WEIL NUMBERS GENERATED BY OTHER WEIL NUMBERS AND TORSION FIELDS OF ABELIAN VARIETIES

E. KOWALSKI

Abstract. Using properties of the Frobenius eigenvalues, we show that, in a precise sense, "most" isomorphism classes of (principally polarized) simple abelian varieties over a finite field are characterized, up to isogeny, by the sequence of their division fields, and a similar result for "most" isogeny classes. Some global cases are also treated.

1. Introduction

Let A/k be an abelian variety defined over a field k. The extensions $k(A[n])$ of k generated by n-torsion points of A, $n \geqslant 1$, are often of great arithmetic interest. In [K1], for k a number field or a finite field, we investigated the extent to which those fields may characterize A. Precisely, we say that two abelian varieties A/k and B/k are isokummerian if there exists an integer N (depending maybe on A and B) such that $k(A[n]) = k(B[n])$ for all n coprime with N. The simplest examples arise when A and B have the same k-simple factors up to isogeny.

If now q is a power of a prime number p, $k = \mathbf{F}_q$ a field with q elements, recall that Weil showed that all eigenvalues π of the Frobenius endomorphism π_A of A are q-Weil numbers, i.e., algebraic integers such that for every automorphism σ of $\mathbf{C}$ we have $|\sigma(\pi)| = \sqrt{q}$. In [K1, Th. 3.4], we showed that $A/\mathbf{F}_q$ and $B/\mathbf{F}_q$ are isokummerian if and only if $\Phi_A = \Phi_B$, where Φ_A is the multiplicative subgroup of $\mathbf{C}^\times$ generated by those eigenvalues.

Denote now w_A the set of q-Weil numbers in Φ_A. If A is simple and w_A is equal to the set of eigenvalues of π_A, it follows that any $B/\mathbf{F}_q$ which is isokummerian to A is in fact isogenous to a power of A.

Some precise results in this direction (e.g., for product of elliptic curves) are given in [K1], and also an example due to Serre of two abelian varieties A and B over a finite field, simple and non-isogenous over $\bar{\mathbf{F}}_q$, such that $\Phi_A = \Phi_B$.

In this paper, we will provide a convenient abstract criterion, applicable to any q-Weil number π, that implies that the set w_π of q-Weil numbers in the subgroup $\Phi_\pi \subset \mathbf{C}^\times$ generated by Galois conjugates of π contains only those conjugates. Applying this criterion, we will show that for "most" abelian varieties over finite fields, w_A is indeed the set of eigenvalues of π_A. What "most" means has to be made precise, of course, and there are actually at least two natural ways of doing this, taking A up to isomorphism or up to isogeny. We will consider both possibilities.

In the isomorphism case, we use rather deep results of Mumford and Chavdarov on what "most" isomorphism classes of abelian varieties over $\mathbf{F}_q$ look like; it is quite appealing that we use here both p-adic methods having to do with ordinariness and ℓ-adic methods related to monodromy of ℓ-adic sheaves. Those also allow us to derive some results for abelian varieties over number fields, although they are conditional on ordinarity

2000 *Mathematics Subject Classification.* Primary 11G10, 11G20, 11G25; Secondary 11N36.

Key words and phrases. Abelian varieties over finite fields, division fields, Weil numbers, ordinary abelian varieties, characteristic polynomial of Frobenius, isogeny classes, large sieve.

assumptions. In the isogeny case, the method is more elementary, based on lattice-point counting, using results of Howe and DiPippo, and the multidimensional large sieve inequality.

We now state precisely our main result. Let $g \geqslant 1$ be an integer, q a power of a prime p. We introduce the following:

- $A_g(q)$ is the set of isomorphism classes of principally polarized[1] abelian varieties of dimension g defined over $\mathbf{F}_q$;
- $I_g(q) \subset A_g(q)$ is the subset of those varieties A such that any B isokummerian with A is isogenous to a power of A;
- $\mathcal{A}_g(q)$ is the set of isogeny classes of abelian varieties of dimension g defined over $\mathbf{F}_q$;
- $\mathcal{I}_g(q) \subset \mathcal{A}_g(q)$ is the subset of those isogeny classes $\mathcal{C}$ such that any variety B isokummerian to a variety $A \in \mathcal{C}$ is (isogenous to) a power of A.

Theorem 1.1. *Let $g \geqslant 1$ and q a power of a prime p. We have*

$$\lim_{n \to +\infty} \frac{|I_g(q^n)|}{|A_g(q^n)|} = 1 \tag{1.1}$$

and

$$\lim_{q \to +\infty} \frac{|\mathcal{I}_g(q)|}{|\mathcal{A}_g(q)|} = 1. \tag{1.2}$$

The case of isogeny classes is thus somewhat more precise, since it holds for instance for the base fields $\mathbf{F}_p$ with $p \to +\infty$.

Acknowledgments. The results of Chavdarov [C] which are crucial for this paper were mentioned by N. Katz during a lecture; shortly afterward a question by U. Zannier made me realize that those results could be quite useful to study Φ_A and w_A and improve on [K1]. I thank them both for these lucky coincidences... Also I thank the referee for a careful reading and for a number of suggestions and references, in particular for providing examples of ordinary isokummerian varieties (see Remark 2.5).

2. Determination of w_π in a special case

In this section we consider only q-Weil numbers, and give a criterion for w_π to be reduced to the conjugates of π. For simplicity we assume that π does not have real conjugates, hence π is of even degree $2g$. Let $K_\pi \subset \bar{\mathbf{Q}}$ be the Galois closure of $\mathbf{Q}(\pi)$. For every conjugate π_i of π, q/π_i is also a conjugate of π; if we fix an embedding $\bar{\mathbf{Q}} \subset \mathbf{C}$, we have $q/\pi_i = \bar{\pi}_i$, the complex conjugate of π_i.

Proposition 2.1. *Let p be prime, q a power of p. Let π be a q-Weil number such that $[\mathbf{Q}(\pi) : \mathbf{Q}] = 2g$. Let G denote the Galois group of the Galois closure K_π of $\mathbf{Q}(\pi)$. Let $(\pi_i, \bar{\pi}_i)$, $1 \leqslant i \leqslant g$, be the Galois conjugates of π in K_π, in complex conjugate pairs. Assume that:*

(1) For all i, $1 \leqslant i \leqslant g$, π_i and $\bar{\pi}_i$ are coprime in the ring of integers of K_π.

(2) For all i, $1 \leqslant i \leqslant g$, there exists $\sigma_i \in G$ such that $\sigma_i(\pi_i) = \pi_i$ and $\sigma_i(\pi_j) = \bar{\pi}_j$ for $j \neq i$.

Then w_π is the set of conjugates of π.

[1] We could consider more general polarizations also, but we need such an additional structure so that moduli spaces make sense.

