finite order. Here, by θ_w, we mean the natural restriction of θ to K_w^*. □

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

Corollary 3.1. 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

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

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 to the idèle class character $\theta = \theta_1\theta_2^{-1}$. The existence of a finite place v of K which is unramified in K and of degree 1 with $\theta_v = 1$ is guaranteed by the positivity of the upper density. ∎

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 3.3 (Shimura–Taniyama)**.** Let A be an Abelian variety defined over a number field K and with CM by a number field F such that

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

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

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

that is trivial on $K^\times$. (Here, $\mathbb{J}_K$ denotes the idéles of K.) For each $\sigma \in \mathrm{Hom}(F, \mathbb{C})$, 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

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

□

Proof. This is the Shimura–Taniyama theory. Our reference for this is an exposition by Milne [7, Theorems 13.1 and 13.2 on page 28 of his notes]. ■

3.2 Proof (complex multiplication case)

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

If A is defined over $\mathbb{C}$ and has CM by a number field F, then it can be shown that it has a model defined over a number field K (Shimura–Taniyama [23]). 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. As A has potential everywhere good reduction, we will also assume that it has everywhere good reduction over K (by extending K if necessary). From here onwards until the end of the proof, 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.

Proof of Theorem 3.1. Let $g := \dim(A)$. Writing $L(A,s) = L(H^1(A),s)$, we have by Theorem 3.3 that the L-function of A over K is given by

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

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

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

Note that as an equality of characters of $\mathbb{J}_K$ into $\mathbb{C}^*$,

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

where $\mathbb{N} = \mathbb{N}_{\mathbb{J}_\mathbb{Q}}^{\mathbb{J}_K}$ 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 as ψ_i is unramified at 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 ψ_i, $1 \le i \le g$ is ramified. Then R is a finite set. Thus, up to a factor, say $*$, associated with the places $v \in R$, we can write

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

Furthermore 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 equation, 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 of Pohlmann [12, p. 177] which verifies a conjecture of Tate [24], the order of pole at $s = 2$ of the H^2 L-function equals the Picard number of A. It is well known that the Picard number of A over K equals g, and thus the order of pole at $s = 2$ equals g. Since $L(\psi_i\psi_j, s)$ does not vanish at $s = 2$, 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 2.1,

$$A_v \sim B_v^r$$

for a simple Abelian variety B_v with $r = r(v) \geq 2$. This implies that the characteristic polynomial of the Frobenius at v is strictly 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 $\alpha_{v,i}$ and their conjugates $\alpha_{v,i+g}$ for $i = 1$ to g. But as a set these are precisely the eigenvalues of the Frobenius acting on $T_l(B_v)$. 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 Theorem 3.2 (or by Corollary 3.1) 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 (that is, a Hecke character of finite order of K. Here, by class field theory, χ may also be considered as a character of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$. 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 $\mathbb{N}^{\mathbb{J}_L}_{\mathbb{J}_K}$ (*relative norm*) map. This is a nonissue because the H^1 L-function of the Abelian variety A over K, when considered over the extension field L, also changes by the norm map $\mathbb{N}^{\mathbb{J}_L}_{\mathbb{J}_K}$, 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 under base change from K to L. Thus, the factor $L(\psi_{i_0}\overline{\psi_{j_0}}, s)$ where $i_0 \neq j_0$, contributes an extra pole to $L(H^2_l(A), s)$ at $s = 2$. This contradicts the fact that $L(H^2_l(A), s)$ has a pole of exact order g at $s = 2$, and that proves the theorem. □

4 Abelian Varieties Attached to Modular Forms of Weight 2

The next theorem is for Abelian varieties attached to newforms of weight 2 for congruence subgroups of $\Gamma := SL(2, \mathbb{Z})$.

