Frobenius Distribution for Quotients of Fermat Curves of Prime Exponent

Dedicated to Josep Grané on the occasion of his 70th birthday

Francesc Fité, Josep González, and Joan-Carles Lario

Abstract. Let $\mathcal{C}$ denote the Fermat curve over $\mathbb{Q}$ of prime exponent ℓ. The Jacobian $\mathrm{Jac}(\mathcal{C})$ of $\mathcal{C}$ splits over $\mathbb{Q}$ as the product of Jacobians $\mathrm{Jac}(\mathcal{C}_k)$, $1 \le k \le \ell - 2$, where $\mathcal{C}_k$ are curves obtained as quotients of $\mathcal{C}$ by certain subgroups of automorphisms of $\mathcal{C}$. It is well known that $\mathrm{Jac}(\mathcal{C}_k)$ is the power of an absolutely simple abelian variety B_k with complex multiplication. We call degenerate those pairs (ℓ, k) for which B_k has degenerate CM type. For a non-degenerate pair (ℓ, k), we compute the Sato–Tate group of $\mathrm{Jac}(\mathcal{C}_k)$, prove the generalized Sato–Tate Conjecture for it, and give an explicit method to compute the moments and measures of the involved distributions. Regardless of whether (ℓ, k) is degenerate, we also obtain Frobenius equidistribution results for primes of certain residue degrees in the ℓ-th cyclotomic field. Key to our results is a detailed study of the rank of certain generalized Demjanenko matrices.

1 Introduction

Both from the theoretical and the computational points of view, the problem of determining Frobenius distributions of low genus curves has attracted a growing interest in the past years (see, for example, [KS09, Ser12, FKRS12, FS14]). In this paper, we consider this problem for a family of curves of arbitrary high genus and that have simple Jacobian in many cases. More concretely, for a prime ℓ and an integer $1 \le k \le \ell - 2$, we are concerned with the limiting distribution of the normalized Euler local factors $L_p(\mathcal{C}_k, T/\sqrt{p})$ attached to the curves $\mathcal{C}_k$ defined by the affine equation

$$v^\ell = u(u+1)^{\ell-k-1}.$$

The curves $\mathcal{C}_k$ have genus $\frac{\ell-1}{2}$ and may be obtained as quotients of the Fermat curve $\mathcal{C} : y^\ell = x^\ell + 1$ by certain subgroups of automorphisms of $\mathcal{C}$. One can in fact show that the Jacobian of $\mathcal{C}$ decomposes up to isogeny over $\mathbb{Q}$ as the product

$$\mathrm{Jac}(\mathcal{C}) \sim_{\mathbb{Q}} \prod_{k=1}^{\ell-2} \mathrm{Jac}(\mathcal{C}_k).$$

It is also well known that the L-function of $\mathrm{Jac}(\mathcal{C}_k)$ can be written in terms of Hecke L-functions attached to Jacobi sums and that $\mathrm{Jac}(\mathcal{C}_k)$ is the power of an absolutely

---

361

simple abelian variety B_k with complex multiplication, say of dimension r_k. This is all recalled in the preliminary Section 2.

We now procced to describe the three main results of the paper. We say that a pair (ℓ, k) is non-degenerate if the dimension of the Hodge group $\mathrm{Hg}(B_k)$ is maximal (that is, equal to r_k). This is equivalent to saying that the CM-type of B_k is non-degenerate (in the sense of Kubota) or that the determinant of the Demjanenko matrix D_k does not vanish. The $r_k \times r_k$ matrix D_k can be elementarily constructed, and has been extensively studied in the literature (see, for example, [Haz90, SS95, Doh94]).

The generalized Sato–Tate Conjecture for $\mathrm{Jac}(\mathcal{C}_k)$ predicts the existence of a compact real Lie group $\mathrm{ST}(\mathrm{Jac}(\mathcal{C}_k)) \subseteq \mathrm{USp}(\ell - 1)$, the Sato–Tate group, that determines the limiting distribution of the normalized Euler local factors $L_p(\mathcal{C}_k, T/\sqrt{p})$. The main result in Section 3 is the computation of $\mathrm{ST}(\mathrm{Jac}(\mathcal{C}_k))$ along with a proof of the equidistribution predicted by the generalized Sato–Tate Conjecture (see Proposition 3.9, Conjecture 3.13, and Theorem 3.15).

Theorem 1.1 *If (ℓ, k) is a non-degenerate pair, the generalized Sato–Tate Conjecture holds for* $\mathrm{Jac}(\mathcal{C}_k)$.

The connected component of $\mathrm{ST}(\mathrm{Jac}(\mathcal{C}_k))$ is a product of a certain number of copies of the unitary group $\mathrm{U}(1)$. This is easy to deduce from the well-known structure of $\mathrm{Hg}(\mathrm{Jac}(\mathcal{C}_k))$. The main novelty concerning the computation of $\mathrm{ST}(\mathrm{Jac}(\mathcal{C}_k))$ is the description of its group of components. Abstractly, the group of components is simply isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^*$. However, if one seeks to provide an explicit description of the limiting distribution of $L_p(\mathcal{C}_k, T/\sqrt{p})$, one needs to supply an explicit embedding of $\mathrm{ST}(\mathrm{Jac}(\mathcal{C}_k))$ inside $\mathrm{USp}(\ell - 1)$.

Following Serre's general strategy, our proof of equidistribution is based on the nonvanishing of certain L-functions attached to the irreducible nontrivial representations of $\mathrm{ST}(\mathrm{Jac}(\mathcal{C}_k))$. Then, we apply a theorem of Hecke on the holomorphicity and nonvanishing for $\Re(s) \geq 1$ of the L-functions attached to unitarized nontrivial Hecke characters. It should be mentioned that it is precisely the nonvanishing of $\det(D_k)$ that ensures that the Hecke character involved in the proof, which is constructed by means of Jacobi sums, is nontrivial. A proof of equidistribution for abelian varieties with complex multiplication in general is certainly well known to the experts (see Johansson [Joh13]). However, in our particular example, once one has an explicit description of $\mathrm{ST}(\mathrm{Jac}(\mathcal{C}_k))$, one can show equidistribution in an elementary and very explicit way, that we illustrate in Theorem 3.15.

Naturally, we call degenerate the pairs (ℓ, k) for which $\mathrm{rk}(D_k) < r_k$. Building on several known results (see [Kub65, Gre80, Rib80]), we prove in the following theorem Section 4 (see Theorem 4.10).

Theorem 1.2 *A pair (ℓ, k) is degenerate if and only if the following three conditions hold:*

(i)   *k is not a primitive cubic root of unity modulo ℓ;*
(ii)   *$\mathrm{ord}(-k^2 - k)$ and $\mathrm{ord}(k)$ are odd, where* ord *means the order in $(\mathbb{Z}/\ell\mathbb{Z})^*$;*
(iii) *$v_3(\mathrm{ord}(k)) > v_3(\mathrm{ord}(k^2 + k))$, where v_3 denotes the 3-adic valuation.*

In this case,

$$\dim\big(\operatorname{Hg}(\operatorname{Jac}(\mathcal{C}_k))\big) = \operatorname{rk}(D_k) = \frac{\ell-1}{2}\Big(1 - \frac{2}{N_k}\Big),$$

where $N_k := \operatorname{lcm}(\operatorname{ord}(-k^2 - k), \operatorname{ord}(k))$.

The previous result has several consequences. As an example, one can deduce that the rank of D_k is "asymptotically non-degenerate"; that is,

$$\lim_{\substack{\ell \to \infty \\ 1 \le k \le \ell-2}} \frac{\operatorname{rk}(D_k)}{r_k} = 1.$$

However, our interest in the previous theorem is motivated by the fact that it constitutes the fundamental technical result for the discussion in Section 5. In that section, we are concerned with limiting distributions when restricting to primes of a given residue degree f in $\mathbb{Q}(\zeta_\ell)$. With this in mind, for each divisor f of $\ell-1$, we define a matrix $D_{k,f}$, which may be seen as a generalization of D_k, and say that f is a *non-k-degenerate residue degree* if $\det(D_{k,f}) \neq 0$. We then achieve the following concrete characterization. A divisor f of $\ell-1$ is non-k-degenerate if and only if it is odd and either

(a) (ℓ, k) is non-degenerate, or
(b) (ℓ, k) is degenerate and $f \in \mathcal{F}_0 \cup \mathcal{F}_1$.

Here, $\mathcal{F}_0$ (resp. $\mathcal{F}_1$) is the set of odd divisors of $\ell-1$ such that $v_3(f) = v_3(N_k) - 1$ and f is a multiple of $N_k/3$ (resp. such that $v_3(f) \ge v_3(N_k)$). We say that f is k-degenerate otherwise. Note that when (ℓ, k) is degenerate, there are still non-k-degenerate divisors f of $\ell-1$. In Section 5, we develop a method to compute the limiting distribution of $L_p(\mathcal{C}_k, T/\sqrt{p})$ when restricting to primes p of any fixed *non-k-degenerate* residue degree f in $\mathbb{Q}(\zeta_\ell)$. This method is based on a detailed analysis of the local factors of $\operatorname{Jac}(\mathcal{C}_k)$ and works independently of the construction of $\operatorname{ST}(\operatorname{Jac}(\mathcal{C}_k))$ (which we recall that we are only able to achieve for non-degenerate pairs (ℓ, k)).

The rank of $D_{k,f}$ depends on the size $n_{k,f}$ of a certain subgroup $W_{k,f}$ of $(\mathbb{Z}/\ell\mathbb{Z})^*$. A comprehensive description of the subgroup $W_{k,f}$ will be given in Section 4. For the purpose of stating our last main result, it will suffice for the moment to mention that

$$n_{k,f} = \begin{cases} 3f & \text{if } k \text{ is a primitive cubic root of unity and } v_3(f) = 0, \\ 3f & \text{if } (\ell, k) \text{ is degenerate and } f \in \mathcal{F}_0, \\ f & \text{otherwise.} \end{cases}$$

The following theorem is a combination of Corollary 5.3 and Theorem 5.5.