Proof. Let $c \in G$ be the restriction of complex conjugation, so that $c(\pi_i) = \bar{\pi}_i$ and $c(\bar{\pi}_i) = \pi_i$ for every i. Thus setting

$$\sigma_{i,j} = c\sigma_i\sigma_j \in G$$

we have for $i \neq j$ the relations

$$\sigma_{i,j}(\pi_i) = \pi_i, \quad \sigma_{i,j}(\pi_j) = \pi_j, \quad \sigma_{i,j}(\pi_k) = \bar{\pi}_k \text{ for } k \notin \{i, j\}. \tag{2.1}$$

Fix a prime ideal $\mathfrak{p}$ in K_π dividing (p). Since $\mathfrak{p} \mid p \mid q = \pi_i\bar{\pi}_i$ and π_i, $\bar{\pi}_i$ are coprime by assumption, we see that $\mathfrak{p}$ divides one and only one of π_i and $\bar{\pi}_i$. We renumber/pair the conjugates so that $\mathfrak{p} \mid \pi_i$, and $\mathfrak{p} \nmid \bar{\pi}_i$ for $1 \leqslant i \leqslant g$. Notice this doesn't affect the existence of σ_i, $\sigma_{i,j}$ with properties as stated for the new numbering.

Let $\nu = v_\mathfrak{p}(q) \geqslant 1$ where $v_\mathfrak{p}$ is the valuation on K_π associated to $\mathfrak{p}$. Notice that by coprimality again we have

$$\nu = v_\mathfrak{p}(q) = v_{\bar{\mathfrak{p}}}(q) = v_\mathfrak{p}(\pi_i\bar{\pi}_i) = v_\mathfrak{p}(\pi_i) = v_{\bar{\mathfrak{p}}}(\bar{\pi}_i). \tag{2.2}$$

Let now $\alpha \in \Phi_\pi$ be a q-Weil number. We can write

$$\alpha = q^m \prod_{1 \leqslant i \leqslant g} \pi_i^{n_i},$$

with m, $n_i \in \mathbf{Z}$. We deduce from $\alpha\bar{\alpha} = q$ that

$$2m + n_1 + \cdots + n_g = 1, \tag{2.3}$$

and from this we notice in particular that the sum $n_1 + \cdots + n_g$ can not be zero, in particular not all the n_i can be zero.

We have $v_\mathfrak{p}(\alpha) \geqslant 0$, $v_{\bar{\mathfrak{p}}}(\alpha) \geqslant 0$, which translate to

$$\nu(m + n_1 + \cdots + n_g) \geqslant 0, \quad \nu m \geqslant 0.$$

Dividing by $\nu \geqslant 1$, summing and comparing with (2.3), we see that one of m and $m + n_1 + \cdots + n_g$ is equal to 0 and the other is equal to 1.

Now we consider $\alpha\alpha^{\sigma_i}$. This is an algebraic integer and therefore $v_\mathfrak{p}(\alpha\alpha^{\sigma_i}) \geqslant 0$, $v_{\bar{\mathfrak{p}}}(\alpha\alpha^{\sigma_i}) \geqslant 0$. We have

$$\alpha\alpha^{\sigma_i} = q^{2m+n_1+\cdots+\cdots+n_g-n_i}\pi_i^{2n_i} = q^{1-n_i}\pi_i^{2n_i},$$

so using (2.2) these two conditions translate to

$$v_\mathfrak{p}(\alpha\alpha^{\sigma_i}) = \nu(1 + n_i) \geqslant 0$$
$$v_{\bar{\mathfrak{p}}}(\alpha\alpha^{\sigma_i}) = \nu(1 - n_i) \geqslant 0,$$

which means that $n_i \in \{0, -1, 1\}$ for all i.

Now consider $\alpha\alpha^{\sigma_{i,j}}$ with $i \neq j$. We have

$$\alpha\alpha^{\sigma_{i,j}} = q^{1-n_i-n_j}\pi_i^{2n_i}\pi_j^{2n_j},$$

by (2.1), hence the integrality conditions $v_\mathfrak{p}(\alpha\alpha^{\sigma_{i,j}}) \geqslant 0$, $v_{\bar{\mathfrak{p}}}(\alpha\alpha^{\sigma_{i,j}}) \geqslant 0$ mean

$$v_\mathfrak{p}(\alpha\alpha^{\sigma_{i,j}}) = \nu(1 + n_i + n_j) \geqslant 0$$
$$v_{\bar{\mathfrak{p}}}(\alpha\alpha^{\sigma_{i,j}}) = \nu(1 - n_i - n_j) \geqslant 0.$$

The first of these shows that at most one n_i can be equal to -1; the second that at most one n_j can be equal to 1. Both of these can not occur because that would give $n_1 + \cdots + n_g = n_i + n_j = 1 - 1 = 0$, which is impossible. So either there exists exactly one i with $n_i = 1$, and the other n_j are 0, which gives $\alpha = \pi_i$ (because one must have $m = 0$, $m + n_1 + \cdots + n_g = 1$); or there exists exactly one j with $n_j = -1$ (and the other n_i are 0), which gives $\alpha = \bar{\pi}_j$ (because then $m = 1$, $m + n_1 + \cdots + n_g = 0$). □

Remark 2.2. (1) This is not the strongest result one can get along these lines, but it will be sufficient for our purposes (for instance, if $g > 2$, the referee pointed out that Condition (2) can be replaced by (2.1)).

(2) Since we actually solved the equations in terms of the parameters (m, n_i) uniquely (for a given α), we have also proved that (q, π_i), $1 \leqslant i \leqslant g$, form a free generating set of Φ_π under the assumptions of the proposition. In particular, the rank of Φ_π is then equal to $g + 1$.

Remark 2.3. Proposition 2.1 also applies to prove that if $A = E_1 \times \cdots \times E_k$ is a product of pairwise geometrically non-isogenous elliptic curves over a finite field $\mathbf{F}_q$ with q elements, the only q-Weil numbers in Φ_A are the conjugates of the Frobenius elements for the E_i (see [K1, Th. 3.4, (5)]). It also gives back in this case the lemma of Spiess used to prove this statement in [K1].

To apply Proposition 2.1 to a simple abelian variety $A/\mathbf{F}_q$ with Frobenius π_A, we need criteria for the two conditions involved. Here we start by Condition (1), which has to do with the "behavior at p" (since all primes dividing π are above p in K_π) of the Frobenius of A.

Recall that an abelian variety A/k of dimension g over a field k of characteristic p is called ordinary if $|A[p](\bar{k})| = p^g$, which is the maximal number of p-torsion points there can be in characteristic p. If $k = \mathbf{F}_q$ is a finite field with q elements, then A is ordinary if and only if the middle coefficient of the characteristic polynomial of Frobenius is coprime with q (see e.g. [DH]). The following lemma is certainly well-known; the proof here was given by the referee and is somewhat simpler than the original.

