Journal de Théorie des Nombres
de Bordeaux **15** (2003), 627–637

Notes on an analogue of the Fontaine-Mazur conjecture

par Jeffrey D. ACHTER et Joshua HOLDEN

Résumé. On estime la proportion des corps de fonctions qui remplissent des conditions qui impliquent un analogue de la conjecture de Fontaine et Mazur. En passant, on calcule la proportion des variétés abeliennes (ou Jacobiennes) sur un corps fini qui possèdent un point rationnel d'ordre ℓ.

Abstract. We estimate the proportion of function fields satisfying certain conditions which imply a function field analogue of the Fontaine-Mazur conjecture. As a byproduct, we compute the fraction of abelian varieties (or even Jacobians) over a finite field which have a rational point of order ℓ.

1. Introduction

The paper [10] discusses the following conjecture, originally stated by Fontaine and Mazur in [8]:

Conjecture 1.1 (Fontaine-Mazur, as restated in [1]). *Let F be a number field and ℓ any prime. There does not exist an infinite everywhere unramified Galois pro-ℓ extension M of F such that* $\mathrm{Gal}(M/F)$ *is uniform.*

The definitions of *powerful* and *uniform* are taken from [6]:

Definition. Let G be a pro-ℓ group. G is *powerful* if ℓ is odd and $G/\overline{G^\ell}$ is abelian, or if $\ell = 2$ and $G/\overline{G^4}$ is abelian. (G^n is the subgroup of G generated by the n-th powers of elements in G, and $\overline{G^n}$ is its closure.)

Definition. A pro-ℓ group is *uniformly powerful*, or just *uniform*, if (i) G is finitely generated, (ii) G is powerful, and (iii) for all i, $\left[\overline{G^{\ell^i}} : \overline{G^{\ell^{i+1}}}\right] = \left[G : \overline{G^\ell}\right]$.

The paper [10] then raises the following question:

Manuscrit reçu le 3 décembre 2001.

Question 1.2. *Let F be a function field over a finite field k_0, and ℓ a prime invertible in k_0. Let $F_\infty = Fk_{\ell^\infty}$ be obtained by taking the maximal pro-ℓ extension of the constant field. Does F satisfy the following property?*

(FM) *Let F' be any non-trivial subextension of F_∞/F, and M be any infinite unramified pro-ℓ extension of F'. If M is Galois over F and M does not contain F_∞, then* $\mathrm{Gal}(M/F')$ *cannot be uniform.*

(See [1] for a discussion of the relationship between the conjecture as phrased here and the conjecture as originally given.)

The general answer to this question is in fact negative, as shown by examples due to Ihara [11] and to Frey, Kani, and Völklein [9]. In fact, there is reason to believe that the correct analogue of the Fontaine-Mazur Conjecture will be found not in questions related to [10] but in work related to that of de Jong [3].

Nevertheless, results of [10] answer the above question affirmatively in a large class of situations (see 4.1 below). Since a great deal of effort has been put into constructing fields which do not satisfy (FM), we would like to know if they are in fact common, or if they are rather rare. The present paper will attempt to quantify in some way the proportion of fields F which satisfy (FM).

The strategy is simple enough. The aforementioned paper [10] provides conditions on F (such as the absence of an ℓ-torsion element in the class group of F; see 4.1) which force an affirmative answer to the question. These conditions may be formulated in terms of the action of Frobenius on the ℓ-torsion of the Jacobian of the smooth, proper model of F. Equidistribution results for ℓ-adic monodromy imply analogous results for mod ℓ monodromy, and show that Frobenius automorphisms are evenly distributed among $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$; counting symplectic similitudes then finishes the analysis. As a pleasant side effect, we calculate the proportion of abelian varieties over k_0 with a k_0-rational point of order ℓ.

Section 2 reviews work of Katz on equidistribution, and axiomatizes our situation. Section 3 studies (the size of) certain conjugacy classes in $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$. The final section gives the quantitative Fontaine-Mazur results alluded to in the title.

This paper was written while the first author visited the second at Duke University as part of the second DMJ-IMRN conference; we thank these institutions for providing such a pleasant working environment. We also thank our anonymous referee for helpful suggestions.

2. Monodromy groups

The main piece of technology which drives this paper is an equidistribution theorem for lisse ℓ-adic sheaves. Originally due to Deligne [4, 3.5], it has since been clarified and amplified by Katz. Deferring to chapter nine of [12] a careful and complete exposition of the theory, we content ourselves by recalling the precise result needed here.

