

On the probability of having rational ℓ -isogenies

Jeffrey D. Achter and Daniel Sadornil

Abstract. We calculate the chance that an elliptic curve over a finite field has a specified number of ℓ -isogenies which emanate from it. We give a partial answer for abelian varieties of arbitrary dimension.

Mathematics Subject Classification (2000). 11G20; 14K02.

Keywords. elliptic curve, isogeny, abelian variety, finite field.

1. Introduction

Suppose E and E' are elliptic curves over a field K . A (K -rational) isogeny is a morphism $\phi : E \rightarrow E'$, defined over K , which takes the identity element of E to that of E' ; such a morphism is necessarily a group homomorphism. Let $\epsilon(E, \ell, K)$ be the number of K -rational isogenies (up to isomorphism) of degree ℓ which emanate from E . In this paper we analyze the distribution of $\epsilon(E, \ell, \mathbb{F}_q)$ as E ranges over all elliptic curves over the finite field \mathbb{F}_q .

Isogenies of prime order ℓ have algorithmic significance. For example, much information about the trace of Frobenius t_E of an elliptic curve E/\mathbb{F}_q is encoded in $\epsilon(E, \ell, \mathbb{F}_q)$. Indeed, let $m_E = t_E^2 - 4q$, and suppose that E is ordinary with $j(E) \notin \{0, 1728\}$, so that $\text{Aut}_{\mathbb{F}_q}(E) = \{\pm 1\}$. If $(\frac{m_E}{\ell}) = 1$, then $\epsilon(E, \ell, \mathbb{F}_q) = 2$; if $(\frac{m_E}{\ell}) = -1$, then $\epsilon(E, \ell, \mathbb{F}_q) = 0$; and if $m_E \equiv 0 \pmod{\ell}$, then $\epsilon(E, \ell, \mathbb{F}_q) \in \{1, \ell + 1\}$. This is exploited in various algorithms for counting $|E(\mathbb{F}_q)|$ such as the Schoof-Elkies-Atkin method (e.g., [4, 6]). Related work gives algorithms for *constructing* isogenies of given degree [7].

With this backdrop, we pose the following question: If an elliptic curve is drawn at random among all elliptic curves over a finite field, what is the probability that it admits a rational isogeny of order ℓ ? A special case of our main result says the following:

Theorem. *Suppose $\text{char}(\mathbb{F}_q) \neq 2$ and ℓ is an odd prime relatively prime to q . Let $\mathcal{M}_{\text{Leg}}(\mathbb{F}_q) = \mathbb{F}_q - \{0, 1\}$, and for $\lambda \in \mathcal{M}_{\text{Leg}}(\mathbb{F}_q)$ let $\mathcal{E}_{\text{Leg}, \lambda}$ be the elliptic curve with*

affine model $y^2 = x(x-1)(x-\lambda)$. Define

$$\omega_{\mathcal{E}_{\text{Leg}} \rightarrow \mathcal{M}_{\text{Leg}}}(\ell, r, \mathbb{F}_q) := \frac{|\{\lambda \in \mathcal{M}_{\text{Leg}}(\mathbb{F}_q) : \epsilon(\mathcal{E}_{\text{Leg}, \lambda}, \ell, \mathbb{F}_q) = r\}|}{|\mathcal{M}_{\text{Leg}}(\mathbb{F}_q)|}.$$

Then

$$\left| \omega_{\mathcal{E}_{\text{Leg}} \rightarrow \mathcal{M}_{\text{Leg}}}(\ell, r, \mathbb{F}_q) - \gamma(\ell, r, q) \right| < \frac{4\ell(\ell^2 - 1)}{\sqrt{q}},$$

where $\gamma(\ell, r, q)$ is given in (2.2).

(This is a restatement of Theorem 2.3 for the Legendre family, using the remarks in 2.1 and 2.5.) The quantity $\gamma(\ell, r, q)$ is purely group-theoretic, and depends only on the combinatorics of $\text{GL}_2(\mathbb{Z}/\ell)$.

We prove something similar for sufficiently general families of abelian varieties arbitrary dimension (Proposition 3.4). Here, the isogeny statistics are controlled by the group of symplectic similitudes $\text{GSp}_{2g}(\mathbb{Z}/\ell)$. The combinatorics of $\text{GSp}_{2g}(\mathbb{Z}/\ell)$ are more intricate than those of $\text{GL}_2(\mathbb{Z}/\ell)$, and we are only able to give an exact formula for the chance that an abelian variety admits *no* isogenies of degree ℓ (Proposition 3.6).