Lemma 2.4. *Let q be a power of a prime p, let $A/\mathbf{F}_q$ be a simple ordinary abelian variety of dimension $g \geqslant 1$. Then for any eigenvalue π of the Frobenius of A, we have $(\pi, q/\pi) = 1$ in the ring $\mathbf{Z}[\pi, q/\pi]$.*

Proof. The characteristic polynomial of Frobenius for A is of the form

$$X^{2g} + a_1 X^{2g-1} + \cdots + a_g X^g + \cdots + a_1 q^{g-1} X + q^g$$

so we have

$$\pi^{2g} + a_1 \pi^{2g-1} + \cdots + a_g \pi^g + \cdots + a_1 q^{g-1} \pi + q^g = 0.$$

Dividing by π^g, we find that

$$\left(\pi^g + \left(\frac{q}{\pi}\right)^g\right) + a_1\left(\pi^{g-1} + \left(\frac{q}{\pi}\right)^{g-1}\right) + \cdots + a_{g-1}\left(\pi + \frac{q}{\pi}\right) + a_g = 0,$$

so the ideal $(\pi, q/\pi) \subset \mathbf{Z}[\pi, q/\pi]$ contains a_g. Since it also contains q and $(a_g, q) = 1$ because A is ordinary, it follows that $(\pi, q/\pi) = \mathbf{Z}[\pi, q/\pi]$.

□

This implies that any ordinary abelian variety satisfies Condition (1) of Proposition 2.1.

Remark 2.5. The examples of Serre in [K1] are not ordinary (by Lemma 2.4 or because their endomorphism rings are not commutative, which is another consequence of ordinarity, see e.g. [W, §7]).

However, the referee gave the following argument that shows that for any dimension g such that $\varphi(g) > 2$ (i.e., $g \notin \{1, 2, 3, 4, 6\}$), there exist infinitely many finite fields $\mathbf{F}_p$ and absolutely simple non-isogenous isokummerian abelian varieties $A/\mathbf{F}_p$, $B/\mathbf{F}_p$.

Start with a CM-field K of degree $2g$ over $\mathbf{Q}$ which is Galois over $\mathbf{Q}$, with maximal real subfield K^+ such that $\mathrm{Gal}(K^+/\mathbf{Q})$ is cyclic (of order g) and the exact sequence

$$1 \to \mathrm{Gal}(K/K^+) \to \mathrm{Gal}(K/\mathbf{Q}) \to \mathrm{Gal}(K^+/\mathbf{Q}) \to 1$$

splits (i.e., K is the compositum of K^+ with an imaginary quadratic field L); denote by $i \mapsto \sigma_i$ the isomorphism $\mathbf{Z}/g\mathbf{Z} \to \mathrm{Gal}(K^+/\mathbf{Q})$ and by $s : \mathrm{Gal}(K^+/\mathbf{Q}) \to \mathrm{Gal}(K/\mathbf{Q})$ a splitting of the exact sequence. Take a prime p that splits completely in K into principal ideals (there are infinitely many such primes by the Chebotarev density theorem since any prime totally split in the Hilbert class field of K will do), let $\mathfrak{p}_0$ be a prime above p in K, and $q_0 \in \mathcal{O}_K$ a generator of $\mathfrak{p}_0$. Put $q_i = s(\sigma_i)(q_0)$ for all i.

For any integer r with $0 < r < n/2$ coprime with g (which exist if $\varphi(g) > 2$), put

$$\pi_r = \overline{q_0} q_1 q_2 \cdots q_{r-1} \overline{q_r} q_{r+1} \cdots q_{g-1}.$$

Then the various π_r are all p-Weil numbers, they are ordinary because π_r is coprime with $\overline{\pi_r}$, they correspond to absolutely simple abelian varieties $A_r/\mathbf{F}_p$ (because $(g, r) = 1$ so that no power of π_r lies in a subfield of K). Also they are not Galois conjugates, but it is easy to check that $\pi_r \in \Phi_{\pi_s}$ for all r, s: for instance, if g is odd, one gets

$$\pi_2 = \sigma_2(\pi_1)\sigma_3(\pi_1)^{-1} \cdots \sigma_{g-3}(\pi_1)\sigma_{g-2}(\pi_1)^{-1}\sigma_{g-1}(\pi_1).$$

So the A_r are pairwise isokummerian.

Now we come to Condition (2), where there is also a simple sufficiency criterion. Denote by W_{2g} the group of permutations of g pairs $(2i-1, 2i)$ such that the couples $\{2i-1, 2i\}$, $1 \leqslant i \leqslant g$, are stable. Equivalently, this is the Weyl group of the symplectic group $Sp(2g)$ (or the Galois group of a generic "self-reciprocal" polynomial P of degree $2g$, as explained in Section 4).

Lemma 2.6. *Let π be a q-Weil number such that $[\mathbf{Q}(\pi) : \mathbf{Q}] = 2g$ and such that the Galois group of K_π over $\mathbf{Q}$ is isomorphic to W_{2g}. Then π satisfies Condition* (2) *of Proposition* 2.1.

Proof. The Galois group of K_π acts on the $2g$ conjugates of π by permutation, leaving the pairs $(\pi_i, q/\pi_i)$ invariant. Thus, as a subgroup of the symmetric group on $2g$ elements, it is identified as a subgroup of W_{2g} acting on those pairs. If the Galois group is equal to W_{2g}, the existence of the required elements σ_i is obvious. □

Corollary 2.7. *Let q be a power of a prime p. For any simple ordinary abelian variety $A/\mathbf{F}_q$ of dimension g such that the Galois group G of K_{π_A} is isomorphic to W_{2g}, the set of q-Weil numbers in Φ_A is equal to the set of conjugates of π_A.*

This is immediate from Proposition 2.1, Lemma 2.4 and Lemma 2.6.

3. General abelian varieties up to isomorphism

We now apply Proposition 2.1 to "generic" isomorphism classes of abelian varieties of dimension g. More precisely, one has to consider (for instance) the moduli space A_g of abelian varieties of dimension g with a principal polarization, which is known to be irreducible of dimension $g(g+1)/2$ over $\mathbf{Z}$.

For Condition (1) of Proposition 2.1, we use Lemma 2.4. It is known that generic abelian varieties are ordinary, see [ON][2]. Thus in A_g, there exists a dense Zariski open subset $U \subset A_g$ such that the polarized abelian variety parameterized by any $u \in U$ is ordinary. (See also [CL, §5] for a sketch; roughly speaking, ordinarity is an open condition, and we know that ordinary abelian varieties of any dimension exist, for instance products of ordinary elliptic curves).

In analogy with $A_g(q)$, $\mathcal{A}_g(q)$, we now denote

[2] The result is attributed by Oort and Norman to Mumford [Mu], although it is not stated there, because Mumford had the main idea for the necessary lifting result (email from F. Oort).