Let $(V, \langle\cdot,\cdot\rangle)$ be a $2g$-dimensional vector space over $\mathbb{F}_\ell$ equipped with a symplectic form. Recall the definition of the group of symplectic similitudes of $(V, \langle\cdot,\cdot\rangle)$:

$$\mathrm{GSp}_{2g}(\mathbb{F}_\ell) \cong \mathrm{GSp}(V, \langle\cdot,\cdot\rangle)$$

$$= \{A \in \mathrm{GL}(V) | \exists\, \mathrm{mult}(A) \in \mathbb{F}_\ell^\times : \forall v, w \in V, \langle Av, Aw\rangle = \mathrm{mult}(A)\langle v, w\rangle\}.$$

The "multiplicator" mult is a character of the group, and its kernel is the usual symplectic group $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$. For $\gamma \in \mathbb{F}_\ell^\times$, let $\mathrm{GSp}_{2g}^\gamma(\mathbb{F}_\ell) = \mathrm{mult}^{-1}(\gamma)$ be the set of symplectic similitudes with multiplier γ. Each GSp_{2g}^γ is a torsor over Sp_{2g}.

Now let $k_0 = \mathbb{F}_q$ be a finite field of characteristic p, prime to ℓ, and let U/k_0 be a smooth, geometrically irreducible variety with geometric generic point $\bar\eta$. If k is a finite extension of k_0, then one may associate to any point $u \in U(k)$ its (conjugacy class of) Frobenius $\mathrm{Fr}_{u/k}$ in $\pi_1(U, \bar\eta)$.

Suppose $\mathcal{F}$ is a local system of symplectic $\mathbb{F}_\ell$-modules of rank $2g$ on U. Recall that such an object is tantamount to a continuous representation $\rho_{\mathcal{F}} : \pi_1(U, \bar\eta) \to \mathrm{Aut}(\mathcal{F}_{\bar\eta}) \cong \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$. (To see this, one may consider the total space of $\mathcal{F}$, which is an étale cover of U. The fundamental group of U acts on covering spaces of U, and in particular on the total space of $\mathcal{F}$; this is the desired representation.)

A simple case of Katz's equidistribution theorem says the following:

Theorem 2.1 (Katz). *In the situation above, suppose the sheaf gives rise to a commutative diagram*

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \pi_1^{\mathrm{geom}}(U, \bar\eta) & \longrightarrow & \pi_1(U, \bar\eta) & \longrightarrow & \mathrm{Gal}(\bar{k}_0/k_0) & \longrightarrow & 1 \\
 & & \Big\downarrow \rho^{\mathrm{geom}} & & \Big\downarrow \rho & & \Big\downarrow \rho^{k_0} & & \\
1 & \longrightarrow & \mathrm{Sp}_{2g}(\mathbb{F}_\ell) & \longrightarrow & \mathrm{GSp}_{2g}(\mathbb{F}_\ell) & \longrightarrow & \mathbb{G}_m(\mathbb{F}_\ell) & \longrightarrow & 1
\end{array}$$

where ρ^{geom} is surjective. There is a constant C such that, for any union of conjugacy classes $W \subset \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ and any finite extension k of k_0,

$$\left| \frac{\#\{u \in U(k) : \rho(\mathrm{Fr}_{u,k}) \in W\}}{\#U(k)} - \frac{\#(W \cap \mathrm{GSp}_{2g}^{\gamma(k)}(\mathbb{F}_\ell))}{\mathrm{Sp}_{2g}(\mathbb{F}_\ell)} \right| \le \frac{C}{\sqrt{\#k}},$$

where $\gamma(k)$ is the image of the canonical generator of $\mathrm{Gal}(k)$ *under ρ^{k_0}.*

Proof. This is a special case of [12, 9.7.13]; see also [2, 4.1]. □

The constant C in Katz's theorem is effectively computable, and the theorem actually holds uniformly in families; but we will not need such developments here.

Let $\mathcal{C} \to \mathcal{M} \to \operatorname{Spec} k_0$ be a smooth, irreducible family of curves of genus $g \geq 1$. There is a sheaf $\mathcal{F} = \mathcal{F}_{\mathcal{C},\ell}$ of abelian groups on $\mathcal{M}$ whose fiber at a geometric point $\bar{x} \in \mathcal{M}$ is the ℓ-torsion of the Jacobian $\operatorname{Jac}(\mathcal{C}_x)[\ell]$. We will say that the family of curves has full ℓ-monodromy if the associated representation $\rho_{\mathcal{F}} : \pi_1^{\mathrm{geom}}(\mathcal{M}, \bar{\eta}) \to \mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ is surjective. In practice, general families of curves tend to have full ℓ-monodromy; see, for instance, the introduction to [7]. Concretely, we will see below that the universal family of curves over ${}_N\mathcal{M}_g$ has full ℓ-monodromy.

Lemma 2.2. *Let $C \to S \to \operatorname{Spec} k_0$ be a geometrically irreducible, smooth versal family of proper smooth curves of genus g. For almost all ℓ, C/S has full ℓ-monodromy.*

Proof. Fix a natural number N relatively prime to p and consider ${}_N\mathcal{C}_g \to {}_N\mathcal{M}_g$, the universal curve of genus g with principal Jacobi structure of level N. If $\ell | N$, then the final paragraphs of [5] imply that this family has full ℓ-monodromy. Indeed, [5, 5.11] shows that it suffices to verify the statement for the analogous family over $\mathbb{C}$, and [5, 5.13,5.15] provides this proof. If ℓ is relatively prime to N, then consider the moduli space ${}_{\ell N}\mathcal{M}_g$. On one hand, the ℓ-torsion of the Jacobian of ${}_{\ell N}\mathcal{C}_g$ has full ℓ-monodromy. On the other hand, the forgetful map ${}_{\ell N}\mathcal{M}_g \to {}_N\mathcal{M}_g$ is finite; therefore, ${}_N\mathcal{C}_g \to {}_N\mathcal{M}_g$ has full ℓ-monodromy, too.