It is tempting, but quite difficult, to use the trace of Frobenius to prove Theorem 2.3 directly. If traces of elliptic curves were equidistributed on the Hasse interval, one could use the relationship between m_E and $\epsilon(E, \ell, \mathbb{F}_q)$ to estimate $\omega(\ell, r, \mathbb{F}_q)$. It is the (conjugacy class of the) Frobenius element in $\text{Aut}(E[\ell](\mathbb{F}_q)) \cong \text{GL}_2(\mathbb{Z}/\ell)$, rather than its trace, which is equidistributed. This is the key to our proof of Theorem 2.3.

We thank the referee for helpful comments.

2. Elliptic curves

If E/\mathbb{F} is an elliptic curve, let $\epsilon(E, \ell, \mathbb{F})$ be the number of \mathbb{F} -isogenies of order ℓ which emanate from E , where we identify isogenies up to isomorphism of the target. Differently put, we identify \mathbb{F} -isogenies $\alpha_1 : E \rightarrow E_1$ and $\alpha_2 : E \rightarrow E_2$ if there exists an \mathbb{F} -isomorphism $\beta : E_1 \rightarrow E_2$ such that $\alpha_2 = \beta \circ \alpha_1$. Our intention is to study the distribution of $\epsilon(E, \ell, \mathbb{F})$ for varying E ; speaking of distributions makes sense only once we have chosen an appropriate sample space. To this end, let \mathcal{M}/\mathbb{F} be a smooth absolutely irreducible variety over a finite field, and let $\mathcal{E} \rightarrow \mathcal{M}$ be a non-isotrivial relative elliptic curve. (The “non-isotrivial” condition means that the j -invariant of this family is not constant.)

Example 2.1. Suppose $\text{char}(\mathbb{F}) \neq 2$. The Legendre family is $\mathcal{E}_{\text{Leg}} \rightarrow \mathcal{M}_{\text{Leg}}$, where $\mathcal{M}_{\text{Leg}} = \mathbb{P}^1 - \{0, 1, \infty\}$, and the fiber of \mathcal{E}_{Leg} over $\lambda \in \mathcal{M}_{\text{Leg}}(\mathbb{F})$ is the elliptic curve with affine model $y^2 = x(x-1)(x-\lambda)$. The j -invariant of this family, $256(\lambda^2 - \lambda + 1)^3 / \lambda^2(\lambda - 1)^2$, is a non-constant function on \mathcal{M}_{Leg} .

For any $r \in \mathbb{Z}_{\geq 0}$ and any finite extension \mathbb{F}_q of \mathbb{F} , let

$$\omega_{\mathcal{E} \rightarrow \mathcal{M}}(\ell, r, \mathbb{F}_q) := \frac{|\{x \in \mathcal{M}(\mathbb{F}_q) : \epsilon(\mathcal{E}_x, \ell, \mathbb{F}_q) = r\}|}{|\mathcal{M}(\mathbb{F}_q)|}.$$

We will see that for almost all ℓ , this value is close to

$$\gamma(\ell, r, q) := \frac{|\{x \in \mathrm{GL}_2(\mathbb{Z}/\ell) : \det(x) \equiv q \pmod{\ell}, x \text{ fixes exactly } r \text{ subspaces of dimension one}\}|}{|\mathrm{SL}_2(\mathbb{Z}/\ell)|}. \quad (2.1)$$

Lemma 2.2. *Suppose ℓ is odd and relatively prime to q . Then*

$$\gamma(\ell, r, q) = \begin{cases} \frac{\ell - \left(\frac{q}{\ell}\right)}{2(\ell+1)} & r = 0 \\ \frac{1 + \left(\frac{q}{\ell}\right)}{\ell} & r = 1 \\ \frac{\ell - 2 - \left(\frac{q}{\ell}\right)}{2(\ell-1)} & r = 2 \\ \frac{1 + \left(\frac{q}{\ell}\right)}{\ell^3 - \ell} & r = \ell + 1 \\ 0 & \text{otherwise} \end{cases} \quad (2.2)$$

where $\left(\frac{q}{\ell}\right)$ is the quadratic character of q modulo ℓ . Moreover, $\gamma(2, 0, 1) = 1/3$; $\gamma(2, 1, 1) = 1/2$; $\gamma(2, 3, 1) = 1/6$; and $\gamma(2, r, 1) = 0$ for all other r .

