Isogeny classes and Frobenius roots statistics for abelian varieties over finite fields

S. G. Vlăduţ*

Let $I(g, q, N)$ be the number of isogeny classes of g-dimensional abelian varieties over a finite field $\mathbf{F}_q$ having a fixed number N of $\mathbf{F}_q$-rational points. We describe the asymptotic (for $q \to \infty$) distribution of $I(g, q, N)$ over possible values of N. We also prove an analogue of the Sato-Tate conjecture for isogeny classes of g-dimensional abelian varieties.

Let g be a fixed positive ineger, A be an abelian variety over a finite field $\mathbf{F}_q$ of dimension g, and let

$$X_{A,q} = \{e^{\pi i \theta_1}, e^{-\pi i \theta_1}, e^{\pi i \theta_2}, \ldots e^{-\pi i \theta_g}\}$$

be the corresponding set of Frobenius eigenvalues,

$$\Theta_{A,v} = (\theta_1, \theta_2, \ldots \theta_g) \in \Sigma_g := \{\theta \in \mathbf{R}^g : \theta_1 \leq \theta_2 \leq \ldots \leq \theta_g\}.$$

One defines the (countable) family $\Xi_g \subset \Sigma_g$ by

$$\Xi_g := \bigcup_{A,q} \Theta_{A,q} \ ,$$

where A runs over *isogeny* classes of g-dimensional abelian varieties over $\mathbf{F}_q$ son that the multiplicity of any element in Ξ_g equals one (i.e., it is just a set, which follows from the Honda-Tate theorem). Our main result on the distribution of the Frobenius roots is

Theorem A. *The set $\Xi_g \subset \Sigma_g$ is uniformly distributed on Σ_g with respect to the probabistic measure*

$$\nu_{g,\infty} := \frac{1}{v_g} \left(\prod_{j<k} (\cos \pi\theta_j - \cos \pi\theta_k) \right) \cdot \prod_i (\sin \pi\theta_i \cdot d\theta_i),$$

Institut de Mathématiques de Luminy, UPR 9016 du CNRS, Luminy, Case 907, 13288, Marseille cedex 9, FRANCE. E-mail: vladut@iml.univ-mrs.fr. This work was supported in part by the RFFI grant 99-01-01204

where the real positive constant v_g *is given by*

$$v_g = \frac{2^g}{g!} \prod_{j=1}^{g} \left(\frac{2j}{2j-1} \right)^{g+1-j} .$$

Other question which we consider is: how many isogeny classes of g-dimensional abelian varieties over a finite field correspond to the given number of rational points?

The question makes sense due to well-known result by A. Weil:

Theorem. *If* A *and* B *are two isogenous abelian varieties over a finite field* $\mathbf{F}_q$ *then*

$$\sharp A(\mathbf{F}_q) = \sharp B(\mathbf{F}_q)$$

We shall investigate this problem asymptotically, for growing q. More precisely, we fix the dimension $g \geq 1$ and for a given prime power q construct a discrete measure $\mu_{g,q}$ on the interval $[-1,1]$ characterizing the distribution of the number of isogeny classes of g-dimensional abelian varieties over N, and then tend q to infinity. It turns out that there exists the limit measure $\mu_{g,\infty}$, it has a continuous density, which can be often calculated explicitly.

Our principal result is

Theorem B. *Let* $g \geq 2$*. The limit measure* $\mu_{g,\infty}$ *on* $[-1,1]$ *is given by*

$$\mu_{g,\infty} = F_g(t)dt,$$

where the function $F_g(t)$ *satisfies the following conditions:*

1. $F_g(t)$ *is continuous, even,* $F_g(-1) = F(1) = 0$*, and* $F_g(t) > 0$ *for* $t \in (-1,1)$;

2. *on each segment* $[-1+\frac{2(i-1)}{g}, -1+\frac{2i}{g}]$, $i = 1, 2, \ldots, g$ *the function* $F_g(t)$ *is given by a polynomial* $P_{g,i}(t) = P_{g,g-i}(-t) \in \mathbf{Q}[t]$ *of degree* $d_{g,i} \leq \frac{(g-1)(g+2)}{2}$;

3. $P_{g,1}(t) = P_{g,g}(-t) = a_g(1-\mid t \mid)^{(g-1)(g+2)/2}$ *with* $a_g \in \mathbf{Q}$;

4. $$\int_{-1}^{1} F_g(t)dt = \frac{2^{g-1}}{g \cdot g!} \prod_{j=1}^{g} \left(\frac{2j}{2j-1} \right)^{g+1-j} .$$