For any C/S as in the statement of the lemma, there is an étale base change $T \stackrel{\phi}{\to} S$ so that ϕ^*T admits a level N structure. Then ϕ^*T is the pullback of ${}_N\mathcal{C}_g$ by the classifying map $\psi : T \to {}_N\mathcal{M}_g$. Moreover, the sheaf of ℓ-torsion on ϕ^*T, $\mathcal{F}_{\phi^*T,\ell}$ is the pullback of the universal ℓ-torsion:

$$\begin{array}{ccc} \mathcal{F}_{\phi^*T,\ell} & \longrightarrow & \mathcal{F}_{{}_N\mathcal{C}_g,\ell} \\ \big\downarrow & & \big\downarrow \\ T & \xrightarrow{\psi} & {}_N\mathcal{M}_g \end{array}$$

By the versality assumption, T has dense image in ${}_N\mathcal{M}_g$. We have seen above that $\mathcal{F}_{{}_N\mathcal{C}_g,\ell} \to {}_N\mathcal{M}_g$ has monodromy group $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$. Thus, as long as $\ell \nmid \deg\psi$, $\mathcal{F}_{\phi^*T,\ell} \to T$ has full ℓ-monodromy; *a fortiori*, C/S does, too. □

We now relate these notions to the quantitative Fontaine-Mazur question posed at the beginning of this paper. Let $\mathcal{P}$ be a property of abelian varieties over finite extensions k of k_0 which is detectable on ℓ-torsion. We will say a curve has $\mathcal{P}$ if its Jacobian does, and that a function field has $\mathcal{P}$ if its smooth, proper model does. (We have in mind, e.g., having a k-rational point of order ℓ.) Define $W_{\mathcal{P}} \subset \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ as the set of Frobenius automorphisms satisfying $\mathcal{P}$, and let $W_{\mathcal{P}}^\gamma = W_{\mathcal{P}} \cap \mathrm{GSp}_{2g}^\gamma$. More precisely, $w \in W_{\mathcal{P}}$ if and only if there exists an abelian variety X/k over a finite extension of k_0 and an isomorphism $(V, w) \xrightarrow{\sim} (X[l](\bar{k}), \mathrm{Fr}_{X/k})$.

Corollary 2.3. *Fix a $\gamma \in \mathbb{F}_\ell^\times$. Let $\{k_n\}$ be a collection of extensions of k_0 such that $\lim_{n\to\infty} \#k_n = \infty$, and, for all n, $\gamma(k_n) = \gamma$. Suppose that $\mathcal{C} \to \mathcal{M} \to k_0$ is a smooth, irreducible family of curves with full ℓ-monodromy. If $\mathcal{P}$ is a property as above, then*

$$\lim_{n\to\infty} \frac{\#\{x \in \mathcal{M}(k) : \mathcal{P}(\mathcal{C}_x)\}}{\#\mathcal{M}(k)} = \frac{\#W_{\mathcal{P}}^\gamma(\mathbb{F}_\ell)}{\#\mathrm{Sp}_{2g}(\mathbb{F}_\ell)}.$$

Proof. In view of the preceding discussion, this is an immediate application of 2.1. □

Let Ξ_g^γ denote the set of all characteristic polynomials of elements of GSp_{2g}^γ. It is well-known that $\Xi_g^\gamma \cong \mathbb{A}^g$; the isomorphism is given by sending a characteristic polynomial to its first g coefficients. For a property $\mathcal{P}$ as above, let $\Psi_{\mathcal{P}}^\gamma$ denote the set of all characteristic polynomials which satisfy $\mathcal{P}$. The proportion of characteristic polynomials satisfying $\mathcal{P}$ is roughly the same as the proportion of actual elements of GSp_{2g}^γ satisfying $\mathcal{P}$.

Lemma 2.4. *For any property as above,*

$$\left(\frac{\ell}{\ell+1}\right)^{2g^2+g} \frac{\#\Psi_{\mathcal{P},g}^\gamma(\mathbb{F}_\ell)}{\#\Xi_g^\gamma(\mathbb{F}_\ell)} \le \frac{\#W_{\mathcal{P}}^\gamma(\mathbb{F}_\ell)}{\#\mathrm{Sp}_{2g}(\mathbb{F}_\ell)} \le \left(\frac{\ell}{\ell-1}\right)^{2g^2+g} \frac{\#\Psi_{\mathcal{P},g}^\gamma(\mathbb{F}_\ell)}{\#\Xi_g^\gamma(\mathbb{F}_\ell)}.$$