Theorem 4.1. Let f be a newform of weight 2 and level N with nebentypus character 1. Let $A_f/\mathbb{Q}$ (defined up to isogeny over $\mathbb{Q}$) be the Abelian variety attached to f by Shimura. Suppose that A_f is absolutely simple. Let S be the set of primes p at which $\tilde{A}_f$, the reduction of A_f modulo p, is split over $\mathbb{F}_p$. If S has positive density, then $\mathrm{End}^0_{\mathbb{Q}}(A_f)$ is noncommutative. □

We begin with some standard notations, definitions and a few well-known results.

4.1 Definitions and background results

Let N be a positive integer. Let

$$\Gamma_1(N) := \left\{ g \in \Gamma : g \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod N \right\}.$$

Let f be a cusp form of weight 2 for $\Gamma_1(N)$ with character ϵ. Write

$$f(z) = \sum_{n=1}^{\infty} a_f(n) e^{2\pi i n z}$$

for the Fourier expansion at $i\infty$. We assume that f is a normalized newform, and in particular, $a_f(1) = 1$. For such an f, it can be shown that $a_f(n)$ is an algebraic number for all n. Here, for $(n, N) = 1$, $a_n(f)$ is the eigenvalue of the Hecke operator T_n. Since the T_n are unitary operators with respect to the Peterson scalar product, it follows that, the $a_f(n)$ are totally real if $\epsilon = 1$. Let K_f be the field generated by the $a_n(f)$ for all n. It is a fact that K_f is a number field. Let $\Phi := \mathrm{Hom}(K_f, \mathbb{C})$. By the work of Shimura [22], to such an f, one associates an Abelian variety, say A_f, defined (up to isogeny) over $\mathbb{Q}$, as a quotient of $J := J_1(N)$, having the following properties.

(1) A_f is defined over $\mathbb{Q}$ and $\dim(A_f) = [K_f : \mathbb{Q}]$.
(2) $K_f \hookrightarrow \mathrm{End}(A_f) \otimes_{\mathbb{Z}} \mathbb{Q}$.
(3) $L(A_f, s) = L(H^1_\ell(A_f), s) = \prod_{\sigma \in \Phi} L(f^\sigma, s)$.

Thus, for f as above, we can write

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

where σ ranges over the embeddings of K_f into $\mathbb{C}$ and $(*)$ consists of a finite product of Euler factors at primes $p \mid N$.

4.2 Twists and inner twists

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

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

that is, for all but finitely many primes p. This implies $b_n = a_f(n)\chi(n)$, 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 a given modular form f is a *twist* of a conjugate of f, say $f^\sigma = \sigma(f) := \sum_n \sigma(a_n) q^n$ for some $\sigma \in \mathrm{Aut}(\mathbb{C})$, we say that f^σ is an *inner twist* of f. Thus, if f is a modular form that is an inner twist of itself, then there is a Dirichlet character $\chi \neq 1$ such that

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

and such a modular form f is said to have *complex multiplication*. It is a fact that if a newform f has complex multiplication, then the corresponding A_f is of complex multiplication type (or has complex multiplication). Since we have discussed Abelian varieties of CM 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 complex multiplication.

As σ varies over $\mathrm{Aut}(\mathbb{C})$, we consider those f^σ that are inner twists of f. Following Momose [8] and Ribet [16], one defines the *twisting group* Γ_f as the subset of $\sigma \in \Phi$, so that

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

for some Dirichlet character χ_σ that depends on σ. Since f does not have CM, χ_σ is uniquely determined by $\sigma \in \Gamma_f$. This makes the notation χ_σ unambiguous. It then follows from [16, Propositions 3.1, 3.2, and 3.3] that Γ_f is an Abelian subgroup of $\mathrm{Aut}(K_f)$. 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 [16, Proposition 3.9 and Theorem 3.9 bis of]) that is important for us.

Proposition 4.1. 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 [8] and Ribet [16]. Theorem 4.2 describes the endomorphism algebra of A_f, when f does not have CM.

