New York Journal of Mathematics

New York J. Math. **25** (2019) 123–144.

Local heuristics and an exact formula for abelian varieties of odd prime dimension over finite fields

Jonathan Gerhard and **Cassandra Williams**

Abstract. Consider a q-Weil polynomial f of degree $2g$. Using an equidistribution assumption that is too strong to be true, we define and compute a product of local relative densities of matrices in $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ with characteristic polynomial $f \mod \ell$ when g is an odd prime. This infinite product is closely related to a ratio of class numbers. When $g = 3$ we conjecture that the product gives the size of an isogeny class of principally polarized abelian threefolds.

Contents

1. Introduction 123
2. Abelian varieties and Weil polynomials 124
3. Conjugacy classes in $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ 127
4. Local factors for f 131
5. Polynomials and primes in K 133
6. Local factors for K 135
7. Matching 135
8. Main results 139
References 143

1. Introduction

This paper is a direct generalization of the work of Achter-Williams [2] to abelian varieties of odd prime dimension, and is guided in philosophy by both Gekeler [4] and Katz [7]. We begin by considering abelian varieties over a finite field $\mathbb{F}_q$, where q is a power of a prime. To each such variety X, we can associate a characteristic polynomial of Frobenius $f_X(T) \in \mathbb{Z}[T]$. A theorem of Tate [11] tells us that two varieties are isogenous if and only if their characteristic polynomials are equal.

Received July 20, 2017.
2010 *Mathematics Subject Classification.* 14K02.
Key words and phrases. abelian varieties, finite fields, matrix groups.

ISSN 1076-9803/2019

Let $\mathcal{A}_g(k)$ denote the moduli space of principally polarized abelian varieties of dimension g over a field k, where each variety is weighted by the size of its automorphism group. Also define $\mathcal{A}_g(\mathbb{F}_q; f)$ to be those members of $\mathcal{A}_g(\mathbb{F}_q)$ with characteristic polynomial $f(T)$. Then $\mathcal{A}_g(\mathbb{F}_q; f)$ denotes the set of isomorphism classes of principally polarized abelian varieties of dimension g over $\mathbb{F}_q$ with characteristic polynomial of Frobenius f, weighted inversely by the size of the automorphism group, and computing $\#\mathcal{A}_g(\mathbb{F}_q; f)$ gives the number of (isomorphism classes of) abelian varieties over $\mathbb{F}_q$ in a particular isogeny class.

The Frobenius endomorphism gives an automorphism of the Tate module $T_\ell X$ (for ℓ not dividing q), so it has a representation as an element of the matrix group $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$. For each ℓ, we define a term $\nu_\ell(f)$ measuring the relative frequency of $f \mod \ell$ as the characteristic polynomial for an element of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$, as well as an archimedean term $\nu_\infty(f)$.

Since (as much as possible) Frobenius elements are equidistributed in $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$, it seems possible that the product of these local densities could at least estimate the value of $\#\mathcal{A}_g(\mathbb{F}_q; f)$. This, of course, is a ridiculous tactic, as the mod ℓ Frobenius elements are only equidistributed when $q \gg_g \ell$. However, as in [2], we again show that this local data does apparently control isogeny class size.

Our main result is as follows. Consider a particular class of q-Weil polynomials f of degree $2g$ (see the next section for details). Let K be the splitting field of f over $\mathbb{Q}$ and K^+ be its maximal totally real subfield, with class numbers h_K and h_{K^+} respectively. A theorem of Everett Howe in the preprint [6], together with the conditions stated in the next section, implies that

$$\#\mathcal{A}_g(\mathbb{F}_q; f) = \frac{h_K}{h_{K^+}}$$

(see Theorem 8.5 and Corollary 8.6). Then an immediate corollary of this theorem and our work is that

$$\nu_\infty(f) \prod_\ell \nu_\ell(f) = \#\mathcal{A}_g(\mathbb{F}_q; f)$$

when $g = 3$ (see Corollary 8.8). (For $g > 3$ an odd prime, there is only a minimal obstruction to this corollary which is explained at the end of section 3.3 and in Remark 8.2.)

2. Abelian varieties and Weil polynomials

Let $X/\mathbb{F}_q$ be an abelian variety of dimension g over a finite field of $q = p^a$ elements, and let $f(T) \in \mathbb{Z}[T]$ be the characteristic polynomial of its Frobenius endomorphism. Then $f(T)$ is a q-Weil polynomial, a polynomial of degree $2g$ with complex roots $\alpha_1, \ldots, \alpha_{2g}$ with $|\alpha_j| = \sqrt{q}$ for every j, where the ordering can be chosen so that $\alpha_j \alpha_{g+j} = q$ for $1 \le j \le g$.

Each q-Weil polynomial $f(T)$ corresponds to a (possibly empty) isogeny class $\mathcal{I}_f$ of abelian varieties of dimension g over $\mathbb{F}_q$. Following [2], we will assume:

(W.1) (*ordinary*) the middle coefficient of f is relatively prime to p;
(W.2) (*principally polarizable*) there exists a principally polarized abelian variety of dimension g with characteristic polynomial f;
(W.3) (*cyclic*) the polynomial $f(T)$ is irreducible over $\mathbb{Q}$, and

$$K_f := \mathbb{Q}[T]/f(T)$$

is Galois, cyclic, and unramified at p;
(W.4) (*maximal*) for π_f a (complex) root of $f(T)$, with complex conjugate $\bar{\pi}_f$, then $\mathcal{O}_f := \mathbb{Z}[\pi_f, \bar{\pi}_f]$, *a priori* an order in K_f, is actually the maximal order $\mathcal{O}_{K_f}$.

Assumptions (W.1), (W.2), and (W.4) are identical to those in [2].

The condition (W.3) is similar; we want to assume K_f is abelian and Galois. In [2, (W.3)], the authors only assumed that K_f is Galois, but as K_f was a number field of degree 4 this also guaranteed it to be abelian. Many of the results proven in the present work require only that K_f is abelian and Galois; however, we will assume that g is an odd prime in many of our major results, and thus K_f will be cyclic (with $\mathrm{Gal}(K_f/\mathbb{Q}) \cong \mathbb{Z}/2g\mathbb{Z}$).

Remark 2.1. It should be noted that (W.3) is in fact a serious restriction, as number fields K_f with a cyclic Galois group are quite rare among all number fields of degree $2g$. Our method does work in broader contexts; for example, in [9] the author proves analogous results to those in [2] and our own for degree 4 fields with a nonabelian Galois group. It seems likely that our methods readily generalize to any abelian Galois extension K_f, at the cost of more elaborate and extensive computations as the factorization of g becomes more complex.

Thus, in this work, we will restrict to cyclic Galois groups in the hope of demonstrating our method and heuristic in the simplest generalized situation, rather than distracting the reader with details that provide no new insight into the problem.

Note that K_f is a CM field, and as such it comes equipped with an intrinsic complex conjugation $\iota \in \mathrm{Gal}(K_f/\mathbb{Q})$. Also, the isomorphism class of $\mathcal{O}_f$ (as an abstract order) is independent of the choice of π_f.

Example 2.2. The polynomial $f(T) = T^6 + 10T^5 + 48T^4 + 151T^3 + 336T^2 + 490T + 343$ is a 7-Weil polynomial that meets all of the assumptions (W.1)-(W.4) when $g = 3$.

The Weil polynomial $f(T)$ factors as $f(T) = \prod_{j=1}^{g}(T - \sqrt{q}e^{i\theta_j})(T - \sqrt{q}e^{-i\theta_j})$; then under our assumptions the polynomial $f^+(T) = \prod_{j=1}^{g}(T - 2\sqrt{q}\cos(\theta_j))$ is the minimal polynomial of $\pi_f + \bar{\pi}_f$ and $K_f^+ = \mathbb{Q}[T]/f^+(T)$ is the maximal totally real subfield of K_f. Note that $\mathbb{Z}[\pi_f] \cong \mathbb{Z}[T]/f(T) \subset \mathcal{O}_f$

and define the conductor of f, $\mathrm{cond}(f)$ as the index $[\mathcal{O}_f : \mathbb{Z}[\pi_f]]$. We will denote the discriminants of the polynomials f and f^+ as $\mathrm{disc}(f)$ and $\mathrm{disc}(f^+)$, respectively, while $\Delta_{\mathcal{O}}$ will represent the discriminant of an order $\mathcal{O}$. Note that $\Delta_{\mathbb{Z}[\pi_f]} = \mathrm{disc}(f)$ and $\Delta_{\mathcal{O}_{K_f^+}} = \mathrm{disc}(f^+)$.

In the following technical lemma, we give explicit forms for $\mathrm{disc}(f)$ and $\mathrm{disc}(f^+)$ for any positive integer g.