- $A_g^{\mathrm{ord}}(q) \subset A_g(q)$ the set of isomorphism classes of principally polarized ordinary abelian varieties of dimension g defined over $\mathbf{F}_q$;
- $\mathcal{A}_g^{\mathrm{ord}}(q)$ the set of isogeny classes of ordinary abelian varieties of dimension g defined over $\mathbf{F}_q$.

Proposition 3.1. *Let p be a prime number. We have*

$$\lim_{n\to+\infty} \frac{|A_g^{\mathrm{ord}}(p^n)|}{|A_g(p^n)|} = 1.$$

Proof. Mumford's result gives this for the corresponding counting of isomorphism classes of principally polarized abelian varieties with some rigidifying structure; then one deduces the statement above by dividing by the number of choices for the rigidifying data, and dealing with possible extra automorphisms, as done for instance in [KS, 10.7,11.3]. □

Remark 3.2. This is much weaker than what the result of Mumford implies: since the moduli space of principally polarized abelian varieties is irreducible of dimension $g(g+1)/2$ and the space of non-ordinary abelian varieties must be of dimension $\leqslant g(g+1)/2-1$, we have for $n \geqslant 1$:

$$|A_g(p^n)| = 2p^{ng(g+1)/2} + O(p^{n(g(g+1)/2-1)}),$$
$$|A_g^{\mathrm{ord}}(p^n)| = |A_g(p^n)| + O(p^{n(g(g+1)/2-1)})$$

(the factor 2 accounts for the fact that each abelian variety comes with its quadratic twist).

Condition (2) is not so easy to treat. We use Lemma 2.6, and the crucial fact is that Chavdarov [C] has shown that "most" abelian varieties $A/\mathbf{F}_{p^n}$ with $n \to +\infty$ are simple and satisfy the assumptions of that lemma.

Proposition 3.3. *Let p be a prime number. Denote by $B_g(p^n)$ the set of isomorphism classes of principally polarized abelian varieties $A/\mathbf{F}_{p^n}$ of dimension g such that the Galois group of K_{π_A} over $\mathbf{Q}$ is isomorphic to W_{2g}. We have*

$$\lim_{n\to+\infty} \frac{|B_g(p^n)|}{|A_g(p^n)|} = 1.$$

Proof. For $p \neq 2$, this follows straightforwardly from [C, Th. 2.1], applied to a suitably "rigidified" universal family of principally polarized abelian varieties of dimension g over $\mathbf{F}_p$, after eliminating as before the extra factor counting the rigidifying parameters (compare again [KS, 11.3]). The monodromy groups modulo ℓ involved in applying Chavdarov's Theorem are as large as possible for $\ell > 2$ because (for instance), it is already the case for the families of jacobians of hyperelliptic curves of the type

$$y^2 = f(x)(x-t)$$

(with f a polynomial of degree $2g$ with distinct roots in $\bar{\mathbf{F}}_p$, t as parameter not a zero of f), considered in [KS, Th. 11.0.4], which are the same as those in [C, Ex. 2.4] (this is where characteristic $\neq 2$ enters). This result about monodromy groups is due to J.K. Yu (unpublished). See also below for more discussion of these examples.

In characteristic 2, no example with such explicit computation of monodromy groups modulo ℓ seems known. However, Sutor [Su] (see also [KS, 10.2.2]) has shown that the family of curves of genus g over $\mathbf{F}_2$ given by

$$y^2 - y = x^{2g-1} + t/x$$

with parameter $t \neq 0$ has geometric $\mathbf{Q}_\ell$-monodromy equal to $Sp(2g)$ for $\ell > 2$. Using a (rather difficult) result of Larsen (Theorem 3.17 of [La] and the first lines of its proof), this is sufficient to ensure that the monodromy modulo ℓ of this family is $Sp(2g, \mathbf{F}_\ell)$ for a sequence of ℓ of density 1, and then the same applies to the rigidified moduli space of abelian varieties, and Chavdarov's argument goes through as before. □

We now deduce from Proposition 3.1 and Proposition 3.3 the first main result of this paper.

Theorem 3.4. *Let q be a power of an odd prime p. For $n \geqslant 1$, let $C_g(q^n)$ be set of isomorphism classes of principally polarized absolutely simple abelian varieties $A/\mathbf{F}_{q^n}$ of dimension g such that $\Phi_A \simeq \mathbf{Z}^{g+1}$ and w_A is equal to the set of conjugates of π_A. Then we have*

$$\lim_{n \to +\infty} \frac{|C_g(q^n)|}{|A_g(q^n)|} = 1.$$

Informally: "most" abelian varieties A of dimension g over $\mathbf{F}_{q^n}$ with n large are simple, ordinary, the group Φ_A is isomorphic to $\mathbf{Z}^{g+1}$ and the only q^n-Weil numbers in Φ_A are π_A and its conjugates.

By the criterion stated in the introduction for two varieties to be isokummerian over a finite field, we see that this theorem is equivalent to the first part (1.1) of Theorem 1.1.

Remark 3.5. As in [C] or [KS], it would be very interesting to have a corresponding result with $n = 1$ and $q = p \to +\infty$; and (as in those cases) this seems very hard.

On the other hand, introducing some analytic ideas (a bilinear form estimate for representations of $\mathbf{F}_\ell$-adic sheaves and "old-fashioned" large sieve as in [G] and Section 4), it is possible to improve Proposition 3.3 in some cases (in particular, if g satisfies $p > 2g + 1$) to obtain a sharper estimate

$$|I_g(q^n)| = q^{ng(g+1)/2} + O(q^{n(g(g+1)/2-\gamma)}(\log q^n))$$

for $\gamma = (10g^2 + 6g + 8)^{-1}$; see [K2, Cor. 6.4].

If one does not wish to deal with the moduli space, one can apply Chavdarov's theorem to any algebraic family of principally polarized abelian varieties over a finite field $\mathbf{F}_q$ for which the monodromy group mod ℓ is equal to $Sp(2g, \mathbf{Z}/\ell\mathbf{Z})$ for almost all ℓ, provided one can check that ordinarity is generic in that family. The simplest example are provided by taking an algebraic family of curves and then the associated jacobian family, which has a canonical principal polarization. If one takes the universal family of curves, then the generic ordinarity is a result of Miller, who gives explicit examples of ordinary curves of every genus and characteristic, so that the result follows from the openness of ordinarity and the irreducibility of the moduli space of curves. The fact that the corresponding monodromy group is $Sp(2g)$ follows again in characteristic $\neq 2$ from the examples of families of hyperelliptic curves of [C, Ex. 2.4] (see also [KS, 10.2]).

