Advances in Mathematics of Communications
Volume 8, No. 4, 2014, 511–519
doi:10.3934/amc.2014.8.511

SPLITTING OF ABELIAN VARIETIES

V. Kumar Murty and Ying Zong

Department of Mathematics, University of Toronto
40 St. George Street, Toronto, Canada M5S 2E4

(Communicated by Marcus Greferath)

Abstract. It is possible that a simple (or absolutely simple) Abelian variety defined over a number field splits modulo every prime of good reduction. This is a new problem that arises in designing crypto systems using Abelian varieties of dimension larger than 1. We discuss what is behind this phenomenon. In particular, we discuss the question of given an absolutely simple abelian variety over a number field, whether it has simple specializations at a set of places of positive Dirichlet density? A conjectural answer to this question was given by Murty and Patankar, and we explain some recent progress towards proving the conjecture. Our result ([14], Theorem 1.1) is based on the classification of pairs (G, V) consisting of a semi-simple algebraic group G over a non-archimedean local field and an absolutely irreducible representation V of G such that G admits a maximal torus acting irreducibly on V.

1. A classical problem

Let us begin with a very simple question. Given an irreducible polynomial $f(T) \in \mathbb{Z}[T]$, and a prime p, does it necessarily remain irreducible modulo a given prime p? Obviously not. A question which is slightly less obvious is: given an irreducible polynomial $f(T) \in \mathbb{Z}[T]$, is there always a prime p such that $f(T) \pmod p$ is irreducible? The answer is still no, and a simple example is

$$f(T) \;=\; T^4 + 1.$$

Indeed, if $p \equiv 1 \pmod 4$, there is an a such that $a^2 \equiv -1 \pmod p$. With this a, we have

$$T^4 + 1 \;=\; (T^2 + a)(T^2 - a) \pmod p.$$

If $p \equiv 7 \pmod 8$, there is a b such that $b^2 \equiv 2 \pmod p$. With this b, we have

$$\begin{aligned} T^4 + 1 &= (T^2 + 1)^2 - 2T^2 \\ &= (T^2 - bT + 1)(T^2 + bT + 1) \pmod p. \end{aligned}$$

If $p \equiv 3 \pmod 8$, there is a c such that $c^2 \equiv -2 \pmod p$ and

$$T^4 + 1 \;=\; (T^2 - 1)^2 - (-2T^2) \;=\; (T^2 - cT - 1)(T^2 + cT - 1) \pmod p.$$

What is behind this? The answer comes from algebraic number theory. Let f be a normal polynomial and let E be the splitting field of f. Let $\mathcal{O}$ be the ring of integers. Dedekind's theorem tells us that for all but finitely many primes p,

2010 *Mathematics Subject Classification:* 11G10, 11G25, 14K15.
Key words and phrases: Abelian variety, endomorphism algebra, Dynkin diagram.

the factorization of $f \pmod p$ is identical to the splitting of the ideal $p\mathcal{O}$ in the Dedekind domain $\mathcal{O}$. In other words,

$$f(T) \;=\; f_1(T)^{e_1} \cdots f_r(T)^{e_r} \pmod p$$

if and only if

$$p\mathcal{O} \;=\; \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

Moreover, the norm of $\mathfrak{p}_i$ is $p^{\deg f_i}$.

To each $\mathfrak{p} = \mathfrak{p}_i$, there is an automorphism $\mathrm{Frob}_\mathfrak{p}$ in the Galois group of $E/\mathbb{Q}$. For most (that is, all but finitely many) primes $\mathfrak{p}$, this is the unique automorphism σ which satisfies

$$\sigma(x) \;\equiv\; x^p \pmod{\mathfrak{p}}.$$

This automorphism $\mathrm{Frob}_\mathfrak{p}$ is an element which is of order equal to $\deg f_i$.

In particular, if f is irreducible $\pmod p$, then $p\mathcal{O}$ stays prime in E and the order of $\mathrm{Frob}_\mathfrak{p}$ is $n \;=\; \deg f$. Thus, $\mathrm{Frob}_\mathfrak{p}$ generates $\mathrm{Gal}(E/\mathbb{Q})$ and so, this group must be cyclic. In the case of $T^4 + 1$, the splitting field is $\mathbb{Q}(\zeta_8)$ which has Galois group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, the smallest non-cyclic Abelian group. In other words, if the Galois group of $E/\mathbb{Q}$ is not cyclic, then f can never be irreducible mod p.

