JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Jeffrey D. ACHTER

Explicit bounds for split reductions of simple abelian varieties

Tome 24, n° 1 (2012), p. 41-55.

<http://jtnb.cedram.org/item?id=JTNB_2012__24_1_41_0>

Journal de Théorie des Nombres
de Bordeaux **24** (2012), 41-55

Explicit bounds for split reductions of simple abelian varieties

par Jeffrey D. ACHTER

Résumé. Soit X/K une variété abélienne absolument simple, définie sur un corps de nombres ; nous étudions comment les réductions $X_{\mathfrak{p}}$ tendent à être simples également. Nous montrons que si $\mathrm{End}(X)$ est une algèbre de quaternions définie, alors la réduction $X_{\mathfrak{p}}$ est géométriquement isogène au self-produit d'une variété abélienne absolument simple, ce pour $\mathfrak{p}$ dans un ensemble de densité strictement positive, alors que si X est de type Mumford, $X_{\mathfrak{p}}$ est simple pour presque tout $\mathfrak{p}$. Pour une large classe de variétés abéliennes avec anneau d'endomorphismes absolus commutatif, nous donnons une borne supérieure explicite pour la croissance de l'ensemble des premiers de réduction non-simple.

Abstract. Let X/K be an absolutely simple abelian variety over a number field; we study whether the reductions $X_{\mathfrak{p}}$ tend to be simple, too. We show that if $\mathrm{End}(X)$ is a definite quaternion algebra, then the reduction $X_{\mathfrak{p}}$ is geometrically isogenous to the self-product of an absolutely simple abelian variety for $\mathfrak{p}$ in a set of positive density, while if X is of Mumford type, then $X_{\mathfrak{p}}$ is simple for almost all $\mathfrak{p}$. For a large class of abelian varieties with commutative absolute endomorphism ring, we give an explicit upper bound for the growth of the set of primes of non-simple reduction.

1. Introduction

Let X/K be an absolutely simple abelian variety over a number field. Evidence indicates that whether or not X has absolutely simple reduction almost everywhere depends on the endomorphism ring $\mathrm{End}(X)$. On one hand, if $\mathrm{End}(X)$ is an indefinite division algebra, then every good reduction $X_{\mathfrak{p}}$ is actually *split*, i.e., isogenous to a product of abelian varieties of smaller dimension [23, Thm. 2(e)].[1] On the other hand, if $\mathrm{End}(X)$ is trivial and $\dim(X)$ is odd [3], or if X has complex multiplication [13], then $X_{\mathfrak{p}}$ is almost always simple.

Manuscrit reçu le 23 octobre 2010, révisé le 22 décembre 2010.
Classification math. 11G25.

[1] This notion should not be confused with the (bad) split multiplicative reduction of an elliptic curve; primes of bad reduction never arise in the present work.

Inspired by this, Murty and Patankar conjectured [13] that in general, X has simple reduction almost everywhere if and only if $\mathrm{End}_{\overline{K}}(X)$ is commutative.

Using known instances of the Mumford-Tate conjecture and ideas of Chavdarov [4], the author made progress [1] towards affirming this conjecture. Moreover, a preprint of [1] elicited two further questions. W. Gajda shared a preprint of his work with Banaszak and Krasoń on the Mumford-Tate conjecture for abelian varieties of type III [2], and inquired whether it might be used to refine the results of [1] in that case. V.K. Murty asked whether one has any control over the size of the exceptional set of primes where an abelian variety with commutative endomorphism ring has split reduction.

Happily, the answer to each question is yes. First, as Gajda suspected, the results of [2] allow one to show:

Theorem A. *Let X/K be an absolutely simple abelian variety over a number field. Suppose that $\mathrm{End}_{\overline{K}}(X)\otimes\mathbb{Q}$ is a definite quaternion algebra over a totally real field F. If $\dim X/2[F:\mathbb{Q}]$ is odd, then for $\mathfrak{p}$ in a set of positive density, $X_{\mathfrak{p}}$ is geometrically isogenous to the self-product of an absolutely simple abelian variety $Y_{\mathfrak{p}}/\overline{\kappa(\mathfrak{p})}$ of dimension $(\dim X)/2$.*

This is worked out in Section 2.

Second, D. Zywina explained to me how the large sieve can be used to address Murty's question. Let $H_{X/K,\mathbb{Q}_\ell}$ be the Zariski closure of the image of the action of $\mathrm{Gal}(K)$ on the Tate module $T_\ell X$. In the present context, the method of [25] yields:

Theorem B. *Let X/K be an absolutely simple abelian variety of dimension g over a number field. Suppose some $H_{X/K,\mathbb{Q}_\ell}$ is connected and that either*

(a) *$\mathrm{End}_{\overline{K}}(X)\otimes\mathbb{Q}\cong F$ is a totally real field, and $r:=\dim X/[F:\mathbb{Q}]$ is odd, in which case let $d=[F:\mathbb{Q}](2r^2+r+1)$ and $t=[F:\mathbb{Q}](r+1)$; or*

(b) *there is some prime ℓ_0 such that $H_{X/K,\mathbb{Q}_{\ell_0}}\cong \mathrm{GSp}_{2g,\mathbb{Q}_{\ell_0}}$, in which case let $d=2g^2+g+1$ and $t=g+1$; or*

(c) *$\mathrm{End}_{\overline{K}}(X)\otimes\mathbb{Q}\cong E$ is a totally imaginary field, and the action of E on X is not special, in which case let $d=2g^2+g+1$ and $t=g+1$.*

Let $R(X/K;z)$ be the set of primes $\mathfrak{p}$ of $\mathcal{O}_K$ such that X has good, split reduction at $\mathfrak{p}$ and $\mathcal{N}(\mathfrak{p})<z$. Then

$$R(X/K;z)\ll\frac{z(\log\log z)^{1+1/3d}}{(\log z)^{1+1/6d}}.$$

If the generalized Riemann hypothesis is true, then

$$|R(X/K;z)| \ll z^{1-\frac{1}{2(2d+t+1)}}(\log z)^{\frac{2}{2d+t+1}}.$$

This is explained in Section 4. (Perhaps some remarks on the hypotheses, which are explained in greater detail in [1, Sec. 4], are in order here. In part (b), if the hypothesis is satisfied for one prime ℓ_0, then it is in fact satisfied for every prime ℓ. This follows from a special case of [9, Thm. 4.3], but it is not hard to give a direct proof. Indeed, let ℓ be any rational prime; then the rank of $H_{X/K,\mathbb{Q}_\ell}$ is again equal to $g+1$ [17], and the centralizer of $H_{X/K,\mathbb{Q}_\ell}(\mathbb{Q}_\ell)$ in $\mathrm{Aut}(T_\ell X \otimes \mathbb{Q}_\ell)$ is $(\mathrm{End}(X)\otimes\mathbb{Q}_\ell)^\times \cong \mathbb{Q}_\ell^\times$ [5]. By the theorem of Borel and de Siebenthal, $H_{X/K,\mathbb{Q}_\ell}$, a priori a subgroup of $\mathrm{GSp}_{2g,\mathbb{Q}_\ell}$, is actually equal to $\mathrm{GSp}_{2g,\mathbb{Q}_\ell}$. In part (c), "not special" is a combinatorial constraint on the signature of the action of E on $\mathrm{Lie}(X)$. The full definition is somewhat technical [24, 6.2.4] but is satisfied if, for instance, $2g/[E:\mathbb{Q}]$ is prime.)