It is natural to want to give similar explicit equations of families of curves which are both generically ordinary and have monodromy $Sp(2g)$. However note that Miller's families

$$\begin{cases} y^2 = x^{2g+1} + tx^{g+1} + x \text{ if } p \nmid g, \\ y^2 = x^{2g+2} + tx^{g+1} + 1 \text{ if } p \mid g \end{cases}$$

fail the monodromy test (because they fail the diophantine irreducibility test, see [KS, Lemma 10.1.15], as a simple computation shows). On the other hand, the author couldn't find references to the ordinarity for the families with large monodromy of [KS]. For the moment, we merely state the following fairly easy result:

Proposition 3.6. *Let $p \geqslant 3$ be a prime number, $g \geqslant 2$ an integer. Put $\delta = 1$ if $p \mid g$, $\delta = 0$ otherwise.*

(1) *The 2-parameter family T of smooth projective curves of genus g over $\mathbf{F}_p$ given by compactification of the affine family*

$$T_{t,u} \,:\, y^2 = (x-u)(x^{2g+\delta} + tx^g + 1)$$

over the open subset

$$U = \{(t,u) \in \mathbf{A}^2 \mid u^{2g+\delta} + tu^g + 1 \neq 0\} \subset \mathbf{A}^2/\mathbf{F}_p$$

is generically ordinary and has geometric monodromy group modulo ℓ equal to $Sp(2g, \mathbf{F}_\ell)$ for $\ell > 2$, $\ell \neq p$.

(2) *In particular, there exists $\nu \geqslant 1$ and $t_0 \in \mathbf{F}_{p^\nu}$ such that the 1-parameter family S of curves of genus g over $\mathbf{F}_{p^\nu}$ given by*

$$S_u \,:\, y^2 = (x-u)(x^{2g+\delta} + t_0 x^g + 1)$$

with $u \in U_{t_0} = \{(t_0, u) \in U\} \subset \mathbf{A}^1/\mathbf{F}_{p^\nu}$ is generically ordinary and has geometric monodromy group modulo ℓ equal to $Sp(2g, \mathbf{F}_\ell)$ for $\ell > 2$, $\ell \neq p$.

(3) *If $p \nmid g$ and g is even, one can in fact take $t_0 = 0$, so the family*

$$S_u \,:\, y^2 = (x-u)(x^{2g} + 1)$$

with $u \in U_0 = \mathbf{A}^1 - \mu_{2g}$, where μ_{2g} is the group of $2g$-roots of unity, is generically ordinary and has geometric monodromy group modulo ℓ equal to $Sp(2g, \mathbf{F}_\ell)$ for $\ell > 2$, $\ell \neq p$.

Proof. Note that for $u = 0$, the family T specializes to Miller's family, and therefore the open set of ordinarity for T is not empty, hence dense. Moreover, for any fixed $t_0 \neq \pm 1$, the family $S_u = T_{u,t_0}$ is of the form

$$y^2 = f_{t_0}(x)(x-u)$$

with f_{t_0} a monic polynomial of degree $2g$ which has distinct roots in $\bar{\mathbf{F}}_p$, as a simple computation shows. Hence it is of the form considered in [C, Ex. 2.4] and [KS, 10.1], and therefore has the required monodromy. As the monodromy groups can only become smaller by taking such a 1-parameter subfamily of T, the result follows.

Now generic ordinarity for T implies that for some $t_0 \in \mathbf{A}^1(\bar{\mathbf{F}}_p) - \{\pm 1\}$ at least the restricted subfamily $S_u = T_{u,t_0}$ with u as parameter must contain an ordinary curve. As it still has the same generic monodromy group, the existence result (2) follows.

When $p \nmid g$, and $t = t_0 = 0$, Miller's curve has equation

$$y^2 = x^{2g+1} + x.$$

The recipe in [Mi, §2] for computing the (dual of the) Hasse-Witt matrix for this curve shows that it is invertible, hence the curve is ordinary, if for every u, $0 \leqslant u \leqslant g-1$, there exist unique integers r, $t \geqslant 0$ such that

$$r + t = \frac{p-1}{2}$$
$$2gt + \frac{p+1}{2} + u = p(v+1),$$

where v is uniquely determined by $0 \leqslant v \leqslant g-1$ and the congruence

$$\frac{p+1}{2} + u \equiv p(v+1) \,(\mathrm{mod}\, g). \tag{3.1}$$

It is easy to see (following Miller's argument) that the equations for r and t have at most one solution, and that this solution exists if and only if

$$v + 1 \equiv u + \frac{p+1}{2} \pmod 2.$$

If g is even, then (3.1) implies this.[3] □

We now come to some global consequences that follow also from other results of Chavdarov's paper. Those have the virtue of concerning individual abelian varieties, as the exceptions become a set of primes of density 0 which does not affect (for instance) Faltings's Isogeny Theorem.

Proposition 3.7. *Let $F/\mathbf{Q}$ be a number field. Let $g \geqslant 1$ be 2, 6, or an odd integer. Let A/F be an abelian variety of dimension g such that $\mathrm{End}(A) = \mathbf{Z}$ and such that the set of primes of good reduction $\mathfrak{p}$ of F where the reduction of A modulo $\mathfrak{p}$ is ordinary is of density 1. Then for any abelian variety B/F, B is isokummerian to A if and only if B is isogenous to a power of A.*

Proof. By Chavdarov's "horizontal" version of his result ([C, Cor. 6.9]), the assumptions on A ensure that for all prime ideals $\mathfrak{p}$ in a set of primes of density 1, the reduced variety $A_\mathfrak{p}/\mathbf{F}_\mathfrak{p}$ is ordinary, absolutely simple and its Frobenius has Galois group W_{2g}. By Corollary 2.7, it follows that $B_\mathfrak{p}$ must be isogenous to a power of $A_\mathfrak{p}$ for any such $\mathfrak{p}$. The dimension of B fixes a $k \geqslant 1$ such that $B_\mathfrak{p} \simeq A_\mathfrak{p}^k$ for all primes in a set of density 1. Then by Faltings's Isogeny Theorem, it follows that $B \simeq A^k$ over F. □

The assumption of ordinarity at almost all places for varieties with $\mathrm{End}(A) = \mathbf{Z}$ is widely expected to hold, but few results are known. For elliptic curves, it is quite easy, but this case of the proposition is already treated in [K1] without this assumption. Here is another situation that can be treated unconditionally (compare with Ogus's theorem quoted in [CL, Th. 6.3]):

Proposition 3.8. *Let $A/\mathbf{Q}$ be an abelian surface over $\mathbf{Q}$ with $\mathrm{End}(A) = \mathbf{Z}$. Then the set of primes of good ordinary reduction for A is of density 1. Hence any $B/\mathbf{Q}$ is isokummerian to A if and only if B is isogenous to a power of A.*

Proof. We use Serre's ℓ-adic methods [S]. Let ℓ be a prime and $\rho_\ell : G_\mathbf{Q} \to Sp(4, \mathbf{Q}_\ell)$ the ℓ-adic representation associated to A. Serre has shown (this is already used in the proof of Chavdarov's horizontal theorem) that the image of ρ_ℓ is dense. Consider the exterior square $\sigma_\ell = \wedge^2\rho_\ell$. It is an ℓ-adic representation of rank 6 and "weight" 1, and it is faithful, so the closure G_ℓ of the image of σ_ℓ is again isomorphic to $Sp(4, \mathbf{Q}_\ell)$. Moreover, for any prime $p \neq \ell$ of good reduction, the properties of ρ_ℓ and standard algebra show that the trace of the image by σ_ℓ of a Frobenius element σ_p at p is the middle coefficient b_2 of the characteristic polynomial of the Frobenius of A modulo p. Hence, by the characterization of ordinarity already stated, A has ordinary reduction at p if and only if this trace $\mathrm{Tr}\,\sigma_\ell(\sigma_p)$ is not divisible by p.