Proof. For $f(x) \in \Xi_g^\gamma$, let $\Delta(f)$ be the number of elements of $\mathrm{GSp}_{2g}^\gamma(\mathbb{F}_\ell)$ whose characteristic polynomial is $f(x)$. One knows [2, 3.5] that, since $\dim \mathrm{Sp}_{2g} = 2g^2 + g$,

$$\frac{\ell^{2g^2}\#\mathrm{Sp}_{2g}(\mathbb{F}_\ell)}{(\ell+1)^{2g^2+g}} \le \Delta(f) \le \frac{\ell^{2g^2}\#\mathrm{Sp}_{2g}(\mathbb{F}_\ell)}{(\ell-1)^{2g^2+g}}.$$

Adding up over all elements of W_g^γ we see that $\#W_{\mathcal{P},g}^\gamma(\mathbb{F}_\ell) = \sum_{f\in\Xi_{\mathcal{P},g}^\gamma} \Delta(f)$, and thus

$$\frac{\ell^{2g^2}\#\mathrm{Sp}_{2g}(\mathbb{F}_\ell)}{(\ell+1)^{2g^2+g}}\#\Psi_{\mathcal{P},g}^\gamma(\mathbb{F}_\ell) \le \#W_{\mathcal{P},g}^\gamma(\mathbb{F}_\ell) \le \frac{\ell^{2g^2}\#\mathrm{Sp}_{2g}(\mathbb{F}_\ell)}{(\ell-1)^{2g^2+g}}\#\Psi_{\mathcal{P},g}^\gamma(\mathbb{F}_\ell);$$

$$\frac{\ell^{2g^2}}{(\ell+1)^{2g^2+g}}\#\Psi_{\mathcal{P},g}^\gamma(\mathbb{F}_\ell) \le \frac{\#W_{\mathcal{P},g}^\gamma(\mathbb{F}_\ell)}{\#\mathrm{Sp}_{2g}(\mathbb{F}_\ell)} \le \frac{\ell^{2g^2}}{(\ell-1)^{2g^2+g}}\#\Psi_{\mathcal{P},g}^\gamma(\mathbb{F}_\ell);$$

$$\left(\frac{\ell}{\ell+1}\right)^{2g^2+g} \frac{\#\Psi_{\mathcal{P},g}^\gamma(\mathbb{F}_\ell)}{\#\Xi_g^\gamma(\mathbb{F}_\ell)} \le \frac{\#W_{\mathcal{P},g}^\gamma(\mathbb{F}_\ell)}{\#\mathrm{Sp}_{2g}(\mathbb{F}_\ell)} \le \left(\frac{\ell}{\ell-1}\right)^{2g^2+g} \frac{\#\Psi_{\mathcal{P},g}^\gamma(\mathbb{F}_\ell)}{\#\Xi_g^\gamma(\mathbb{F}_\ell)}.$$

□

3. Remarks on symplectic groups

3.1. Eigenvalue one. We start by counting the number of matrices for which 1 is an eigenvalue; these will correspond to a certain class of function fields which we will later show (in Theorem 4.1) satisfy (FM). Let (E) be the property of having 1 as an eigenvalue. Writing $f_A(x)$ for the characteristic polynomial of $A \in \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$, we see that $A \in W_{(\mathsf{E}),g}$ if and only if $f_A(1) = 0$. Barring any obvious reason to the contrary, one might suppose that the values $\{f_A(1)\}_{A\in\mathrm{GSp}_{2g}(\mathbb{F}_\ell)}$ are evenly distributed in $\mathbb{F}_\ell$, and thus that $\#W_{(\mathsf{E}),g}/\#\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ is about $\frac{1}{\ell}$. We will now show that this rough estimate is the approximate truth – and that, confounding our initial expectations, $\frac{1}{\ell-1}$ is an even better estimate.

We need a little more notation in order to state our result precisely. Let $T(g,\gamma,\mathbb{F}_\ell) = \#W^{\gamma}_{(\mathsf{E}),g}$ be the number of elements of $\mathrm{GSp}^{\gamma}_{2g}(\mathbb{F}_\ell)$ which have one as an eigenvalue. If $\gamma \neq 1$, let $S(g,\gamma,\mathbb{F}_\ell)$ be the number of elements of $\mathrm{GSp}^{\gamma}_{2g}(\mathbb{F}_\ell)$ for which the eigenspace associated to 1 has dimension g, and let $S(g,1,\mathbb{F}_\ell)$ be the number of unipotent symplectic matrices of rank $2g$. Our goal in this section is to compute $T(g,\gamma,\mathbb{F}_\ell)/\#\mathrm{GSp}^{\gamma}_{2g}(\mathbb{F}_\ell)$. As an organizational tool, we collect intermediate results in a series of easy lemmas.