Finally, since the method of [1] relies crucially on the image of mod-ℓ Galois representations, it seems reasonable to explore the conjecture of Murty and Patankar in cases where the endomorphism ring alone does not determine these groups. Mumford described the simplest such situation in [12]; there are abelian fourfolds with trivial endomorphism ring whose Mumford-Tate group is smaller than the full symplectic group.

Theorem C. *Let X/K be an abelian variety of Mumford's type over a number field. Possibly after a finite extension of the base field, $X_\mathfrak{p}$ is simple for $\mathfrak{p}$ in a set of density one.*

Notation. Let X/K be an abelian variety over a number field. For each rational prime ℓ, let $T_\ell(X)$ be its ℓ-adic Tate module, and let $X_\ell = X[\ell](\overline{K})$. Attached to X and ℓ are Galois representations $\rho_{X/K,\ell} : \mathrm{Gal}(K) \to \mathrm{Aut}(X_\ell)$ and $\rho_{X/K,\mathbb{Q}_\ell} : \mathrm{Gal}(K) \to \mathrm{Aut}(T_\ell(X)\otimes\mathbb{Q}_\ell)$. Let $H_{X/K,\ell}$ be the image of $\rho_{X/K,\ell}$, and let $H_{X/K,\mathbb{Q}_\ell}$ be the Zariski closure of the image of $\rho_{X/K,\mathbb{Q}_\ell}$ in the group (scheme) $\mathrm{Aut}_{T_\ell(X)\otimes\mathbb{Q}_\ell}$.

Suppose X admits an action by an order in a number field F. For each prime $\lambda \subset \mathcal{O}_F$, we have the λ-torsion $X_\lambda = X[\lambda](\overline{K})$, Tate module $T_\lambda(X) = \varprojlim_n X[\lambda^n](\overline{K})$, and associated Galois representations $\rho_{X/K,\lambda}$ and $\rho_{X/K,F_\lambda}$ with images $H_{X/K,\lambda}$ and $H_{X/K,F_\lambda}$.

Let $M(X/K)$ be the set of places of good reduction of X. If $\mathfrak{p} \in M(X/K)$, then the reduction $X_\mathfrak{p}$ is an abelian variety over the residue field $\kappa(\mathfrak{p})$. Let $\sigma_\mathfrak{p} \in \mathrm{Gal}(K)$ be a Frobenius element at $\mathfrak{p}$. If $\mathfrak{p}\nmid\ell$ then the characteristic polynomial of $\rho_{X/K,\mathbb{Q}_\ell}(\sigma_\mathfrak{p})$, *a priori* an element of $\mathbb{Q}_\ell[t]$, is actually defined over $\mathbb{Z}$. More generally, if X supports an F-action and if λ is a prime of F, then the characteristic polynomial of $\rho_{X/K,F_\lambda}(\sigma_\mathfrak{p})$ is defined over F and is independent of λ [16, Ch. II].

Acknowledgments. This paper is the outcome of conversations with Gajda, Murty and Zywina; it's a pleasure to thank all of them. I also thank the referee for helpful suggestions.

2. Abelian varieties of type III

In this section, recent work by Banaszak, Gajda and Krasoń [2] is used to characterize the splitting behavior of reductions of abelian varieties of type III. We make use of Katz's analysis of orthogonal groups over finite fields [7], which was carried out in the service of an irreducibility statement somewhat like Lemma 2.5. This is perhaps not surprising, insofar as both [1] and to a lesser extent [7] are inspired by the methods developed in the thesis of (Katz's student) Chavdarov [4].

Let Δ be a natural number divisible by all primes less than 7. Let F be a totally real field. Let V be a free $\mathcal{O}_F[1/\Delta]$-module of rank $2r$ equipped with a split nondegenerate symmetric quadratic form ψ. Using this data, define group schemes

$$\begin{aligned} G^* &= \mathrm{GO}(V,\psi) \\ SG^* &= \mathrm{SO}(V,\psi) \\ \Omega^* &= \mathrm{SO}(V,\psi)^{\mathrm{der}}. \end{aligned}$$

There are isomorphisms $G^*(\mathbb{F}_\lambda) \cong \mathrm{GO}_{2r}(\mathbb{F}_\lambda)$; $SG^*(\mathbb{F}_\lambda) \cong \mathrm{SO}^+_{2r}(\mathbb{F}_\lambda)$; and $\Omega^*(\mathbb{F}_\lambda) \cong \mathrm{SO}^+_{2r}(\mathbb{F}_\lambda)^{\mathrm{der}}$ is the set of elements of determinant and spinor norm one. Let G be the restriction of scalars $\mathbf{R}_{\mathcal{O}_F[1/\Delta]/\mathbb{Z}[1/\Delta]}G^*$, and define SG and Ω analogously. In particular, $G(\mathbb{Z}/\ell) = \oplus_{\lambda|\ell} G^*(\mathbb{F}_\lambda)$, where λ runs over the primes of $\mathcal{O}_F$ over ℓ and $\mathbb{F}_\lambda = \mathcal{O}_F/\lambda$.

Say that an abstract group H_λ is of type $G^*(\mathbb{F}_\lambda)$ if it is equipped with inclusions $\Omega^*(\mathbb{F}_\lambda) \subseteq H_\lambda \subseteq G^*(\mathbb{F}_\lambda)$; the notion of a group H_ℓ of type $G(\mathbb{F}_\ell)$ is defined in a similar way.

For a pair of natural numbers $\underline{a} = \{a_1, a_2\}$ with $a_1 + a_2 = r$, define a subset $J_{\lambda,\underline{a}} \subset G^*(\mathbb{F}_\lambda)$ as follows. Let $J_{\lambda,\underline{a}}$ be the set of semisimple $x \in G^*(\mathbb{F}_\lambda)$ such that there exists an orthogonal decomposition $V \otimes \mathcal{O}_F/\lambda \cong U_1 \oplus U_2$ where $\dim_{\mathbb{F}_\lambda} U_i = 2a_i$ and x acts irreducibly on each U_i. Also, for $\underline{a} = \{r, r\}$, let $J_{\lambda,\underline{a}}$ be the set of semisimple $x \in G^*(\mathbb{F}_\lambda)$ such that there exists a decomposition $V \otimes \mathcal{O}_F/\lambda \cong U_1 \oplus U_2$ such that $\dim_{\mathbb{F}_\lambda} U_i = r$; x acts irreducibly on each U_i; the characteristic polynomials $f_{x|_{U_i}}(t)$ of x on U_1 and U_2 are not associates, but $f_{x|_{U_1}}(t)$ and $t^r f_{x|_{U_2}}(1/t)$ are; and U_1 and U_2 are dual to each other under ψ. For H_λ of type $G^*(\mathbb{F}_\lambda)$, let $J_{\lambda,\underline{a}}(H_\lambda) = H_\lambda \cap J_{\lambda,\underline{a}}$.