Proof. (Compare [8, Lemma 4.1].) Since $\gamma(2, r, 1)$ may be calculated by examining each element of $\mathrm{GL}_2(\mathbb{Z}/2)$, we henceforth assume ℓ odd. In Table 1 we have partitioned conjugacy classes of GL_2 according to the structure of their eigenspaces. The four rows correspond to, respectively, elements which are semisimple with no eigenvalues in \mathbb{Z}/ℓ ; not semisimple; semisimple with distinct eigenvalues defined over \mathbb{Z}/ℓ ; and semisimple with a single eigenvalue. For each class we describe the centralizer of a representative element; calculate the size of each conjugacy class; and list the number of subspaces of dimension one of $(\mathbb{Z}/\ell)^2$ which are stable under an element of a conjugacy class. Then $\gamma(\ell, r, q)$ is readily computed using this data. For example, there are $\frac{\ell - 2 - \left(\frac{q}{\ell}\right)}{2}$ conjugacy classes in $\mathrm{GL}_2(\mathbb{Z}/\ell)$ with determinant q and distinct, \mathbb{Z}/ℓ -rational eigenvalues, and the size of each conjugacy class is $|\mathrm{GL}_2(\mathbb{Z}/\ell)|/(\ell-1)^2$. Dividing the size of such a conjugacy class by $|\mathrm{SL}_2(\mathbb{Z}/\ell)|$ yields the calculation of $\gamma(\ell, 2, q)$ in (2.2); $\gamma(\ell, r, q)$ for other values of r are computed analogously. \square

The following result says that for the typical family $\mathcal{E} \rightarrow \mathcal{M}$ of elliptic curves, $\omega_{\mathcal{E} \rightarrow \mathcal{M}}(\ell, r, \mathbb{F}_q) \approx \gamma(\ell, r, q)$, where the right-hand side is calculated in Lemma 2.2.

Theorem 2.3. *Let \mathcal{M} be a smooth absolutely irreducible variety over a finite field \mathbb{F} , and let $\mathcal{E} \rightarrow \mathcal{M}$ be a non-isotrivial relative elliptic curve.*

representative	centralizer	size of class	stable subspaces
$\begin{pmatrix} \lambda & \mu \\ \delta\mu & \lambda \end{pmatrix} \delta \notin ((\mathbb{Z}/\ell)^\times)^2$	$\begin{pmatrix} a & b \\ \delta b & a \end{pmatrix}$	$\ell^2 - \ell$	0
$\begin{pmatrix} \lambda & 1 \\ \lambda & \lambda \end{pmatrix}$	$\begin{pmatrix} a & b \\ a & a \end{pmatrix}$	$\ell^2 - 1$	1
$\begin{pmatrix} \lambda & \\ & \mu \end{pmatrix} \lambda \neq \mu$	$\begin{pmatrix} * & \\ & * \end{pmatrix}$	$\ell^2 + \ell$	2
$\begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix}$	$\begin{pmatrix} * & * \\ * & * \end{pmatrix}$	1	$\ell + 1$

TABLE 1. Conjugacy classes in GL_2

- a. For all but finitely many ℓ there exists a constant $B_\ell = B(\mathcal{E} \rightarrow \mathcal{M}, \ell)$ such that for all finite extensions \mathbb{F}_q/\mathbb{F} ,

$$|\omega_{\mathcal{E} \rightarrow \mathcal{M}}(\ell, r, \mathbb{F}_q) - \gamma(\ell, r, q)| < \frac{B_\ell}{\sqrt{q}}. \quad (2.3)$$

- b. There exists a constant B_0 such that for all but finitely many ℓ with $|\mathrm{SL}_2(\mathbb{Z}/\ell)|$ relatively prime to $\mathrm{char}(\mathbb{F})$, one may take $B_\ell = B_0 |\mathrm{SL}_2(\mathbb{Z}/\ell)|$ in inequality (2.3).

Remark 2.4. This shows that the chance an elliptic curve chosen at random from the family $\mathcal{E} \rightarrow \mathcal{M}$ admits an isogeny of degree ℓ is about $1 - \gamma(\ell, 0, q) \approx 1/2$. Note, however, that the *expected number* of isogenies of degree ℓ emanating from a member of this family is close to $\sum_r r\gamma(\ell, r, q) = 1$. This reflects the fact that the “relative moduli space” of fibers of $\mathcal{E} \rightarrow \mathcal{M}$ equipped with an isogeny of degree ℓ is an absolutely irreducible variety whose dimension is the same as that of \mathcal{M} .