Lemma 2.3. *Let f be a q-Weil polynomial of degree $2g$ with $g \geq 1$. Then*

$$\mathrm{disc}(f) = (-1)^g 2^{2g^2} q^{2g^2-g} \left(\prod_{j=1}^{g} \sin^2(\theta_j) \right) \left(\prod_{1 \leq k < t \leq g} (\cos(\theta_k) - \cos(\theta_t))^2 \right)^2$$

and

$$\mathrm{disc}(f^+) = 2^{g(g-1)} q^{\frac{g(g-1)}{2}} \prod_{1 \leq k < t \leq g} (\cos(\theta_k) - \cos(\theta_t))^2.$$

Proof. Recall that the roots of $f(T)$ are of the form $\sqrt{q}e^{\pm i\theta_j}$ for $1 \leq j \leq g$. Then the proof of the first formula proceeds by induction on g using elementary methods and is omitted here. A direct computation of the discriminant of f^+, which has roots $\sqrt{q}e^{i\theta_j} + \sqrt{q}e^{-i\theta_j} = 2\sqrt{q}\cos(\theta_j)$ for $1 \leq j \leq g$, proves the second formula. □

Remark 2.4. See [6, Theorem 4.3] for a similar computation relating the Frobenius angles θ_i to (in our notation)

$$\sqrt{\frac{\Delta_{\mathcal{O}_{K_f}}}{\Delta_{\mathcal{O}_{K_f^+}}}}.$$

The explicit forms of Lemma 2.3 will be helpful in proving the following lemma, as well as for defining local factors in section 4.

Lemma 2.5. *The index of $\mathbb{Z}[\pi_f]$ in $\mathcal{O}_f$ is $q^{\frac{g(g-1)}{2}}$.*

Proof. From [5], we have

$$\Delta_{\mathcal{O}_f} = (-1)^g \,\mathrm{disc}(f^+)^2 \, N_{K_f/\mathbb{Q}}(\pi_f - \bar{\pi}_f)$$

and $\mathrm{disc}(f) = \mathrm{cond}(f)^2 \, \Delta_{\mathcal{O}_f}$. Then

$$\mathrm{cond}(f)^2 = (-1)^g \frac{\mathrm{disc}(f)}{\mathrm{disc}(f^+)^2 N_{K_f/\mathbb{Q}}(\pi_f - \bar{\pi}_f)}.$$

Without loss of generality, choose $\pi_f = \sqrt{q}e^{i\theta_1}$. Then

$$\pi_f - \bar{\pi}_f = 2i\sqrt{q}\sin(\theta_1)$$

and all of its Galois conjugates are of the form $\pm 2i\sqrt{q}\sin(\theta_j)$ for $j \in \{1, 2, \ldots, g\}$. Therefore,

$$N_{K_f/\mathbb{Q}}(\pi_f - \bar{\pi}_f) = \prod_{j=1}^{g} (2i\sqrt{q}\sin(\theta_j))(-2i\sqrt{q}\sin(\theta_j)) = 4^g q^g \prod_{j=1}^{g} \sin^2(\theta_j).$$

Applying $\mathrm{disc}(f)$ and $\mathrm{disc}(f^+)$ from Lemma 2.3, we find $\mathrm{cond}(f)^2 = q^{g(g-1)}$, and the lemma follows. □

Corollary 2.6. *If $\ell \neq p$, then $\mathcal{O}_{K_f} \otimes \mathbb{Z}_{(\ell)} \cong \mathbb{Z}_{(\ell)}[T]/f(T)$.*

Corollary 2.6 is proved, independent of the dimension of the abelian variety, in [2] and so its proof is omitted here.

Lastly, we prove that $\mathbb{Z}[T]/f^+(T)$ is the maximal order of K_f^+.

Lemma 2.7. *The order $\mathbb{Z}[T]/f^+(T)$ is the maximal order $\mathcal{O}_{K_f^+}$.*

Proof. Condition (W.4) implies that $\mathcal{O}_f \cap K_f^+ = \mathcal{O}_{K_f} \cap K_f^+ = \mathcal{O}_{K_f^+}$. Certainly $\mathbb{Z}[T]/f^+(T) = \mathbb{Z}[\pi_f + \bar{\pi}_f] \subseteq \mathcal{O}_f \cap K_f^+$.

Let $\alpha \in K_f^+ = \mathbb{Q}[T]/f^+(T) = \mathbb{Q}(\pi_f + \bar{\pi}_f)$, which has dimension g over $\mathbb{Q}$. Then

$$\alpha = a_0 + a_1(\pi_f + \bar{\pi}_f) + a_2(\pi_f + \bar{\pi}_f)^2 + \cdots + a_{g-1}(\pi_f + \bar{\pi}_f)^{g-1}$$

with all $a_i \in \mathbb{Q}$. Suppose α is also an element of $\mathcal{O}_f$, so $\alpha \in \mathcal{O}_f \cap K_f^+$. It is straightforward to show that the set

$$\left\{1, \pi_f, \pi_f^2, \ldots, \pi_f^g, \bar{\pi}_f, \bar{\pi}_f^2, \ldots, \bar{\pi}_f^{g-1}\right\}$$

forms a basis for $\mathcal{O}_f = \mathbb{Z}[\pi_f, \bar{\pi}_f]$. Recall that $\pi_f \bar{\pi}_f = q$; expand α and collect powers of π_f and $\bar{\pi}_f$. Notice that the coefficient of π_f^{g-1} in α is exactly a_{g-1}, and so $a_{g-1} \in \mathbb{Z}$. Using back substitution on the coefficients of powers of π_f and $\bar{\pi}_f$, we find that $a_{g-2} \in \mathbb{Z}$, $a_{g-3} \in \mathbb{Z}$, and so on. Therefore, all $a_i \in \mathbb{Z}$ and $\alpha \in \mathcal{O}_f \cap K_f^+$ is such that $\alpha \in \mathbb{Z}[\pi_f, \bar{\pi}_f]$ and $\mathcal{O}_f \cap K_f^+ \subseteq \mathbb{Z}[\pi_f + \bar{\pi}_f]$. Therefore, $\mathbb{Z}[\pi_f + \bar{\pi}_f] = \mathcal{O}_{K_f^+}$. □

3. Conjugacy classes in $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$

3.1. Symplectic groups and conjugacy. Recall that the symplectic group $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ is the subgroup of $\mathrm{GL}_{2g}(\mathbb{F}_\ell)$ preserving an antisymmetric bilinear form J up to a scalar multiple. We choose

$$J = \begin{bmatrix} 0 & \mathrm{I_g} \\ -\mathrm{I_g} & 0 \end{bmatrix}$$

but note that different choices of J produce isomorphic copies of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$.

Explicitly,

$$\mathrm{GSp}_{2g}(\mathbb{F}_\ell) = \{M \in \mathrm{GL}_{2g}(\mathbb{F}_\ell) \mid MJM^T = mJ \text{ for some } m \in \mathbb{F}_\ell^\times\}.$$

The value m is called the *multiplier* of M. All matrices in $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ have the property that there exists a pairing (dictated by the choice of antisymmetric bilinear form) of its eigenvalues such that each pair has product m.

In [10, Theorem 1.18], Shinoda parametrizes the set of conjugacy classes of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$. For our purposes, we do not need their parametrization in

full generality, and will describe the relevant portions in our own notation. Let

$$f(T) = T^d + c_{d-1}T^{d-1} + \cdots + c_1T + c_0$$

be a polynomial in $\mathbb{F}_\ell[T]$. Define the *dual* of $f(T)$ with respect to the multiplier m to be

$$\bar{f}^m(T) = \frac{T^d}{c_0} f(mT^{-1}).$$

(We will occasionally omit the m on the left hand side for notational convenience.) Then we have three types of polynomials:

(1) *Root polynomials* are polynomials of the form $f(T) = T^2 - m$ when m is not a square, or either of $f(T) = T \pm \sqrt{m}$ when m is a square. (It is easy to check that all root polynomials satisfy $\bar{f}^m(T) = f(T)$.)
(2) α *pairs* are pairs of polynomials $(f(T), \bar{f}^m(T))$ such that $\bar{f}^m(T) \neq f(T)$.
(3) β *polynomials* are polynomials $f(T)$ such that $\bar{f}^m(T) = f(T)$ and $f(T)$ is not a root polynomial.

Note that any linear polynomial satisfying $\bar{f}^m(T) = f(T)$ is a root polynomial. One consequence of these definitions is as follows.