Lemma 2.1. *There exists a constant $\epsilon = \epsilon(r) > 0$ such that for any data $\underline{a} = \{a_1, a_2\}$ as above, any prime $\lambda \nmid \Delta$, and any H_λ of type $G^*(\mathbb{F}_\lambda)$,*

$$\frac{\# J_{\lambda,\underline{a}}(H_\lambda)}{\# H_\lambda} > \epsilon.$$

Proof. The case where $H_\lambda \subseteq SG^*(\mathbb{F}_\lambda)$ is [7, Lemmas 6.5 and 6.6]. The general case follows from the argument used in the second half of the proof of [1, Lemma 1.1]. (The key point is that, after passage to adjoint groups, the index of the abstract group in the derived group is bounded, independently of ℓ.) ☐

Lemma 2.2. *Given an absolutely simple abelian variety X over a number field K_0, there exists a finite extension K/K_0 such that:*

(i) $\mathrm{End}_K(X_K) = \mathrm{End}_{\overline{K}}(X_{\overline{K}})$*;*
(ii) *For each ℓ, the Zariski closure $H_{X/K,\mathbb{Q}_\ell}$ of $\rho_{X/K,\mathbb{Z}_\ell}$ in $\mathrm{Aut}_{T_\ell(X)\otimes\mathbb{Q}_\ell}$ is a connected algebraic group;*
(iii) *There exists ℓ_0 such that $\mathrm{im}(\prod_{\ell\geq\ell_0}\rho_{X/K,\ell}) \cong \prod_{\ell\geq\ell_0} H_{X/K,\ell}$.*

Proof. Each of these properties is preserved by any finite extension; and field extensions satisfying (i), (ii) and (iii) are explicitly calculated in [21, Thm. 2.4], [22, Thm. 4.6] and [18, Lemme 1.2.1], respectively. ☐

The groups $H_{X/K,\ell}$ are calculated for abelian varieties of type III in [2]. Suppose X/K is a polarized simple abelian variety such that $\mathrm{End}_K(X)\otimes\mathbb{Q}$ is a definite quaternion algebra. Then the polarization induces a nondegenerate *symmetric* quadratic form on each X_ℓ.

Lemma 2.3. *Let X/K be a simple abelian variety over a number field satisfying the conclusions of 2.2. Suppose that $\mathrm{End}_K(X)\otimes\mathbb{Q}$ is a definite quaternion algebra over a totally real field F such that $r = \dim(X)/2[F:\mathbb{Q}]$ is odd. For ℓ in a set $\mathbb{L}_+$ of positive density,*

(a) *there is a continuous linear action of $\mathrm{Gal}(K)$ on $V\otimes\mathbb{Z}/\ell$ which induces an isomorphism $X_\ell \cong (V\otimes\mathbb{Z}/\ell)^{\oplus 2}$ of quadratic spaces with $\mathrm{Gal}(K)$-action; and*
(b) $\Omega(\mathbb{Z}/\ell) \subseteq H^{\mathrm{der}}_{X/K,\ell} \subseteq SG(\mathbb{Z}/\ell) \subsetneq H_{X/K,\ell} \subseteq G(\mathbb{Z}/\ell)$.

Proof. Possibly at the cost of restricting to ℓ in a set $\mathbb{L}_+$ of positive density, we may and do assume that the discriminant of some polarization of X is a square in $\mathbb{F}_\ell$. Then part (a) is [2, Thm. 3.23], while part (b) is [2, Thm. 6.29]. ☐

Let $\mathbb{L}_+^*$ be the set of primes of F which lie over elements of $\mathbb{L}_+$. For data $\underline{a}$ and a set $A\subset\mathbb{L}_+^*$, let

$$I(X/K;\underline{a};A) = \{\mathfrak{p} : \forall\lambda\in A, \rho_{X/K,\lambda}(\sigma_\mathfrak{p}) \notin J_{\lambda,\underline{a}}(H_{X/K,\lambda})\}.$$

It turns out that $I(X/K;\underline{a};\mathbb{L}_+^*)$ has density zero:

Lemma 2.4. *Suppose X/K satisfies the hypotheses of Lemma 2.3. If $A\subset\mathbb{L}_+^*$ is infinite, then $I(X/K;\underline{a};A)$ has density zero.*

Proof. Let ϵ be the constant of Lemma 2.1, and let $A_0 \subset A$ be any finite subset. By the Chebotarev theorem, condition (iii) of Lemma 2.2, and Lemmas 2.3 and 2.1, the density of $I(X/K; \underline{a}; A_0)$ is at most $(1-\epsilon)^{|A_0|}$. The result now follows by taking ever-larger sets A_0. $\square$

Consequently, the F-linear characteristic polynomial of a reduction of X is almost always the square of an irreducible polynomial:

Lemma 2.5. *Suppose X/K satisfies the hypotheses of Lemma 2.3. For $\mathfrak{p}$ in a set of density one, the F-linear characteristic polynomial of Frobenius of $X_\mathfrak{p}$ is the square of an irreducible polynomial.*

Proof. Let $g_\mathfrak{p}^*(t) \in \mathcal{O}_F[t]$ be the F-linear characteristic polynomial of Frobenius of $X_\mathfrak{p}$. Then there exists a polynomial $f_\mathfrak{p}^*(t) \in \mathcal{O}_F[t]$ of degree $2r$ such that $g_\mathfrak{p}^*(t) = f_\mathfrak{p}^*(t)^2$ (e.g., [1, Lemmas 3.2 and 2.6]; this also follows swiftly from [2, Thm. 3.23]).

Since there is no absolutely simple abelian variety in characteristic zero with $r = 1$ [20, Prop. 15], and since r is odd by hypothesis, assume $r \geq 3$. Consider some d with $1 \leq d < \deg f_\mathfrak{p}^*(t)$. If $d = r$, let $\underline{a} = \{1, r-1\}$; otherwise, let $\underline{a} = \{r, r\}$. If there exists some $\lambda \in \mathbb{L}_+^*$ with $\rho_{X/K,\lambda}(\sigma_\mathfrak{p}) \in J_{\lambda,\underline{a}}(H_{X/K,\lambda})$, then $f_\mathfrak{p}^*(t)$ has no factor of degree d. Consequently, if $f_\mathfrak{p}^*(t)$ has an irreducible factor of degree d, then $\mathfrak{p} \in I(X/K; \underline{a}; \mathbb{L}_+^*)$, which is a set of density zero (Lemma 2.4). $\square$

If $\mathfrak{p}$ is in the density-one set described in Lemma 2.5, then $X_\mathfrak{p}$ is either simple as F-abelian variety or it is isogenous to the self-product of a simple F-abelian variety. In the former case, it does not follow that $X_\mathfrak{p}$ is simple as abelian variety; indeed, it is possible that there is an isogeny $X_\mathfrak{p} \sim Y^s$ and an embedding $F \hookrightarrow \mathrm{Mat}_s(\mathrm{End}(Y) \otimes \mathbb{Q})$ such that F acts irreducibly on the s-fold product of Y. Such behavior can be ruled out with a further condition on the characteristic polynomial, as follows.