Proof of Theorem 2.3. Fix a base point $s \in \mathcal{M}(\bar{\mathbb{F}})$. Since $\mathcal{E} \rightarrow \mathcal{M}$ is not isotrivial, for all but finitely many primes ℓ , the geometric monodromy representation $\pi_1(\mathcal{M} \times \bar{\mathbb{F}}, s) \rightarrow \mathrm{Aut}(\mathcal{E}_s[\ell])$ has image $\mathrm{SL}_2(\mathbb{Z}/\ell)$ (e.g., [2, Lemma 2.2]). Let ℓ be any such prime; the family is said to be general at ℓ .

The presence of ℓ -isogenies emanating from E/\mathbb{F}_q is controlled by the \mathbb{F}_q -structure of $E[\ell](\bar{\mathbb{F}}_q)$, which in turn is described by the action of Frobenius $\sigma_{\ell, E, \mathbb{F}_q} \in \mathrm{Aut}(E[\ell](\bar{\mathbb{F}}_q))$. After an identification $E[\ell](\bar{\mathbb{F}}_q) \cong (\mathbb{Z}/\ell)^2$, we may regard $\sigma_{\ell, E, \mathbb{F}_q}$ as an element of $\mathrm{GL}_2(\mathbb{Z}/\ell)$, well-defined up to conjugacy. Since we identify isogenies which differ by an isomorphism of the target, the ℓ -isogenies emanating from E are in bijection with subgroups of $E[\ell](\bar{\mathbb{F}}_q)$ of order ℓ which are stable under $\sigma_{\ell, E, \mathbb{F}_q}$ ([14, III.4.13.2]; see also Lemma 3.1 below).

For any union of conjugacy classes $W \subset \mathrm{GL}_2(\mathbb{Z}/\ell)$ and any $a \in \mathbb{Z}/\ell^\times$, let $W^{(a)} = \det^{-1}(a) \cap W$ be the subset of elements with determinant a . A special case of an equidistribution theorem of Katz [10, 9.6.10 and 9.7.13] states that there

exists a constant B_ℓ such that

$$\left| \frac{|\{x \in \mathcal{M}(\mathbb{F}_q) : \sigma_{\ell, \mathcal{E}_x, \mathbb{F}_q} \in W\}|}{|\mathcal{M}(\mathbb{F}_q)|} - \frac{W^{(q)}}{|\mathrm{SL}_2(\mathbb{Z}/\ell)|} \right| < \frac{B_\ell}{\sqrt{q}}.$$

(See also [1, 5] for an explanation of Katz's theorem in this context.) In particular, we have

$$|\omega_{\mathcal{E} \rightarrow \mathcal{M}}(\ell, r, \mathbb{F}_q) - \gamma(\ell, r, q)| < \frac{B_\ell}{\sqrt{q}}.$$

This proves (a). Part (b) follows immediately from Kowalski's complement [11, Prop. 4.7] to Katz's theorem. \square

Example 2.5. If $\mathcal{E} \rightarrow \mathcal{M}$ globally admits an isogeny of order ℓ , then the family is not general at ℓ . For example, the full two-torsion subgroup of $\mathcal{E}_{\mathrm{Leg}}$ is defined over the base $\mathcal{M}_{\mathrm{Leg}}$, and $\mathcal{E}_{\mathrm{Leg}} \rightarrow \mathcal{M}_{\mathrm{Leg}}$ is not general at $\ell = 2$. In fact, the Legendre family of elliptic curves is general at ℓ for each odd prime ℓ which is invertible in the base field. Moreover, since the base $\mathcal{M}_{\mathrm{Leg}}$ is isomorphic to $\mathbb{P}^1 - \{0, 1, \infty\}$ and thus has Euler characteristic -1 , and since the sheaf of ℓ -torsion is tamely ramified and of rank 2, one may take $B(\mathcal{E}_{\mathrm{Leg}} \rightarrow \mathcal{M}_{\mathrm{Leg}}, \ell) = B_{\mathrm{Leg}} = 2 \cdot (-(-1)) \cdot 2 = 4$ in (2.3) [10, 9.2.5].