Lemma 3.1. *There are no irreducible β polynomials of odd degree. That is, for all irreducible nonlinear polynomials $f(T)$ of odd degree and all multipliers $m \in \mathbb{F}_q^\times$,*

$$\bar{f}^m(T) \neq f(T).$$

Proof. Let $f(T) = T^d + c_{d-1}T^{d-1} + \cdots + c_1T + c_0$ be an irreducible polynomial with $d \geq 3$ odd and suppose $\bar{f}^m(T) = f(T)$. This implies $c_0^2 = m^d$, but if m is non-square then m^d is non-square since d is odd, which is a contradiction. If instead m is a square, then $-\sqrt{m} \in \mathbb{F}_\ell$ is a root of $f(T)$, contradicting the fact that $f(T)$ is irreducible. □

The general theory of conjugacy classes in GL_n as well as the additional intricacies of conjugacy in GSp_n are given (briefly) in [2, Section 3.2], and the reader is encouraged to revisit this section if needed. For our current purposes, recall that to each irreducible factor of the characteristic polynomial of a matrix, we associate a partition of its multiplicity; the characteristic polynomial together with its partition data determine conjugacy in GL_n. We also remind the reader that *cyclic* matrices are those for which the characteristic and minimal polynomials coincide, and thus are those where all partitions are maximal (consist of only one part). Then characteristic polynomials for conjugacy classes of cyclic matrices in $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ are constructed as follows.

Theorem 3.2. *The following characteristic polynomials uniquely determine a conjugacy class of cyclic matrices in $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$, where, for each m, the first product is over all α pairs and the second product is over all β polynomials.*

(1) *For square* $m \in \mathbb{F}_\ell^\times$,

$$f(T) = (T - \sqrt{m}\,)^{e_{R_1}}(T + \sqrt{m}\,)^{e_{R_2}} \prod_\alpha (f_\alpha(T)\bar{f}_\alpha(T))^{e_\alpha} \prod_\beta (f_\beta(T))^{e_\beta}$$

for a choice of $e_{R_1}, e_{R_2}, e_\alpha$, *and* e_β *such that any odd parts in the partitions of* e_{R_1} *and* e_{R_2} *have even multiplicity and*

$$e_{R_1} + e_{R_2} + 2\sum_\alpha \deg(f_\alpha)e_\alpha + \sum_\beta \deg(f_\beta)e_\beta = 2g.$$

(2) *For non-square* $m \in \mathbb{F}_\ell^\times$,

$$f(T) = (T^2 - m)^{e_R} \prod_\alpha (f_\alpha(T)\bar{f}_\alpha(T))^{e_\alpha} \prod_\beta (f_\beta(T))^{e_\beta}$$

for a choice of e_R, e_α, *and* e_β *such that any odd parts in the partition of* e_R *have even multiplicity and*

$$2e_R + 2\sum_\alpha \deg(f_\alpha)e_\alpha + \sum_\beta \deg(f_\beta)e_\beta = 2g.$$

For each exponent e_k *defined above, the only allowable partition is* $[e_k]$.

Remark 3.3. Shinoda's parameterization ([10, Theorem 1.18]) also includes sets of (nondegenerate symmetric) bilinear forms with ranks relating to the number of parts of even sizes in the partitions of any root polynomials present in the factorization of the characteristic polynomial. The number of equivalence classes of these bilinear forms detect when a characteristic polynomial (and associated set of partitions) gives rise to two conjugacy classes in $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$, indexed by $\{+,-\}$. We omit this component of Shinoda's parameterization because, when g is odd, all of the characteristic polynomials that we will declare as *relevant* in the next section give rise to only one conjugacy class.

3.2. Relevant conjugacy classes of $\mathbf{GSp_{2g}(\mathbb{F}_\ell)}$. For the remainder of section 3, let g be an odd prime.

We want to identify the possible shapes (factorization structures) of characteristic polynomials which correspond to conjugacy classes of cyclic matrices in $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ which respect the assumptions (W.1)-(W.4). Therefore, a *relevant* characteristic polynomial is one such that

- the factorization is as in Theorem 3.2,
- the degrees of all irreducible factors are equal, and
- the multiplicities of each irreducible factor are equal.

The first condition forces our matrices to be cyclic elements of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$, and the other two correspond with the requirement that K_f be Galois from (W.3).

Let $[d]$ denote a monic irreducible degree d polynomial in $\mathbb{F}_\ell[T]$, and assume that $[d]_i \neq [d]_j$ if $i \neq j$. Then the following are the shapes of all relevant characteristic polynomials.

$$\begin{array}{ll} [1]_1 \dots [1]_{2g} & [1]^{2g} \\ [2]_1 \dots [2]_g & [1]_1^g [1]_2^g \\ [g]_1 [g]_2 & [2]^g \\ [2g] & \end{array}$$

We exclude the shape $[g]^2$ by Lemma 3.1. Additionally, we exclude $[1]_1^2 \dots [1]_g^2$; since there are an odd number of factors, it must be that one of these linear factors is a root polynomial while the rest are α pairs. Then the Galois group of K_f cannot act transitively on the roots of such an f.

The seven relevant conjugacy class shapes fall into two categories: regular semisimple and non-semisimple. A regular semisimple conjugacy class contains elements with a squarefree characteristic polynomial (and thus are cyclic by definition). A class is not semisimple when the characteristic polynomial of its elements is not squarefree.

We list the relevant conjugacy classes by the shape of their characteristic polynomial in Tables 3.1 (regular semisimple) and 3.2 (non-semisimple). Each table also contains information about the multiplier m and the type of the irreducible factors.

Char. Pol. Shape	Valid m	Polynomial type
$[1]_1 \dots [1]_{2g}$	All m	α pairs
$[2]_1 \dots [2]_g$	All m	β polynomials
$[g]_1 [g]_2$	All m	α pair
$[2g]$	All m	β polynomial

TABLE 3.1. Relevant characteristic polynomial shapes for regular semisimple conjugacy classes

Char. Pol. Shape	Valid m	Polynomial type
$[1]^{2g}$	Square m	Root polynomial
$[1]_1^g [1]_2^g$	All m	α pair
$[2]^g$	All m	β polynomial

TABLE 3.2. Relevant characteristic polynomial shapes for non-semisimple conjugacy classes

3.3. Centralizer orders. Denote by $\mathcal{C}$ a conjugacy class of matrices in $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ with characteristic polynomial $f_{\mathcal{C}}(T)$. For each relevant conjugacy class, we will find its order by instead finding the order of its centralizer. Let $\mathcal{Z}_{\mathrm{GSp}_{2g}(\mathbb{F}_\ell)}(\mathcal{C})$ be the centralizer in $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ of an element of $\mathcal{C}$. Since we need only the size of the centralizer, the choice of this element is arbitrary.

Lemma 3.4. *Let $\mathcal{C}$ be a regular semisimple conjugacy class with characteristic polynomial having one of the shapes listed in Table 3.1. Then we have*

$$\#\mathcal{Z}_{\mathrm{GSp}_{2g}(\mathbb{F}_\ell)}(\mathcal{C}) = \begin{cases} (\ell-1)^{g+1} & \text{if } f_{\mathcal{C}}(T) \text{ has shape } [1]_1 \dots [1]_{2g}, \\ (\ell^2-1)(\ell+1)^{g-1} & \text{if } f_{\mathcal{C}}(T) \text{ has shape } [2]_1 \dots [2]_g, \\ (\ell^g-1)(\ell-1) & \text{if } f_{\mathcal{C}}(T) \text{ has shape } [g]_1[g]_2, \\ (\ell^g+1)(\ell-1) & \text{if } f_{\mathcal{C}}(T) \text{ has shape } [2g]. \end{cases}$$

Proof. Since each class is regular and semisimple, their centralizers are tori. For example, consider the case where $f_{\mathcal{C}}(T)$ has the shape $[2g]$. Then $f_{\mathcal{C}}(T)$ has roots $\alpha, \alpha^\ell, \dots, \alpha^{\ell^{2g-1}}$ in $\mathbb{F}_{\ell^{2g}}^\times$ in a single orbit under the action of Galois. Since $\mathcal{C} \subseteq \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$, it must be that the elements of $\mathcal{C}$ have multiplier $m = \alpha^{\ell^i}\alpha^{\ell^{g+i}}$ for $i \in \{0, 1, \dots, g-1\}$. Thus, elements of the centralizer of $\mathcal{C}$ are those where roots of the characteristic polynomial are elements of $\mathbb{F}_{\ell^{2g}}^\times$ with an $\mathbb{F}_{\ell^g}$-norm lying in $\mathbb{F}_\ell^\times$. There are $\frac{\ell^{2g}-1}{\ell^g-1} = \ell^g+1$ elements of $\mathbb{F}_{\ell^{2g}}^\times$ with such a norm for a fixed m. Since we have $\ell-1$ choices for the multiplier, $\#\mathcal{Z}_{\mathrm{GSp}_{2g}(\mathbb{F}_\ell)}(\mathcal{C}) = (\ell^g+1)(\ell-1)$.