Recall that $G(\mathbb{Z}/\ell) \cong \oplus_{\lambda|\ell} G^*(\mathbb{F}_\lambda)$. If $x = \{x_\lambda\}_{\lambda|\ell} \in G(\mathbb{Z}/\ell)$, then the $\mathbb{F}_\ell$-linear characteristic polynomial $f_x(t)$ of x (acting on V) is

$$f_x(t) = \prod_{\lambda|\ell} \mathbf{N}_{\mathbb{F}_\lambda/\mathbb{F}_\ell} f_{x_\lambda}(t)$$

where

$$\mathbf{N}_{\mathbb{F}_\lambda/\mathbb{F}_\ell} g(t) = \prod_{\tau \in \mathrm{Gal}(\mathbb{F}_\lambda/\mathbb{F}_\ell)} g^\tau(t).$$

For a divisor s of $[F : \mathbb{Q}]$ with $s \geq 2$, let $M_{\ell,s}(G)$ be the set of $x \in G(\mathbb{Z}/\ell)$ such that $f_x(t)$ is an s^{th} power; for H_ℓ of type $G(\mathbb{Z}/\ell)$, let $M_{\ell,s}(H_\ell) = H_\ell \cap M_{\ell,s}(G)$.

Lemma 2.6. *Suppose H_ℓ is of type $G(\mathbb{Z}/\ell)$. Then $|M_{\ell,s}(H_\ell)|/|H_\ell|$ is bounded below* 1*, independently of ℓ.*

Proof. If ℓ is inert in F, then $J_{\ell,\{1,r-1\}}(H_\ell)$ is in the complement of $M_{\ell,s}(H_\ell)$ and the result follows from Lemma 2.1.

Otherwise, fix some prime λ_0 lying over ℓ, and suppose components $\{x_\lambda\}_{\lambda\neq\lambda_0}$ are fixed. To prove the lemma, it suffices to bound away from 1 the proportion of $x_{\lambda_0}\in G^*(\mathbb{F}_{\lambda_0})$ such that $f_x(t)$ is an s^{th} power. Given data $\{x_\lambda\}_{\lambda\neq\lambda_0}$, let $f^{\lambda_0}(t)=\prod_{\lambda\neq\lambda_0}\mathbf{N}_{\mathbb{F}_\lambda/\mathbb{F}_\ell}f_{x_\lambda}(t)$.

If $f^{\lambda_0}(t)$ is itself an s^{th} power, then $\mathbf{N}_{\mathbb{F}_{\lambda_0}/\mathbb{F}_\ell}f_{x_{\lambda_0}}(t)f^{\lambda_0}(t)$ is an s^{th} power if and only if $\mathbf{N}_{\mathbb{F}_{\lambda_0}/\mathbb{F}_\ell}f_{x_\lambda 0}(t)$ is an s^{th} power, too. This is precluded if $f_{x_{\lambda_0}}(t)$ is not an s^{th} power (e.g., if $x_{\lambda_0}\in J_{\lambda,\{1,r-1\}}(H_{\lambda_0})$) and if $f_{x_{\lambda_0}}(t)$ is not defined over any proper subfield of $\mathbb{F}_{\lambda_0}$. These two conditions account for a positive proportion of elements of H_{λ_0}.

Otherwise, there is a unique polynomial $g(t)$ such that $g(t)f^{\lambda_0}(t)$ is an s^{th} power, and thus at most $[\mathbb{F}_{\lambda_0}:\mathbb{F}_\ell]$ polynomials $h(t)$ such that $\mathbf{N}_{\mathbb{F}_{\lambda_0}/\mathbb{F}_\ell}h(t)f^{\lambda_0}(t)$ is an s^{th} power.

We now show that, given a polynomial $h(t)\in\mathbb{F}_\lambda[t]$, the proportion of elements of H_λ with characteristic polynomial $h(t)$ is bounded from above, independently of λ. First, suppose that $H_\lambda=\Omega^*(\mathbb{F}_\lambda)$. By the Lang-Weil estimate – the locus of non-semisimple elements is a closed subscheme of Ω^* – it suffices to bound the number of semisimple $x\in\Omega^*(\mathbb{F}_\lambda)$ with $f_x(t)=h(t)$. Given such an x, choose some maximal torus S^* containing x. The number of elements of $y\in S^*(\mathbb{F}_\lambda)$ with $f_y(t)=f_x(t)$ may be bounded in terms of the rank of S^*, while $|S^*(\mathbb{F}_\lambda)|$ is polynomial in $|\mathbb{F}_\lambda|$. The desired assertion for $\Omega^*(\mathbb{F}_\lambda)$ now follows. Now consider an arbitrary H_λ of type $G^*(\mathbb{F}_\lambda)$. If there is any $x\in H_\lambda$ with $f_x(t)=h(t)$ then the same argument, applied to the coset $x\cdot\Omega^*(\mathbb{F}_\lambda)$ in H_λ, shows that a vanishingly small proportion of elements of H_λ have characteristic polynomial $h(t)$.

Consequently, for each choice of data $\{x_\lambda\}_{\lambda\neq\lambda_0}\in\prod_{\lambda\neq\lambda_0}H_\lambda\subseteq\prod_{\lambda\neq\lambda_0}G^*(\mathbb{F}_\lambda)$, the proportion of choices for $x_{\lambda_0}\in H_{\lambda_0}$ such that $f_x(t)$ is an s^{th} power is bounded above, independently of ℓ. □

Lemma 2.7. *Suppose X/K satisfies the hypotheses of Lemma 2.3. For $\mathfrak{p}$ in a set of density one, the $\mathbb{Q}$-linear characteristic polynomial of Frobenius of $X_\mathfrak{p}$ is the square of an irreducible polynomial.*

Proof. Consider a prime $\mathfrak{p}$ of good reduction of X. Let $g^*_\mathfrak{p}(t)$ be the F-linear characteristic polynomial of Frobenius of $X_\mathfrak{p}$; then $g_\mathfrak{p}(t)=\mathbf{N}_{F/\mathbb{Q}}g^*_\mathfrak{p}(t)$ is the $\mathbb{Q}$-linear characteristic polynomial of Frobenius of $X_\mathfrak{p}$. We have seen that $g^*_\mathfrak{p}(t)=(f^*_\mathfrak{p}(t))^2$ for some $f^*_\mathfrak{p}(t)\in\mathcal{O}_F[t]$, and thus $g_\mathfrak{p}(t)=f_\mathfrak{p}(t)^2$ where $f_\mathfrak{p}(t)=\mathbf{N}_{F/\mathbb{Q}}f^*_\mathfrak{p}(t)$. By Lemma 2.6 and the Chebotarev argument used in

Lemma 2.4, for $\mathfrak{p}$ in a set of density one, $f_{\mathfrak{p}}(t)$ is not an s^{th} power for any $2 \le s \le [F : \mathbb{Q}]$.