3. Abelian varieties

One can use a similar framework to study ℓ -isogenies emanating from abelian varieties over a finite field. Let X/\mathbb{F} be an abelian variety over a finite field, and let $\epsilon(X, \ell, \mathbb{F})$ be the number of \mathbb{F} -isogenies of order ℓ which emanate from X , where as before we identify two isogenies if they differ by an isomorphism of the target.

Lemma 3.1. *Let X/\mathbb{F} be an abelian variety over a finite field. Then $\epsilon(X, \ell, \mathbb{F})$ is equal to the number of one-dimensional subspaces of $X[\ell](\overline{\mathbb{F}}) \cong (\mathbb{Z}/\ell)^{2 \dim X}$ which are stabilized by the Frobenius $\sigma_{\ell, X, \mathbb{F}}$.*

Proof. By descent, the one-dimensional subspaces of $X[\ell](\overline{\mathbb{F}})$ stable under Frobenius are precisely the \mathbb{F} -rational sub-group schemes of X of order ℓ , which are the group schemes which are kernels of \mathbb{F} -rational isogenies of order ℓ which emanate from X . By [12, p.72, Thm. 4], isogenies up to isomorphism of the target are classified by their kernels. \square

Now let \mathcal{M}/\mathbb{F} be a smooth absolutely irreducible variety over a finite field, and let $\mathcal{X} \rightarrow \mathcal{M}$ be a principally polarized abelian scheme of relative dimension g over \mathcal{M} , i.e., a family of principally polarized abelian varieties parametrized by \mathcal{M} . If $s \in \mathcal{M}(\overline{\mathbb{F}})$ is a geometric point, there is a natural representation $\pi_1(\mathcal{M} \times \overline{\mathbb{F}}, s) \rightarrow \mathrm{Aut}(\mathcal{X}[\ell]_s)$. The image of this representation is contained in $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell)$,

and we say that the family $\mathcal{X} \rightarrow \mathcal{M}$ is general at ℓ if the image is the full symplectic group.

For example, if $\mathcal{C} \rightarrow \mathcal{M}$ is a versal family of smooth proper curves of genus g , then the relative Picard variety $\text{Pic}^0(\mathcal{C}) \rightarrow \mathcal{M}$ is general at ℓ for all but finitely many ℓ [2, Lemma 2.2]. The space of hyperelliptic curves of fixed genus is a natural, but nontrivial, example:

Example 3.2. Fix a natural number $g \geq 2$ and a finite field \mathbb{F} with $\text{char}(\mathbb{F})$ odd, and let $\mathcal{H}_{2g+2}/\mathbb{F}$ be the space of monic separable polynomials of degree $2g+2$. Let $\mathcal{C}_g \rightarrow \mathcal{H}_{2g+2}$ be the relative smooth proper curve whose fiber over $f(x) \in \mathcal{H}_{2g+2}(\overline{\mathbb{F}})$ is the hyperelliptic curve with affine model $y^2 = f(x)$. Let $\mathcal{X}_g = \text{Pic}^0(\mathcal{C}_g)$ be the relative Picard variety. For each odd ℓ invertible in \mathbb{F} , $\mathcal{X}_g \rightarrow \mathcal{H}_{2g+2}$ is general at ℓ . (This has been proved independently by Yu (unpublished; see [5, Ex. 2.4]); by the first author and Pries [3, Thm. 3.4]; and by Hall [9, Thm. 4.1].)

Consider the group $\text{GSp}_{2g}(\mathbb{Z}/\ell)$, the group of symplectic similitudes over \mathbb{Z}/ℓ , in its natural representation. Each element $x \in \text{GSp}_{2g}(\mathbb{Z}/\ell)$ has a ‘‘multiplier’’ $\text{mult}(x) \in (\mathbb{Z}/\ell)^\times$. For $a \in (\mathbb{Z}/\ell)^\times$, let $\text{GSp}_{2g}(\mathbb{Z}/\ell)^{(a)} = \text{mult}^{-1}(a)$. Define

$$\gamma_g(\ell, r, q) := \frac{\left| \{x \in \text{GSp}_{2g}(\mathbb{Z}/\ell)^{(q)} : x \text{ stabilizes exactly } r \text{ subspaces of dimension one}\} \right|}{\left| \text{Sp}_{2g}(\mathbb{Z}/\ell) \right|}. \quad (3.1)$$

(Recall that $\text{Sp}_2 \cong \text{SL}_2$, so that $\gamma_1(\ell, r, q) = \gamma(\ell, r, q)$.)