The centralizer sizes for the other cases are computed similarly. □

In the case where $\mathcal{C}$ is not semisimple, the process for determining the order of its centralizer is significantly more challenging. In these cases, we must construct an explicit matrix γ which is a representative of $\mathcal{C}$, and verify that γ has the correct characteristic polynomial, that γ is cyclic, and that $\gamma \in \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$. Then we must find an explicit matrix C which is a generic member of the centralizer of that γ (also in $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$) and use it to count the number of possible elements of $\mathcal{Z}_{\mathrm{GSp}_{2g}(\mathbb{F}_\ell)}(\mathcal{C})$.

For any particular g, this process is possible. (As an example, the centralizer orders of the non-semisimple classes for $g = 3$ are given in Proposition 7.5.) However, we have not yet constructed representatives for all three non-semisimple classes for a general (odd prime) g and thus do not have formulae for their centralizer orders. We hope, in future work, to address this gap.

4. Local factors for f

In this section we define local factors $\nu_\ell(f)$ for each finite rational prime ℓ and one for the archimedean prime, $\nu_\infty(f)$. For all $\ell \neq p$, this local factor is given by the density of elements of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ with a fixed multiplier and characteristic polynomial f with respect to the "average" frequency. We also define $\nu_p(f)$ and $\nu_\infty(f)$ based on the same notions. These definitions are in direct analogue with those of [2], and are thus philosophically guided by [4] as well.

4.1. $\nu_\ell(f)$. Suppose $\ell \neq p$ is a rational prime and consider a principally polarized abelian variety $X/\mathbb{F}_q$ of dimension g. The Frobenius endomorphism $\pi_{X/\mathbb{F}_q}$ of X acts as an automorphism of X_ℓ, and scales by a factor of q the symplectic pairing on X_ℓ induced by the polarization. Thus, we can consider $\pi_{X/\mathbb{F}_q}$ as an element of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)^{(q)}$ (the set of elements of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ with multiplier q).

Note that there are ℓ^g possible characteristic polynomials for an element of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)^{(q)}$, and so the average frequency of a particular polynomial occurring as the characteristic polynomial of an element of the group (with respect to all such polynomials) is given by

$$\#\,\mathrm{GSp}_{2g}(\mathbb{F}_\ell)^{(q)}/\ell^g.$$

Then for primes ℓ unramified in K_f, we define $\nu_\ell(f)$ as

$$\nu_\ell(f) = \frac{\#\left\{\gamma \in \mathrm{GSp}_{2g}(\mathbb{F}_\ell)^{(q)} \mid \mathrm{charpol}(\gamma) \equiv f \bmod \ell\right\}}{\#\,\mathrm{GSp}_{2g}(\mathbb{F}_\ell)^{(q)}/\ell^g}. \tag{4.1}$$

(See (5.1) for a definition for all $\ell \neq p$.)

4.2. $\nu_p(f)$. The definition of $\nu_p(f)$ is similar to but more intricate than (4.1). Under our assumptions, $X/\mathbb{F}_q$ is an ordinary abelian variety of (odd prime) dimension g with characteristic polynomial of Frobenius

$$f_X(T) = T^{2g} + c_1T^{2g-1} + \cdots + c_gT^g + qc_{g-1}T^{g-1} + \cdots + q^{g-1}c_1T + q^g.$$

Thus, as in [2], we have a canonical decomposition of the p-torsion group scheme into étale and toric components $X[p] \cong X[p]^{\mathrm{et}} \oplus X[p]^{\mathrm{tor}}$. By ordinarity, $X[p]^{\mathrm{et}}(\bar{\mathbb{F}}_q) \cong (\mathbb{Z}/p)^g$ and $(X[p]^{\mathrm{tor}})^*(\bar{\mathbb{F}}_q) \cong (\mathbb{Z}/p)^g$, and the q-power Frobenius $\pi_{X/\mathbb{F}_q}$ acts invertibly on $X[p](\bar{\mathbb{F}}_q)$. This action of $\pi_{X/\mathbb{F}_q}$ on both the étale and toric components of $X[p]$ has characteristic polynomial $g_X(T) = T^g + c_1T^{g-1} + \cdots + c_g \bmod p$, and must preserve the decomposition of $X[p]$. Let m_g be the multiplier of g_X (so m_g is a g^{th} root of c_g^2). Thus, we set $\nu_p(f)$ to be

$$\frac{\#\left\{\gamma \in \mathrm{GSp}_{2g}(\mathbb{F}_p)^{(m_g)} \mid \mathrm{charpol}(\gamma) \equiv (g_X)^2 \bmod p \text{ and } \gamma \text{ semisimple}\right\}}{\#\,\mathrm{GSp}_{2g}(\mathbb{F}_p)^{(m_g)}/p^g}. \tag{4.2}$$

4.3. $\nu_\infty(f)$. Lastly, we define an archimedean term, which is related to the Sato-Tate measure. As stated in [2], the Sato-Tate measure on abelian varieties conjecturally explains the distribution of Frobenius elements, and is a pushforward of Haar measure on the space of "Frobenius angles", $0 \leq \theta_1 \leq \cdots \leq \theta_g \leq \pi$. The Weyl integration formula [13, p218, 7.8B] gives the Sato-Tate measure on abelian varieties of dimension g explicitly as

$$\mu_{ST}(\theta_1, \ldots, \theta_g) = 2^{g^2}\left(\prod_{j<k}(\cos(\theta_j) - \cos(\theta_k))^2\right)\prod_{i=1}^{g}\left(\frac{1}{\pi}\sin^2(\theta_i)d\theta_i\right).$$

Fixing a particular q, the set of angles $\{\theta_1, \dots, \theta_g\}$ gives rise to a q-Weil polynomial. We use the induced measure on the space of all such polynomials to define the archimedean term $\nu_\infty(f)$. To derive this induced measure, we first write the polynomial in terms of its roots and in terms of its coefficients as

$$\begin{aligned} f(T) &= \prod_{j=1}^{g} (T - \sqrt{q}e^{i\theta_j})(T - \sqrt{q}e^{-i\theta_j}) \\ &= T^{2g} + c_1 T^{2g-1} + \cdots + c_g T^g + c_{g-1} q T^{g-1} + \cdots + c_1 q^{g-1} T + q^g, \end{aligned}$$

and perform a change of variables. Thus, we find our induced measure on the space of all q-Weil polynomials to be

$$\mu(c_1, \dots, c_g) = \frac{1}{q^{g^2}(2\pi)^g} \sqrt{\left| \frac{\operatorname{disc}(f)}{\operatorname{disc}(f^+)} \right|}\, dc_1 \dots dc_g.$$

Note that there are approximately $q^{\dim \mathcal{A}_g} = q^{\frac{g(g+1)}{2}}$ principally polarized abelian varieties over $\mathbb{F}_q$, so $q^{\frac{g(g+1)}{2}} \mu(c_1, \dots, c_g)$ can be thought of as an archimedean predictor for $\#\mathcal{A}_g(\mathbb{F}_q; f)$. Then we define

$$\nu_\infty(f) = \frac{1}{\operatorname{cond}(f)(2\pi)^g} \sqrt{\left| \frac{\operatorname{disc}(f)}{\operatorname{disc}(f^+)} \right|}. \tag{4.3}$$

(We note that definition (4.3) holds for any g, not just odd prime g.)

5. Polynomials and primes in K

Fix a q-Weil polynomial $f(T)$ which satisfies conditions (W.1)-(W.4). For the remainder of the paper, we write K for K_f, $\mathcal{O}_K$ for $\mathcal{O}_f$, K^+ for K_f^+, Δ_K for $\Delta_{\mathcal{O}_K}$, and Δ_{K^+} for $\Delta_{\mathcal{O}_{K^+}}$. Let $\kappa_\ell = \mathcal{O}_K \otimes \mathbb{F}_\ell$, a $2g$-dimensional vector space over $\mathbb{F}_\ell$.

Our goal in this section is to relate the polynomial $f(T) \bmod \ell$ to (a representative of) one of the conjugacy classes defined in section 3.2. There are two lenses through which we can consider such a correspondence, as outlined in [2, Section 5].