Theorem 4.2 (Momose–Ribet)**.** Let f be a newform of level N and nebentypus ϵ_f and without CM. Let A_f, K_f, F_f, and Γ_f be as defined above. Let $\gamma := [K_f : F_f] = |\Gamma_f|$. Let $E_f := \mathrm{End}^0_{\mathbb{Q}}(A_f)$. Then

(1) E_f is central simple algebra over F_f and $[E_f : F_F] = \gamma^2$;
(2) K_f is a maximal commutative semisimple subalgebra of E_f;
(3) $[E_f : \mathbb{Q}] = [K_f : F_f][K_f : \mathbb{Q}] = \gamma^2[F_f : \mathbb{Q}]$. □

Proof. The above theorem is essentially a suitable restatement of Theorem 5.1 on page 56 of [16] in our notation. The result also follows from Theorem 3.1 on page 102 of [8]. ■

Remark. Though we do not need it for our purposes, we note for completeness that the work of Momose and Ribet gives the following additional information about the endomorphism algebra.

(1) The algebra E_f is either a matrix algebra over F_f or else a matrix algebra over a quaternion division algebra with center F_f. This is part of Remark 5.8 on page 59 of [16] and also Theorem 1 on page 264 of [17].
(2) E_f is unramified at the Archimedean places v of F_f. This follows from Theorem 3.1(2) on page 102 of [8].
(3) E_f is unramified at all places v of F_f at which A_f has ordinary reduction. This is the content of Theorem (6) on page 274 of [17]. □

As a consequence of the above theorem, we have the following corollary.

Corollary 4.1. Let f be as above. Suppose that Γ_f, the twisting group attached to f, is nontrivial. Then, $\mathrm{End}^0_{\mathbb{Q}}(A_f)$ is noncommutative. □

We also have the following corollary.

Corollary 4.2. Let f be a newform with trivial nebentypus and square-free level N. Then, A_f defined over $\mathbb{Q}$ is absolutely simple with

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

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. ∎

4.3 Proof of the theorem for A_f

Proof of Theorem 4.1. It is a fact that A_f has good reduction outside primes dividing N. Let $\tilde{A}_f/\mathbb{F}_p$ be the reduction of A_f at a prime $p \nmid N$. Then the L-function of $\tilde{A}_f$ is given by

$$\begin{aligned} L(\tilde{A}_f/\mathbb{F}_p, t) &:= \prod_\sigma (t - \pi_p^\sigma)(t - \overline{\pi_p^\sigma}) \\ &= \prod_\sigma (t^2 - a_f(p)^\sigma t + p), \end{aligned}$$

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

$$a_f(p)^\sigma = \pi_p^\sigma + \overline{\pi_p^\sigma} \tag{2}$$

and

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

Further more, it is a fact that $L(\tilde{A}_f, t)$ equals the monic characteristic polynomial of the *Frobenius* endomorphism $\tilde{A}_f/\mathbb{F}_p$ relative to $\mathbb{F}_p$. This is a consequence of Shimura theory, and is inherent in the preliminary results stated at the beginning of Section 4.1.

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, $\sqrt{p}$ does not lie in K_f, and so $\pi_p^\sigma \neq \overline{\pi_p^\sigma}$ for all $\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q})$. Now by Proposition 2.2, it follows that if $\tilde{A}_f$ splits over $\mathbb{F}_p$, then the characteristic polynomial of the Frobenius of $\tilde{A}_f/\mathbb{F}_p$ has repeated roots. This then implies that at least two different factors of $\prod_\sigma (t - \pi_p^\sigma)(t - \overline{\pi_p^\sigma})$ coincide. In other words, for some pair

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

we have

$$\pi_p^{\sigma_1} = \pi_p^{\sigma_2} \text{ or } \overline{\pi_p^{\sigma_2}}. \tag{3}$$

By equation (2), we get

$$a_f(p)^{\sigma_1} = a_f(p)^{\sigma_2}. \tag{4}$$

Furthermore, viewing σ_1 and σ_2 as automorphisms of $\mathbb{C}$, and setting $\sigma := \sigma_2\sigma_1^{-1} \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q})$, we deduce that

$$a_f(p) = a_f(p)^{\sigma}. \tag{5}$$

Now, if A_f splits over $\mathbb{F}_p$ at a set of primes p of positive upper density, then there exists a pair (σ_1, σ_2) such that the above relation (4) holds for a set of primes of positive upper density. Thus, for $\sigma = \sigma_2\sigma^{-1}$, the above relation (5) 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

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

Indeed, this is a direct application of Corollary 1 of [13] applied to the two modular forms f^{σ_1} and f^{σ_2}. (For easy reference, we restate this Corollary 1 of Rajan [13] as the Proposition 4.2 below.)