Theorem 1.3   *Let* $p \neq \ell$ *be a prime of residue degree* f *in* $\mathbb{Q}(\zeta_\ell)$. *Then*

$$L_p(\mathcal{C}_k, T/\sqrt{p}) = \begin{cases} (1 + T^f)^{(\ell-1)/f} & \text{if } f \text{ is even,} \\ \prod_{i=1}^{r_{k,f}} (1 + s_i(p) T^f + T^{2f})^{(n_{k,f})/f} & \text{if } f \text{ is non-}k\text{-degenerate,} \end{cases}$$

where $s_i(p) \in [-2, 2]$ *and* $r_{k,f} = (\ell-1)/(2n_{k,f})$. *Moreover, in the case that* f *is non-k-degenerate, the sequence* $\{(s_1(p), \ldots, s_{r_{k,f}}(p))\}_p$, *where* $p \neq \ell$ *runs over the set of*

primes of residue degree f in $\mathbb{Q}(\zeta_\ell)$, is equidistributed over $[-2,2]^{r_{k,f}}/\mathfrak{S}_{r_{k,f}}$ with respect to the measure

$$\prod_{i=1}^{r_{k,f}} \frac{1}{\pi} \frac{dx_i}{\sqrt{4-x_i^2}},$$

where $\mathfrak{S}_{r_{k,f}}$ denotes the symmetric group on $r_{k,f}$ letters.

The case of even f is easy and well known (see [GR78, Lemma 1.1]). The proof for the case of non-k-degenerate f relies again on the result of Hecke mentioned above. Now, the nontriviality of the Hecke character appearing in the core of the proof is ensured by the nonvanishing of the determinant of the matrix $D_{k,f}$. In Section 6, examples and numerical data are shown. Tables 2 and 3 compare the theoretical moments with the moment statistics up to 2^{27} for the first trace of $L_p(\mathcal{C}_k, T/\sqrt{p})$ for a few choices of (ℓ, k).

Notation and conventions Throughout the article, we will write ζ_ℓ for a primitive ℓ-th root of unity, $F := \mathbb{Q}(\zeta_\ell)$, $G := (\mathbb{Z}/\ell\mathbb{Z})^*$, and g for a generator of G. Also, for $a \in G$ or a a rational number with denominator coprime to ℓ, the symbol $\langle a \rangle \in \mathbb{Z}$ will denote the unique representative of a modulo ℓ between 0 and $\ell-1$ (to avoid any potential confusion, $\langle a \rangle$ should not be thought of as the subgroup of of G generated by a). We will use left exponential notation for Galois actions. We will identify G and $\mathrm{Gal}(F/\mathbb{Q})$ via the isomorphism

$$G \longrightarrow \mathrm{Gal}(F/\mathbb{Q}), \qquad t \longmapsto \sigma_t, \qquad \text{where } {}^{\sigma_t}(\zeta_\ell) := \zeta_\ell^t.$$

Any number field will K be assumed to belong to a fixed algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$, and we will write $G_K := \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ for its absolute Galois group. We will refer to the prime ideals of the ring of integers $\mathcal{O}_K$ of a number field K, simply as primes of K. For an algebraic variety X defined over a number field K and an extension L/K, we will denote by X_L the base change of X to L. For an abelian variety A over K and a prime ideal $\mathfrak{p}$ of K of good reduction for A, we will let

$$L_{\mathfrak{p}}(A, T) = \prod_{i=1}^{2\dim(A)} (1 - \alpha_i T)$$

denote the local factor of A at $\mathfrak{p}$, that is the polynomial with the defining property that for each positive integer n

$$|A(\mathbb{F}_{q^n})| = \prod_{i=1}^{2\dim(A)} (1 - \alpha_i^n),$$

where $q = N\mathfrak{p}$ is the norm of $\mathfrak{p}$.

2 Preliminaries

Fix a prime $\ell \geq 3$. Let us denote by $\mathcal{C}$ the Fermat curve over $\mathbb{Q}$ defined as the projective closure of the affine curve $y^\ell = x^\ell + 1$. It is well known that the curve $\mathcal{C}$ has genus $\binom{\ell-1}{2}$,

good reduction at all primes $p \neq \ell$, and no singular points. Moreover, the set

$$\omega_{i,j} := \frac{x^{j-1}}{y^i} dx,$$

for $2 \leq i \leq \ell - 1$ and $1 \leq j \leq i - 1$ is a basis of the $\mathbb{Q}$-vector space of regular differentials $\Omega^1_{\mathcal{C}/\mathbb{Q}}$. In this section we will recall results concerning the decomposition of the Jacobian of $\mathcal{C}$ over $\mathbb{Q}$. We will particularize a result of [KR78] to the case of prime exponent ℓ that completely characterizes the absolutely simple factors of this decomposition. Then we will introduce the Hecke characters that describe the L-functions attached to these simple factors.

2.1 Decomposing the Jacobian of a Fermat Curve

Proposition 2.1 *For every integer k such that $1 \leq k \leq \ell - 2$ we denote by $\mathcal{C}_k$ the normalization of the projective closure of the affine curve given by the equation*

$$v^\ell = u(u+1)^{\ell-k-1}.$$

(i) *The morphism $\pi_k \colon \mathcal{C} \to \mathcal{C}_k$ defined by the assignment*

$$(x, y) \longmapsto (u, v) = (x^\ell, x\, y^{\ell-k-1})$$

has degree ℓ.

(ii) *Let $\mathcal{A}_k$ be the $\mathrm{Gal}(F/\mathbb{Q})$-stable subgroup of automorphisms of $\mathcal{C}$ generated by γ_k, where γ_k is defined by the assignment $(x, y) \mapsto (x\, \zeta_\ell^{k+1}, y\, \zeta_\ell)$. The curve $\mathcal{C}_k$ is the quotient curve of $\mathcal{C}$ by $\mathcal{A}_k$ and its genus is $\frac{\ell-1}{2}$.*

(iii) *$\mathrm{Jac}(\mathcal{C})$ is isogenous over $\mathbb{Q}$ to the abelian variety $\prod_{k=1}^{\ell-2} \mathrm{Jac}(\mathcal{C}_k)$.*

Proof Since γ_k has order ℓ and $\pi_k \circ \gamma_k = \pi_k$, it follows that $\mathcal{C}_k \simeq \mathcal{C}/\mathcal{A}_k$. Due to the fact that $\mathcal{A}_k$ is $\mathrm{Gal}(F/\mathbb{Q})$-stable, the isomorphism between both curves is defined over $\mathbb{Q}$. The automorphism γ_k has no fixed points, and, thus, π_k is unramified. By applying Hurwitz's formula, we deduce that the genus of $\mathcal{C}_k$ is equal to $(\ell-1)/2$, yielding (ii).

It can be checked that $\pi_k^*(\Omega^1_{\mathcal{C}_k/\mathbb{Q}}) = (\Omega^1_{\mathcal{C}/\mathbb{Q}})^{\mathcal{A}_k}$ is the space generated by the differentials $\omega_{i,j}$, where

(2.1) $$2 \leq i \leq \ell - 1, \quad 1 \leq j \leq i - 1, \quad (k+1) \cdot j \equiv i \pmod{\ell},$$

and hence we obtain that

$$\Omega^1_{\mathcal{C}/\mathbb{Q}} = \bigoplus_{k=2}^{\ell-1} \pi_k^*(\Omega^1_{\mathcal{C}_k/\mathbb{Q}}),$$

and (iii) follows. ∎

For $r, s \geq 1$ with $r + s \leq \ell - 1$, define the set $H_{r,s}$ and the group $V_{r,s}$ as

$$H_{r,s} := \{ j \in G \mid \langle rj \rangle + \langle sj \rangle < \ell \}, \qquad V_{r,s} := \{ w \in G \mid wH_{r,s} = H_{r,s} \}.$$

Remark 2.2 Observe that $H_{r,s} = tH_{\langle tr \rangle, \langle ts \rangle}$ for any $t \in G$.

Theorem 2.3 (see [KR78, Theorem 1], [ST61]) *For $1 \leq k \leq \ell - 2$, we have*

(i) $\mathrm{Jac}(\mathcal{C}_k) \sim_F B_k^{|V_{k,1}|}$, where B_k is a simple abelian variety defined over F of dimension $\frac{\ell-1}{2|V_{k,1}|}$ with CM by the fixed subfield $F^{V_{k,1}}$ and CM type equal to $H_{k,1}/V_{k,1}$;

(ii) $\mathrm{Jac}(\mathcal{C}_k) \sim_F \mathrm{Jac}(\mathcal{C}_{k'})$ if and only if we have an equality of sets $H_{k,1} = H_{k',1}$.

(iii) $H_{r,s} = H_{r',s'}$ if and only if $\{r, s, \ell - r - s\} = \{\langle t \rangle, \langle tr' \rangle, \langle -t(r' + s')\rangle\}$ for some $t \in G$.

Remark 2.4   The previous theorem is stated in [KR78] in terms of abelian varieties $A_{k,1}$ defined by certain lattices $L_{k,1}$. To see that $A_{k,1}$ and $\mathrm{Jac}(\mathcal{C}_k)$ coincide we refer the reader to the Appendix of Rohrlich in [Gro78].

Let S and T be the permutations of the set of indices $\{1, \dots, \ell - 2\} \subseteq \mathbb{Z}$ defined by $T(k) := \langle \frac{-k}{k+1} \rangle$ and $S(T) := \langle \frac{1}{k} \rangle$, and let $\mathcal{M}$ be the group of permutations generated by S and T, which is isomorphic to the dihedral group of six elements. The orbit of k under the action of $\mathcal{M}$ is

$$\mathcal{M}(k) := \left\{ M(k) \mid M \in \mathcal{M} \right\} = \left\{ k, \left\langle \frac{-1}{k+1} \right\rangle, \left\langle \frac{-k-1}{k} \right\rangle, \left\langle \frac{-k}{k+1} \right\rangle, \langle -k-1 \rangle, \left\langle \frac{1}{k} \right\rangle \right\}.$$

For $\ell > 3$, this set has generically six elements, except when $k \in \{\ell - 2, 1, (\ell - 1)/2\}$, in which case $\mathcal{M}(k) = \{\ell - 2, 1, (\ell - 1)/2\}$, or k is a primitive cubic root of unity modulo ℓ, in which case $\mathcal{M}(k) = \{k, \ell - k - 1\}$.

Lemma 2.5   *For $1 \le k, k' \le \ell - 2$, the following statements are equivalent:*

(i) $\mathcal{C}_k \simeq_{\mathbb{Q}} \mathcal{C}_{k'}$.