Remark 3.3. Suppose $x \in \text{GSp}_{2g}(\mathbb{Z}/\ell)$. Each one-dimensional space stable under x is contained in some \mathbb{Z}/ℓ -rational eigenspace of x . For $\lambda \in (\mathbb{Z}/\ell)^\times$, let $d(x, \lambda) = \dim \ker(x - \lambda)$. Then the number of one-dimensional spaces stabilized by x is

$$\sum_{\lambda \in (\mathbb{Z}/\ell)^\times} \left| \mathbb{P}^{d(x, \lambda) - 1}(\mathbb{Z}/\ell) \right|,$$

where we adopt the convention that $\mathbb{P}^{-1}(\mathbb{Z}/\ell)$ is the empty set. This observation generalizes the fact that $\gamma_1(\ell, r, q) = 0$ if $r \notin \{0, 1, 2, \ell + 1\}$.

The following result is a natural generalization of Theorem 2.3 to higher dimension.

Proposition 3.4. *Let \mathcal{M} be a smooth absolutely irreducible variety over a finite field \mathbb{F} , and let $\mathcal{X} \rightarrow \mathcal{M}$ be a principally polarized abelian scheme of relative dimension g . Suppose that ℓ is a rational prime invertible in \mathbb{F} , and that $\mathcal{X} \rightarrow \mathcal{M}$ is general at ℓ . There exists a constant $B = B(\mathcal{X} \rightarrow \mathcal{M}, \ell)$ such that for each finite extension \mathbb{F}_q/\mathbb{F} ,*

$$\left| \omega_{\mathcal{X} \rightarrow \mathcal{M}}(\ell, r, \mathbb{F}_q) - \gamma_g(\ell, r, q) \right| < \frac{B}{\sqrt{q}}. \quad (3.2)$$

Proof. The proof is quite similar to that of Theorem 2.3. By Lemma 3.1, $\omega_{\mathcal{X} \rightarrow \mathcal{M}}(\ell, r, \mathbb{F}_q)$ is the proportion of elements $s \in \mathcal{M}(\mathbb{F}_q)$ for which the Frobenius element $\sigma_{\ell, \mathcal{X}_s, \mathbb{F}_q} \in \text{Aut}(\mathcal{X}_s[\ell](\overline{\mathbb{F}}_q))$ stabilizes exactly r one-dimensional subspaces. Katz's theorem [10, 9.6.10], combined with the hypothesis that $\mathcal{X} \rightarrow \mathcal{M}$ is general at ℓ , means that Frobenius elements of fibers \mathcal{X}_s ($s \in \mathcal{M}(\mathbb{F}_q)$) are approximately equidistributed in $\text{mult}^{-1}(q) \subset \text{GSp}_{2g}(\mathbb{Z}/\ell)$, with an error term of the form B/\sqrt{q} for some constant B . By construction, $\gamma_g(\ell, r, q)$ is the number of elements of $\text{mult}^{-1}(q)$ which stabilize exactly r one-dimensional subspaces in the natural representation. \square

Example 3.5. Suppose that $\text{char}(\mathbb{F})$ is relatively prime to $|\text{Sp}_{2g}(\mathbb{Z}/\ell)|$. In the special case of the family of hyperelliptic curves $\mathcal{C}_g \rightarrow \mathcal{H}_{2g+2}$, by [1, Thm. 3.1] one may take $B = 2(2g+1)!|\text{Sp}_{2g}(\mathbb{Z}/\ell)|$ for the constant in (3.2).

Explicit calculation of $\gamma_g(\ell, r, q)$ seems difficult. Still, the beautiful work of Neumann and Praeger on “eigenvalue-free” elements of classical groups over finite fields [13] lets us calculate $\gamma_g(\ell, 0, q)$. In what follows, we follow the method (and, where possible, the notation) of [13]. Define the generating function

$$G(y, z) := \prod_{i \geq 1} (1 - y^{-i}z).$$

For each $a \in (\mathbb{Z}/\ell)^\times$, define the generating function

$$\Gamma(\ell, a, z) := \sum_{g \geq 0} \gamma_g(\ell, 0, a) z^g.$$

Proposition 3.6. *If ℓ is odd, then there is an equality of generating functions*

$$\Gamma(\ell, a, z) = (1-z)^{-1} G(\ell^2; \ell z)^{1 + \binom{a}{\ell}} G(\ell; z)^{(\ell - \binom{a}{\ell} - 2)/2},$$

while $\Gamma(2, 1, z) = (1-z)^{-1} G(4; 2z)$.