2. A geometric analogue

We now ask for a geometric analogue of this question. A natural place to start is in the setting of Abelian varieties. In dimension 1, Abelian varieties are elliptic curves. One can also construct higher dimensional Abelian varieties starting with curves of higher genus. Thus, if C is a smooth algebraic curve of genus g, the Jacobian variety $Jac(C)$ is an Abelian variety of dimension g which is 'spanned' by C^g.

A simple Abelian variety is one which does not have any non-trivial Abelian subvariety. If the Abelian variety A is defined over a field K and $\overline{K}$ is an algebraic closure of K, we say A is *absolutely simple* if A is simple viewed over $\overline{K}$. Any Abelian variety is isogenous to a product of simple (absolutely simple) Abelian varieties and this factorization is essentially unique.

Now we can formulate the geometric question. Given a simple or absolutely simple Abelian variety over a number field, is there always a prime v (infinitely many primes, a positive density of primes ...) for which the reduction A_v modulo v is simple or absolutely simple?

Just as in the case of polynomials, the answer is no. In fact, an absolutely simple Abelian surface A defined over a number field K with an endomorphism algebra equal to an indefinite quaternion division algebra, has the property that it has everywhere good reduction, and at any prime v of K, the reduction A_v of A has the property that it is isogenous to the square of an elliptic curve E_v^2. On the other hand, there are many examples of simple Abelian varieties whose reduction stays simple at a set of primes of positive density. This naturally raises the question of how to explain these phenomenon. For example, as in the case of polynomials, is there a Galois-theoretic explanation?

This question was discussed in Murty and Patankar [13]. More precisely the question asked there was as follows.

Question. *Let A_K be an absolutely simple abelian variety over a number field K. Does there exist a finite extension L of K such that the base change of A_K to every*

finite extension of L has simple specializations at a set of places of positive Dirichlet density?

There it was conjectured that if the ground field was sufficiently large, then there exists a positive density of such primes if and only if the endomorphism algebra of A is commutative.

3. Cryptographic motivation

The one dimensional case of Abelian varieties over finite fields, namely elliptic curves, have proved extremely useful in the design of public-key cryptosystems. To use Abelian varieties over finite fields of higher dimension as the basis of a discrete-log based cryptosystem, the usual problems of point counting and efficient arithmetic have to be solved. This has been extensively studied for Abelian varieties that are Jacobians of hyperelliptic curves and there is also work on the Jacobians of other families of curves. However, the case of a general Abelian variety is still in an early stage.

One way to study good candidates for cryptographically useful Abelian varieties is to begin with one over $\mathbb{Q}$ or over a number field and reduce mod p (or v). In doing this, we encounter the problem that a simple Abelian variety over a number field may split mod v for *every* prime v. This problem, which doesn't arise in the elliptic curve case, is the main topic of discussion in this article. But besides this, there are also significant problems in developing efficient arithmetic. It poses new challenges because we have to develop a more abstract approach which is less dependent on equations. In the case of elliptic curves, a lot of research has been done in improving the efficiency of arithmetic but it begins with an explicit model for the curve given in terms of equations. In the higher dimensional case, one may need to invoke more general methods as the equations tend to involve a large number of variables. In joint work in progress, Kumar Murty and Pramath Sastry are developing such an approach.

It should be pointed out that even in the case of elliptic curves, there are important open problems. In particular, given an elliptic curve E over the rationals, we expect that if there is a prime p such that $E(\mathbb{F}_p)$ is cyclic, then there are infinitely many such primes. Some results of this genre are known through the many papers of Ram Murty on this subject (see, for example, [16]). For example, let us assume a *quasi*-Riemann Hypothesis. This means that there is an $\epsilon > 0$ so that Dedekind zeta functions do not have zeros in the half-plane $Re(s) > 1 - \epsilon$. Then, in [16], it is shown that for any elliptic curve E defined over $\mathbb{Q}$ which does not have complex multiplication and which has an irrational 2-division point, we have $E(\mathbb{F}_p)$ is cyclic for a positive density of primes p. He had earlier proved this unconditionally (see [15]) for elliptic curves with complex multiplication. An interesting aspect of this work is that the existence of such a prime can be formulated in terms of a global condition.