Lemma 3.1. *For $\gamma \in \mathbb{F}_\ell^\times$ and S as above,*

$$S(r,\gamma,\mathbb{F}_\ell) = \begin{cases} \ell^{2r^2} & \gamma = 1, \\ \ell^{r^2-r}\frac{\#\mathrm{Sp}_{2r}(\mathbb{F}_\ell)}{\#\mathrm{GL}_r(\mathbb{F}_\ell)} & \gamma \neq 1. \end{cases}$$

Proof. These computations use the following chain of standard observations [2]. Any characteristic polynomial of an element in $\mathrm{GSp}_{2r}(\mathbb{F}_\ell)$ is the characteristic polynomial of some semisimple element A. Moreover, the number of elements with such a characteristic polynomial is

$$\ell^{\dim Z(A)-r}\frac{\#\mathrm{Sp}_{2r}(\mathbb{F}_\ell)}{\#Z(A)(\mathbb{F}_\ell)},$$

where $Z(A)$ is the group of elements of Sp_{2r} which commute (inside GSp_{2r}) with A. From this, the computation of S immediately follows. Indeed, $A = \mathrm{diag}(1,\cdots,1,\gamma,\cdots,\gamma)$ is the unique semisimple element with characteristic polynomial $(x-1)^r(x-\gamma)^r$. If $\gamma = 1$, then $Z(A) = Z(\mathrm{id}) = \mathrm{Sp}_{2r}$, and $\dim Z(A) = 2r^2 + r$. If $\gamma \neq 1$, then the centralizer $Z(A)$ is $\left\{\begin{pmatrix} M & 0 \\ 0 & (M^{-1})^T \end{pmatrix}\right\} \cong \mathrm{GL}_r$, a group of dimension r^2. In either case, the lemma now follows. □

Lemma 3.2. *With notation as above,* $T(1,\gamma,\mathbb{F}_\ell)=S(1,\gamma,\mathbb{F}_\ell)$. *For* $g\geq 2$,

$$T(g,\gamma,\mathbb{F}_\ell)=\sum_{\substack{r+s=g\\1\leq r\leq g}}\frac{\#\mathrm{Sp}_{2g}(\mathbb{F}_\ell)}{\#\mathrm{Sp}_{2r}(\mathbb{F}_\ell)\#\mathrm{Sp}_{2s}(\mathbb{F}_\ell)}S(r,\gamma,\mathbb{F}_\ell)(\#\mathrm{Sp}_{2s}(\mathbb{F}_\ell)-T(s,\gamma,\mathbb{F}_\ell)).$$

Proof. The first claim is a tautology. For dimension $g\geq 2$, we enumerate elements of $\mathrm{GSp}^\gamma_{2g}(\mathbb{F}_\ell)$ which have one as an eigenvalue. First, we index elements A of $W^\gamma_{(\mathsf{E}),g}(\mathbb{F}_\ell)$ by r, the order of vanishing of f_A at 1 if $\gamma\neq 1$, and half that multiplicity if $\gamma=1$. To such an A corresponds a decomposition of V as $U_{(\mathsf{E}),r}\oplus U_{(\mathsf{N}),s}$, where $U_{(\mathsf{E}),r}$ and $U_{(\mathsf{N}),s}$ are symplectic subspaces of dimensions $2r$ and $2s$, respectively; $f_{A|_{U_{(\mathsf{E}),r}}}(x)=(x-1)^r(x-\gamma)^r$; and $f_{A|_{U_{(\mathsf{N}),s}}}(1)\neq 0$.

The factor $\frac{\#\mathrm{Sp}_{2g}(\mathbb{F}_\ell)}{\#\mathrm{Sp}_{2r}(\mathbb{F}_\ell)\#\mathrm{Sp}_{2s}(\mathbb{F}_\ell)}$ counts the number of ways of decomposing $V=U_{(\mathsf{E}),r}\oplus U_{(\mathsf{N}),s}$. The penultimate factor $S(r,\gamma,\mathbb{F}_\ell)$ counts the possibilities for A acting on U_r, and the last factor enumerates all choices for $A|_{U_{(\mathsf{N}),s}}$. □

Roughly speaking, $\#W^\gamma_{(\mathsf{E}),g}/\#\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ is about $\frac{1}{\ell}$. In fact, an argument similar to (but easier than) 3.4 shows that this ratio is between $(\ell/(\ell+1))^{2g^2+g}\frac{1}{\ell}$ and $(\ell/(\ell-1))^{2g^2+g}\frac{1}{\ell}$. Still, a more precise estimate isn't too difficult.

Lemma 3.3. *For each* $g\geq 1$ *there is a constant* $c(g)$ *such that*

$$\left|\frac{T(g,\gamma,\mathbb{F}_\ell)}{\#\mathrm{Sp}_{2g}(\mathbb{F}_\ell)}-\tau^\gamma_{(\mathsf{E}),g}\right|\leq c(g)(\tau^\gamma_{(\mathsf{E}),g})^3,$$

where

$$\tau^\gamma_{(\mathsf{E}),g}=\begin{cases}\frac{1}{\ell-1} & \gamma\neq 1,\\ \frac{\ell}{\ell^2-1} & \gamma=1.\end{cases}$$