Now suppose that $f_{\mathfrak{p}}(t)$ is not an s^{th} power and that $\mathfrak{p}$ is in the density-one set constructed in Lemma 2.4. Then $f^*_{\mathfrak{p}}(t)$ is irreducible over F, and $f_{\mathfrak{p}}(t)$ is irreducible over $\mathbb{Q}$. □

Corollary 2.8. *Suppose X/K satisfies the hypotheses of Lemma 2.3. For $\mathfrak{p}$ in a set of density one, $X_{\mathfrak{p}}$ is isogenous to the self-product of a simple abelian variety with itself.*

Proof. By Lemma 2.7, there is a set of primes S of density one such that for $\mathfrak{p} \in S$, $X_{\mathfrak{p}}$ is either simple or isogenous to the self-product of a simple abelian variety with itself. In the former case, $X_{\mathfrak{p}}$ itself has noncommutative endomorphism ring; but this cannot happen for those $\mathfrak{p}$ with $|\kappa(\mathfrak{p})|$ prime. The intersection of S with the density one set of primes with residue degree one is the desired set. □

Proof of Theorem A. Let K'/K be an extension such that X/K' satisfies the conclusions of Lemma 2.2. The set of primes $\mathfrak{p}'$ of K' such that $X_{\mathfrak{p}'}$ is isogenous to the self-product of a simple abelian variety has density one (Corollary 2.8), and the set of primes $\mathfrak{p}$ of K lying under such $\mathfrak{p}'$ has positive density. □

Remark 2.9. The proofs of [1, Thms. 4.1, 4.2 and 5.4] are incomplete, as written; they rely on the existence of a rational prime ℓ which stays prime in a given totally real field F. Instead, one should proceed as in the proof given here of Theorem A. In somewhat more detail, in [1] one works with a group scheme $G/\mathbb{Z}[1/\Delta]$, which is constructed as $\mathbf{R}_{\mathcal{O}_F[1/\Delta]/\mathbb{Z}[1/\Delta]}G^*$ for a certain algebraic group G^*. By working with the λ-adic Galois representations $\mathrm{Gal}(K) \to G^*(\mathbb{F}_\lambda)$, one can show that for primes $\mathfrak{p}$ in a set of density one, $X_{\mathfrak{p}}$ is simple as an abelian variety with F-action. Then as in Lemma 2.7, one can show for a possibly smaller, but still density one, set of primes, these irreducible F-abelian varieties are actually irreducible.

Note that the local conditions which force irreducibility are detectable on the modℓ Galois representations $\rho_{X/K,\ell}$, even though these conditions are perhaps best understood in terms of the modλ representations. In short, in each of the cases considered in [1], for ℓ in a set of density one one can find a subgroup $J_\ell \subset H_{X/K,\ell}$ such that (a) $|J_\ell|/\left|H_{X/K,\ell}\right| > C > 0$; and (b) if $\rho_{X/K,\ell}(\sigma_{\mathfrak{p}}) \in J_\ell$ then $X_{\mathfrak{p}}$ is irreducible.

3. Abelian varieties of Mumford's type

Let X/K be a g-dimensional abelian variety over a number field with $\mathrm{End}_K(X) = \mathrm{End}_{\overline{K}}(X) = \mathbb{Z}$. If g is odd, or if g is 2 or 6, then $H_{X/K,\mathbb{Q}_\ell} \cong$

$\mathrm{GSp}_{2g,\mathbb{Q}_\ell}$ [19]. For general even dimension, however, there are other possibilities for the image of Galois. The simplest examples occur in dimension four, and were explored by Mumford in [12]. Briefly, from a totally real cubic field F and a suitable quaternion algebra D/F, Mumford constructs a simple algebraic group $G/\mathbb{Q}$ whose derived group is isogenous to a twist of SL_2^3, such that if X is an abelian fourfold with Mumford-Tate group G then $\mathrm{End}_K(X) \cong \mathbb{Z}$. Conversely, if X is an abelian fourfold with trivial absolute endomorphism ring such that some $H_{X/K,\mathbb{Q}_\ell}$ is not isomorphic to $\mathrm{GSp}_{2g,\mathbb{Q}_\ell}$, then X comes from such a construction (e.g., [15, Prop. 1.5]).

The group G comes equipped with a representation $G \to \mathrm{GL}(V)$ on an 8-dimensional vector space over $\mathbb{Q}$. While Mumford describes this group and representation in detail, for present purposes it suffices to describe the simply connected cover of G.

Let $D_1^\times \subset D^\times$ be the group of norm-one elements, thought of as a group scheme over $\operatorname{Spec} F$. Let $\widetilde{G}^{\mathrm{der}}$ be the restriction of scalars $\widetilde{G}^{\mathrm{der}} = \mathbf{R}_{F/\mathbb{Q}} D_1^\times$ and let $\widetilde{G} = \mathbb{G}_m \times \widetilde{G}^{\mathrm{der}}$. Then there is a central isogeny $\nu : \widetilde{G} \to G$. Suppose ℓ splits completely in F, and that D is split at each prime lying over ℓ. Then $\widetilde{G}^{\mathrm{der}}_{\mathbb{Q}_\ell} \cong \mathrm{SL}^3_{2,\mathbb{Q}_\ell}$, and the representation $\widetilde{G}^{\mathrm{der}}_{\mathbb{Q}_\ell} \to G_{\mathbb{Q}_\ell} \to \mathrm{Aut}(V \otimes \mathbb{Q}_\ell)$ is the third (external) tensor power of the standard representation of SL_2.

Let Δ be the product of all rational primes ramified in F or in D. Since there is a unique G-invariant alternating form on V, we may and do choose a reductive model G over $\mathbb{Z}[1/\Delta]$ and a free $\mathbb{Z}[1/\Delta]$-module V of rank 8 such that $G \subset \mathrm{GL}(V)$ and $G(\mathbb{Z}_\ell)$ is the unique hyperspecial subgroup of $G(\mathbb{Q}_\ell)$. Similarly define $\widetilde{G}^{\mathrm{der}}/\operatorname{Spec}\mathbb{Z}[1/\Delta]$. Let $\widetilde{F}$ be the Galois closure of F over $\mathbb{Q}$.