(ii) $\mathrm{Jac}(\mathcal{C}_k) \sim_F \mathrm{Jac}(\mathcal{C}_{k'})$.

(iii) $k' \in \mathcal{M}(k)$.

In particular, for $\ell > 3$, there are exactly $(\ell + 5)/6$ or $(\ell + 1)/6$ isogeny classes among the jacobians of the $\ell - 2$ curves $\mathcal{C}_k$ depending on whether $\ell \equiv 1 \pmod 3$ or not.

Proof   It is obvious that (i) implies (ii). It is a straightforward computation to see that $\{1, k, \ell - k - 1\} = \{\langle t \rangle, \langle tk' \rangle, \langle -t(k' + 1)\rangle\}$ for some $t \in G$ if and only if $k' \in \mathcal{M}(k)$, and then use (ii) and (iii) of Theorem 2.3. To see that (iii) implies (i), let $\lambda, \mu \in \mathrm{Aut}_{\mathbb{Q}}(\mathcal{C})$ be the automorphisms defined by the assignments

$$\lambda \colon (x, y) \longmapsto (-y, -x), \quad \mu \colon (x, y) \longmapsto (1/x, y/x).$$

Since

$$\gamma_{\langle -k/(k+1)\rangle}^{-(k+1)} \circ \lambda \circ \gamma_k = \lambda \quad \text{and} \quad \gamma_{\langle 1/k\rangle}^{k} \circ \mu \circ \gamma_k = \mu,$$

it follows that λ (resp. μ) induces an isomorphism between $\mathcal{C}_{\langle -k/(k+1)\rangle}$ (resp. $\mathcal{C}_{\langle 1/k\rangle}$) and $\mathcal{C}_k$ defined over $\mathbb{Q}$. Thus, $\mathcal{C}_{M(k)}$ and $\mathcal{C}_k$ are isomorphic over $\mathbb{Q}$ for all $M \in \mathcal{M}(k)$. ∎

For $1 \le k \le \ell - 2$, set $M_k := H_{k,1}$ and $W_k := V_{k,1}$ in order to simplify notation. Let n_k denote the cardinality of W_k. Note that we have

(2.2)
$$M_k = \left\{ j \in G \mid \langle kj \rangle + \langle j \rangle < \ell \right\} = \left\{ j \in G \mid \langle j \rangle < \langle (k+1)j \rangle \right\},$$
$$W_k = \{ w \in G \mid wM_k = M_k \}.$$

Remark 2.6 Observe that the previous description of M_k, together with the conditions in (2.1), shows that

$$\omega_j := \frac{x^{\langle j \rangle - 1}}{y^{\langle (k+1)j \rangle}} \, dx \qquad \text{with} \qquad j \in M_k$$

is a basis of $\pi_k^*(\Omega^1_{\mathcal{C}_k/\mathbb{Q}})$.

Lemma 2.7 (see [KR78, Theorem 2]) *For $1 \le k \le \ell - 2$, we have that n_k is 1 or 3. Moreover, $n_k = 3$ if and only if k is a primitive cubic root of unity modulo ℓ. In this case, we have that $W_k = \{1, k, -k-1\} \subseteq G$.*

Proof We will show that for $1 \le k \le \ell - 2$, the cardinality of $V_{k,1}$ is 1 or 3. Suppose that $w \ne 1$ lies in $V_{k,1}$; that is, $wH_{k,1} = H_{k,1}$. Note that by Remark 2.2 this means that $H_{wk,w} = H_{k,1}$. We will show that both w and k are primitive cubic roots of unity modulo ℓ. By Theorem 2.3(iii), we have

$$\{1, k, \ell - k - 1\} = \left\{ \langle w \rangle, \langle wk \rangle, \langle -w(k+1) \rangle \right\}.$$

Therefore, either $w \equiv k \pmod{\ell}$ or $w \equiv -k-1 \pmod{\ell}$. Suppose first that $w \equiv k \pmod{\ell}$. Then

$$\{1, w, \ell - w - 1\} = \left\{ \langle w \rangle, \langle w^2 \rangle, \langle -w^2 - w \rangle \right\}.$$

Then either $1 \equiv w^2 \pmod{\ell}$ or $1 \equiv -w - w^2 \pmod{\ell}$. The first option is impossible since it implies that $w \equiv -1 \pmod{\ell}$, and thus $k + 1 \equiv 0 \pmod{\ell}$, which is a contradiction. Thus, $w^2 + w + 1 \equiv 0 \pmod{\ell}$ as desired. The case $w \equiv -k-1 \pmod{\ell}$ is completely analogous. Conversely, assume that k is a primitive cubic root of unity. We want to see that if $j \in M_k$, then also $kj \in M_k$. This follows from

$$\langle kj \rangle + \langle k^2 j \rangle = \langle kj \rangle + \left\langle -(k+1)j \right\rangle = \langle kj \rangle + \ell - \langle kj \rangle - \langle j \rangle < \ell. \qquad \blacksquare$$

Remark 2.8 We can now show that B_k may be taken as the Jacobian of a curve defined over $\mathbb{Q}$. Assume that k is a primitive cubic root of unity modulo ℓ (otherwise $n_k = 1$, and there is nothing to prove). Let $t \in \mathbb{Z}$ be such that $1 + k + k^2 = \ell t$. The automorphism $\nu := \mu \circ \lambda$ of $\mathcal{C}$ (λ and μ as in the proof of Lemma 2.5) induces an automorphism of $\mathcal{C}_k$ of order 3 with two fixed points, which is explicitly given by the assignment

$$(u, v) \mapsto \left(-\frac{u+1}{u}, (-1)^{k-1} \frac{(1+u)^{t-k}}{u} v^k \right).$$

Hurwitz's formula shows that the genus of the quotient curve of $\mathcal{C}_k$ by the subgroup generated by ν has genus $\frac{\ell-1}{6}$. Although B_k can be taken over $\mathbb{Q}$, the isogeny $\text{Jac}(\mathcal{C}_k) \sim_F B_k^3$ does not come from an isogeny defined over $\mathbb{Q}$. Indeed, Theorem 1.3 shows that the local factor of $\mathcal{C}_k$ at a prime of residue degree $\ell - 1$ in F cannot be a cube.

2.2 Hecke Characters Attached to the Quotient Curves $\mathcal{C}_k$

For a prime $\mathfrak{p}$ in F not lying over ℓ and $x \in \mathbb{F}_{\mathfrak{p}}^*$, with $\mathbb{F}_{\mathfrak{p}} := \mathcal{O}_F/\mathfrak{p}$, let $\chi_{\mathfrak{p}}(x) \in F^*$ be the only ℓ-th root of unity satisfying the condition $\pi(\chi_{\mathfrak{p}}(x)) = x^{(N\mathfrak{p}-1)/\ell}$, where

$\pi \colon \mathcal{O}_F \to \mathbb{F}_\mathfrak{p}$ is the residue map. Then, $\chi_\mathfrak{p} \colon \mathbb{F}_\mathfrak{p}^* \to F^*$ is a character of $\mathbb{F}_\mathfrak{p}^*$ of order ℓ that we extend to $\mathbb{F}_\mathfrak{p}$ by defining $\chi_\mathfrak{p}(0) := 0$. Let $I_F(\ell)$ stand for the set of all fractional ideals of $\mathcal{O}_F$ coprime to ℓ. Then for any $a \in G$ and $1 \le k \le \ell - 2$, consider the map $J_{(ka,a)} \colon I_F(\ell) \to \mathbb{C}^*$, defined on prime ideals $\mathfrak{p}$ of $I_F(\ell)$ by

$$J_{(ka,a)}(\mathfrak{p}) := - \sum_{\nu \in \mathbb{F}_\mathfrak{p}} \chi_\mathfrak{p}(\nu)^{ka} \chi_\mathfrak{p}(\nu + 1)^a,$$

and extended to any ideal of $I_F(\ell)$ by the rule

$$J_{(ka,a)}(\mathfrak{a}\mathfrak{b}) = J_{(ka,a)}(\mathfrak{a}) J_{(ka,a)}(\mathfrak{b}).$$

If $\sigma_t \in \mathrm{Gal}(F/\mathbb{Q})$ and $\mathfrak{p}$ is a prime ideal in $I_F(\ell)$, then the following properties are satisfied

$$(2.3) \qquad {}^{\sigma_t}\big(J_{(ka,a)}(\mathfrak{p})\big) = J_{(ka,a)}({}^{\sigma_t}\mathfrak{p}), \quad {}^{\sigma_t}\big(J_{(ka,a)}(\mathfrak{p})\big) = J_{(tka,tk)}(\mathfrak{p}),$$
$$J_{(ka,a)}(\mathfrak{p})\mathcal{O}_F = \prod_{j \in M_k} {}^{\sigma_{aj^{-1}}}\mathfrak{p}.$$

It is easy to check the first equality, and the second and third are [Wei52, equalities (11) and (9)], respectively (see also [Sti90]). Weil [Wei52] showed that $J_{(ka,a)}$ is a Grössencharakter of infinity type $a M_k^{-1} := \{\langle aj^{-1}\rangle \mid j \in M_k\}$ and modulus $\ell^2 \mathcal{O}_F$; that is,

$$(2.4) \qquad J_{(ka,a)}(\alpha \mathcal{O}_F) = \prod_{j \in M_k} {}^{\sigma_{aj^{-1}}}(\alpha) \qquad \text{for all } \alpha \in F^* \text{ with } \alpha \equiv^\times 1 \pmod{\ell^2}.[1]$$

Later Hasse [Has55] showed that the conductor of $J_{(ka,a)}$ is $(1 - \zeta_\ell)\mathcal{O}_F$ or $(1 - \zeta_\ell)^2 \mathcal{O}_F$ depending on whether $\sum_{j \in M_k} j^{-1}$ is zero or not modulo ℓ. The weight of $J_{(ka,a)}$ is 1, since exactly one of j and $-j$ belongs to $a M_k^{-1}$, and thus $J_{(ka,a)}(\mathfrak{a}) J_{(ka,a)}(\overline{\mathfrak{a}}) = N\mathfrak{a}$ for every $\mathfrak{a} \in I_F(\ell)$. Moreover, for a prime ℓ', the ℓ'-adic rational Tate module of $\mathrm{Jac}(\mathcal{C}_k)$, simply denoted $V_{\ell'}(\mathcal{C}_k)$, admits a decomposition of G_F-modules

$$V_{\ell'}(\mathcal{C}_k) = \bigoplus_{a \in G} V_{(ka,a)},$$

where $V_{(ka,a)}$ is a 1-dimensional $\mathbb{Q}_{\ell'}$-vector space, on which the action of an arithmetic Frobenius $\mathrm{Frob}_\mathfrak{p}$ at $\mathfrak{p} \nmid \ell\ell'$ is by multiplication of $J_{(ka,a)}(\mathfrak{p})$ (see Deligne [Del82, §7] for a general result on the decomposition of the middle étale cohomology group of a Fermat hypersurface). In terms of L-functions, this amounts to saying that

$$L((\mathcal{C}_k)_F, s) = \prod_{a \in G} L(J_{(ka,a)}, s), \quad \text{where } L(J_{(ka,a)}, s) = \prod_{\mathfrak{p} \nmid \ell} \Big(1 - \frac{J_{(ka,a)}(\mathfrak{p})}{N\mathfrak{p}^s}\Big)^{-1}.$$

Remark 2.9 This may also be seen as a consequence of the theory of complex multiplication, which predicts that the reflex CM type M_k^{-1} of $\mathrm{Jac}(\mathcal{C}_k)$ coincides with the infinity type of the Hecke character attached to its L-function.