Proof. We follow the proof of [13, Thm. 5.1], which is the special case $a = 1$ of Proposition 3.6. Let $u(\text{GL}, m, \ell)$ be the proportion of elements of $\text{GL}_m(\mathbb{Z}/\ell)$ which are unipotent, and let $u(\text{Sp}, m, \ell)$ be the proportion of elements of $\text{Sp}_{2m}(\mathbb{Z}/\ell)$ which are unipotent. Define generating functions

$$U(\text{GL}, \ell, z) := \sum_{m \geq 0} u(\text{GL}, m, \ell) z^m$$

$$U(\text{Sp}, \ell, z) := \sum_{g \geq 0} u(\text{Sp}, g, \ell) z^g.$$

In fact, one has $U(\text{GL}, \ell, z) = G(\ell, z)^{-1}$ and $U(\text{Sp}, \ell, z) = G(\ell^2, \ell z)^{-1}$ [13, Thm. 4.2 and Thm. 5.2]. Therefore, it suffices to verify the equality of generating functions

$$\Gamma(\ell, a, z) = (1-z)^{-1} \cdot U(\text{Sp}, \ell, z)^{-(1 + \binom{a}{\ell})} \cdot U(\text{GL}, \ell, z)^{(2 + \binom{a}{\ell} - \ell)/2}. \quad (3.3)$$

Let $\Theta_a = \{\theta \in (\mathbb{Z}/\ell)^\times : \theta^2 = a\}$, and let Ψ_a be a set of representatives, one from each pair $\{\psi, a\psi^{-1}\}$, of elements of $(\mathbb{Z}/\ell)^\times - \Theta_a$.

Let V be a symplectic space over \mathbb{Z}/ℓ of dimension $2g$, and suppose $x \in \mathrm{GSp}(V)^{(a)} \cong \mathrm{GSp}_{2g}(\mathbb{Z}/\ell)^{(a)}$. Then x uniquely determines an orthogonal decomposition

$$V = \tilde{V} \oplus (\oplus_{\theta \in \Theta_a} V_\theta) \oplus (\oplus_{\psi \in \Psi_a} V_\psi \oplus V_\psi^\vee) \quad (3.4)$$

where V_λ is the generalized λ -eigenspace of x , and where x has no \mathbb{Z}/ℓ -rational eigenvalue on \tilde{V} . In the special case $a = 1$, Neumann and Praeger deduce (3.3) by enumerating all decompositions (3.4), and then counting the possibilities for the action of x on each summand. We briefly explain how to adapt their proof for any $a \in (\mathbb{Z}/\ell)^\times$.

Suppose $\theta \in \Theta_a$. For any r , multiplication by $\theta \cdot \mathrm{id}$ yields a bijection between the set of unipotent elements of $\mathrm{Sp}_{2r}(\mathbb{Z}/\ell)$ and the set of elements of $\mathrm{GSp}_{2r}(\mathbb{Z}/\ell)^{(a)}$ whose only eigenvalue (over the algebraic closure of \mathbb{Z}/ℓ) is θ . Therefore, the proof of [13, Thm. 5.1] shows that there is an equality of generating functions

$$\frac{1}{1-z} = \Gamma(\ell, a, z) \cdot U(\mathrm{Sp}, \ell, z)^{|\Theta_a|} \cdot U(\mathrm{GL}, \ell, z)^{|\Psi_a|}.$$

□

Corollary 3.7. *Suppose ℓ is odd. Then*

$$\lim_{g \rightarrow \infty} \gamma_g(\ell, 0, a) = G(\ell^2, \ell)^{1 + \binom{a}{\ell}} G(\ell, 1)^{(\ell - \binom{a}{\ell}) - 2} / 2 \quad (3.5)$$

$$= \begin{cases} e^{-1/2} (1 - \frac{5}{4}\ell^{-1} + \frac{131}{96}\ell^{-2} - \frac{997}{384}\ell^{-3} + \mathcal{O}(\ell^{-4})) & \binom{a}{\ell} = 1 \\ e^{-1/2} (1 - \frac{1}{4}\ell^{-1} + \frac{11}{96}\ell^{-2} - \frac{89}{384}\ell^{-3} + \mathcal{O}(\ell^{-4})) & \binom{a}{\ell} = -1 \end{cases} \quad (3.6)$$

while $\lim_{g \rightarrow \infty} \gamma_g(2, 0, 1) = G(2^2, 2) \approx 0.4194$.