Lemma 3.1. *Let X/K be an abelian variety of Mumford's type. Let $\mathfrak{p}$ be a prime of good ordinary reduction. There is a totally imaginary field L with $F \subseteq L \subseteq D$ such that either:*

(a) *There is a quadratic imaginary subfield $E \subset L$ such that $L = EF$. Then $X_{\mathfrak{p}}$ is isogenous to $Y^{(1)} \times Y^{(3)}$, where $Y^{(i)}$ is a simple abelian variety of dimension i, $Y^{(1)}$ has complex multiplication by E, and $Y^{(3)}$ has complex multiplication by L; or*

(b) *There is no quadratic imaginary subfield of L. Let $\widetilde{L}$ be the Galois closure of L over $\mathbb{Q}$. Then $\mathrm{Gal}(\widetilde{L}/\mathbb{Q}) \cong \{\pm 1\}^3 \rtimes H$ for some group $A_3 \subseteq H \subseteq S_3$. Let $E = \widetilde{L}^H$. Then $X_{\mathfrak{p}}$ is a simple abelian variety with complex multiplication by E.*

Proof. By examining maximal tori of $G_{\mathbb{Q}}$, Noot has produced a complete classification of the possibilities for the CM type of a specialization of an abelian variety of Mumford's type [15, Sec. 3]. An ordinary abelian variety $Y/\kappa(\mathfrak{p})$ admits a (unique, canonical) lift $\widehat{Y}$ to characteristic zero such that

$\mathrm{End}(\hat{Y}) \cong \mathrm{End}(Y)$. Lemma 3.1 is deduced by applying Noot's classification to $\widehat{X_{\mathfrak{p}}}$. $\square$

Corollary 3.2. *In the situation of Lemma 3.1, suppose there is a rational prime ℓ which splits in F as $\ell\mathcal{O}_F = \lambda_1 \cdot \lambda_2 \cdot \lambda_3$. Suppose that for $i = 1, 2$ there exists a prime λ_i' of $\mathcal{O}_L$ lying over λ_i such that $[\mathcal{O}_L/\lambda_1' : \mathcal{O}_F/\lambda_1] \neq [\mathcal{O}_L/\lambda_2' : \mathcal{O}_F/\lambda_2]$. Then $X_{\mathfrak{p}}$ is simple.*

Proof. Let $\widetilde{F}$ be the Galois closure of F over $\mathbb{Q}$. The hypothesis guarantees that $\widetilde{F}L$ is not Galois over $\mathbb{Q}$, and thus L is not of the form FE for a quadratic imaginary field E. Since case (a) of Lemma 3.1 is ruled out, the dichotomy shows that $X_{\mathfrak{p}}$ is simple. $\square$

Proof of Theorem C. As in the proof of [1, Thm. 4.1], it suffices to prove the result after finite extension of the base. Consequently, we assume that each $H_{X/K,\mathbb{Q}_\ell}$ is connected, and that $X_{\mathfrak{p}}$ is ordinary for $\mathfrak{p}$ in a set of density one [14, Thm. 2.2].

By Larsen's theorem [10, Thm. 3.17], for ℓ in a set $\widetilde{\mathbb{L}}$ of density one, the derived group of $H_{X/K,\ell}$ is $G^{\mathrm{der}}(\mathbb{Z}/\ell)$. Possbily after removing finitely many primes from $\widetilde{\mathbb{L}}$, since $\mathrm{Gal}(K) \to G(\mathbb{Z}/\ell) \to G(\mathbb{Z}/\ell)/G^{\mathrm{der}}(\mathbb{Z}/\ell)$ is the ℓ-cyclotomic character, $H_{X/K,\ell} = G(\mathbb{Z}/\ell)$ for $\ell \in \widetilde{\mathbb{L}}$. Let $\mathbb{L} \subset \widetilde{\mathbb{L}}$ be the subset of primes which split completely in F. Then $\mathbb{L}$ has positive density, and in particular is infinite. Since $\mathrm{PSL}_2(\mathbb{Z}/\ell)$ and $\mathrm{PSL}_2(\mathbb{Z}/\ell')$ are nonisomorphic simple groups for distinct odd primes ℓ and ℓ', if $A \subset \mathbb{L}$, then the image of $\mathrm{Gal}(K)$ under $\times_{\ell \in A} \rho_{X/K,\ell}$ is $\times_{\ell \in A} H_{X/K,\ell}$.

For each $\ell \in \mathbb{L}$ choose a maximal torus $\widetilde{S}_\ell \subset \widetilde{G}_{\mathbb{Z}/\ell}$ which, under the isomorphism $\widetilde{G}_{\mathbb{Z}/\ell} \cong \mathrm{SL}_2^3 \times \mathbb{G}_m$, is the product of an anisotropic torus, two split tori, and the full $\mathbb{G}_m$; and let $S_\ell = \nu(\widetilde{S}_\ell)$. On one hand, by Corollary 3.2, if $\rho_{X/K,\ell}(\sigma_{\mathfrak{p}})$ is a regular element of a conjugate of $S_\ell(\mathbb{Z}/\ell)$, then $X_{\mathfrak{p}}$ is simple. On the other hand, the usual Chebotarev argument (e.g., Lemma 2.4) shows that the set of $\mathfrak{p}$ such that $\rho_{X/K,\ell}(\sigma_{\mathfrak{p}})$ *avoids* all conjugates of $S_\ell(\mathbb{Z}/\ell)$ for each $\ell \in \mathbb{L}$ has density zero. $\square$

4. Explicit bounds

Let X/K be a simple abelian variety over a number field such that $\mathrm{End}(X) = \mathrm{End}_{\overline{K}}(X)$ is commutative. In favorable conditions, one can prove that the reduction $X_{\mathfrak{p}}$ is simple for almost all $\mathfrak{p}$, as follows. If $X_{\mathfrak{p}}$ is *not* simple, then the characteristic polynomial of Frobenius $f_{\mathfrak{p}}(t)$ of $X_{\mathfrak{p}}$ factors over $\mathbb{Z}$, and in particular factors modℓ for all ℓ. If the Galois representations $\rho_{X/K:\ell}$ are sufficiently well understood, then a crude appeal to the Chebotarev density theorem shows that the set of $\mathfrak{p}$ such that $\rho_{X/K,\ell}(\sigma_{\mathfrak{p}})$ acts reducibly for each ℓ has density zero. In this section, we explain how the large sieve yields more control over this exceptional set. The formulation of Zywina's thesis is used here [25], although one could just as easily apply the setting developed by Kowalski [8].

Throughout this section, G is a connected algebraic group over $\mathbb{Z}[1/\Delta]$ with fibers of dimension $d(G)$ and rank $t(G)$.

We will often have cause to consider a subset R of the primes of a number field K. Let $f_R(z) = |\{\mathfrak{p} \in R : \mathcal{N}(\mathfrak{p}) < z\}|/|\{\mathfrak{p} \subset \mathcal{O}_K : \mathcal{N}(\mathfrak{p}) < z\}|$. Then the natural density of R is $\lim_{z\to\infty} f_R(z)$, while its lower natural density is $\liminf_{z\to\infty} f_R(z)$.