Lemma 2.10 *For any $a \in G$, one has*

$$L((\mathcal{C}_k)_F, s) = L(J_{(ka,a)}, s)^{\ell - 1}, \qquad L(\mathcal{C}_k, s) = L(J_{(ka,a)}, s).$$

---

[1]For $\alpha, \beta \in F^*$ and an ideal $\mathfrak{m} \subseteq \mathcal{O}_F$, we write $\alpha \equiv^\times \beta \pmod{\mathfrak{m}}$ if α and β are multiplicatively congruent modulo $\mathfrak{m}$, that is, if $v(\alpha/\beta - 1) \ge v(\mathfrak{m})$ for every discrete valuation v of F.

Proof By (2.3), we have that for every rational prime p

$$\prod_{\mathfrak{p}|p} \prod_{t \in G} \left(1 - \frac{J_{(kat,at)}(\mathfrak{p})}{N\mathfrak{p}^s}\right)^{-1} = \prod_{\mathfrak{p}|p} \prod_{\sigma \in \mathrm{Gal}(F/\mathbb{Q})} \left(1 - \frac{J_{(ka,a)}(^\sigma\mathfrak{p})}{(N^\sigma\mathfrak{p})^s}\right)^{-1}$$

$$= \prod_{\mathfrak{p}|p} \left(1 - \frac{J_{(ka,a)}(\mathfrak{p})}{N\mathfrak{p}^s}\right)^{-(\ell-1)},$$

from which the first assertion follows. For the second, note that from the Artin formalism we get the equality

$$L((\mathcal{C}_k)_F, s) = \prod_{\chi: \mathrm{Gal}(F/\mathbb{Q}) \to \mathbb{C}^*} L(\mathrm{Jac}(\mathcal{C}_k) \otimes \chi, s).$$

Therefore, it is enough to show that $L(\mathrm{Jac}(\mathcal{C}_k) \otimes \chi, s) = L(\mathrm{Jac}(\mathcal{C}_k), s)$ for every character $\chi: \mathrm{Gal}(F/\mathbb{Q}) \to \mathbb{C}^*$, or equivalently, that $V_{\ell'}(\mathcal{C}_k) \otimes \chi \simeq V_{\ell'}(\mathcal{C}_k)$ as $G_\mathbb{Q}$-modules. For this last isomorphism it is enough to show that

$$\mathrm{Tr}\, V_{\ell'}(\mathcal{C}_k)(\mathrm{Frob}_p) = 0$$

for every prime $p \nmid \ell$ and $p \not\equiv 1 \pmod{\ell}$, or equivalently that $|\mathcal{C}_k(\mathbb{F}_p)| = p + 1$ for every such prime. But it is clear that

$$\mathcal{C}_k: v^\ell = u(u+1)^{\ell-k-1}$$

has exactly p affine points defined over $\mathbb{F}_p$ if $p \not\equiv 1 \pmod{\ell}$, since in this case exponentiation by ℓ is an isomorphism of $\mathbb{F}_p^*$, and then every value of $u \in \mathbb{F}_p$ uniquely determines the value of $v \in \mathbb{F}_p$. $\blacksquare$

3 The Generalized Sato–Tate Conjecture for $\mathrm{Jac}(\mathcal{C}_k)$

In Section 2, we have seen that $\mathrm{Jac}(\mathcal{C}_k)$ decomposes over F as $B_k^{n_k}$, where B_k is an abelian variety with complex multiplication by $F_k := F^{W_k}$ and primitive CM type equal to M_k/W_k. The results of this section, will hold for pairs (ℓ, k) such that M_k/W_k is non-degenerate, notion that we will now recall.

Definition 3.1 For $k \in \{1, \ldots, \ell - 2\}$ and for $a \in G$, define

$$E_k(a) := \begin{cases} 0 & \text{if } a \in M_k, \\ 1 & \text{if } a \notin M_k. \end{cases}$$

The generalized k-Demjanenko matrix is defined as $D_k := (E_k(-c^{-1}a) - \frac{1}{2})_{c, a \in M_k/W_k}$. We will denote the size of D_k by $r_k := \frac{\ell-1}{2n_k}$ (recall that $n_k = |W_k|$).

The notion of rank of M_k/W_k was first introduced by Kubota [Kub65]. It is by definition the rank of $\Phi_k^*(\mathbb{Z}[G/W_k])$, where

$$\Phi_k^*: \mathbb{Z}[G/W_k] \to \mathbb{Z}[G/W_k], \quad \Phi_k^*([a]) = \sum_{b \in M_k/W_k} [b^{-1}][a] = \sum_{c \in G/W_k} E_k(-c^{-1}a)[c].$$

Note that Φ_k^* is well defined precisely because W_k is the subgroup of G fixing M_k.

Remark 3.2 Write $X(T_{F_k}) := \mathbb{Z}[G/W_k]$ for the character group of the torus T_{F_k} defined by F_k^*. We may see $\Phi_k^*: X(T_{F_k}) \to X(T_{F_k})$ as a map between character groups induced by a map $\Phi_k: T_{F_k} \to T_{F_k}$ between algebraic tori (see [Rib80]).

Lemma 3.3 (see [Kub65, Lemma 1]) *The rank of M_k/W_k is equal to* $\mathrm{rk}(D_k) + 1$.

Proof Let $A = (E_k(-c^{-1}a))_{c,a \in G/W_k}$ denote the matrix of Φ_k^* in the basis $M_k/W_k \cup M_{-k}/W_k$. If we write U for the $r_k \times r_k$ matrix whose entries are all ones, we obtain

$$A = \begin{pmatrix} D_k + \frac{1}{2}U & \frac{1}{2}U - D_k \\ \frac{1}{2}U - D_k & D_k + \frac{1}{2}U \end{pmatrix} \sim \begin{pmatrix} D_k + \frac{1}{2}U & \frac{1}{2}U - D_k \\ U & U \end{pmatrix}$$
$$\sim \begin{pmatrix} D_k + \frac{1}{2}U & U \\ U & 2U \end{pmatrix} \sim \begin{pmatrix} D_k & U \\ 0 & 2U \end{pmatrix}. \quad \blacksquare$$

We say that M_k/W_k is *non-degenerate* if its rank is $r_k + 1$; equivalently, if $\mathrm{rk}(D_k)$ is maximal, that is, if D_k has determinant distinct from zero, we say that the pair (ℓ, k) is non-degenerate if M_k/W_k is non-degenerate, and we say that ℓ is non-degenerate if (ℓ, k) is non-degenerate for every $1 \le k \le \ell - 2$.

Remark 3.4 For example, the degenerate primes ℓ with $3 < \ell < 400$ are

67, 127, 139, 151, 157, 163, 199, 211, 223, 271, 277, 283, 307, 331, 367, 379, 397.

Observe that Theorem 1.2 implies that any prime $\ell \equiv 2 \pmod 3$ is non-degenerate. Lenstra and Stark noticed that every sufficiently large prime $\ell \equiv 7 \pmod{12}$ is degenerate (see [Gre80, p. 354]). In fact, every prime $\ell \equiv 7 \pmod{12}$ distinct from 7 and 19 is degenerate (see [FS16] for this and also for an answer to the question concerning the proportion of $1 \le k \le \ell - 2$ for which (ℓ, k) is degenerate).

We refer the reader to Section 4 for a more explicit characterization of the degenerate pairs (k, ℓ).

3.1 The Algebraic Sato–Tate Group of $\mathrm{Jac}(\mathcal{C}_k)$

Let us start by fixing some notation. Set

$$I_2 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad J_2 := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

For any $m \ge 1$, the symplectic group $\mathrm{Sp}_{2m}/\mathbb{Q}$ is taken with respect to the symplectic form given by the block matrix $J := \mathrm{diag}(J_2, \overset{m}{\dots}, J_2)$. We have a diagonal embedding

$$\iota_{n_k}: \mathrm{Sp}_{2r_k} \hookrightarrow \mathrm{Sp}_{\ell-1}, \qquad \iota_{n_k}(A) = \mathrm{diag}(A, \overset{n_k}{\dots}, A).$$

Recall that $\mathrm{Jac}(\mathcal{C}_k) \sim_F B_k^{n_k}$. Let us write $A_k := \mathrm{Jac}(\mathcal{C}_k)$ to shorten notation. For a prime ℓ', let

$$\rho: G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(V_{\ell'}(A_k))$$

denote the ℓ'-adic representation attached to A_k. Write $G_{\ell'} := \rho(G_{\mathbb{Q}})$ and let $G_{\ell'}^{\mathrm{Zar}}$ denote its Zariski closure. Let $G_{\ell'}^1 := G_{\ell'} \cap \mathrm{Sp}_{\ell-1}$ and let $G_{\ell'}^{1,\mathrm{Zar}}$ be its Zariski closure. One may also obtain $G_{\ell'}^{1,\mathrm{Zar}}$ as $G_{\ell'}^{\mathrm{Zar}} \cap \mathrm{Sp}_{\ell-1}$ (see [BK15, §2]).