Regardless of the perspective, we will use the factorization of $f(T) \bmod \ell$ to determine a cyclic element of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ whose semisimplification is conjugate to γ_ℓ, the image of the action of π_f on κ_ℓ. Then we define

$$\nu_\ell(f) = \frac{\#\left\{\gamma \in \mathrm{GSp}_{2g}(\mathbb{F}_\ell) \mid \gamma \text{ is cyclic with semisimplification } \gamma_\ell\right\}}{\#\,\mathrm{GSp}_{2g}(\mathbb{F}_\ell)^{(q)}/\ell^g}. \tag{5.1}$$

Lemma 5.1. *If $\ell \nmid p\Delta_K$, then definitions (4.1) and (5.1) coincide.*

Proof. If $\ell \nmid p\Delta_K$ then $\ell \nmid \operatorname{disc}(f)$ and so $f(T) \bmod \ell$ has distinct roots. Under condition (W.3), any factorization of $f(T) \bmod \ell$ with distinct roots appears in Table 3.1, and so any element with characteristic polynomial

$f(T) \bmod \ell$ is conjugate to γ_ℓ. All regular semisimple elements are cyclic, so the lemma is proven. □

Note that charpol(γ_ℓ) is precisely $f(T) \bmod \ell$. Also note that $\kappa_\ell = \mathcal{O}_K/\ell \cong \mathbb{F}_\ell[T]/f(T)$ by Corollary 2.6, so the factorization of $f(T) \bmod \ell$ is determined by the splitting of ℓ in $\mathcal{O}_K$. That is, if $f(T) \bmod \ell = \prod_{1\le j\le r} g_j(T)^{e_j}$, then $\ell = \prod_{1\le j\le r} \lambda_j^{e_j}$ for primes λ_j of $\mathcal{O}_K$ where the residue degree of λ_j equals the degree of the irreducible polynomial $g_j(T)$.

Because of Condition (W.3), $K/\mathbb{Q}$ is a finite Galois extension with

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2g\mathbb{Z}.$$

Then the residue degrees of the λ_j are all equal to a common value $\mathfrak{f}$, and the ramification degrees of the λ_j are all equal to a common value e. In particular $2g = e\mathfrak{f}r$. (Notice that this restriction is precisely how we identified relevant class shapes in Section 3.2.) Without loss of generality, let λ be a prime of $\mathcal{O}_K$ over ℓ. Let $D(\ell)$ and $I(\ell)$ denote the decomposition and inertia groups, respectively, of a rational prime ℓ. Lastly, if $\ell \nmid \mathrm{disc}(f)$, then $\mathrm{Gal}(\kappa(\lambda)/\mathbb{F}_\ell)$ (the residue field of λ) is cyclic. Let $\mathrm{Frob}_K(\ell) \in \mathrm{Gal}(K/\mathbb{Q})$ be the element which induces the generator of this group, and call it the Frobenius endomorphism of λ over ℓ.

Let $\mathrm{Gal}(K/\mathbb{Q}) = \langle\sigma\rangle$ so that complex conjugation is given by $\iota = \sigma^g$. We classify the splitting of rational primes of K by enumerating the possibilities for $D(\ell)$ and $I(\ell)$.

Lemma 5.2. *Suppose f satisfies Conditions (W.1)-(W.4). Let $\ell \neq p$ be a rational prime. The cyclic shape of γ_ℓ is determined by the decomposition and inertia groups $D(\ell)$ and $I(\ell)$ as in Table 5.1.*

$D(\ell)$	$I(\ell)$	$\mathrm{Frob}_K(\ell)$	$(e, \mathfrak{f}, r)$	Class shape
$\{1\}$	$\{1\}$	1	$(1, 1, 2g)$	$[1]_1 \dots [1]_{2g}$
$\langle\sigma^g\rangle$	$\{1\}$	σ^g	$(1, 2, g)$	$[2]_1 \dots [2]_g$
$\langle\sigma^2\rangle$	$\{1\}$	σ^2	$(1, g, 2)$	$[g]_1[g]_2$
$\langle\sigma^2\rangle$	$\langle\sigma^2\rangle$	-	$(g, 1, 2)$	$[1]_1^g[1]_2^g$
$\langle\sigma\rangle$	$\{1\}$	σ^i for $(i, g) = 1$	$(1, 2g, 1)$	$[2g]$
$\langle\sigma\rangle$	$\langle\sigma^2\rangle$	-	$(g, 2, 1)$	$[2]^g$
$\langle\sigma\rangle$	$\langle\sigma\rangle$	-	$(2g, 1, 1)$	$[1]^{2g}$

TABLE 5.1. Prime factorizations and conjugacy class shapes for K.

Note that in every case, the data $D(\ell)$ and $I(\ell)$ determines a unique conjugacy class from those given in Tables 3.1 and 3.2.

Proof. In Table 5.1, we enumerated all possibilities for pairs of subgroups $I(\ell) \subseteq D(\ell) \subseteq \mathrm{Gal}(K/\mathbb{Q})$. In every case, there are $r = \#\mathrm{Gal}(K/\mathbb{Q})/\#D(\ell)$ distinct irreducible factors of $f(T)$ mod ℓ, each with degree $\mathfrak{f} = \#D(\ell)/\#I(\ell)$ and multiplicity $e = \#I(\ell)$. In all cases, this factorization pattern exactly determines the conjugacy class for which γ_ℓ is a representative. □

6. Local factors for K

Recall that $K/\mathbb{Q}$ is a finite Galois extension with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2g\mathbb{Z}$. Then K has two unique subfields, the maximal totally real field K^+ of index 2 in K, and a complex quadratic extension of $\mathbb{Q}$ which we will call K_1 in what follows.

Let $X(K)$ be the character group of the Galois group of K. For $\chi \in X(K)$, let K^χ be the fixed field of $\ker(\chi)$. For a rational prime ℓ, define

$$\chi(\ell) = \begin{cases} \chi(\mathrm{Frob}_{K^\chi}(\ell)) & \text{if } \ell \text{ is unramified in } K^\chi, \\ 0 & \text{otherwise.} \end{cases}$$

Let $S(K) = X(K) \smallsetminus X(K^+)$ and define

$$\nu_\ell(K) = \prod_{\chi \in S(K)} \left(1 - \frac{\chi(\ell)}{\ell}\right)^{-1}. \tag{6.1}$$

Recall that σ is a generator of $\mathrm{Gal}(K/\mathbb{Q})$ and let χ be a generator of $X(K)$. Then $\langle \sigma^2 \rangle = \mathrm{Gal}(K^+/\mathbb{Q})$ and $\langle \chi^2 \rangle = X(K^+)$, so $S(K) = \{\chi, \chi^3, \ldots, \chi^{2g-1}\}$. A quick computation shows $K^{\chi^g} = K_1$ and $K^{\chi^i} = K$ for all other $\chi^i \in S(K)$. We have $\chi^i(\ell) = (\chi(\ell))^i$ for all odd $i \neq g$, and so to compute $\chi^i(\ell)$ for odd i, we only need to know $\chi(\ell)$ and $\chi^g(\ell)$.

Lemma 6.1. *The values of $\chi(\ell)$ and $\chi^g(\ell)$ are determined by $D(\ell)$ and $I(\ell)$, as given in Table 6.1.*

Proof. The values in the table follow from the definitions of χ and χ^g above, the Frobenius elements given in Table 5.1, and the fact that $\mathrm{Gal}(K/\mathbb{Q})$ and $X(K)$ are cyclic. Then when $\mathrm{Frob}_K(\ell)$ generates $\mathrm{Gal}(K/\mathbb{Q})$, $\chi(\ell)$ is a primitive $2g^{th}$ root of unity. In particular, the values in Table 6.1 are independent of the choice of generator for each of $D(\ell)$, $I(\ell)$, and $X(K)$. □

7. Matching

In this section, we will prove a series of propositions to establish equalities between the local factor defined for f in Section 4 and the local term intrinsic to $K = K_f$ defined in Section 6 both for general odd prime g and for the specific case when $g = 3$.

$D(\ell)$	$I(\ell)$	$\{\chi(\ell), \chi^g(\ell)\}$	Class shape
$\{1\}$	$\{1\}$	$\{1, 1\}$	$[1]_1 \dots [1]_{2g}$
$\langle\sigma^g\rangle$	$\{1\}$	$\{-1, -1\}$	$[2]_1 \dots [2]_g$
$\langle\sigma^2\rangle$	$\{1\}$	$\{e^{2\pi i/g}, 1\}$	$[g]_1[g]_2$
$\langle\sigma^2\rangle$	$\langle\sigma^2\rangle$	$\{0, 1\}$	$[1]_1^g[1]_2^g$
$\langle\sigma\rangle$	$\{1\}$	$\{e^{\pi i/g}, -1\}$	$[2g]$
$\langle\sigma\rangle$	$\langle\sigma^2\rangle$	$\{0, -1\}$	$[2]^g$
$\langle\sigma\rangle$	$\langle\sigma\rangle$	$\{0, 0\}$	$[1]^{2g}$

TABLE 6.1. Values of imaginary characters for K.

7.1. General case. Let g be an odd prime.

In Proposition 7.1, we must restrict to regular semisimple conjugacy classes because we only have $\#\mathcal{Z}_{\mathrm{GSp}_{2g}(\mathbb{F}_\ell)}(\mathcal{C})$ for all odd prime g in those cases.