Proof. We treat the case $\gamma\neq 1$, and leave the remaining case for the industrious reader. Lemma 3.2 shows that $T(1,\gamma,\mathbb{F}_\ell)/\#\mathrm{Sp}_2(\mathbb{F}_\ell)=\tau^\gamma_1$, and that $|T(2,\gamma,\mathbb{F}_\ell)/\#\mathrm{Sp}_4(\mathbb{F}_\ell)|=(\ell^2-2)/((\ell-1)^2(\ell+1))$. For $g\geq 3$,

$$\begin{aligned}\frac{T(g,\gamma,\mathbb{F}_\ell)}{\#\mathrm{Sp}_{2g}(\mathbb{F}_\ell)}&=\sum_{\substack{r+s=g\\1\leq r\leq g}}\frac{S(r,\gamma,\mathbb{F}_\ell)}{\#\mathrm{Sp}_{2r}(\mathbb{F}_\ell)}\frac{\#\mathrm{Sp}_{2s}(\mathbb{F}_\ell)-T(s,\gamma,\mathbb{F}_\ell)}{\#\mathrm{Sp}_{2s}(\mathbb{F}_\ell)}\\&=\sum_{\substack{r+s=g\\1\leq r\leq g-1}}\frac{\ell^{r^2-r}}{\#\,\mathrm{GL}_r(\mathbb{F}_\ell)}\left(1-\frac{T(s,\gamma,\mathbb{F}_\ell)}{\#\mathrm{Sp}_{2s}(\mathbb{F}_\ell)}\right)+\frac{\ell^{g^2-g}}{\#\,\mathrm{GL}_g(\mathbb{F}_\ell)}.\end{aligned}$$

Now, for any $j \geq 1$, $\ell^j - 1 \geq (\ell-1)\ell^{j-1}$. Thus,

$$\begin{aligned}\frac{\ell^{r^2-r}}{\#\,\mathrm{GL}_r(\mathbb{F}_\ell)} &= \frac{\ell^{r^2-r}}{\ell^{\frac{r(r-1)}{2}}\prod_{j=1}^r(\ell^j-1)} \\ &\leq \frac{\ell^{\frac{r(r-1)}{2}}}{\prod_{j=1}^r \ell^{j-1}(\ell-1)} \\ &= \frac{1}{(\ell-1)^r}.\end{aligned}$$

Higher order terms – those coming from $r > 2$ – contribute less than $O((\tau^\gamma_{(\mathsf{E}),g})^3)$ to $T(g,\gamma,\mathbb{F}_\ell)$; the lemma is proved. □

3.2. An intricate condition. Fix as before a dimension g, and consider $W^\gamma_{(\mathsf{R}),g} \subset \mathrm{GSp}^\gamma_{2g}(\mathbb{F}_\ell)$, the set of all elements A whose characteristic polynomial $f_A(x)$ satisfies the following condition:

(R) Pairs of distinct roots of $f(x)$ over $\bar{\mathbb{F}}_\ell$ do not multiply to 1; $f(x)$ has at most a single root at -1; and $f(x)$ has at most a double root at 1.

While $W^\gamma_{(\mathsf{R}),g}$ is presumably amenable to analysis in the style of Lemma 3.3, we content ourselves with the following, coarser estimate.

Lemma 3.4. *If $\gamma \neq 1$, then there is a constant $C(g)$ depending only on g such that*

$$\frac{\#W^\gamma_{(\mathsf{R}),g}(\mathbb{F}_\ell)}{\#\mathrm{Sp}_{2g}(\mathbb{F}_\ell)} \geq \left(1-\frac{C(g)}{\ell}\right)\left(\frac{\ell}{\ell+1}\right)^{2g^2+g}.$$

Proof. Fix a $\gamma \in \mathbb{F}_\ell^\times$. In fact, assume $\gamma \neq 1$; for otherwise, $W^\gamma_{(\mathsf{R}),g} = \emptyset$. Consider the space $\Xi^\gamma_g \cong \mathbb{A}^g$ of characteristic polynomials of elements of GSp^γ_{2g}. By considering successively the requirements for a point in Ξ^γ_g to satisfy (R), we will show that (R) is a Zariski open condition.

The first condition is that $f(x)$ and $f(1/x)$ have no common root. This is clearly an open condition, as it is equivalent to the disjointness of Spec $\frac{\mathbb{F}_\ell[x]}{f(x)}$ and Spec $\frac{\mathbb{F}_\ell[x]}{f(1/x)}$ inside Spec $\mathbb{F}_\ell[x] \cong \mathbb{A}^1_{\mathbb{F}_\ell}$. The second condition says that at least one of $f(-1)$ and $f'(-1)$ is nonzero; and the final condition says that at least one of $f(1)$, $f'(1)$, and $f''(1)$ is nonzero.