The algebraic Sato–Tate Conjecture for A_k predicts the existence of an algebraic subgroup $\mathrm{AST}(A_k)$ of $\mathrm{Sp}_{\ell-1}/\mathbb{Q}$, called the algebraic Sato–Tate group of A_k, such that

$$G_{\ell'}^{1,\mathrm{Zar}} = \mathrm{AST}(A_k) \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell'}$$

for every prime ℓ' (see [FKRS12, §2.2]). We now recall the definition of the *twisted Lefschetz group*, which we will denote by $\mathrm{TL}(A_k)$. For $\tau \in G_{\mathbb{Q}}$, set

$$\mathrm{L}(A_k)(\tau) := \{\gamma \in \mathrm{Sp}_{\ell-1} \mid \gamma\alpha\gamma^{-1} = \tau(\alpha) \text{ for all } \alpha \in \mathrm{End}((A_k)_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}\},$$

where α is seen as an endomorphism of $H_1((A_k)_{\mathbb{C}}, \mathbb{Q})$. Then one defines

$$\mathrm{TL}(A_k) := \bigcup_{\tau \in G_{\mathbb{Q}}} \mathrm{L}(A_k)(\tau).$$

Lemma 3.5 *Suppose that* (ℓ, k) *is a non-degenerate pair. The algebraic Sato–Tate Conjecture holds for* A_k *with* $\mathrm{AST}(A_k) = \mathrm{TL}(A_k)$.

Proof We will apply [FKRS12, Theorem 2.16.(a)]. It is thus enough to show that $\mathrm{Hg}(A_k) = \mathrm{L}(A_k)$, and that the Mumford–Tate Conjecture[2] holds for A_k. Here, $\mathrm{Hg}(A_k)$ denotes the Hodge group of A_k and $\mathrm{L}(A_k)$ is the *Lefschetz group*, which is $(\mathrm{L}(A_k)(\mathrm{id}))^0$ by definition. Deligne [Del82, I,Prop. 6.2] showed that $G_{\ell'}^{1,\mathrm{Zar},0} \subseteq \mathrm{Hg}(A_k) \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell'}$ for every prime ℓ'. Moreover, one has the inclusion $\mathrm{Hg}(A_k) \subseteq \mathrm{L}(A_k)$ (see [BK15, Rem. 4.3]). We will prove the two required facts simultaneously by showing that the inclusions

(3.1) $$G_{\ell'}^{1,\mathrm{Zar},0} \subseteq \mathrm{Hg}(A_k) \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell'} \subseteq \mathrm{L}(A_k) \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell'}$$

are in fact equalities. It is well known that if the first inclusion is an equality for one prime, then it is so for every prime (see [Tan96]). The same is obviously true for the second inclusion. Since the objects of the chain of inclusions (3.1) do not depend on base change by finite extensions, we can replace A_k by its base change $(A_k)_F$ to F. But then we can write (3.1) as

$$\iota_{n_k}\left(G_{\ell'}^{1,\mathrm{Zar},0}(B_k)\right) \subseteq \iota_{n_k}\left(\mathrm{Hg}(B_k) \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell'}\right) \subseteq \iota_{n_k}\left(\mathrm{L}(B_k) \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell'}\right),$$

and it thus suffices to show that the inclusions

$$G_{\ell'}^{1,\mathrm{Zar},0}(B_k) \subseteq \mathrm{Hg}(B_k) \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell'} \subseteq \mathrm{L}(B_k) \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell'}$$

are in fact equalities for some prime ℓ'. Since B_k is simple and has non-degenerate CM type, the results of [BGK03] yield

$$G_{\ell'}^{\mathrm{Zar},0}(B_k) = \left\{\mathrm{diag}(x_1, y_1, \ldots, x_{r_k}, y_{r_k}) \mid x_i, y_i \in \mathbb{Q}_{\ell'}^*, x_1 y_1 = \cdots = x_{r_k} y_{r_k}\right\}$$

for every prime ℓ' of good reduction for A_k that splits completely in F. This implies

(3.2) $G_{\ell'}^{1,\mathrm{Zar},0}(B_k) =$
$$\left\{\mathrm{diag}(x_1, y_1, \ldots, x_{r_k}, y_{r_k}) \mid x_i, y_i \in \mathbb{Q}_{\ell'}^*, x_1 y_1 = \cdots = x_{r_k} y_{r_k} = 1\right\}.$$

---

[2]The Mumford–Tate Conjecture for abelian varieties with CM is known in general, as it follows from the work of Shimura and Taniyama (see Ribet's review on [Ser68]). The recent expository article [Yu15] gives a detailed proof.

To compute $L(B_k) \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell'}$, observe that any matrix commuting with any $\beta \in \mathrm{End}(H_1((B_k)_{\mathbb{C}}, \mathbb{Q}))$ (as in Lemma 3.6, for example) must be diagonal. Imposing that it preserves J, we deduce that

$$L(B_k) \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell'} = \left\{ \mathrm{diag}\left(x_1, \frac{1}{x_1}, \dots, x_{r_k}, \frac{1}{x_{r_k}} \right) \mid x_i \in \mathbb{Q}_{\ell'}^* \right\},$$

yielding the desired equality.   ∎

Lemma 3.6   *Let* $\alpha \colon \mathcal{C}_k \to \mathcal{C}_k$ *be the automorphism defined by* $\alpha(u,v) = (u, \zeta_\ell v)$. *It induces an endomorphism of* $H_1((A_k)_{\mathbb{C}}, \mathbb{Q})$ *that we also denote by* α. *Then* $\beta := \sum_{w \in W_k} {}^w \alpha$ *is an endomorphism of* $H_1((B_k)_{\mathbb{C}}, \mathbb{Q})$ *and there exist symplectic basis of* $H_1((A_k)_{\mathbb{C}}, \mathbb{C})$ *and* $H_1((B_k)_{\mathbb{C}}, \mathbb{C})$ *(with respect to J) for which*

$$\alpha = \mathrm{diag}\left(\{\Theta_i\}_{i \in \{1, \dots, \frac{\ell-1}{2}\}} \right), \qquad \beta = \mathrm{diag}\left(\left\{ \sum_{w \in W_k} {}^w \Theta_i \right\}_{i \in \{1, \dots, \frac{\ell-1}{2n_k}\}} \right),$$

where, if g is a generator of G, then

$$\Theta_i := \begin{cases} \{\zeta_\ell^{g^i}, \overline{\zeta}_\ell^{g^i}\} & \text{if } g^i \in M_k, \\ \{\overline{\zeta}_\ell^{g^i}, \zeta_\ell^{g^i}\} & \text{if } g^i \notin M_k. \end{cases}$$

Proof   According to Remark 2.6, fix the basis

$$B := \left\{ \omega_j := \frac{x^{\langle j \rangle - 1}}{y^{\langle (k+1)j \rangle}} dx \mid j \in M_k \right\}$$

of $\pi_k^*(\Omega^1_{\mathcal{C}_k/\mathbb{Q}})$. Since $\alpha^*(\omega_j) = \zeta_\ell^j \omega_j$, we have that the matrix of α^* in the basis B is $\mathrm{diag}(\{\zeta_\ell^j \mid j \in M_k\})$. The lemma follows from taking the symplectic basis of $H_1((A_k)_{\mathbb{C}}, \mathbb{C})$ corresponding to B and the symplectic basis of $H_1((B_k)_{\mathbb{C}}, \mathbb{C})$ corresponding to $\{\omega_j \mid j \in M_k/W_k\}$.   ∎

Corollary 3.7   *The group of components of* $G_{\ell'}^{1,\mathrm{Zar}}$ *and* $\mathrm{AST}(A_k)$ *are isomorphic to* $\mathrm{Gal}(F/\mathbb{Q})$. *The connected component* $\mathrm{AST}(A_k)^0$ *is isomorphic to* $\mathrm{AST}((A_k)_F)$.

Proof   This follows from Lemma 3.5 (see [FKRS12, Prop. 2.17]).   ∎

3.2   The Sato–Tate Group of $\mathrm{Jac}(\mathcal{C}_k)$

Proposition 3.8   *If* (ℓ, k) *is a non-degenerate pair, then*

$$\mathrm{ST}\left(\mathrm{Jac}(\mathcal{C}_k)_F \right) = \left\{ \iota_{n_k}(\mathrm{diag}(u_1, \overline{u}_1, \dots, u_{r_k}, \overline{u}_{r_k})) \mid u_1, \dots, u_{r_k} \in \mathrm{U}(1) \right\} \subseteq \mathrm{USp}(\ell - 1).$$

Proof   Let ℓ' be a prime and $\mathbb{Q}_{\ell'} \hookrightarrow \mathbb{C}$ an embedding. By definition, $\mathrm{ST}(\mathrm{Jac}(\mathcal{C}_k)_F)$ is a maximal compact subgroup of

$$\mathrm{AST}\left((A_k)_F \right) \otimes_{\mathbb{Q}} \mathbb{C} \simeq \mathrm{AST}(A_k)^0 \otimes_{\mathbb{Q}} \mathbb{C} \simeq G_{\ell'}^{1,\mathrm{Zar},0} \otimes_{\mathbb{Q}_{\ell'}} \mathbb{C}.$$

But it follows immediately from (3.2) that one can take

$$\left\{ \iota_{n_k}\left(\mathrm{diag}(u_1, \overline{u}_1, \dots, u_{r_k}, \overline{u}_{r_k}) \right) \mid u_1, \dots, u_{r_k} \in \mathrm{U}(1) \right\}$$

as such a maximal compact subgroup. ∎

Proposition 3.9 *Suppose that (ℓ, k) is a non-degenerate pair. Then*

$$\mathrm{ST}\big(\mathrm{Jac}(\mathcal{C}_k)\big) \simeq \mathrm{U}(1) \times .\overset{r_k}{.}. \times \mathrm{U}(1) \rtimes (\mathbb{Z}/\ell\mathbb{Z})^*.$$

More precisely, if g is a generator of G, let

$$\gamma = \begin{pmatrix} 0 & \Gamma_2 & 0 & \ldots & 0 & 0 \\ 0 & 0 & \Gamma_3 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & \Gamma_{\frac{\ell-3}{2}} & 0 \\ 0 & 0 & 0 & \ldots & 0 & \Gamma_{\frac{\ell-1}{2}} \\ \Gamma_1 & 0 & 0 & \ldots & 0 & 0 \end{pmatrix},$$

where

$$\Gamma_i = \begin{cases} I_2 & \text{if } g^{i-1}, g^i \in M_k, \text{ or } g^{i-1}, g^i \notin M_k, \\ J_2 & \text{if } g^{i-1}, -g^i \in M_k \text{ or } -g^{i-1}, g^i \in M_k. \end{cases}$$

Then, as a subgroup of $\mathrm{USp}(\ell - 1)$, the group $\mathrm{ST}(\mathrm{Jac}(\mathcal{C}_k))$ is conjugate to the group generated by $\mathrm{ST}(\mathrm{Jac}((\mathcal{C}_k)_F))$ and γ.