We also expect that the order $E(\mathbb{F}_p)$ should be (nearly) a prime for infinitely many primes, but this is not yet known in general. In fact, Koblitz [10] has conjectured that the number of such primes $\leq x$ should be

$$\sim c_E \frac{x}{(\log x)^2}$$

for some constant $c_E \geq 0$. We say "nearly" a prime because if $E(\mathbb{Q})$ has non-trivial torsion, then the order of the torsion subgroup will divide $|E(\mathbb{F}_p)|$ for all primes of

good reduction. In fact, we have to consider the torsion not just in $E(\mathbb{Q})$ but in the rational points of curves that are $\mathbb{Q}$-isogenous to E. Indeed, if we set

$$T \;=\; \text{lcm}\; |E'(\mathbb{Q})|$$

where the lcm ranges over elliptic curves E' defined over $\mathbb{Q}$ and $\mathbb{Q}$-isogenous to E, then Katz [9] showed that

$$\gcd\; |E(\mathbb{F}_p)| \;=\; T$$

where the gcd is taken over all primes p of good reduction for E. This was made effective in [12] in the following sense. If ℓ is a prime that does not divide T, then assuming the GRH, there is a prime p satisfying

$$p \;\ll\; (\ell \log N\ell)^2$$

so that ℓ does not divide $|E(\mathbb{F}_p)|$. Here N is the conductor of E.

The best that we know is (assuming GRH) the existence of infinitely many p for which $|E(\mathbb{F}_p)|$ has a bounded number of factors. The first such result was in the work of Ali Miri and Kumar Murty [11] in which it was shown that the bound could be taken to be 16. This was refined by several authors and the best result at present is due to David and Wu [5] where the bound of 8 is established. If we assume that the elliptic curve E has complex multiplication, then it is possible to obtain unconditional results. For example, Cojocaru [4] showed unconditionally that if $T = 1$, then there are infinitely many primes p for which $|E(\mathbb{F}_p)|$ has at most 5 prime factors (counting multiplicities). This has been improved by Urroz [19] who showed (building on earlier work with Iwaniec) that 5 can be replaced by 2.

4. A more precise formulation

Returning to the main problem being considered here, we give in this section, a more precise formulation. Let us recall some notions before we formulate the question in more precise terms and impose a natural hypothesis on the Abelian varieties that can be handled by our approach.

Let K be a number field and A_K an Abelian variety defined over K. Let $t = \text{Spec}(K)$, $\bar{t}$ a geometric point of t, S an open subset of the spectra of the ring of integers of K such that $A_t = A_K$ extends to an abelian scheme A over S.

We call an arbitrary S-fiber of A a specialization of A_t. A specialization $A_s = A \times_S s$, $s \in S$, is simple, if it is a simple object in the category of s-Abelian varieties up to isogenies, that is, if A_s is a simple Abelian variety over the residue field $k(s)$ of s. This is equivalent to the condition that $\text{End}_s(A_s) \otimes_{\mathbf{Z}} \mathbf{Q}$ is a $\mathbf{Q}$-division algebra. A specialization A_s is absolutely simple, if $A_s \times_s \overline{s}$ is simple, for $\overline{s}$ a geometric point of s (equivalently, A_s is simple over the algebraic closure $\overline{k(s)}$ of the residue field at s.)

A subset Ξ of $S\backslash\{t\}$ has Dirichlet density d, $0 \leq d \leq 1$, if

$$\text{Card}(\{s \in \Xi, \text{Card}(k(s)) \leq x\}) = \; (d + o(1))\frac{x}{\log\, x}$$

as $x \to \infty$. As a fundamental example, the set

$$\{s \in S\backslash\{t\}, k(s) \text{ is a prime field}\}$$

has Dirichlet density 1.

What we asked above is whether there exists some finite extension L of K such that for each finite extension K' of L, if S' denotes a sufficiently small non-empty

open sub-scheme of the spectra of the ring of integers of K', the set

$$\{s' \in S'\backslash\{t'\}, A \times_S s' \text{ is simple}\},$$

or what amounts to the same, the subset

$$\{s' \in S'\backslash\{t'\}, k(s') \text{ is a prime field}, A \times_S s' \text{ is simple}\}$$

has positive Dirichlet density.