However, by the Riemann Hypothesis for A modulo p, we have

$$|\,\mathrm{Tr}\,\sigma_\ell(\sigma_p)| \leqslant 6p,$$

so if A is not ordinary at p, the trace must belong to set $\{-6p, -5p, \ldots, 0, p, \ldots, 6p\}$. Let t be any of these thirteen values. We claim that the set of primes p for which $\mathrm{Tr}\,\sigma_\ell(\sigma_p) = t$ is of density 0. Clearly this implies the proposition.

[3] On the other hand, if g is odd, the residue modulo 2 of this expression will take both values.

The proof of the claim is easy: since $\det \sigma_\ell(\sigma_p) = p^4$, if p satisfies the stated condition then we have

$$\sigma_p \in X_t = \{g \in G_\ell \mid (\operatorname{Tr} g)^4 - t^4 \det g = 0\}.$$

Using $G_\ell \simeq Sp(4, \mathbf{Q}_\ell)$ and simple computations, it is easy to see that X_t is a closed subset of G_ℓ of Minkowski dimension $< \dim Sp(4)$ (see [S, §3] for the definition of Minkowski, or M-dimension). Hence by Theorem 10 of [S], the set of primes with $\sigma_p \in X_t$ is of density 0. □

In a general higher dimensional situation (over $\mathbf{Q}$, say), the non-ordinary primes are such that the trace t of the g-th exterior power of the representation on the Tate module is divisible by p, which for $g \geqslant 3$ allows an unbounded number of values of t (for $g = 3$, $\operatorname{Tr} \wedge^3 \rho_\ell(\sigma_p) = pk$ with $|k| \leqslant 20\sqrt{p}$). Even using explicit forms of the Chebotarev density theorem (on GRH) to detect each value, the uniformity is not sufficient to obtain any non-trivial result.

Remark 3.9. In [K1], the question of the "splitting behavior" of a simple abelian variety $A/\mathbf{Q}$ at all primes is also raised: is it true that the reduction modulo p of A remains simple for almost all p? In fact, the "horizontal" statements of Chavdarov can already deal with this. For instance, this property holds if $A/\mathbf{Q}$ has the property that the Galois group of the field $\mathbf{Q}(A[\ell])$ generated by the points of ℓ-torsion of A is equal to $Sp(2g, \mathbf{Z}/\ell\mathbf{Z})$ for ℓ large.

On the other hand, the referee pointed out that it is known that there exists an abelian surface $A/\mathbf{Q}$ with quaternionic multiplication such that $A \pmod p$ is non-simple for all primes of good reduction; this follows from the review MR0447259 by Robert J. Fisher of a paper by C. Adimoolam (correcting serious errors in the latter), and from results of Hashimoto and Murabayashi [HM] to obtain surfaces with the correct endomorphism algebra to apply the argument sketched in this review.

4. General abelian varieties up to isogeny

Since Weil numbers, ordinarity, and having Galois group W_{2g} are all isogeny-invariant properties of abelian varieties, it is natural to ask for analogs of the results of the previous section for isogeny classes of abelian varieties, instead of isomorphism classes. Going directly from one to the other is not easy, since finding the number of isomorphism classes in an isogeny class is a quite delicate question, typically related with class numbers (as can be seen most easily in the case of elliptic curves), see [W, §4.3].

However, we can use results of DiPippo and Howe to deal directly with isogeny classes. Note then that it is not necessary to introduce a polarization. This is rather satisfactory since not all isogeny classes contain a principally polarized one; see for instance [H, Th. 1.3]; however it is proved there (Th. 1.2) that any isogeny class of odd-dimensional, simple, ordinary abelian varieties over a finite field, contains a principally polarized one.

Proposition 4.1. *Let $g \geqslant 1$. We have*

$$\lim_{q \to +\infty} \frac{|\mathcal{A}^{\mathrm{ord}}(q)|}{|\mathcal{A}_g(q)|} = 1,$$

and

$$|\mathcal{A}_g(q)|,\ |\mathcal{A}_g^{\mathrm{ord}}(q)| \sim v_g \frac{\varphi(q)}{q} q^{g(g+1)/4} \text{ as } q \to +\infty, \tag{4.1}$$

for some constant $v_g > 0$.

This is proved by DiPippo and Howe in [DH] (see Theorem 1.1), in fact in a much more precise form. Note in particular that this says intuitively that the "dimension" of the "space" of isogeny classes of abelian varieties of dimension g is $g(g+1)/4$, half that of the moduli space.

Proposition 4.2. *Denote by $\mathcal{B}_g(q)$ the set of isogeny classes of abelian varieties $A/\mathbf{F}_q$ of dimension g such that the Galois group of K_{π_A} over $\mathbf{Q}$ is isomorphic to W_{2g}. We have*

$$\lim_{q\to+\infty} \frac{|\mathcal{B}_g(q)|}{|\mathcal{A}_g(q)|} = 1.$$

Using Lemma 2.6, this shows that the analog of Theorem 3.4 holds for isogeny classes, and therefore that the second part (1.2) of Theorem 1.1 holds.

To prove Proposition 4.1, DiPippo and Howe identify the set of isogeny classes considered with a set of lattice points in a region $V_{g,n} \subset \mathbf{R}^g$. We argue similarly for Proposition 4.2, except that we do not need to be so precise because we only look for an upper bound on the number of isogeny classes with "smaller" Galois group, which is a question of probabilistic Galois theory. It is straightforward to adapt here the method of Gallagher [G] based on the large sieve inequality. It has already been shown, using those methods, that self-reciprocal polynomials of degree $2g$ and bounded height have generically W_{2g} as Galois group (see [DDS]), but our parameter set is different.

Let $A/\mathbf{F}_q$ be an abelian variety of dimension g over a finite field. The (reversed) characteristic polynomial of Frobenius f_A of A is of degree $2g$ with real roots of even multiplicity and complex roots arising in pairs $(\alpha, q/\alpha)$. Therefore one can write

$$f_A = (X^{2g} + q^g) + a_1(X^{2g-1} + q^{g-1}X) + \cdots + a_g X^g,$$

with $a_i \in \mathbf{Z}$. To A we associate the vector $a = (a_1, \ldots, a_g) \in \mathbf{Z}^g$.