Proof Let σ_g be a generator of $\mathrm{Gal}(F/\mathbb{Q})$. By Proposition 3.8 and Corollary 3.7, it suffices to prove that:

(i) $\gamma \in \mathrm{ST}(\mathrm{Jac}(\mathcal{C}_k))$;

(ii) $\gamma^{\ell-1} \in \mathrm{ST}(\mathrm{Jac}((\mathcal{C}_k)_F))$ but $\gamma^d \notin \mathrm{ST}(\mathrm{Jac}((\mathcal{C}_k)_F))$ for any proper divisor d of $\ell - 1$.

For (i) it is enough to check that $\gamma \in \mathrm{L}(A_k)(\sigma_g)$, but this is true, since one easily checks that

$$\gamma \, \mathrm{diag}\big(\{\Theta_i\}_{i \in \{1, \ldots, \frac{\ell-1}{2}\}} \big) \gamma^{-1} = \mathrm{diag}\big({}^{\sigma_g}\{\Theta_i\}_{i \in \{1, \ldots, \frac{\ell-1}{2}\}} \big)$$

(for this observe that $J_2 \big(\begin{smallmatrix} u & 0 \\ 0 & u \end{smallmatrix} \big) J_2^{-1} = \big(\begin{smallmatrix} \bar{u} & 0 \\ 0 & u \end{smallmatrix} \big)$). We now show (ii). It is obvious that if $\gamma^d \in \mathrm{ST}(\mathrm{Jac}((\mathcal{C}_k)_F))$, then $\frac{\ell-1}{2}$ divides d. It is easily checked that

$$\gamma^{\frac{\ell-1}{2}} = \mathrm{diag}\bigg(\prod_{i=1}^{\frac{\ell-1}{2}} \Gamma_i, .\overset{\frac{\ell-1}{2}}{.}., \prod_{i=1}^{\frac{\ell-1}{2}} \Gamma_i \bigg) = \mathrm{diag}\big(J_2^{\mathcal{N}_g}, .\overset{\frac{\ell-1}{2}}{.}., J_2^{\mathcal{N}_g} \big),$$

where $\mathcal{N}_g := |\{j \in M_k \,|\, gj \notin M_k\}|$. The condition $\gamma^{\frac{\ell-1}{2}} \notin \mathrm{ST}(\mathrm{Jac}((\mathcal{C}_k)_F))$ follows from $\mathcal{N}_g$ being an odd integer (note that g is not a quadratic residue modulo ℓ and then apply Lemma 3.10). This also implies

$$\gamma^{\ell-1} = \mathrm{diag}\big((-I_2)^{\mathcal{N}_g}, .\overset{\frac{\ell-1}{2}}{.}., (-I_2)^{\mathcal{N}_g} \big) = -I_{\ell-1} \in \mathrm{ST}\big(\mathrm{Jac}((\mathcal{C}_k)_F) \big). \qquad \blacksquare$$

Lemma 3.10 (Gauss Lemma) *Let $a \in G$ and write $\mathcal{N}_a := |\{j \in M_k \,|\, aj \notin M_k\}|$. Then*

$$(-1)^{\mathcal{N}_a} = \left(\frac{a}{\ell} \right).$$

Proof   Consider the product

(3.3)
$$Z_k := \prod_{j \in M_k} aj = a^{\frac{\ell-1}{2}} \prod_{j \in M_k} j \in G.$$

For $j \in G$, define

$$|j|_k := \begin{cases} j & \text{if } j \in M_k, \\ -j & \text{if } j \notin M_k. \end{cases}$$

Observe that $\{|aj|_k\}_{j \in M_k} = M_k$. Then by definition of $\mathcal{N}_a$, we have

(3.4)
$$Z_k = (-1)^{\mathcal{N}_a} \prod_{j \in M_k} |aj|_k = (-1)^{\mathcal{N}_a} \prod_{j \in M_k} j.$$

By comparing (3.3) and (3.4), we obtain $(-1)^{\mathcal{N}_a} = a^{\frac{\ell-1}{2}} = \left(\frac{a}{\ell} \right)$.   ∎

As in [FKRS12, Prop. 2.17]), Lemma 3.5 and Proposition 3.9 yield the next result.

Corollary 3.11   *Let $E/\mathbb{Q}$ be a subextension of $F/\mathbb{Q}$ and let σ_{g^i} be a generator of $\mathrm{Gal}(F/E)$ for some $0 \le i \le \ell-2$. Then $\mathrm{ST}(\mathrm{Jac}((\mathcal{C}_k)_E))$ is generated by $\mathrm{ST}(\mathrm{Jac}((\mathcal{C}_k)_F))$ and γ^i.*

3.3 Equidistribution Statements

Our next goal is to prove the generalized Sato–Tate Conjecture for $\mathrm{Jac}(\mathcal{C}_k)$, roughly speaking, the equidistribution of the Frobenius conjugacy classes on $\mathrm{ST}(\mathrm{Jac}(\mathcal{C}_k))$ with respect to its Haar measure.

Let us first recall the paradigm of Serre to prove results of equidistribution. Let $\mathcal{G}$ be a compact group and let $\mathcal{X}$ be the set of its conjugacy classes. Let P denote an infinite subset of the set of primes of a number field, and let $\{\mathfrak{p}_i\}_{i \ge 1}$ be an ordering by norm of P (there are in principle many such orderings, but equidistribution statements do not depend of fixing a particular one). Assume an assignment $\mathcal{A} : \mathfrak{p} \in P \to x_{\mathfrak{p}} \in \mathcal{X}$ is given. If $\rho : \mathcal{G} \to \mathrm{GL}_n(\mathbb{C})$ is a representation of $\mathcal{G}$, write

$$L_{\mathcal{A}}(\rho, s) = \prod_{\mathfrak{p} \in P} \det\left(1 - \rho(x_{\mathfrak{p}}) N\mathfrak{p}^{-s} \right)^{-1}.$$

Theorem 3.12   ([Ser68, p. I-23])   *Assume that for every irreducible nontrivial representation ρ of $\mathcal{G}$ the Euler product $L_{\mathcal{A}}(\rho, s)$ converges for $\mathfrak{R}(s) > 1$ and extends to a holomorphic and nonvanishing function for $\mathfrak{R}(s) \ge 1$. Then the sequence $\{x_{\mathfrak{p}_i}\}_{i \ge 1}$ is equidistributed over $\mathcal{X}$ with respect to the projection on $\mathcal{X}$ of the Haar measure of $\mathcal{G}$.*

Returning to our case, let $E/\mathbb{Q}$ be a subextension of $F/\mathbb{Q}$. Denote by $\mathcal{G}_E$ the group $\mathrm{ST}(\mathrm{Jac}(\mathcal{C}_k)_E)$ and let $\mathcal{X}_E$ be the set of conjugacy classes of $\mathcal{G}_E$. For $\wp$ a prime of E, we define a conjugacy class $x_{\wp}$ of $\mathcal{G}_E$ using the isomorphism $\mathcal{G}_E \simeq \mathcal{G}_F \rtimes \mathrm{Gal}(F/E)$.

Indeed, set

$$x_\wp := \left(\iota_{n_k}\left(\operatorname{diag}\left(\frac{J_{(ka_1,a_1)}(\mathfrak{p})}{\sqrt{N\mathfrak{p}}}, \frac{J_{(ka_1,a_1)}(\overline{\mathfrak{p}})}{\sqrt{N\mathfrak{p}}}, \ldots, \right. \right. \right.$$
$$\left. \left. \left. \frac{J_{(ka_{r_k},a_{r_k})}(\mathfrak{p})}{\sqrt{N\mathfrak{p}}}, \frac{J_{(ka_{r_k},a_{r_k})}(\overline{\mathfrak{p}})}{\sqrt{N\mathfrak{p}}} \right) \right), \operatorname{Frob}_\wp \right) \in \mathcal{X}_E,$$

where $a_1, \ldots a_{r_k}$ is a complete system of representatives of M_k/W_k, and $\mathfrak{p}$ is a prime of F lying over $\wp$.[3] Now let $\{\wp_i\}_{i \geq 1}$ be an ordering by norm of the set of primes of good reduction for $(\mathcal{C}_k)_E$. Define the assignment

$$\mathcal{A}_E : \{\wp_i\}_{i \geq 1} \longrightarrow \mathcal{X}_E, \quad \wp_i \longmapsto x_{\wp_i}.$$

Conjecture 3.13 (Generalized Sato–Tate) *The sequence $x_E := \{x_{\wp_i}\}_{i \geq 1}$ is equidistributed on $\mathcal{X}_E$ with respect to the image on $\mathcal{X}_E$ of the Haar measure of $\mathcal{G}_E$.*

3.4 Equidistribution Over $\mathbb{Q}(\zeta_\ell)$

Theorem 3.14 Assume that (ℓ, k) is non-degenerate. The sequence $x_F := \{x_{\mathfrak{p}_i}\}_{i \geq 1}$ is equidistributed on $\mathcal{X}_F$; i.e., *Conjecture* 3.13 holds for $\operatorname{Jac}(\mathcal{C}_k)_F$.