It is clear that $\Psi^\gamma_{(\mathsf{R}),g}$ is nonempty if and only if $\gamma \neq 1$. So there is a constant $C(g)$, depending on g but not on ℓ, such that

$$\#\Psi^\gamma_{(\mathsf{R}),g}(\mathbb{F}_\ell) \geq \ell^g - C(g)\ell^{g-1}.$$

Invoking 2.4 now proves the lemma. □

4. (FM) holds generically

Following the abstract situation at the end of Section 2, say that an abelian variety X over a finite field k has (N) if it *does not* have a rational ℓ-torsion point over k. Say that X/k has (R) if its characteristic polynomial of Frobenius, taken modulo ℓ, satisfies (R) as in Section 3.2. Recall that a curve has (N) or (R) if its Jacobian does, and that a function field has such a property if its proper, smooth model does.

Theorem 4.1. *If a function field satisfies* (N) *or* (R)*, then it satisfies* (FM)*.*

Proof. If the function field satisfies (N), then we know that ℓ does not divide the class number of the function field. We thus have the conditions of Theorem 2 of [10], which shows that the function field satisfies (FM). On the other hand if the function field satisfies (R), then we are in the situation of Remark 4.10 of [10], and again the function field satisfies (FM). □

We will now see that, in some sense, most function fields fall under the aegis of 4.1.

Theorem 4.2. *Let* $\mathcal{C} \to \mathcal{M} \to \operatorname{Spec} k_0$ *be a smooth, irreducible, proper family of proper curves of genus* $g \geq 1$ *with full* ℓ*-monodromy. Fix a* $\gamma \in \mathbb{F}_\ell^\times$*. Let* $\{k_n\}$ *be a collection of extensions of* k_0 *such that* $\lim_{n\to\infty} \#k_n = \infty$*, and, for all* n*,* $\gamma(k_n) = \gamma$*. For* $\bullet = (\mathsf{N}), (\mathsf{R})$*,*

$$\lim_{n\to\infty} \frac{\#\{x \in \mathcal{M}(k_n) : \mathcal{P}^\gamma_\bullet(\mathcal{C}_x)\}}{\#\mathcal{M}(k_n)} = \frac{\#W^\gamma_{\bullet,g}(\mathbb{F}_\ell)}{\#\mathrm{Sp}_{2g}(\mathbb{F}_\ell)} = \sigma^\gamma_{\bullet,g}.$$

There are constants $C^\gamma_{\bullet,g}$*, independent of* ℓ*, such that:*

$$\sigma^1_{(\mathsf{R}),g} = 0;$$

$$\sigma^\gamma_{(\mathsf{R}),g} \geq \left(1 - \frac{C^\gamma_{(\mathsf{R}),g}}{\ell}\right)\left(\frac{\ell}{\ell+1}\right)^{2g^2+g} \quad \textit{if } \gamma \neq 1;$$

$$\left|\sigma^\gamma_{(\mathsf{N}),g} - \tau^\gamma_{(\mathsf{N}),g}\right| \leq C^\gamma_{(\mathsf{N}),g}(1-\tau^\gamma_{(\mathsf{N}),g})^3 = O\left(\frac{1}{\ell^3}\right);$$

$$\tau^1_{(\mathsf{N}),g} = 1 - \frac{\ell}{\ell^2-1};$$

$$\tau^\gamma_{(\mathsf{N}),g} = 1 - \frac{1}{\ell-1} \quad \textit{if } \gamma \neq 1.$$

Proof. By 2.1, the proportion of curves with either property (N) or (R) converges to $\sigma^\gamma_{\bullet,g}$, the appropriate proportion of elements of $\mathrm{GSp}^\gamma_{2g}(\mathbb{F}_\ell)$. Lemmas 3.3 and 3.4 estimate these values for (N) and (R), respectively. □

The exact same techniques let us compute the proportion of abelian varieties over a finite field which have a rational ℓ-torsion point. For a natural number N, let $\mathcal{A}_{g,N}$ denote the fine moduli scheme of triples (A, λ, ϕ) consisting of an abelian scheme A, a principal polarization λ, and symplectic principal level N structure ϕ.

Proposition 4.3. *Let $N = \ell N' \geq 3$ be a natural number relatively prime to p, and let k_0 be a finite field of characteristic p containing a primitive N^{th} root of unity. Let $\{k_n\}$ be a tower of extensions of k_0 such $\lim_{n\to\infty} \#k_n = \infty$ and, for n sufficiently large, $\#k_n \equiv 1 \bmod \ell$. Then*

$$\lim_{n\to\infty} \frac{\#\{(A,\lambda,\phi) \in \mathcal{A}_{g,N}(k_n) : A[\ell](k_n) \supsetneq \{1\}\}}{\#A_{g,N}(k_n)} = \frac{\ell}{\ell^2 - 1} + O(\frac{1}{\ell^3}),$$

where the constant in the error term $O(\frac{1}{\ell^3})$ depends only on g.