If H is an abstract group, let $H^\sharp$ be the set of conjugacy classes of H.

Lemma 4.1. *There exists a constant $\alpha = \alpha(G)$ such that*

$$|G(\mathbb{Z}/\ell)| \leq \ell^{d(G)} \tag{4.1}$$

$$\left|G(\mathbb{Z}/\ell)^\sharp\right| < (\alpha\ell)^{t(G)}. \tag{4.2}$$

Proof. The first assertion is clear, while the estimate (4.2) follows from [11, Th. 1] and [6, Eq. (3)]. □

Lemma 4.2. *Let A be a subgroup of a finite group B. Then*

$$\left|A^\sharp\right||A| \leq \left|B^\sharp\right||B|.$$

Proof. This follows immediately from the fact [6, Eq. (1)] that $\left|A^\sharp\right| \leq [B : A]\left|B^\sharp\right|$. □

Let $R(X/K) = \{\mathfrak{p} \in M(X/K) : X_\mathfrak{p} \text{ is split}\}$. For a real number z, let $R(X/K; z) = \{\mathfrak{p} \in R(X/K) : \mathcal{N}(\mathfrak{p}) < z\}$.

Lemma 4.3. *Let X/K be a simple abelian variety over a number field. Suppose there is a set $\mathbb{L}$ of positive lower natural density such that for each $\ell \in \mathbb{L}$, $H_{X/K,\ell}$ is of type $G(\mathbb{Z}/\ell)$; and for each finite subset $A \subset \mathbb{L}$, the image of* $\mathrm{Gal}(K)$ *under $\times_{\ell\in A}\rho_{X/K,\ell}$ is $\times_{\ell\in A}H_{X/K,\mathbb{L}}$.*

Further suppose that for each $\ell \in \mathbb{L}$ there is a subset $J_\ell(G) \subseteq G(\mathbb{Z}/\ell)$ such that $\left|J_\ell(G) \cap H_{X/K,\ell}\right|/\left|H_{X/K,\ell}\right| > \epsilon > 0$; and if $\rho_{X/K,\ell}(\sigma_\mathfrak{p}) \in J_\ell(G)$, then $X_\mathfrak{p}$ is simple.

(a) *Then*

$$|R(X/K; z)| \ll \frac{z(\log\log z)^{1+1/3d(G)}}{(\log z)^{1+1/6d(G)}}.$$

(b) *If the generalized Riemann hypothesis is true, then*

$$|R(X/K; z)| \ll z^{1-\frac{1}{2(2d(G)+t(G)+1)}}(\log z)^{\frac{2}{2d(G)+t(G)+1}}.$$

Proof. The argument of [25, Sec. 6.4] works here. For any positive number Q, define

$$\begin{aligned}\mathbb{L}_Q &= \mathbb{L} \cap [2, Q] \\ \Xi(Q) &= \{D \text{ square-free} : \alpha^{\omega(D)} D < Q, \ell | D \implies \ell \in \mathbb{L}\} \\ I(X/K; G; \mathbb{L}_Q; z) &= \{\mathfrak{p} : \mathcal{N}(\mathfrak{p}) \le z \text{ and } \rho_{X/K,\ell}(\sigma_\mathfrak{p}) \notin J_\ell(G) \text{ for all } \ell \in \mathbb{L}_Q\}.\end{aligned}$$

where $\omega(D)$ is the number of prime divisors of D. For $D \in \Xi(Q)$, let $H_{X/K,D} = \prod_{\ell|D} H_{X/K,\ell}$, and let $G_D = \prod_{\ell|D} G(\mathbb{Z}/\ell)$. (In all cases of interest, $G_D \cong G(\mathbb{Z}/D)$.) By Lemmas 4.1 and 4.2,

$$\begin{aligned}\left|H_{X/K,D}\right| &\le |G_D| \le Q^{d(G)} \\ \left|H^\sharp_{X/K,D}\right|\left|H_{X/K,D}\right| &\le \left|G^\sharp_D\right||G_D|.\end{aligned}$$

Following Zywina, define and estimate the associated sieve constant by

$$\begin{aligned}L(Q) &= \sum_{D \in \Xi(Q)} \prod_{\ell|D} \frac{\epsilon}{1-\epsilon} \\ &\ge \sum_{\ell \in \mathbb{L}_{Q/\alpha}} \frac{\epsilon}{1-\epsilon} \\ &= \frac{\epsilon}{1-\epsilon}\left|\mathbb{L}_{Q/\alpha}\right| \\ &\gg \frac{Q}{\log Q},\end{aligned}$$

since $\mathbb{L}$ has positive lower natural density.

By hypothesis,

$$R(X/K; z) \subseteq I(X/K; G; \mathbb{L}_Q; z). \tag{4.3}$$

To prove (a), let $Q(z) = c(\log z/(\log\log z)^2)^{1/6d(G)}$ for a sufficiently small positive constant c. Then

$$\begin{aligned}L(Q(z)) &\gg \frac{Q(z)}{\log(Q(z))} \\ &\gg \frac{(\log z)^{1/6d(G)}}{(\log\log z)^{1+1/3d(G)}}.\end{aligned}$$

Using [25, Theorem 3.3(i)], we estimate the size of the right-hand side of (4.3) as

$$\begin{aligned}\left|I(X/K; G; \mathbb{L}_{Q(z)}; z)\right| &\ll \frac{z}{\log z} L(Q(z))^{-1} \\ &\ll \frac{z(\log\log z)^{1+1/3d(G)}}{(\log z)^{1+1/6d(G)}}.\end{aligned}$$

We now address part (b). We have the estimate

$$\begin{aligned}
\max_{D\in\Xi(Q)} |H_D| \cdot \sum_{D\in\Xi(Q)} \left|H^\sharp_D\right||H_D| &\le \max_{D\in\Xi(Q)} |G_D| \cdot \sum_{D\in\Xi(Q)} \left|G^\sharp_D\right||G_D| \\
&\le Q^{d(G)} \cdot \sum_{D\in\Xi(Q)} (\prod_{\ell|D} (\alpha\ell)^{t(G)})(\prod_{\ell|D} \ell^{d(G)}) \\
&\le Q^{d(G)}|\Xi(Q)|Q^{t(G)}Q^{d(G)} \ll Q^{f(G)},
\end{aligned}$$

where we have set $f(G) = 2d(G) + t(G) + 1$ to ease notation.