Proof Note that the group $\mathcal{G}_F$ is isomorphic to $U(1) \times \overset{r_k}{\ldots} \times U(1)$. The irreducible representations of $U(1) \times \overset{r_k}{\ldots} \times U(1)$ are the characters

$$(3.5) \qquad \phi_{b_1,\ldots,b_{r_k}} : U(1) \times \overset{r_k}{\ldots} \times U(1) \longrightarrow \mathbb{C}^*, \qquad \phi_{b_1,\ldots,b_{r_k}}(z_1,\ldots,z_{r_k}) = \prod_{i=1}^{r_k} z_i^{b_i},$$

where $b_1, \ldots, b_{r_k} \in \mathbb{Z}$. By Theorem 3.12, we have to prove that for any $b_1, \ldots, b_{r_k} \in \mathbb{Z}$, not all of them zero, the L-function

$$L_{\mathcal{A}_F}(\phi_{b_1,\ldots,b_{r_k}}, s) = \prod_{i \geq 1}\left(1 - \frac{J_{(ka_1,a_1)}(\mathfrak{p}_i)^{b_1} \ldots J_{(ka_{r_k},a_{r_k})}(\mathfrak{p}_i)^{b_{r_k}}}{\sqrt{N\mathfrak{p}_i}^{b_1 + \cdots + b_{r_k}}} N\mathfrak{p}_i^{-s} \right)^{-1}$$

is holomorphic and nonvanishing for $\Re(s) \geq 1$. But, up to a finite number of local Euler factors, this is just the L-function $L(\Psi, s)$ of the unitarized Grössencharakter

$$\Psi := \frac{J_{(ka_1,a_1)}(\cdot)^{b_1} \ldots J_{(ka_{r_k},a_{r_k})}(\cdot)^{b_{r_k}}}{\sqrt{N(\cdot)}^{b_1 + \cdots + b_{r_k}}}.$$

By unitarized we mean that it takes values in $U(1) \subseteq \mathbb{C}^*$ and not just in $\mathbb{C}^*$. Hecke [Hec20] showed that the L-function of a nontrivial unitarized Grössencharakter is holomorphic and nonvanishing for $\Re(s) \geq 1$. Therefore, it only remains to prove that the Grössencharakter Ψ is nontrivial. Suppose it were, and let $B := (b_1 + \cdots + b_{r_k})/2$.

---

[3]One may give an explicit matricial description of $x_\wp$ by making use of the results of Brünjes [Brü04, Prop. 11.4].

For every prime $\mathfrak{p}$ of F, reindexing the b_j's on the set M_k/W_k for notation simplicity, we have that (2.3) implies

$$\mathcal{O}_F = \Psi(\mathfrak{p})\mathcal{O}_F = \prod_{t \in G} \frac{\prod_{j \in M_k/W_k} (\sigma_t \mathfrak{p})^{b_j E_k(-t^{-1}j)}}{(\sigma_t \mathfrak{p})^B}.$$

It follows from Artin's Theorem on independence of characters that for every $t \in G$, we have $\sum_{j \in M_k/W_k} b_j E_k(-t^{-1}j) = B$. But this implies that $\det(D_k) = 0$, which is a contradiction with the assumption of (ℓ, k) being non-degenerate. ∎

The proof above extends naturally to the case of an absolutely simple abelian variety with complex multiplication (see [Fit15, §3.5]).

3.5 Irreducible Representations of $U(1) \times \overset{r_k}{\dots} \times U(1) \rtimes G$

In Subsection 3.6 we will prove the generalized Sato–Tate Conjecture for $\mathrm{Jac}(\mathcal{C}_k)$ over $\mathbb{Q}$ when (ℓ, k) is a non-degenerate pair. Thus, we are led by Theorem 3.12 to the study of the irreducible representations of $\mathcal{G}_{\mathbb{Q}} \simeq U(1) \times \overset{r_k}{\dots} \times U(1) \rtimes G$, where the action of a generator g of G on $U(1) \times \overset{r_k}{\dots} \times U(1)$ is given by the rule

$$\iota_{n_k}\left({}^g \mathrm{diag}(u_1\overline{u}_1, \dots, u_{r_k}, \overline{u}_{r_k})\right) = \gamma \iota_{n_k}\left(\mathrm{diag}(u_1, \overline{u}_1, \dots, u_{r_k}, \overline{u}_{r_k})\right)\gamma^{-1}.$$

To shorten notation, we will write

$$\mathcal{G}_0 := U(1) \times \overset{r_k}{\dots} \times U(1), \qquad \mathcal{G} := \mathcal{G}_0 \rtimes G.$$

We now follow [Ser77, §8.2], where the irreducible representations of a semidirect product by an abelian group are characterized. For any character $\phi_{b_1, \dots, b_{r_k}}$ of $\mathcal{G}_0$ as in (3.5), let $H_{b_1, \dots, b_{r_k}} \subseteq G$ be the subgroup such that

(3.6) $$\phi_{b_1, \dots, b_{r_k}}(u_1, \dots, u_{r_k}) = \phi_{b_1, \dots, b_{r_k}}({}^h(u_1, \dots, u_{r_k}))$$

for every $h \in H_{b_1, \dots, b_{r_k}}$. Write $\mathcal{H} := \mathcal{G}_0 \rtimes H_{b_1, \dots, b_{r_k}}$. One has that

$$\phi_{b_1, \dots, b_{r_k}} : \mathcal{H} \longrightarrow \mathbb{C}^*, \qquad \phi_{b_1, \dots, b_{r_k}}(z_1, \dots, z_{r_k}, h) = \prod_{i=1}^{r_k} z_i^{b_i}$$

is a character of $\mathcal{H}$. Then by [Ser77, Prop. 25] every irreducible representation of $\mathcal{G}$ is of the form $\theta := \mathrm{Ind}_{\mathcal{G}}^{\mathcal{H}}(\chi \otimes \phi_{b_1, \dots, b_{r_k}})$, where χ is a character of $H_{b_1, \dots, b_{r_k}}$ that we may view as a character of $\mathcal{H}$ by composing with the projection $\mathcal{H} \to H_{b_1, \dots, b_{r_k}}$.

3.6 Equidistribution Over $\mathbb{Q}$

In this section, we write $\doteq$ to indicate equality of L-functions up to a finite number of local Euler factors.

Theorem 3.15 *Assume that (ℓ, k) is non-degenerate. The sequence $x_{\mathbb{Q}} := \{x_{p_i}\}_{i \geq 1}$ is equidistributed on $X_{\mathbb{Q}}$; i.e., Conjecture 3.13 holds for $\mathrm{Jac}(\mathcal{C}_k)$.*

Proof Let $\theta = \mathrm{Ind}_{\mathcal{G}}^{\mathcal{H}}(\chi \otimes \phi_{b_1,\dots,b_{r_k}})$ be as in Subsection 3.5. We have to show that

$$L_{\mathcal{A}_{\mathbb{Q}}}(\theta, s) = \prod_{i \geq 1, \, p_i \subseteq \mathbb{Z}} \det\big(1 - \theta(x_{p_i})p_i^{-s}\big)^{-1}$$

is holomorphic and nonvanishing for $\mathfrak{R}(s) \geq 1$. Let us first consider the case $\chi = 1$. Write $n := |H_{b_1,\dots,b_{r_k}}|$. By the Artin formalism, we have that

$$
\begin{aligned}
L_{\mathcal{A}_F}(\phi_{b_1,\dots,b_{r_k}}, s) &= L_{\mathcal{A}_{\mathbb{Q}}}(\mathrm{Ind}_{\mathcal{G}}^{\mathcal{H}} \, \mathrm{Ind}_{\mathcal{H}}^{\mathcal{G}_0} \phi_{b_1,\dots,b_{r_k}}, s) \\
&= L_{\mathcal{A}_{\mathbb{Q}}}(n \, \mathrm{Ind}_{\mathcal{G}}^{\mathcal{H}} \phi_{b_1,\dots,b_{r_k}}, s) = L_{\mathcal{A}_{\mathbb{Q}}}(\theta, s)^n.
\end{aligned}
$$

The second equality follows from (3.6). But in the proof of Theorem 3.14, we have seen that $L_{\mathcal{A}_F}(\phi_{b_1,\dots,b_{r_k}}, s) \doteq L(\Psi, s)$ is holomorphic and nonvanishing for $\mathfrak{R}(s) \geq 1$, from which the desired result follows. For the general case (χ not necessarily trivial), let $\widetilde{\chi}$ be a character of G such that $\widetilde{\chi}|_{H_{b_1,\dots,b_{r_k}}} = \chi$ (the existence of $\widetilde{\chi}$ is guaranteed by the fact of G being cyclic). Then

$$\theta = \mathrm{Ind}_{\mathcal{G}}^{\mathcal{H}}(\chi \otimes \phi_{b_1,\dots,b_{r_k}}) = \widetilde{\chi} \otimes \mathrm{Ind}_{\mathcal{G}}^{\mathcal{H}}(\phi_{b_1,\dots,b_{r_k}}).$$

The cyclicity of G additionally implies that

$$n\theta = \widetilde{\chi} \otimes \mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}_0} \phi_{b_1,\dots,b_{r_k}} = \mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}_0} \phi_{b_1,\dots,b_{r_k}},$$

from which $L(\Psi, s) \doteq L_{\mathcal{A}_{\mathbb{Q}}}(\theta, s)^n$ follows again. ∎

We have thus shown that Conjecture 3.13 holds for $E = F$ and $E = \mathbb{Q}$. The choice $E = \mathbb{Q}$ in Subsections 3.5 and 3.6 was made only for the purpose of simplifying the exposition; the proof of Theorem 3.15 can be immediately generalized for an arbitrary intermediate extension $E/\mathbb{Q}$ of $F/\mathbb{Q}$.

4 Vanishing of the Determinant of a Demjanenko Matrix

For non-degenerate pairs (ℓ, k), one may explicitly determine the limiting distributions of the coefficients of the normalized local factors attached to $\mathcal{C}_k$ from the results of Section 3.

In Section 5, we will describe an alternative method to compute these limiting distributions. The interest of this method relies on the fact that, for a degenerate pair (ℓ, k), there still exist some residue degrees exhibiting a "non-degenerate behavior". As a consequence, we will be able to compute the limiting distributions when we restrict to primes of such residue degrees. These residue degrees f may be characterized by the fact that the rank of $D_{k,f}$ is maximal, where $D_{k,f}$ is a generalization of the Demjanenko matrix D_k.