Remark. The above claim may also be proved using results of Ribet in [16] and Momose [8] about the image of ℓ-adic Galois representations attached to modular forms. □

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

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

By Corollary 4.1, this implies that $\mathrm{End}^0_{\overline{\mathbb{Q}}}(A_f)$ is noncommutative and that completes the proof. □

Proposition 4.2 (Corollary 1 of Rajan [13]). 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-CM (complex multiplication) cusp form 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 $f_2 \sim f_1 \otimes \chi$, i.e. f_2 is a twist of f_1 by χ. □

As a consequence, we have the following theorem.

Theorem 4.3. Let f be a newform of weight 2, level N, and with nebentypus character 1. Suppose that N is square-free. Then

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

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 Ribet [16] and is separated out in the Corollary 4.2. In particular, the endomorphism algebra is a commutative field. Suppose that A_f splits modulo a positive upper density of primes p. Then, Theorem 4.1 implies that the endomorphism algebra is *noncommutative*. This contradiction proves the theorem. ■

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

5 Conjecture

The results of the previous sections point to the following general conjectural resolution of the splitting problem.

Conjecture 5.1. 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 $A_v := A \bmod v$ splits (up to isogeny) over k_v, the residue field of K at v. Then S has positive density if and only if $\mathrm{End}_{\bar{K}}(A)$ is noncommutative. □

This conjecture predicts that, if A is an absolutely simple Abelian variety over a number field K such that $\mathrm{End}^0_K(A) = \mathrm{End}^0_{\bar{K}}(A)$ is commutative, then A remains absolutely simple at a set of places v of K of density 1.

Remark. It is likely that one may need to refine the conjecture by weakening the condition to let the splitting occur over some finite extension (depending on v) of the residue field k_v rather than over k_v itself. This is being studied further in a work in progress. □

In the remainder of this section, we indicate a few results that support this conjecture. Let T_ℓ be a free $2g$-dimensional $\mathbb{Z}_\ell$ module and let e_ℓ be an alternating form on T_ℓ with nonzero discriminant. The group $\mathrm{GSp}(T_\ell, e_\ell) \simeq \mathrm{Gsp}(2g, \mathbb{Z}_\ell)$ of symplectic similitudes is the set of automorphisms σ of T_ℓ with the property that for any pair of elements $v, w \in T_\ell$, we have

$$e_\ell(\sigma v, \sigma w) = \nu(\sigma) e_\ell(v, w)$$

for some $\nu(\sigma) \in \mathbb{Z}_\ell^\times$. Let A be a polarized Abelian variety defined over K. The polarization induces an alternating form e_ℓ (say) on the Tate module $T_\ell(A)$ with nonzero discriminant. The action of $\mathrm{Gal}(\overline{K}/K)$ on $T_\ell(A)$ thus gives a homomorphism

$$\rho_l \;: \mathrm{Gal}(\overline{K}/K) \to \mathrm{GSp}(2g, \mathbb{Z}_\ell). \tag{6}$$

An important result of Serre gives conditions under which the above map is surjective.

Theorem 5.1 (Theorem 3 of [18]). Let A be an Abelian variety over a number field K with

$$\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$$

and $\dim(A) = 2,\ 6$ or odd. Then for all primes ℓ, the image of ρ_l as in equation (6) is open in $\mathrm{GSp}(2g, \mathbb{Z}_\ell)$ and for a sufficiently large prime ℓ, the image is equal to $\mathrm{GSp}(2g, \mathbb{Z}_\ell)$. □

Chavdarov [3, Corollary 6.10] uses this to prove the following result.