5. A necessary condition

A fundamental theorem of Tate gives us a lot of information about the endomorphism algebra of an Abelian variety over a finite field. In particular, it allows us to deduce that if $\mathrm{End}_t(A_t)$ is not commutative, $A_s = A \times_S s$ is not simple at any of the points of S with values in a finite prime field. Indeed, for a simple Abelian variety A_s over $k(s)$, Tate's theorem gives the invariants of the division algebra

$$\mathrm{End}_s(A_s) \otimes_{\mathbf{Z}} \mathbf{Q}.$$

In particular, in the case that $k(s)$ is the prime field $\mathbb{F}_p$ (where p is the characteristic of $k(s)$), Tate's theorem ([17], p. 98, line 1) implies that this division algebra is in fact a (commutative) field. On the other hand, the specialization homomorphism

$$sp : \mathrm{End}_t(A_t) \xleftarrow{\sim} \mathrm{End}_S(A) \hookrightarrow \mathrm{End}_s(A_s)$$

is injective, forcing $\mathrm{End}_t(A_t)$ to be commutative as well.

Therefore, in order that the question does not have a trivial negative answer, one should and does impose that $\mathrm{End}_{\overline{t}}(A_{\overline{t}}) \otimes_{\mathbf{Z}} \mathbf{Q}$ be a field.

6. ℓ-adic methods

Now, given a prime number ℓ invertible on S, consider an ℓ-adic approach to the question.

Choose for each closed point $s \in S$ a geometric point $\overline{s}$ localized at s, and a "path" ch_s connecting $\overline{s}$ to $\overline{t}$ (SGA 1, Éxposé V, 7, [8]). Let $F_s \in \pi_1(s, \overline{s})$ be the geometric Frobenius, and F_s^* the image of F_s under the composition

$$\pi_1(s, \overline{s}) \to \pi_1(S, \overline{s}) \xrightarrow{ch_s} \pi_1(S, \overline{t}) \xrightarrow{\rho_{\ell,\overline{t}}} \mathrm{GL}(H^1(A_{\overline{t}}, \mathbf{Q}_\ell)),$$

where $\rho_{\ell,\overline{t}}$ is the ℓ-adic monodromy representation associated to the abelian scheme A. Write $M_\ell = \mathrm{Im}(\rho_{\ell,\overline{t}})$ for the monodromy, and M_ℓ^{Zar} its Zariski closure in $\mathrm{GL}(H^1(A_{\overline{t}}, \mathbf{Q}_\ell))$.

For the purpose of our question, enlarging K to a finite extension if necessary, we suppose $\mathrm{End}_t(A_t) = \mathrm{End}_{\overline{t}}(A_{\overline{t}})$ and that M_ℓ^{Zar} is connected.

Tate's theorem applied to a closed fibre A_s asserts that

$$\mathrm{End}_s(A_s) \otimes_{\mathbf{Z}} \mathbf{Q}_\ell \xrightarrow{\sim} \mathrm{End}_{F_s^*}(H^1(A_{\overline{t}}, \mathbf{Q}_\ell))^{\mathrm{opposite}}.$$

In particular, it shows that A_s is simple if F_s^* acts irreducibly on $H^1(A_{\overline{t}}, \mathbf{Q}_\ell)$. The subset X_ℓ of the compact ℓ-adic Lie group M_ℓ consisting of those elements acting irreducibly on $H^1(A_{\overline{t}}, \mathbf{Q}_\ell)$ is a union of conjugacy classes, and by Krasner's lemma, open in M_ℓ. By the Chebotarev density theorem, the volume of X_ℓ in the normalized Haar measure of M_ℓ equals the Dirichlet density of the set

$$\{s \in S\backslash\{t\}, F_s^* \in X_\ell\},$$

which is less than or equal to the density of

$$\{s \in S\backslash\{t\}, A_s \text{ is simple}\}.$$

Thus, our question will have a positive answer, if X_ℓ is non-empty over every finite extension of K.