Proof. Equation (3.5) follows from Proposition 3.6 and [13, Thm. 5.3], as does the identification of $\lim_{g \rightarrow \infty} \gamma_g(2, 0, 1)$. The series expansions (3.6) for $\binom{a}{\ell} = 1$ and $\binom{a}{\ell} = -1$ follow from [13, Thm. 5.4] and from [13, Thm. 4.4] and the binomial theorem, respectively. □

Remark 3.8. Suppose q is large relative to g and ℓ . Roughly speaking, Proposition 3.4 says that the chance that a random abelian variety of dimension g admits no isogeny of order ℓ is close to $\gamma_g(\ell, 0, q)$. If g is large, this probability is close to the limit $\lim_{g \rightarrow \infty} \gamma_g(\ell, 0, q)$ calculated in Corollary 3.7. Nonetheless, suppose $\mathcal{X} \rightarrow \mathcal{M}$ satisfies the hypotheses of Proposition 3.4. Since $\mathcal{X} \rightarrow \mathcal{M}$ is general at ℓ , as in Remark 2.4 the relative moduli space \mathcal{Y} parametrizing fibers of \mathcal{X} equipped with an isogeny of order ℓ is irreducible, and of the same dimension as \mathcal{M} . Therefore, $\lim_{q \rightarrow \infty} |\mathcal{Y}(\mathbb{F}_q)| / |\mathcal{M}(\mathbb{F}_q)| = 1$, and the expected value of $\epsilon(\mathcal{X}_s, \ell, \mathbb{F}_q)$ approaches 1 as q grows large.

References

- [1] J. D. Achter. Results of Cohen-Lenstra type for quadratic function fields. In K. Lauter and K. Ribet, editors, *Computational Arithmetic Geometry*. American Mathematical Society, 2007. in press.
- [2] J. D. Achter and J. Holden. Notes on an analogue of the Fontaine-Mazur conjecture. *Journal de Théorie des Nombres de Bordeaux*, 15(3):627–637, 2003.
- [3] J. D. Achter and R. J. Pries. The integral monodromy of hyperelliptic and trielliptic curves. *Math. Ann.*, 338(1):187–206, 2007.
- [4] I. F. Blake, G. Seroussi, and N. P. Smart. *Elliptic curves in cryptography*, volume 265 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2000. Reprint of the 1999 original.
- [5] N. Chavdarov. The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy. *Duke Math. J.*, 87(1):151–180, 1997.
- [6] M. Fouquet and F. Morain. Isogeny volcanoes and the SEA algorithm. In *Algorithmic number theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 276–291. Springer, Berlin, 2002.
- [7] S. D. Galbraith. Constructing isogenies between elliptic curves over finite fields. *LMS J. Comput. Math.*, 2:118–138 (electronic), 1999.
- [8] E.-U. Gekeler. Frobenius distributions of elliptic curves over finite prime fields. *Int. Math. Res. Not.*, (37):1999–2018, 2003.
- [9] C. Hall. Big symplectic or orthogonal monodromy modulo ℓ . *Duke Math. J.*, 2007. in press, arXiv:math.NT/0608718.
- [10] N. M. Katz and P. Sarnak. *Random matrices, Frobenius eigenvalues, and monodromy*. American Mathematical Society, Providence, RI, 1999.
- [11] E. Kowalski. The large sieve, monodromy and zeta functions of curves. *J. Reine Angew. Math.*, 601:29–69, 2006.
- [12] D. Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay, 1970.
- [13] P. M. Neumann and C. E. Praeger. Derangements and eigenvalue-free elements in finite classical groups. *J. London Math. Soc. (2)*, 58(3):564–586, 1998.
- [14] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.

Jeffrey D. Achter
Department of Mathematics
Colorado State University
Fort Collins, CO 80523
USA
e-mail: j.achter@colostate.edu

Daniel Sadornil
Dpto. Matemáticas
Plaza de la Merced 1
37008 Salamanca
España
e-mail: sadornil@usal.es