Proposition 5.1. Let A be an Abelian variety over a number field K satisfying the following two conditions:

(1) $\mathrm{End}^0_{\overline{K}}(A) = \mathbb{Q}$;
(2) The dimension g of A is either 2, 6, or an odd integer.

Then, for a set of places v of K of density 1, the reduction of A at v is absolutely simple. □

There is also the following related result of Chai and Oort [4].

Proposition 5.2 (Chai-Oort, [4, Proposition 4 and Remarks 5(iv)]). Let A be an Abelian variety of dimension g over a number field K. Suppose that for a prime ℓ, the image of the ℓ-adic Galois representation ρ_ℓ as in equation (6) is equal to $\mathrm{GSp}(2g, \mathbb{Z}_l)$. 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. $\square$

The following result is well known.

Proposition 5.3. Let A be a simple ordinary Abelian variety over a finite field k. Then $\mathrm{End}^0_k(A)$ is commutative. $\square$

Proof. This is relatively easy and follows from Tate's description of invariants of the endomorphism algebra of an Abelian variety defined over a finite field as in the Proposition 7.1 of [26]. $\blacksquare$

The next result is about Abelian varieties with noncommutative endomorphism algebras.

Proposition 5.4. Let A be an absolutely simple Abelian variety over a number field K. Let $D := \mathrm{End}^0_K(A) = \mathrm{End}^0_{\bar{K}}(A)$ be a noncommutative division algebra over $\mathbb{Q}$. Let S denote the set of places v of K such that A_v is ordinary over k_v. If $v \in S$ is a place of good reduction for A, then A_v is not simple over k_v. In fact, there exists an Abelian variety B_v defined over k_v and an inclusion $B_v^2 \hookrightarrow A_v$. In particular, if S has positive density then it follows that A_v splits at all places $v \in S$. $\square$

Proof. We know that

$$D \hookrightarrow \mathrm{End}^0_k(A_v).$$

In particular, $\mathrm{End}^0_k(A_v)$ is noncommutative. But by Proposition 5.3, the endomorphism algebra of a simple ordinary Abelian variety over a finite field is commutative. This is a contradiction. Thus, it follows that A_v cannot remain simple over k_v if v is place of ordinary reduction for A. Thus A_v (up to isogeny) is a unique product of smaller dimensional ordinary Abelian varieties. If there is no repeated factor in this product, then we would get an injection of D into a commutative algebra and that would be a contradiction. $\blacksquare$

Remark. There is a *belief*, which says the following: Let A be an Abelian variety defined over a number field K. Then, for some finite extension L of K, the set of places v of L

such that A (considered over L) has ordinary reduction at v has positive density. Serre makes such a statement in the $\dim(A) = 2$ case, and states [20, lines 12–17, p. 14], that naively speaking, one would have the tendency to think that the set of ordinary places should occur with density 1 (over a sufficiently large extension). Furthermore, in Note 14.8 [19, p. 637], Serre mentions Corollary 2.9 of Ogus [11, p. 372] where the above *belief* is proved for $\dim(A) = 2$. □

In fact, a more precise form of this belief says that there exists a finite extension L of K so that the set of places w of L for which A has ordinary reduction at w, has density 1.

Assuming that this is true, Proposition 5.4 implies that an absolutely simple Abelian variety with noncommutative endomorphism algebra splits at a set of places of positive density, as predicted by our Conjecture 5.1.

References

[1] Albert, A. A. "Involutorial simple algebras and real Riemann matrices." *Annals of Mathematics* 36 (1935): 886–994.

[2] Adimoolam, C. "A note on good reduction of simple Abelian varieties." *Proceedings of the American Mathematical Society* 64 (1977): 196–8.

[3] Chavdarov, N. "The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy." *Duke Mathematical Journal* 87 (1997): 151–80.

[4] Chai, C.-L., and F. Oort. "A note on the existence of absolutely simple Jacobians." *Journal of Pure and Applied Algebra* 155 (2001): 115–20.