Lemma 4.3. *Let $g \geqslant 1$ and let q be a power of a prime p. For any abelian variety $A/\mathbf{F}_q$, the vector a above satisfies $a \in \mathbf{Z}^g \cap R_{g,q}$ where*

$$R_{g,q} = \left\{(x_1, \ldots, x_g) \in \mathbf{R}^g \mid |x_i| \leqslant \binom{g}{i} q^{i/2}\right\}.$$

Proof. This is obvious by the Riemann Hypothesis and the definition of a_i. □

The analytic ingredient we need is the following consequence of the large sieve inequality.

Lemma 4.4. *Let $g \geqslant 1$. For $1 \leqslant i \leqslant g$, let $X_i \geqslant 1$ and let*

$$R = \{(x_1, \ldots, x_g) \in \mathbf{Z}^g \mid |x_i| \leqslant X_i \text{ for } 1 \leqslant i \leqslant g\} \subset \mathbf{R}^g.$$

Let $y \geqslant 2$ and for all primes $p \leqslant y$, let $\Omega(p) \subset (\mathbf{Z}/p\mathbf{Z})^g$ be a finite set of cardinality $\omega(p)$. Let

$$P(y) = \sum_{p\leqslant y} \omega(p) p^{-g}$$

and for any $a \in \mathbf{Z}^g$ let $P(a, y)$ denote the number of $p \leqslant y$ such that $a \pmod p \in \Omega(p)$. Then we have

$$\sum_{a\in R} (P(a, y) - P(y))^2 \ll P(y) \prod_{j=1}^{k} (X_i + y^2),$$

the implied constant depending only on g.

Proof. We derive this from the following multidimensional (trigonometric) large sieve inequality: for any finite set of vectors $Y \subset (\mathbf{R}/\mathbf{Z})^g$ such that $\max \|\alpha_k - \beta_k\| \geqslant \delta$ for two elements $\alpha \neq \beta$ in Y (where $\|x-y\|$ is the distance in $\mathbf{R}/\mathbf{Z}$), and for any complex numbers $f(x)$ defined for $x \in R$, we have

$$\sum_{\alpha \in Y} \Big| \sum_{x \in R} f(x) e(\langle x, \alpha \rangle) \Big|^2 \ll \prod_{k=1}^{g} (X_i + \delta^{-1}) \sum_{x \in R} |f(x)|^2, \tag{4.2}$$

where the implied constant depends only on g. This is a special case of [Hu, Th. 1].

To obtain the lemma from this, proceed as in Lemma A of [G], which we repeat for convenience: let χ_p be the characteristic function of $\Omega(p)$, and expand it in Fourier series

$$\chi_p(a) = \sum_{\alpha \in (\mathbf{Z}/p\mathbf{Z})^g} \hat{\chi}_p(\alpha) e(\langle a, \alpha \rangle / p) \text{ with } \hat{\chi}_p(\alpha) = p^{-g} \sum_{a \in \Omega(p)} e(\langle -a, \alpha \rangle / p).$$

Thus we have

$$\hat{\chi}_p(0) = p^{-g}\omega(p), \quad \sum_{\alpha \neq 0} |\hat{\chi}_p(\alpha)|^2 \leqslant \sum_{\alpha} |\hat{\chi}_p(\alpha)|^2 = p^{-g}\omega(p). \tag{4.3}$$

We have for $a \in R$

$$P(a,y) = \sum_{p \leqslant y} \sum_{\alpha \in (\mathbf{Z}/p\mathbf{Z})^g} \hat{\chi}_p(\alpha) e(\langle a, \alpha \rangle / p) = P(y) + \sum_{p \leqslant y} \sum_{\alpha \neq 0} \hat{\chi}_p(\alpha) e(\langle a, \alpha \rangle / p). \tag{4.4}$$

Denote by $R(a,y)$ the inner sum. We now write by Cauchy's inequality and (4.3)

$$\begin{aligned}
\sum_{a \in R} |R(a,y)|^2 &= \sum_{p \leqslant y} \sum_{\alpha \neq 0} \hat{\chi}_p(\alpha) \sum_{a \in R} R(a,y) e(\langle a, \alpha \rangle / p) \\
&\leqslant \Big(\sum_{p \leqslant y} \sum_{\alpha \neq 0} |\hat{\chi}_p(\alpha)|^2 \Big)^{1/2} \Big(\sum_{p \leqslant y} \sum_{\alpha \neq 0} \Big| \sum_{a \in R} R(a,y) e(\langle a, \alpha \rangle / p) \Big|^2 \Big)^{1/2} \\
&\leqslant P(y)^{1/2} \Big(\sum_{p \leqslant y} \sum_{\alpha \neq 0} \Big| \sum_{a \in R} R(a,y) e(\langle a, \alpha \rangle / p) \Big|^2 \Big)^{1/2}
\end{aligned}$$

and applying the trigonometric large sieve inequality (4.2) with the trivial spacing estimate for distinct vectors α/p, $\beta/q \in (\mathbf{R}/\mathbf{Z})^g$, p, $q \leqslant y$, this gives

$$\sum_{a \in R} |R(a,y)|^2 \ll P(y)^{1/2} \Big(\prod_{k=1}^{g} (X_i + y^2) \sum_{a \in R} |R(a,y)|^2 \Big)^{1/2},$$

so

$$\sum_{a \in R} |R(a,y)|^2 \ll P(y) \prod_{k=1}^{g} (X_i + y^2).$$

As, by (4.4), we have

$$\sum_{a \in R} (P(a,y) - P(y))^2 = \sum_{a \in R} |R(a,y)|^2,$$

we are done. □

of Proposition 4.2. First, for any g-tuple $a = (a_1, \dots, a_g)$ in a ring R, we denote

$$h_a = X^g + a_1 X^{g-1} + \cdots + a_{g-1} X + a_1 \in R[X]$$

and

$$f_a = X^g h_a(qX + X^{-1}) \in R[X].$$

Let $A/\mathbf{F}_q$ be an abelian variety and f_A the reversed characteristic polynomial of Frobenius for A and G the Galois group of its splitting field, which can be seen (in possibly many ways) as a subgroup of W_{2g}. By Lemma 2 of [DDS], we have $G = W_{2g} \subset \mathfrak{S}_{2g}$ if G contains a 2-cycle, a 4-cycle, a $(2g-2)$-cycle and a $2g$-cycle.