Proposition 7.1. *Suppose f is a q-Weil polynomial of degree $2g$ such that $f \mod \ell = f_{\mathcal{C}}$ for one of the conjugacy class shapes in Table 3.1. If $\ell \neq p$ then $\nu_\ell(f) = \nu_\ell(K)$.*

Proof. Let $\mathcal{C}$ be a conjugacy class from Table 3.1. Using the orbit-stabilizer theorem, we can rewrite $\nu_\ell(f)$ in terms of $\#\mathcal{Z}_{\mathrm{GSp}_{2g}(\mathbb{F}_\ell)}(\mathcal{C})$ as

$$\frac{\#\mathcal{C}}{\#\,\mathrm{GSp}_{2g}(\mathbb{F}_\ell)^{(q)}/\ell^g} = \frac{\#\,\mathrm{GSp}_{2g}(\mathbb{F}_\ell)/\#\mathcal{Z}_{\mathrm{GSp}_{2g}(\mathbb{F}_\ell)}(\mathcal{C})}{\#\,\mathrm{GSp}_{2g}(\mathbb{F}_\ell)^{(q)}/\ell^g} = \frac{\ell^g(\ell-1)}{\#\mathcal{Z}_{\mathrm{GSp}_{2g}(\mathbb{F}_\ell)}(\mathcal{C})}.$$

Since we found the centralizer orders for each regular semisimple class in Theorem 3.4, we use this expression for $\nu_\ell(f)$ to calculate the third column of Table 7.1.

Additionally, from (6.1), $\nu_\ell(K)$ is equal to

$$\prod_{\chi\in S(K)}\left(1-\frac{\chi(\ell)}{\ell}\right)^{-1} = \left(\frac{\ell}{\ell-\chi(\ell)}\right)\left(\frac{\ell}{\ell-\chi^3(\ell)}\right)\cdots\left(\frac{\ell}{\ell-\chi^{2g-1}(\ell)}\right).$$

The fourth column of Table 7.1 contains the relevant values from Table 6.1 from which we compute $\nu_\ell(K)$ in the fifth column.

To compute the third and fourth rows of the fifth column of Table 7.1, recall that if z is a primitive $(2g)^{th}$ root of unity, then z^2 is a primitive g^{th} root of unity. Then since $(\ell^{2g}-1) = (\ell^g-1)(\ell^g+1)$,

$$\ell^{2g}-1 = \prod_{j=1}^{2g}(\ell - z^j), \text{ and } \ell^g - 1 = \prod_{j=1}^{g}(\ell - z^{2j}),$$

we must have

$$(\ell^g+1) = \prod_{j=1}^{g}(\ell - z^{2j-1}).$$

We see the third and fifth columns of Table 7.1 match, so the proposition is proved. □

Class Shape	$\#\mathcal{Z}(\mathcal{C})$	$\nu_\ell(f)$	$\{\chi(\ell), \chi^g(\ell)\}$	$\nu_\ell(K)$
$[1]_1 \dots [1]_{2g}$	$(\ell-1)^{g+1}$	$\frac{\ell^g}{(\ell-1)^g}$	$\{1,1\}$	$\left(\frac{\ell}{\ell-1}\right)^g$
$[2]_1 \dots [2]_g$	$(\ell^2-1)(\ell+1)^{g-1}$	$\frac{\ell^g}{(\ell+1)^g}$	$\{-1,-1\}$	$\left(\frac{\ell}{\ell+1}\right)^g$
$[g]_1[g]_2$	$(\ell^g-1)(\ell-1)$	$\frac{\ell^g}{\ell^g-1}$	$\{e^{2\pi i/g}, 1\}$	$\frac{\ell^g}{\ell^g-1}$
$[2g]$	$(\ell^g+1)(\ell-1)$	$\frac{\ell^g}{\ell^g+1}$	$\{e^{\pi i/g}, -1\}$	$\frac{\ell^g}{\ell^g+1}$

TABLE 7.1. Evaluating $\nu_\ell(f)$ and $\nu_\ell(K)$ for regular semisimple classes.

In order to show that $\nu_p(f) = \nu_p(K)$, we first must determine the possible factorizations of p in $\mathcal{O}_K$.

Lemma 7.2. *Let $K/\mathbb{Q}$ be a degree $2g$ CM number field, and let X be an ordinary abelian variety of dimension g over $\mathbb{F}_q$. Suppose K acts on X. Then any prime of K^+ over p splits in K.*

Proof. Recall that $K^+ = \mathbb{Q}(\pi + \bar{\pi})$, and that $\pi, \bar{\pi}$ are roots of $T^2 - (\pi + \bar{\pi})T + q$ over K. Let $\mathfrak{p}^+$ be a prime of K^+ over p; since $\pi\bar{\pi} = q$, at least one of π or $\bar{\pi}$ lies in $\mathfrak{p}$, a prime of K over $\mathfrak{p}^+$. However, if $\pi + \bar{\pi} \in \mathfrak{p}^+$, then both π and $\bar{\pi}$ are in $\mathfrak{p}$. This contradicts the assumption that f was ordinary, so $\pi + \bar{\pi} \notin \mathfrak{p}^+$. Then

$$\begin{aligned} T^2 - (\pi+\bar{\pi})T + q &\equiv T^2 - uT \bmod \mathfrak{p}^+ \\ &\equiv T(T-u) \bmod \mathfrak{p}^+ \end{aligned}$$

where $u \mod \mathfrak{p}^+$ is nonzero. Therefore, $\mathfrak{p}^+$ splits in K. □

Proposition 7.3. *Suppose f is as in Proposition 7.1. Then $\nu_p(f) = \nu_p(K)$.*

Proof. We assumed in (W.3) that p is unramified in K and $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2g\mathbb{Z}$, and by Lemma 7.2 all primes of K^+ over p split in K. Then the only possible factorizations of p in $\mathcal{O}_K$ are that p splits completely, or that $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$.

If p splits completely, then $g_X(T)$ (from (4.2)) factors as a product of linear polynomials over $\mathbb{F}_p$ and the set of *semisimple* matrices with characteristic polynomial $(g_X(T))^2$ has the same cardinality as $[1]_1 \dots [1]_{2g}$. Then $\nu_p(f) = \nu_p(K)$ by the first row of Table 7.1.

If instead $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ (so p is inert in $\mathcal{O}_{K^+}$), then $g_X(T)$ is irreducible so the set of *semisimple* matrices with characteristic polynomial $(g_X(T))^2$ has the same cardinality as $[g]_1[g]_2$. Then $\nu_p(f) = \nu_p(K)$ by the third row of Table 7.1. □

The following proposition is true for any value of g.

Proposition 7.4. *Let f be a q-Weil polynomial of degree $2g$ with splitting field K and $\mathcal{O}_K = \mathbb{Z}[\pi, \bar{\pi}]$. Then*

$$\nu_\infty(f) = \frac{1}{(2\pi)^g}\sqrt{\left|\frac{\Delta_K}{\Delta_{K^+}}\right|}.$$

Proof. This follows from the fact that $\operatorname{disc}(f) = \operatorname{cond}(f)^2\Delta_K$ and $\operatorname{disc}(f^+) = \Delta_{K^+}$. □

7.2. Specific case ($g = 3$). In the particular case when $g = 3$, we can also prove that $\nu_\ell(f)$ and $\nu_\ell(K)$ match in the case when $f \bmod \ell = f_{\mathcal{C}}$ for a non-semisimple conjugacy class $\mathcal{C}$. We begin by giving the orders of the centralizers for the non-semisimple conjugacy classes in $\mathrm{GSp}_6(\mathbb{F}_\ell)$.

Proposition 7.5. *Let $\mathcal{C}$ be one of the non-semisimple conjugacy classes of matrices in $\mathrm{GSp}_6(\mathbb{F}_\ell)$ with characteristic polynomial in one of the shapes listed in Table 3.2. Then we have*

$$\#\mathcal{Z}_{\mathrm{GSp}_6(\mathbb{F}_\ell)}(\mathcal{C}) = \begin{cases} \ell^3(\ell-1) & \text{if } f_{\mathcal{C}}(T) \text{ has shape } [1]^6, \\ \ell^2(\ell-1)^2 & \text{if } f_{\mathcal{C}}(T) \text{ has shape } [1]_1^3[1]_2^3, \\ \ell^2(\ell^2-1) & \text{if } f_{\mathcal{C}}(T) \text{ has shape } [2]^3. \end{cases}$$

Proof. Refer back to the end of section 3 for an outline of the general method for determining centralizer orders for non-semisimple classes. We demonstrate this method for $g = 3$ in the case where $f_{\mathcal{C}}(T)$ has the shape $[1]_1^3[1]_2^3$.