Each element of X_ℓ lies in a maximal torus of M_ℓ^{Zar} acting irreducibly on $H^1(A_{\overline{t}}, \mathbf{Q}_\ell)$. Conversely, each torus of M_ℓ^{Zar} irreducible on $H^1(A_{\overline{t}}, \mathbf{Q}_\ell)$ contains an open dense subset whose every $\mathbf{Q}_\ell$-point acts irreducibly on $H^1(A_{\overline{t}}, \mathbf{Q}_\ell)$. Since M_ℓ is open in $M_\ell^{\mathrm{Zar}}(\mathbf{Q}_\ell)$ (Bogomolov [1]), the condition that X_ℓ be non-empty is equivalent to the condition that some maximal torus of M_ℓ^{Zar} act irreducibly on $H^1(A_{\overline{t}}, \mathbf{Q}_\ell)$.

However, if $\mathrm{End}_t(A_t) \otimes_{\mathbf{Z}} \mathbf{Q}_\ell$ is not a field, one has even that the entire M_ℓ^{Zar} acts reducibly on $H^1(A_{\overline{t}}, \mathbf{Q}_\ell)$, for by Faltings [7],

$$\mathrm{End}_t(A_t) \otimes_{\mathbf{Z}} \mathbf{Q}_\ell \xrightarrow{\sim} \mathrm{End}_{M_\ell^{\mathrm{Zar}}}(H^1(A_{\overline{t}}, \mathbf{Q}_\ell))^{\mathrm{opposite}}.$$

If, for instance, $E := \mathrm{End}_t(A_t) \otimes_{\mathbf{Z}} \mathbf{Q}$ contains an abelian field of group $(\mathbf{Z}/p\mathbf{Z})^4$, p prime, or a non-solvable sub-Galois extension of $\mathbf{Q}$, no completion $E \otimes_{\mathbf{Q}} \mathbf{Q}_\ell$ is a field.

We need to assume that

$$\mathrm{End}_t(A_t) \otimes_{\mathbf{Z}} \mathbf{Q}_\ell = E_\ell$$

is a field for some prime number ℓ, that is, ℓ is either totally ramified or inert in E. Without this assumption, X_ℓ will always be empty and we have little to say.

Besides cyclic fields, many more examples of E satisfying the above assumption can be obtained as follows. For any fixed prime ℓ, for any given finite extension E_ℓ of $\mathbf{Q}_\ell$, by Hilbert's irreducibility theorem, a large number of totally real number fields E have E_ℓ as their ℓ-adic completions, i.e. $E \otimes_{\mathbf{Q}} \mathbf{Q}_\ell = E_\ell$. Every such E is realizable as the endomorphism algebra of an absolutely simple abelian variety A_K, which furnishes a desired example.

From the view point of genericity, most abelian varieties of dimension g have GSp_{2g} as their monodromy and $\mathbf{Z}$ as their endomorphism rings. In this sense, the condition that $E \otimes_{\mathbf{Q}} \mathbf{Q}_\ell$ is a field for some prime ℓ is restrictive on E, but not so much on the abelian variety itself.

From now on, assume that $E_\ell = E \otimes_{\mathbf{Q}} \mathbf{Q}_\ell$ is a field for a particular prime ℓ.

Then, $H^1(A_{\overline{t}}, \mathbf{Q}_\ell)$, as an E_ℓ-linear representation of M_ℓ^{Zar} or its derived group, is absolutely irreducible.

7. The representation theory question

One is led to the following basic question.

Question. *Let G be a semi-simple algebraic group over a finite extension E of $\mathbf{Q}_\ell$, and*

$$\rho_V : G \to \mathrm{GL}(V)$$

an absolutely irreducible E-linear representation with finite kernel. Does some maximal torus of G act irreducibly on V?

The question of the previous section corresponds to the special case $G = [M_\ell^{\mathrm{Zar}}, M_\ell^{\mathrm{Zar}}]$, and $V = H^1(A_{\overline{t}}, \mathbf{Q}_\ell)$.

One may further suppose G simply connected. A maximal torus $\mathfrak{T}$ acts irreducibly on V if and only if the weights of $\overline{V} = V \otimes \overline{E}$ relative to $\overline{\mathfrak{T}} = \mathfrak{T} \otimes \overline{E}$ are permuted transitively by $\mathrm{Gal}(\overline{E}/E)$. So if such a torus exists, all the weights have the same length, that is, by definition, $\overline{V}$ is minuscule ([2], Ch. 8, prop. 6, p.127).