Suppose that GRH holds. By [25, Th. 3.3(ii)],

$$\begin{aligned}
|I(X/K;G;\mathbb{L}_Q;z)| &\ll \left(\frac{z}{\log z} + (\max_{D\in\Xi(Q)} \left|H_{X/K,D}\right| \cdot \right. \\
&\qquad \left. \sum_{D\in\Xi(Q)} \left|H^\sharp_{X/K,D}\right|\left|H_{X/K,D}\right|)\sqrt{z}\log(z)\right) L(Q)^{-1} \\
&\ll \left(\frac{z}{\log z} + Q^{f(G)}\right)\frac{\log(Q)}{Q}.
\end{aligned}$$

So, take $Q(z) = (\frac{\sqrt{z}}{(\log z)^2})^{1/f(G)}$. Then $\log(Q) \ll \log z$, and

$$\begin{aligned}
\left|I(X/K;G;\mathbb{L}_{Q(z)};z)\right| &\ll \frac{z}{\log(z)}\frac{\log Q(z)}{Q(z)} \\
&\ll \frac{z}{\log(z)}\log(z)\frac{(\log z)^{2/f(G)}}{z^{1/2f(G)}} \\
&= z^{1-1/2f(G)}(\log z)^{2/f(G)}.
\end{aligned}$$

□

Lemma 4.3 allows for explicit versions of the results of [1, Sec. 4], as follows.

Proof of Theorem B. Only the necessary changes to the proof of [1, Thm. A] are indicated here, although Remark 2.9 should also be borne in mind.

If K'/K is finite and Galois, then the number of primes $\mathfrak{p} \subset \mathcal{O}_K$ with $\mathcal{N}(\mathfrak{p}) < z$ such that $\mathfrak{p}\mathcal{O}_{K'}$ is not prime is $\ll \frac{z^{1/2+\epsilon}}{\log(z)}$. Therefore, it suffices to prove the result after a finite extension of K, and thus we can and do assume that $\operatorname{End}_K(X) = \operatorname{End}_{\overline{K}}(X)$ and each $H_{X/K,\mathbb{Q}_\ell}$ is connected. For part (a), for $\mathbb{L}$ take the set of primes ℓ such that $H_{X/K,\ell}$ is of type $G(\mathbb{Z}/\ell) = (\mathbf{R}_{\mathcal{O}_F/\mathbb{Z}} \operatorname{GSp}_{2r})(\mathbb{Z}/\ell)$. Then $\mathbb{L}$ contains all but finitely many primes; now use Lemma 4.3.

For parts (b) and (c), the key point is that in the context of the compatible system of representations associated to an abelian variety over a number field, Larsen's result [10, Thm. 3.17] actually holds for a set of natural density one. (In part (c), the estimates d and t are upper bounds on the dimension and rank of the associated Mumford-Tate group.) ☐

References

[1] Jeffrey D. Achter, *Split reductions of simple abelian varieties*, Math. Res. Lett. **16** (2009), no. 2, 199–213.

[2] Grzegorz Banaszak, Wojciech Gajda, and Piotr Krasoń, *On the image of Galois l-adic representations for abelian varieties of type III*, Tohoku Math. J. (2) **62** (2010), no. 2, 163–189. MR 2663452

[3] Ching-Li Chai and Frans Oort, *A note on the existence of absolutely simple Jacobians*, J. Pure Appl. Algebra **155** (2001), no. 2-3, 115–120. MR MR1801409 (2002a:14020)

[4] Nick Chavdarov, *The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy*, Duke Math. J. **87** (1997), no. 1, 151–180. MR 99d:11071

[5] Gerd Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366. MR MR718935 (85g:11026a)

[6] Patrick X. Gallagher, *The number of conjugacy classes in a finite group*, Math. Z. **118** (1970), 175–179. MR MR0276318 (43 #2065)

[7] Nicholas M. Katz, *Report on the irreducibility of L-functions*, Number Theory, Analysis and Geometry, Springer-Verlag, New York, 2012, pp. 321–353.

[8] E. Kowalski, *The large sieve and its applications*, Cambridge Tracts in Mathematics, vol. 175, Cambridge University Press, Cambridge, 2008. MR MR2426239 (2009f:11123)

[9] M. J. Larsen and R. Pink, *Abelian varieties, l-adic representations, and l-independence*, Math. Ann. **302** (1995), no. 3, 561–579. MR MR1339927 (97e:14057)

[10] Michael J. Larsen, *Maximality of Galois actions for compatible systems*, Duke Math. J. **80** (1995), no. 3, 601–630. MR MR1370110 (97a:11090)

[11] Martin W. Liebeck and László Pyber, *Upper bounds for the number of conjugacy classes of a finite group*, J. Algebra **198** (1997), no. 2, 538–562. MR MR1489911 (99c:20023)

[12] D. Mumford, *A note of Shimura's paper "Discontinuous groups and abelian varieties"*, Math. Ann. **181** (1969), 345–351. MR MR0248146 (40 #1400)

[13] V. K. Murty and V. M. Patankar, *Splitting of abelian varieties*, IMRN **2008** (2008), Art. ID rnn033, 27 pages.

[14] Rutger Noot, *Abelian varieties—Galois representation and properties of ordinary reduction*, Compositio Math. **97** (1995), no. 1-2, 161–171, Special issue in honour of Frans Oort. MR MR1355123 (97a:11093)

[15] ———, *On Mumford's families of abelian varieties*, J. Pure Appl. Algebra **157** (2001), no. 1, 87–106. MR MR1809220 (2002a:14023)

[16] Kenneth A. Ribet, *Galois action on division points of Abelian varieties with real multiplications*, Amer. J. Math. **98** (1976), no. 3, 751–804. MR MR0457455 (56 #15660)

[17] Jean-Pierre Serre, *Lettre à Ken Ribet 1/1/1981*, Œuvres. Collected papers. IV, Springer-Verlag, Berlin, 2000, pp. 1–16. MR MR1730973 (2001e:01037)

[18] ———, *Lettre à Ken Ribet 7/3/1986*, Œuvres. Collected papers. IV, Springer-Verlag, Berlin, 2000, pp. 56–65. MR MR1730973 (2001e:01037)

[19] ———, *Lettre à Marie-France Vignéras 10/2/1986*, Œuvres. Collected papers. IV, Springer-Verlag, Berlin, 2000, pp. 38–55. MR MR1730973 (2001e:01037)

[20] Goro Shimura, *On analytic families of polarized abelian varieties and automorphic functions*, Ann. of Math. (2) **78** (1963), 149–192. MR MR0156001 (27 #5934)

[21] A. Silverberg, *Fields of definition for homomorphisms of abelian varieties*, J. Pure Appl. Algebra **77** (1992), no. 3, 253–262. MR MR1154704 (93f:14022)

[22] A. Silverberg and Yu. G. Zarhin, *Connectedness extensions for abelian varieties*, Math. Z. **228** (1998), no. 2, 387–403. MR MR1630512 (99d:11065)

[23] John Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144. MR MR0206004 (34 #5829)

[24] Adrian Vasiu, *Some cases of the Mumford-Tate conjecture and Shimura varieties*, Indiana Univ. Math. J. **57** (2008), 1–76.
[25] David Zywina, *The large sieve and Galois representations*, (2008).

Jeffrey D. Achter
Department of Mathematics
Colorado State University
Fort Collins, CO 80523
E-mail: j.achter@colostate.edu
URL: http://www.math.colostate.edu/~achter