Suppose $f_{\mathcal{C}}(T) = (T-a)^3(T-b)^3$ with $a, b \in \mathbb{F}_q^\times$. Since these are α polynomials (by Table 3.2), $m = ab$. A representative of the class $\mathcal{C}$ is

$$\gamma = \begin{bmatrix} a & -a & 0 & 0 & 0 & 0 \\ 0 & a & -a & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 \\ 0 & 0 & 0 & b & b & b \\ 0 & 0 & 0 & 0 & b & b \\ 0 & 0 & 0 & 0 & 0 & b \end{bmatrix},$$

where we verify that $\operatorname{charpol}(\gamma) = f_{\mathcal{C}}(T)$, $\gamma \in \mathrm{GSp}_6(\mathbb{F}_\ell)$ with multiplier ab, and $\operatorname{minpol}(\gamma) = \operatorname{charpol}(\gamma)$ (so that γ is cyclic). Then a generic element of $\mathcal{Z}_{\mathrm{GSp}_6(\mathbb{F}_\ell)}(\mathcal{C})$ has the form

$$C = \begin{bmatrix} c_1 & y_1 & y_2 & 0 & 0 & 0 \\ 0 & c_1 & y_1 & 0 & 0 & 0 \\ 0 & 0 & c_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & c_2 & c_3 & c_4 \\ 0 & 0 & 0 & 0 & c_2 & c_3 \\ 0 & 0 & 0 & 0 & 0 & c_2 \end{bmatrix}$$

where

$$y_1 = -\frac{c_1 c_3}{c_2} \quad \text{and} \quad y_2 = c_1\left(\frac{c_3^2 - c_2 c_4}{c_2^2}\right).$$

Since $\det C = c_1^3 c_2^3$, it must be that $c_1, c_2 \in \mathbb{F}_\ell^\times$, while $c_3, c_4 \in \mathbb{F}_\ell$. Then

$$\#\mathcal{Z}_{\mathrm{GSp}_6(\mathbb{F}_\ell)}(\mathcal{C}) = \ell^2(\ell-1)^2.$$

The other cases require similar computations. □

Proposition 7.6. *Suppose f is a q-Weil polynomial of degree 6 such that $f \bmod \ell = f_{\mathcal{C}}$ for one of the conjugacy classes in Table 3.2. If $\ell \neq p$ then $\nu_\ell(f) = \nu_\ell(K)$.*

Proof. This proof is identical to the proof of Proposition 7.1, but for non-semisimple classes. The second column of Table 7.2 comes from Proposition 7.5, which we use to compute the third column.

The fourth column comes from Table 6.1, which we use to compute the fifth column. Seeing that the third and fifth columns match, we are done. □

Class Shape	$\#\mathcal{Z}(\mathcal{C})$	$\nu_\ell(f)$	$\{\chi(\ell), \chi^g(\ell)\}$	$\nu_\ell(K)$
$[1]^6$	$\ell^3(\ell-1)$	1	$\{0,0\}$	$\left(\frac{\ell}{\ell-1}\right)^g$
$[1]_1^3[1]_2^3$	$\ell^2(\ell-1)^2$	$\frac{\ell}{\ell-1}$	$\{0,1\}$	$\frac{\ell}{\ell-1}$
$[2]^3$	$\ell^2(\ell^2-1)$	$\frac{\ell}{\ell+1}$	$\{0,-1\}$	$\frac{\ell}{\ell+1}$

TABLE 7.2. Evaluating $\nu_\ell(f)$ and $\nu_\ell(K)$ for non-semisimple classes when $g = 3$.

8. Main results

This section generalizes many of the results of [2, Section 7]. We define an infinite product of numbers $\{a_\ell\}$ indexed by finite primes by

$$\prod_\ell a_\ell = \lim_{B\to\infty} \prod_{\ell<B} a_\ell$$

so that $\prod_\ell a_\ell \prod_\ell b_\ell = \prod_\ell (a_\ell b_\ell)$.

For a number field L, let h_L, ω_L, and R_L denote the class number, number of roots of unity, and regulator of L respectively.

Proposition 8.1. *Let f be a degree $2g$ q-Weil polynomial that is ordinary, principally polarizable, cyclic, and maximal. Let K be the splitting field of f over $\mathbb{Q}$ and let K^+ be its maximal totally real subfield. Then*

$$\frac{h_K}{h_{K^+}} = \omega_K \nu_\infty(f) \prod_\ell \nu_\ell(K). \tag{8.1}$$

Proof. By the analytic class number formula, the ratio of class numbers on the left side of (8.1) is

$$\frac{h_K}{h_{K^+}} = \lim_{s\to 1} \frac{(s-1)\zeta_K(s)}{(s-1)\zeta_{K^+}(s)} \frac{\sqrt{|\Delta_K|}2^g \omega_K R_{K^+}}{\sqrt{|\Delta_{K^+}|}(2\pi)^g \omega_{K^+} R_K}.$$

For a finite abelian extension $L/\mathbb{Q}$, we have

$$\lim_{s\to 1}(s-1)\zeta_L(s) = \prod_{\chi\in \mathrm{Gal}(L/\mathbb{Q})^*\setminus \mathrm{id}} L(1,\chi)$$

where we interpret the Dirichlet L-function as the conditionally convergent Euler product

$$L(1,\chi) = \lim_{B\to\infty} \prod_{\ell<B} \frac{1}{1-\chi(\ell)/\ell}.$$

We then see that

$$\begin{aligned}\lim_{s\to 1} \frac{(s-1)\zeta_K(s)}{(s-1)\zeta_{K^+}(s)} &= \frac{\prod_{\chi\in \mathrm{Gal}(K/\mathbb{Q})^*\setminus \mathrm{id}} \left(\prod_\ell \frac{1}{1-\chi(\ell)/\ell}\right)}{\prod_{\chi\in \mathrm{Gal}(K^+/\mathbb{Q})^*\setminus \mathrm{id}} \left(\prod_\ell \frac{1}{1-\chi(\ell)/\ell}\right)} \\ &= \prod_{\chi\in S(K)} \prod_\ell \frac{1}{1-\chi(\ell)/\ell} \\ &= \prod_\ell \nu_\ell(K)\end{aligned}$$

where $S(K)$ is as in Section 6.

By [12, Proposition 4.16] $R_K = \frac{1}{Q}2^{g-1}R_{K^+}$, where Q is Hasse's unit index. Since $K/\mathbb{Q}$ is cyclic, $Q = 1$ by [3, Theorem 3]. Therefore, $R_K = 2^{g-1}R_{K^+}$.

Lastly, $\omega_{K^+} = 2$ since K^+ is totally real, so

$$\begin{aligned}\frac{h_K}{h_{K^+}} &= \sqrt{\left|\frac{\Delta_K}{\Delta_{K^+}}\right|}\frac{\omega_K R_{K^+}}{2\pi^g R_K}\prod_\ell \nu_\ell(K) \\ &= \sqrt{\left|\frac{\Delta_K}{\Delta_{K^+}}\right|}\frac{\omega_K}{(2\pi)^g}\prod_\ell \nu_\ell(K) \\ &= \omega_K \nu_\infty(f)\prod_\ell \nu_\ell(K).\end{aligned}$$

□

Remark 8.2. Propositions 7.1 and 7.3 tell us that in many cases the $\nu_\ell(K)$ in the previous proposition is in fact equal to $\nu_\ell(f)$. While we did not give the orders of the centralizers of the non-semisimple conjugacy classes for all odd prime g in this paper, we have partial progress which suggests that Proposition 7.6 will also generalize to all odd prime g. On the assumption that Proposition 7.6 in fact generalizes to all odd prime g, we make the following conjecture.

Conjecture 8.3. *Let g be an odd prime, and let f be a degree $2g$ q-Weil polynomial that is ordinary, principally polarizable, cyclic, and maximal. Let K be the splitting field of f over $\mathbb{Q}$ and let K^+ be its maximal totally real subfield. Then*

$$\nu_\infty(f)\prod_\ell \nu_\ell(f) = \frac{1}{\omega_K}\frac{h_K}{h_{K^+}}. \tag{8.2}$$

Proof. For any primes ℓ where $f_{\mathcal{C}} = f \bmod \ell$ has one of the regular semisimple shapes in Table 3.1, Propositions 7.1 and 7.3 give that $\nu_\ell(f) = \nu_\ell(K)$.

Assume that $\nu_\ell(f) = \nu_\ell(K)$ for primes ℓ where $f_{\mathcal{C}} = f \bmod \ell$ is non-semisimple for all odd prime g. (That is, assume a version of Proposition 7.6 is true for all odd prime g.) Then for all primes ℓ we have $\nu_\ell(f) = \nu_\ell(K)$, and so by Proposition 8.1 the conjecture would be true. □

In the case where $g = 3$, we can say more.