For $\ell \in \{2, 4, 2g-2, 2g\}$, let E_ℓ be the number of lattice points $a = (a_1, \dots, a_g)$ in the region $R_{g,q}$ defined in Lemma 4.3 such that the polynomial $f = f_a$ is either reducible or such that the Galois group G_a of the splitting field of f, seen as a subgroup of W_{2g} again, does not contain an ℓ-cycle. By the observation above and Lemma 4.3, it follows that the number E of isogeny classes of abelian varieties $A/\mathbf{F}_q$ with f_A not having Galois group W_{2g} satisfies

$$E \leqslant E_2 + E_4 + E_{2g-2} + E_{2g}.$$

For each ℓ, we know from classical algebraic number theory (see e.g. [vdW, §61]) that if the polynomial f_a reduces modulo some prime p to a polynomial $f_a \pmod p \in \mathbf{F}_p[X]$ which factorizes as a product of $2g - \ell$ distinct linear factors and a single irreducible polynomial of degree ℓ, then G_a contains an ℓ-cycle. Therefore, choosing $y \geqslant 2$ arbitrary and putting

$$\Omega(p) = \{a = (a_1, \dots, a_g) \in (\mathbf{Z}/p\mathbf{Z})^g \mid f_a \pmod p \text{ factorizes as } 2g-\ell \text{ distinct linear factors, and one irreducible factor of degree } \ell\}$$

for $p \leqslant y$, we see that for a such that G_a does not contain an ℓ-cycle we have $f_a \pmod p \notin \Omega(p)$ for all $p \leqslant y$. With notation as in Lemma 4.4 with $X_i = \binom{g}{i} q^{i/2}$ (so $R = R_{g,q}$), we have therefore $P(a, y) = 0$, and the large sieve inequality implies by positivity that

$$E_\ell P(y)^2 \ll P(y) \prod_{1 \leqslant i \leqslant g} (q^{i/2} + y^2)$$

where the implied constant depends only on g. However by Lemma 3 of [DDS] (see p. 269, or compare [G, p. 96, l. 10]) we have for $y \geqslant 3$ the lower bound

$$P(y) = \frac{C_\ell}{|W_{2g}|}\pi(y) + O(\log\log y) \gg \pi(y),$$

where C_ℓ is the number of ℓ-cycles in W_{2g}, where the implied constant depend only on g. Thus we get by the Prime Number Theorem (Chebychev's elementary lower-bound estimate suffices) that

$$E_\ell \ll \prod_{1 \leqslant i \leqslant g} (q^{i/2} + y^2) y^{-1} \log y.$$

We choose $y^2 = q^{1/2}$, so that

$$\prod_{1 \leqslant i \leqslant g} (q^{i/2} + y^2) \leqslant 2^g q^{g(g+1)/4}$$

and

$$E_\ell \ll q^{g(g+1)/4 - 1/4} \log q,$$

hence

$$E \ll q^{g(g+1)/4 - 1/4} \log q$$

with an implied constant depending only on g. By comparison with (4.1), we see that Proposition 4.2 is proved since $\varphi(q)/q \gg (\log\log q)^{-1}$. □

Remark 4.5. The bound obtained from the large sieve estimate may seem quite poor because of the choice of a rather small y, constrained by the smallest X_i. One may certainly expect that having a small Galois group would be of "codimension" at least 1, which would mean essentially $E \ll q^{g(g+1)/4-1/2}$. There is a similar discrepancy between what is proved and what is expected in other problems of probabilistic Galois theory.

Remark 4.6. In contrast with the isomorphism case, the results above do not yield examples of "thinner" families of isogeny classes which would be ordinary and have W_{2g} as associated Galois group. Most notably, it is by no means clear how to prove the analogue of (1.2) where the isogeny classes are jacobians of curves of genus g (equivalently, where arbitrary Weil numbers are replaced by those associated with curves). Distinguishing jacobians among abelian varieties over a finite field is a deep unsolved problem.

References

[CL] A. Chambert-Loir: *Cohomologie cristalline: un survol*, Exposition. Math. 16 (1998), 333–382.

[C] N. Chavdarov: *The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy*, Duke Math. J. 87 (1997), 151–180.

[DDS] S. Davis, W. Duke and X. Sun: *Probabilistic Galois theory of reciprocal polynomials*, Exposition. Math. 16 (1998), no. 4, 263–270.

[DH] S. DiPippo and E. Howe: *Real polynomials with all roots on the unit circle and abelian varieties over finite fields*, J. Number Theory 73 (1998), 426–450; Corrig., J. Number Theory 83 (2000), 182.

[G] P.X. Gallagher: *The large sieve and probabilistic Galois theory*, in Proc. Sympos. Pure Math., Vol. XXIV, Amer. Math. Soc. (1973), 91–101.

[HM] K. Hashimoto and N. Murabayashi: *Shimura curves as intersections of Humbert surfaces and defining equations of QM-curves of genus two*, Tohoku Math. J. (2) 47 (1995), no. 2, 271–296.

[H] E. Howe: *Principally polarized ordinary abelian varieties over finite fields*, Trans. Amer. Math. Soc. 347 (1995), 2361–2401.

[Hu] M.N. Huxley: *The large sieve inequality for algebraic number fields*, Mathematika 15 (1968), 178–187.

[KS] N. Katz and P. Sarnak: *Random matrices, Frobenius eigenvalues and monodromy*, A.M.S Colloquium Publ. 45, 1999.

[K1] E. Kowalski: *Some local-global applications of Kummer theory*, manuscripta math. 111 (2003), 105–139.

[K2] E. Kowalski: *The large sieve, monodromy and zeta functions of curves*, J. reine angew. Math, to appear, `arXiv:math/NT0503714`.

[La] M. Larsen: *Maximality of Galois actions for compatible systems*, Duke Math. J. 80 (1995), no. 3, 601–630.

[Mi] L. Miller: *Curves with invertible Hasse-Witt matrix*, Math. Annalen 197 (1972), 123–127.

[Mu] D. Mumford: *Bi-extensions of formal groups*, in Algebraic Geometry (Internat. Colloq., Tata Inst. Fund. Res., Bombay, 1968), Oxford Univ. Press, 307–322.

[ON] P. Norman and F. Oort: *Moduli of abelian varieties*, Ann. of Math. (2) 112 (1980), no. 3, 413–439.

[S] J-P. Serre: *Quelques applications du théorème de densité de Chebotarev*, Publ. Math. I.H.E.S 54 (1981), 123–201.

[Su] R. Sutor: *The calculation of some geometric monodromy groups*, Princeton University Ph.D. thesis (1992).

[vdW] B.L. van der Waerden: *Moderne algebra*, vol I, Springer 1935.

[W] W. Waterhouse: *Abelian Varieties over Finite Fields*, Ann. scient. Éc. Norm. Sup. 4ème série, 2 (1969), 521–560.

Université Bordeaux I - A2X, 351, cours de la Libération, 33405 Talence Cedex, France

E-mail address: `emmanuel.kowalski@math.u-bordeaux1.fr`