Let $\overline{D}$ be the Dynkin diagram ([2], Ch. 6, p. 197) of $G_{\overline{E}}$, and set

$$\rho_D : \mathrm{Gal}(\overline{E}/E) \to \mathrm{Aut}(\overline{D})$$

the natural Galois action on $\overline{D}$ ([18], 2.3), and let α_i, $i = 1, \cdots, r$, be the Galois orbits in $\overline{D}$ consisting of minuscule vertices corresponding to a minuscule representation $V = V_1 \otimes \cdots \otimes V_r$ of $G = G_1 \times \cdots \times G_r$, G_i being the simple factors. Put $D = (\overline{D}, \rho_D)$, and $\alpha_V = \sum \alpha_i$.

Whether or not G has a maximal torus acting irreducibly on V depends in fact only on (D, α_V) ([14], Theorem 2.3, Lemma 3.1) ; if G admits such a torus, we call (D, α_V) an elliptic minuscule pair.

For example, in the case of type C_n, $n \geq 1$, with its unique minuscule vertex α_1, the pair (C_n, α_1) is elliptic if and only if there exists a Galois representation

$$\rho : \mathrm{Gal}(\overline{E}/E) \to \mathrm{GL}_n(\mathbf{Z})$$

whose image $\mathfrak{G}$ lies in the group generated by the diagonal matrices and monomial matrices, and such that $\mathfrak{G}$ acts transitively on

$$\{e_1, \cdots, e_n, -e_1, \cdots, -e_n\},$$

where $e_1, \cdots, e_n$ denote the standard basis of $\mathbf{Z}^n$ (cf. [14], Lemma 3.1, 3).

Building on this criterion, here is how one proves that (C_n, α_1) is indeed elliptic (cf. [14], prop. 8.1) : The subgroup $\mathfrak{G} = \langle \tau\zeta \rangle$ of $\mathrm{GL}_n(\mathbf{Z})$, where $\zeta : e_1 \mapsto e_2, \cdots, e_n \mapsto e_1$, and $\tau : e_1 \mapsto -e_1$, $e_i \mapsto e_i$, $\forall\ i > 1$, acts simply transitively on $\{e_1, \cdots, e_n, -e_1, \cdots, -e_n\}$. Now, $\mathbf{Z}/2n\mathbf{Z} = \mathfrak{G}$ is the Galois group of an unramified extension of E of degree $2n$, in particular, is a quotient of $\mathrm{Gal}(\overline{E}/E)$. So (C_n, α_1) is elliptic.

The detailed enumeration of all elliptic minuscule pairs with connected Dynkin diagrams is documented in [14], Theorem 3.2.

Recall that we have explained as above that $A_K = A_t$ will have simple specializations at a set of places of positive density, provided that X_ℓ is non-empty over every finite extension of K, which in turn is equivalent to the existence of maximal tori in M_ℓ^{Zar} acting irreducibly on $H^1(A_{\overline{t}}, \mathbf{Q}_\ell)$, and with our hypothesis that E_ℓ is a field, is further equivalent to the condition that the monodromy representation is minuscule and that the pair (D, α_V) is an elliptic minuscule pair.

Our partial answer with "simple specializations" improved to "absolutely simple specializations" is given below.

Theorem 1. *Let ℓ be a prime number. Suppose* $\mathrm{End}_t(A_t) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell = \mathrm{End}_{\overline{t}}(A_{\overline{t}}) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell = E_\ell$ *is a field, M_ℓ^{Zar} connected and that the monodromy representation $H^1(A_{\overline{t}}, \mathbb{Q}_\ell)$ is minuscule whose associated minuscule pair over* $\mathrm{Spec}(E_\ell)$ *is elliptic. Then A_t specializes to absolutely simple abelian varieties at a set of places of positive Dirichlet density.*

In particular, if $\mathrm{End}(A) = \mathbb{Z}$ and the monodromy representation is the standard representation of the group of symplectic similitudes, then A has absolutely simple specializations at a set of places of positive density. We thus recover a result of Chai and Oort [3].