Theorem 8.4. *Let f be a degree 6 q-Weil polynomial that is ordinary, principally polarizable, cyclic, and maximal. Let K be the splitting field of f over $\mathbb{Q}$ and let K^+ be its maximal totally real subfield. Then*

$$\nu_\infty(f)\prod_\ell \nu_\ell(f) = \frac{1}{\omega_K}\frac{h_K}{h_{K^+}}.$$

Proof. Combine Proposition 7.6 with Propositions 7.1, 7.3, and 8.1 for $g = 3$, and the theorem is proven. □

While Theorem 8.4 and Conjecture 8.3 are interesting in their own right as an unexpected equality of a product of local densities of matrices to a ratio of class numbers, there is an interpretation of this quantity related to isogeny classes of abelian varieties via results in a preprint of Everett Howe [6].

We begin with some notation. Given a Weil polynomial $f \in \mathbb{Z}[T]$, let K, π_f, $\bar{\pi}_f$, K^+, and $\mathcal{O}_f$ be defined as in section 2 and let $\mathcal{O}_{f^+} = \mathbb{Z}[\pi_f + \bar{\pi}_f]$. Let U be the unit group of $\mathcal{O}_f$ and let $U^+_{>0}$ be the group of totally positive units in $\mathcal{O}_{f^+}$. Denote the narrow class number of K^+ by $h^+_{K^+}$.

Theorem 8.5 (Howe)**.** *Let $\mathcal{I}$ be an isogeny class of simple ordinary abelian varieties over $\mathbb{F}_q$ corresponding to an irreducible Weil polynomial $f \in \mathbb{Z}[T]$. Using the notation above, suppose that $\mathcal{O}_f$ is the maximal order of K, and suppose that K is ramified over K^+ at a finite prime. Then the number of abelian varieties in $\mathcal{I}$ that have a principal polarization is equal to $\frac{h_K}{h^+_{K^+}}$, and each such variety has (up to isomorphism) exactly $[U^+_{>0} : N(U)]$ principal polarizations, where N is the norm map from U to $U^+_{>0}$.*

We note that the conditions in Theorem 8.5 are indeed met under our conditions; we assume that the abelian varieties are ordinary in (W.1), the polynomial f is irreducible in (W.3), and $\mathcal{O}_f$ is the maximal order of K

in (W.4). By [5, Lemma 10.2], K is ramified over K^+ at a finite prime whenever g is odd.

Corollary 8.6. *Let everything be as in Theorem 8.5. If in addition the unit groups of K and K^+ are equal, then the total number of principally polarized varieties lying in the isogeny class $\mathcal{I}$ is equal to h_K/h_{K^+}.*

Proof. If the unit groups of K and K^+ are equal, then the ratio $\frac{h^+_{K^+}}{h_{K^+}}$ is equal to $[U^+_{>0} : N(U)]$ and the result follows from Theorem 8.5. □

Remark 8.7. Corollary 8.6 generalizes the classical result that the number of elliptic curves in a fixed isogeny class is given by the class number of an appropriate imaginary quadratic field.

We assume in (W.3) that $K/\mathbb{Q}$ is cyclic, which implies that Hasse's unit index is 1 (see the proof of Proposition 8.1). Thus, under our conditions, the unit groups of K and K^+ are equal, and so we can apply Corollary 8.6.

Recall that $\mathcal{A}_g(\mathbb{F}_q; f)$ denotes the set of isomorphism classes of principally polarized abelian varieties of dimension g over $\mathbb{F}_q$ with characteristic polynomial of Frobenius f, weighted inversely by the size of the automorphism group. Then we have the following corollary of Theorem 8.4.

Corollary 8.8. *Let f be as in Theorem 8.4. Then*

$$\nu_\infty(f) \prod_\ell \nu_\ell(f) = \#\mathcal{A}_3(\mathbb{F}_q; f).$$

Proof. From Corollary 8.6, the (unweighted) size of the isogeny class of principally polarized abelian threefolds with characteristic polynomial $f(T)$ is $\frac{h_K}{h_{K^+}}$. The size of the automorphism group of any element of that isogeny class is ω_K, so

$$\frac{1}{\omega_K} \frac{h_K}{h_{K^+}} = \#\mathcal{A}_3(\mathbb{F}_q; f)$$

and the corollary is proven. □

If we also assume Conjecture 8.3, then we can state the following corollary, which generalizes the previous result.

Corollary 8.9. *Assume that Conjecture 8.3 is true and let f be as in that conjecture. Then*

$$\nu_\infty(f) \prod_\ell \nu_\ell(f) = \#\mathcal{A}_g(\mathbb{F}_q; f).$$

Recent work of Marseglia gives an algorithm for computing isomorphism classes of abelian varieties in certain isogeny classes [8]. One possible application of the algorithm, according to the author, is to provide computational evidence for the main formulas in [2], [1], and the present work.

Acknowledgments. We thank Everett Howe for sharing with us his work related to isogeny classes of principally polarized abelian varieties, and Jeff Achter for very helpful conversations. We also thank the referee for useful suggestions and insightful questions.

References

[1] Achter, Jeffrey D.; Gordon, Julia. Elliptic curves, random matrices and orbital integrals. *Pacific J. Math.* **286** (2017), no. 1, 1–24. MR3582398, Zbl 1379.11065, arXiv:1510.07068, doi: 10.2140/pjm.2017.286.1. 142

[2] Achter, Jeffrey; Williams, Cassandra. Local heuristics and an exact formula for abelian surfaces over finite fields. *Canad. Math. Bull.* **58** (2015), no. 4, 673–691. MR3415659, Zbl 1354.14068, arXiv:1403.3037, doi: 10.4153/CMB-2015-050-8. 123, 124, 125, 127, 128, 131, 132, 133, 139, 142

[3] Furuya, Hisako. Principal ideal theorems in the genus field for absolutely Abelian extensions. *J. Number Theory* **9** (1977), no. 1, 4–15. MR0429820 (55 #2830), Zbl 0347.12006, doi: 10.1016/0022-314X(77)90045-2. 140

[4] Gekeler, Ernst-Ulrich. Frobenius distributions of elliptic curves over finite prime fields. *Int. Math. Res. Not.* **2003** no. 37, 1999–2018. MR1995144 (2004d:11048), Zbl 1104.11033, doi: 10.1155/S1073792803211272. 123, 131

[5] Howe, Everett W. Principally polarized ordinary abelian varieties over finite fields. *Trans. Amer. Math. Soc.* **347** (1995), no. 7, 2361–2401. MR1297531 (96i:11065), Zbl 0859.14016, doi: 10.2307/2154828. 126, 142

[6] Howe, Everett W. Variations in the distribution of principally-polarized abelian varieties among isogeny classes. Preprint, 2018. 124, 126, 141

[7] Katz, Nicholas M. Lang–Trotter revisited. *Bull. Amer. Math. Soc.* (N.S.) **46** (2009), no. 3, 413–457. MR2507277 (2010f:11088), Zbl 1234.11072, doi: 10.1090/S0273-0979-09-01257-9. 123

[8] Marseglia, Stefano. Computing square-free polarized abelian varieties over finite fields. Preprint, 2018. arXiv:1805.10223. 142

[9] Rauch, Job. Using heuristics on local matrix groups to count Abelian surfaces. Master's thesis, Leiden University, August 2017. 125

[10] Shinoda, Ken-ichi. The characters of Weil representations associated to finite fields. *J. Algebra* **66** (1980), no. 1, 251–280. MR591256 (81k:20017), Zbl 0444.20034, doi: 10.1016/0021-8693(80)90123-4. 127, 129

[11] Tate, John. Endomorphisms of abelian varieties over finite fields. *Invent. Math.* **2** (1966), 134–144. MR0206004 (34 #5829), Zbl 0147.20303, doi: 10.1007/BF01404549. 123

[12] Washington, Lawrence C. Introduction to cyclotomic fields. Second Edition. Graduate Texts in Mathematics, 83. *Springer-Verlag, New York*, 1997. xiv+487 pp. ISBN: 0-387-94762-0. MR1421575 (97h:11130), Zbl 0966.11047, doi: 10.1007/978-1-4612-1934-7. 140

[13] Weyl, Hermann. The classical groups. Their invariants and representations. Fifteenth printing. Princeton Landmarks in Mathematics. Princeton Paperbacks. *Princeton University Press, Princeton, NJ*, 1997. xiv+320 pp. ISBN: 0-691-05756-7. MR1488158 (98k:01049), Zbl 1024.20501. 132

(Jonathan Gerhard) James Madison University, Harrisonburg, VA 22807, USA
gerha2jm@dukes.jmu.edu

(Cassandra Williams) James Madison University, Harrisonburg, VA 22807, USA
willi5cl@jmu.edu
http://educ.jmu.edu/~willi5cl

This paper is available via http://nyjm.albany.edu/j/2019/25-5.html.