[5] Harder, G. "Some results on the Eisenstein cohomology of arithmetic subgroups of GL_n." In *Cohomology of Arithmetic Groups and Automorphic Forms*, edited by J.-P. Labesse and J. Schwermer. Lecture Notes in Mathematics, 1447. Berlin: Springer, 1990.

[6] Mazur, B. "On the passage from local to global in number theory." *American Mathematical Society. Bulletin* 29 (1993): 14–50.

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

[8] Momose, F. "On the l-adic representations attached to modular forms." *Journal of the Faculty of Science, University of Tokyo Sect. 1 A Mathematics* 28 (1981): 89–109.

[9] Mumford, D. *Abelian Varieties*. Oxford and Bombay: Oxford University Press and Tata Institute of Fundamental Research, 1988 (reprint of 1974 edition).

[10] Murty, V. K. "Splitting of Abelian varieties: A new local-global problem." In *Algebra and Number Theory*, edited by R. Tandon, 258–68. New Delhi: Hindustan Book Agency, 2005.

[11] Ogus, A. "Hodge cycles and crystalline cohomology." In *Hodge Cycles, Motives, and Shimura Varieties*, 357–414. Lecture Notes in Mathematics, 900. Berlin: Springer, 1982.

[12] Pohlmann, H. "Algebraic cycles on Abelian varieties of complex multiplication type." *Annals of Mathematics* 88 (1968): 161–80.

[13] Rajan, C. S. "On strong multiplicity one for l-adic representations." *International Mathematics Research Notices* 1998, no. 3 (1998): 161–72.

[14] Rajan, C. S. "Refinement of strong multiplicity one for automorphic representations of GL(n)." *Proceedings of the American Mathematical Society* 128 (2000): 691–700.

[15] Ramakrishnan, D. *Fourier Analysis on Number Fields*. Graduate Texts in Mathematics, 186. Berlin: Springer, 2002.

[16] Ribet, K. "Twists of modular forms and endomorphisms of Abelian varieties." *Mathematische Annalen* 253 (1980): 43–62.

[17] Ribet, K. "Endomorphism algebras of Abelian varieties attached to newforms of weight 2." In *Séminaire de Théorie des Nombres, Paris 1979–80* (Séminaire Delange-Pisot-Poitou). Progress in Mathematics, 12. Boston, MA: Birkhauser Boston, 1981.

[18] Serre, J.-P. *Résumé des cours de 1985–1986, Annuaire du Collège de France*, 95–99, 1986. (See also *Collected Papers,* vol. 4, 33–37. Berlin: Springer, 2000.)

[19] Serre, J.-P. "Notes on article 133." In *Collected Papers,* vol. 4, 637. Berlin: Springer, 2000.

[20] Serre, J.-P. "Article 133, Lettres á Ken Ribet du 1/1/1981 et du 29/1/1981." In *Collected Papers,* vol. 4, 1–20. Berlin: Springer, 2000.

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

[22] Shimura, G. *Introduction to the Arithmetic Theory of Automorphic Functions*. Princeton, NJ: Princeton University Press, 1994.

[23] Shimura, G., and Y. Taniyama. *Complex Multiplication of Abelian varieties and Its Applications to Number Theory*. Publications of the Mathematical Society of Japan, 6. Tokyo, Japan: Mathematical Society of Japan, 1961.

[24] Tate, J. "Algebraic cycles and poles of zeta functions." In *Arithmetic Algebraic Geometry*, edited by O. F. G. Schilling, 93–110. New York: Harper and Row, 1965.

[25] Tate, J. "Endomorphisms of Abelian varieties over finite fields." *Inventiones Mathematicae* 2 (1966): 134–44. See also Appendix to [9].

[26] Waterhouse, W. C. "Abelian varieties over finite fields." *Annales Scientifiques de l'Ecole Normale Superieure* 42 (1969): 521–60.

[27] Waterhouse, W. C., and J. S. Milne. "Abelian varieties over finite fields." *Proceedings of Symposia in Pure Mathematics* 20 (1971): 53–64.