In the above theorem, the reason why A_t has absolutely simple rather than just simple specializations at a set of places of positive density results from the assertions i) and ii) below :

i) A specialization A_s is absolutely simple if it is simple and if $\mathrm{End}_{\overline{s}}(A_s \times_s \overline{s})$ is commutative.

ii) Whenever M_ℓ^{Zar} is connected and the monodromy representation $H^1(A_{\overline{t}}, \mathbf{Q}_\ell)$ has no multiple weights, the set

$$\{s \in S\backslash\{t\}, \mathrm{End}_{\overline{s}}(A_s \times_s \overline{s}) \text{ is commutative}\}$$

has density 1.

The proof of i) and ii) is elementary and can be found in [14], 2.9.

Note that the truth of the Mumford-Tate conjecture will imply that the monodromy representation is minuscule ([6], 1.3.9), and in particular, is multiplicity free. Conversely, if A_t turns out to have simple specializations at a set of places of positive density, we can show that the tensor components of the monodromy representation are almost always minuscule, without assuming the Mumford-Tate conjecture nor that E admits totally ramified or inert rational primes ([14], 2.10). The exceptions are among $(A_n, r\omega_i)$, $i = 1, n$, $n \geq 1$, $r > 1$, (B_n, ω_1), $n > 1$, (C_3, ω_3), (G_2, ω_1).

Acknowledgements

We would like to thank the referees for comments that helped us to improve the exposition.

References

[1] F. Bogomolov, Sur l'algébricité des représentations ℓ-adiques, *Comptes Rendus Acad. Sci. Paris*, **290** (1980), 701–703.
[2] N. Bourbaki, *Groupes et Algèbres de Lie*, Hermann, Paris, 1975.
[3] C.-L. Chai and F. Oort, A note on the existence of absolutely simple Jacobians, *J. Pure Appl. Algebra*, **155** (2001), 115–120.
[4] A. Cojocaru, Reductions of an elliptic curve with almost prime orders, *Acta Arith.*, **119** (2005), 265–289.
[5] C. David and J. Wu, Almost prime values of the order of elliptic curves over finite fields, *Forum Math.*, **24** (2012), 99–119.
[6] P. Deligne, Variétés de Shimura: Interprétation modulaire, et techniques de construction de modèles canoniques, in *Proc. Symp. Pure Math.* (eds. A. Borel and W. Casselman), AMS, Providence, 1979, 247–289.
[7] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.*, **73**(1983), 349–366.
[8] A. Grothendieck, *Revêtements étales et Groupe Fondamental*, Springer, Berlin, 1971.
[9] N. Katz, Galois properties of torsion points of abelian varieties, *Invent. Math.*, **62** (1981), 481–502.
[10] N. Koblitz, Primality of the number of points on an elliptic curve over a finite field, *Pacific J. Math.*, **131** (1988),157–165.
[11] S. A. Miri and V. Kumar Murty, An application of sieve methods to elliptic curves, in *INDOCRYPT 2001*, Springer, Berlin, 2001, 91–98.
[12] V. Kumar Murty, The least prime which does not split completely, *Forum Math.*, **6** (1994), 555–565.
[13] V. Kumar Murty and V. Patankar, Splitting of abelian varieties, *Intl. Math. Res. Notices*, **12** (2008), Article ID rnn 033, 27 pp.
[14] V. Kumar Murty and Y. Zong, Splitting of abelian varieties, elliptic minuscule pairs, preprint, arXiv:1211.4286
[15] M. Ram Murty, On Artin's conjecture, *J. Number Theory*, **16** (1983), 147–168.
[16] M. Ram Murty, Artin's conjecture and elliptic analogues, in *Sieve methods, exponential sums, and their applications in number theory* (eds. G.R.H. Greaves, G. Harman and M.N. Huxley), Cambridge Univ. Press, Cambridge, 1996, 325–344.

[17] J. Tate, Classes d'isogénie de variétés abéliennes sur un corps fini (d'après T.Honda), in *Séminaire Bourbaki*, Springer, Heidelberg, 1971, 95–110.
[18] J. Tits, Classification of algebraic semisimple groups, in *Proc. Sympos. Pure Math.* (eds. A. Borel and G. Mostow), AMS, Providence, 1966, 33–62.
[19] J.-J. Urroz, Almost prime order of CM elliptic cures modulo p, in *Algorithmic Number Theory*, Springer, Berlin, 2008, 74–87.

Received February 2014; revised September 2014.

E-mail address: murty@math.toronto.edu
E-mail address: zongying@math.toronto.edu