Proof. The proof of 4.2 uses only statements about abelian varieties, and thus applies in this setting, too. Let $\mathcal{G}/\mathcal{A}_{g,N}$ be the sheaf of ℓ-torsion of the universal abelian variety over $\mathcal{A}_{g,N}$. Fix a geometric point $\bar{x} \in \mathcal{A}_{g,N}$ which is the Jacobian of a curve. Since the Torelli locus already has full monodromy (2.2), the image of $\pi_1^{\mathrm{geom}}(\mathcal{A}_{g,N}, \bar{x}) \to \mathcal{G}_{\bar{x}}$ is $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$. Thus, all the machinery exposed in this paper applies, and the result follows. By 2.1, as $\#k_n \to \infty$ the proportion of abelian varieties with a rational ℓ-torsion point approaches the proportion of symplectic matrices with one as an eigenvalue. The latter ratio, or at least its leading term, is computed in 3.3. □

Remark. We would like to comment briefly on the collections of fields $\{k_n\}$ in 4.2 and 4.3. On one hand, the collection of extensions k of k_0 with $\#k \equiv 1 \bmod \ell$ is cofinal, in that any extension of k_0 is a subfield of such a subfield. Thus, it seems natural to take limits over towers of such fields; this explains our choice in 4.3. (It is not hard to adapt the statement for a different $\gamma(k_n)$.)

On the other hand, if $\gamma, \gamma' \neq 1$, then $W^{\gamma}_{(\mathsf{N}),g} = W^{\gamma'}_{(\mathsf{N}),g}$. Thus, in 4.2, the collection of fields $\{k_n\}$ may be generalized to any collection of increasingly large finite extensions of k_0, so long as $\gamma(k_n) \neq 1$ for sufficiently large γ.

Remark. Theorem 4.2 shows that approximately $\frac{\ell-2}{\ell-1}$ of all function fields satisfy (N), and thus (FM). Similarly, roughly $\frac{\ell-1}{\ell}$ of all function fields satisfy (R). In fact, it seems likely that on the order of $1 - \frac{1}{\ell^2}$ function fields satisfy (N) or (R), and that at least this proportion of function fields has (FM). (One could compute this number directly, but at present the relatively modest payoff does not seem to warrant the detailed combinatorics required.) To see this, we argue on the level of characteristic polynomials, using Lemma 2.4 to help us pass from characteristic polynomials to group elements. In 3.4 we showed that (R) is a Zariski open condition on Ξ^{γ}_g. Similarly, one directly sees that (E) is a closed condition on Ξ^{γ}_g since

$f(x) \in \Psi^{\gamma}_{(\mathsf{E}),g}$ if and only if $f(1) = 0$ and that (N) is Zariski open. The closed conditions which trace the complement of $\Psi^{\gamma}_{(\mathsf{R}),g}$ and $\Psi^{\gamma}_{(\mathsf{N}),g}$ are independent, and $\Psi^{\gamma}_{(\mathsf{N})\text{ or }(\mathsf{R}),g}$ is the complement of a closed set of codimension two in Ξ^{γ}_{g}. If proportions of characteristic polynomials are directly reflected in proportions of elements of the symplectic group, then about $1 - \frac{1}{\ell^2}$ function fields satisfy (N) or (R).

References

[1] N. Boston, *Some cases of the Fontaine-Mazur conjecture, II.* J. Number Theory **75** (1999), 161–169.

[2] 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.

[3] A. J. de Jong, *A conjecture on arithmetic fundamental groups.* Israel J. Math. **121** (2001), 61–84.

[4] P. Deligne, *La conjecture de Weil. II.* Hautes Études Sci. Publ. Math. **52** (1980), 137–252.

[5] P. Deligne, D. Mumford, *The irreducibility of the space of curves of given genus.* Inst. Hautes Études Sci. Publ. Math. **36** (1969), 75–109.

[6] J. Dixon, M. P. F. du Sautoy, A. Mann, D. Segal, *Analytic Pro-p Groups.* London Math. Soc. Lecture Note Series. **157** (1991).

[7] T. Ekedahl, *The action of monodromy on torsion points of Jacobians.* Arithmetic algebraic geometry (Texel, 1989). Birkhäuser Boston (1991), 41–49.

[8] J.-M. Fontaine, B. Mazur, *Geometric Galois representations.* J. Coates and S.-T. Yau, editors, Elliptic Curves, Modular Forms, & Fermat's Last Theorem, Series in Number Theory **1** (1995), 41–78.

[9] G. Frey, E. Kani, H. Völklein, *Curves with infinite K-rational geometric fundamental group.* H. Völklein, D. Harbater, P. Müller, and J. G. Thompson, editors, Aspects of Galois theory (Gainesville, FL, 1996), London Mathematical Society Lecture Note Series **256**, 85–118.

[10] J. Holden, *On the Fontaine-Mazur Conjecture for number fields and an analogue for function fields.* J. Number Theory **81** (2000), 16–47.

[11] Y. Ihara, *On unramified extensions of function fields over finite fields.* Y. Ihara, editor, Galois Groups and Their Representations, Adv. Studies in Pure Math. **2** (1983), 89–97.

[12] N. M. Katz, P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy.* American Mathematical Society, 1999.

Jeffrey D. Achter
Department of Mathematics
Columbia University
New York, NY 10027, USA
E-mail : achter@math.columbia.edu

Joshua Holden
Department of Mathematics
Rose-Hulman Institute of Technology
Terre Haute, IN 47803, USA
E-mail : holden@rose-hulman.edu