The goal of this section is to provide the technical results for the method that will be presented in Section 5 (essentially Theorem 4.10, see below). To a certain extent, it is an independent section and for the reader exclusively interested in determinants of Demjanenko matrices, it should suffice to review (2.2) and Definition 3.1, and skip everything else from the previous sections. Conversely, the reader exclusively interested in equidistribution questions concerning quotients of the Fermat curves may just look at Definitions 4.1 and 4.2, assume Theorem 4.10 and Proposition 4.9, and ignore the rest of the section at a first reading.

Definition 4.1 Let E_k be as in Definition 3.1. For a divisor f of $\ell - 1$, let H_f be the subgroup of G of order f, and for $a \in G$ let

$$E_{k,f}(a) := \sum_{h \in H_f} E_k(ah).$$

Define also $W_{k,f} := \{ w \in G \mid E_{k,f}(a) = E_{k,f}(aw), \forall a \in G \}$ and let $n_{k,f}$ denote its cardinality.

We will use the following notation: for every subset $X \subseteq G$, we will denote by $[X]$ the element $\sum_{x \in X} [x] \in \mathbb{Z}[G]$. Observe that

(4.1) $W_{k,f} = \left\{ w \in G \mid [H_f][M_k^{-1}]\big([w] - [1] \big) = 0 \text{ in } \mathbb{Z}[G] \right\},$

since we have the following equalities:

$$[H_f][M_k^{-1}] = \sum_{j \in G} E_{k,f}(-j^{-1})[j], \quad [H_f][M_k^{-1}][w] = \sum_{j \in G} E_{k,f}(-j^{-1}w)[j].$$

Definition 4.2 The generalized (k, f)-Demjanenko matrix is

$$D_{k,f} = \left(E_{k,f}(-c^{-1}a) - \frac{f}{2} \right)_{c,a \in M_k/W_{k,f}}.$$

We will denote the size of $D_{k,f}$ by $r_{k,f} := \frac{\ell - 1}{2n_{k,f}}$.

Remark 4.3 Observe that $E_{k,1} = E_k$, $W_{k,1} = W_k$, $D_{k,1} = D_k$, $n_{k,1} = n_k$, $r_{k,1} = r_k$, $H_f \subseteq W_{k,f}$, and that $E_{k,f}(-a) = f - E_{k,f}(a)$.

Lemma 4.4 *A divisor f of $\ell - 1$ is even if and only if $W_{k,f} = G$. In this case, we have $D_{k,f} = 0$.*

Proof Since f is even, $-1 \in H_f$, but this means that $[H_f][M_k^{-1}] = \frac{f}{2}[G]$, from which one implication of the lemma is clear in virtue of (4.1). For the other implication, first note that

$$|H_f \cap M_k| = \sum_{h \in H_f} E_k(h) = E_{k,f}(1), \qquad |H_f \cap -M_k| = \sum_{h \in H_f} E_k(-h) = E_{k,f}(-1).$$

If $W_{k,f} = G$, then $E_{k,f}(1) = E_{k,f}(-1)$, and thus $|H_f \cap M_k| = |H_f \cap -M_k|$. It follows that $f = |H_f \cap M_k| + |H_f \cap -M_k|$ is even. ∎

Before proceeding to prove Theorem 4.10, we need four auxiliary results: Propositions 4.5, 4.7, 4.8, and 4.9. We first introduce some notation. For an abelian group A, let $X(A)$ denote the group of characters of A. For every odd divisor f of $\ell - 1$, let $X_{k,f}^-(G)$ (resp. $X_{k,f}^+(G)$) denote the set of odd (resp. even) characters of G that are trivial on $W_{k,f}$. Write simply $X_k^-(G)$ and $X_k^+(G)$ when $f = 1$.

Proposition 4.5 *For $1 \le k \le \ell - 2$ and f an odd divisor of $\ell - 1$, we have*

$$\det(D_{k,f}) = \left(\frac{-f}{2} \right)^{r_{k,f}} \prod_{\chi \in X_{k,f}^-(G)} \sum_{a \in M_k/W_{k,f}} \chi(a) = \left(\frac{-f}{2n_{k,f}} \right)^{r_{k,f}} \prod_{\chi \in X_{k,f}^-(G)} \sum_{a \in M_k} \chi(a).$$

Proof   We will apply the Dedekind determinant formula (DDF)[4], following the strategy considered in [Haz90], [Doh94], or [SS95]. Let us write

$$\delta_k(a) := \begin{cases} 1 & \text{if } a \in M_k, \\ -1 & \text{if } a \notin M_k. \end{cases}$$

Note that by Lemma 4.4, $X_{k,f}^-(G)$ is non-empty and thus there is a bijection between $X_{k,f}^-(G)$ and $X_{k,f}^+(G)$. Choose $\omega \in X_{k,f}^-(G)$. Observe that the function $\mathcal{F}(a) = \sum_{h \in H_f} \omega(ha)\delta_k(ha)$, for $a \in G$, is well defined on $G/(\{\pm 1\} W_{k,f})$, since $\omega(a)\delta_k(a) = \omega(-a)\delta_k(-a)$ and

$$\mathcal{F}(a) = \omega(a)\big(f - 2E_{k,f}(a)\big) = \omega(wa)\big(f - 2E_{k,f}(wa)\big) = \mathcal{F}(wa)$$

for every $w \in W_{k,f}$. Then we have

$$\prod_{\chi \in X_{k,f}^-(G)} \sum_{a \in M_k} \chi(a) = \prod_{\chi \in X_{k,f}^+(G)} \sum_{a \in M_k} \chi(a) \cdot \omega(a) = \prod_{\chi \in X_{k,f}^+(G)} \sum_{a \in M_k} \chi(a) \cdot \omega(a)\delta_k(a)$$

$$= \prod_{\psi \in X(G/(\{\pm 1\} W_{k,f}))} \sum_{a \in M_k/W_{k,f}} \frac{n_{k,f}}{f} \psi(a) \cdot \mathcal{F}(a)$$

$$= \det\Big(\frac{n_{k,f}}{f}\mathcal{F}(ab^{-1})\Big)_{a,b \in M_k/W_{k,f}}$$

$$= \Big(\frac{-n_{k,f}}{f}\Big)^{r_{k,f}} \det\big(\omega(ab^{-1})(2E_{k,f}(-ab^{-1}) - f)\big)_{a,b \in M_k/W_{k,f}}.$$

Multiplying the a-row of the matrix by $\omega(a)^{-1}$ and the b-column by $\omega(b)$ for every $a, b \in M_k/W_{k,f}$ cancels out the factor $\omega(ab^{-1})$ without changing the determinant. ∎

Kubota [Kub65, Lem. 2] showed that the rank of D_k is the number of characters $\chi \in X_k^-(G)$ for which the sum $\sum_{a \in M_k/W_k} \chi(a)$ is nonzero. We will now show that an analogous statement holds true when we consider $D_{k,f}$. To this end, we will extend Ribet's proof [Rib80, Prop. 3.10] of the result of Kubota. Define the map

$$\Phi_{k,f}^*: \mathbb{Z}[G/W_{k,f}] \longrightarrow \mathbb{Z}[G/W_{k,f}],$$
$$\Phi_{k,f}^*\big([a]\big) = [H_f][M_k^{-1}][a] = \sum_{c \in G/W_{k,f}} E_{k,f}(-c^{-1}a)[c].$$

Note that $\Phi_{k,f}^*$ is well defined precisely because of the definition of $W_{k,f}$.

Lemma 4.6   *The rank of $\Phi_{k,f}^*(\mathbb{Z}[G/W_{k,f}])$ is $\mathrm{rk}(D_{k,f}) + 1$.*

Proof   The proof goes exactly as in Lemma 3.3. ∎

Proposition 4.7   *The rank of $D_{k,f}$ is the number of characters $\chi \in X_{k,f}^-(G)$ for which the sum $\sum_{a \in M_k/W_{k,f}} \chi(a)$ is nonzero.*

---

[4]Recall that for a finite abelian group A and $\mathcal{F}$ a function on A, the DDF establishes that
$$\det(\mathcal{F}(ab^{-1}))_{a,b \in A} = \prod_{\psi \in X(A)} \sum_{a \in A} \psi(a)\mathcal{F}(a).$$

Proof Consider the basis vectors $v_\chi := \sum_{c \in G/W_{k,f}} \chi(c)[c]$ of $\mathbb{C}[G/W_{k,f}]$, where χ runs over the set $X(G/W_{k,f}) \simeq X_{k,f}(G)$. Observe that

$$\Phi_{k,f}^*(v_\chi) = f\Big(\sum_{a \in M_k} \chi(a)\Big) v_\chi.$$

And one concludes by noting that the only even character for which

$$\sum_{a \in M_k/W_{k,f}} \chi(a) \neq 0$$

is the trivial one. ∎

Proposition 4.8 *For $\psi \in X_k^-(G)$, one has*

$$\sum_{a \in M_k/W_k} \psi(a) = \frac{1}{n_k} \sum_{a \in M_k} \psi(a) = \frac{B_{1,\psi}}{n_k}\Big(\frac{1}{\psi(k+1)} - 1 - \frac{1}{\psi(k)}\Big).$$

Here, $B_{1,\psi} := \frac{1}{\ell} \sum_{a=1}^{\ell-1} \psi(a)a$ stands for the first generalized Bernoulli number.[5]

Proof From a theorem of Stickelberger, Greenberg [Gre80] derived the equality

$$(4.2) \qquad \sum_{a \in M_k} [a^{-1}] = \frac{1}{\ell}\big([1] + [k] - [1+k]\big) \sum_{a \in G} \langle a \rangle [-a^{-1}]$$

of elements in $\mathbb{Z}[G]$. By evaluating it at an odd character ψ^{-1} of G, he obtained

$$(4.3) \qquad \sum_{a \in M_k} \psi(a) = B_{1,\psi}\Big(\frac{1}{\psi(k+1)} - 1 - \frac{1}{\psi(k)}\Big)$$

from which the statement of the proposition follows immediately. Nevertheless, we would like to present an alternative proof of (4.3) by generalizing the method used by Leopold [Leo62] to deal with the case $k = 1$. We will write the nonzero number $\ell B_{1,\psi}$ in two different ways. First, using that $\langle (k+1)a \rangle = \langle a \rangle + \langle ak \rangle$ for every $a \in M_k$, we obtain

$$
\begin{aligned}
(4.4)\,\ell B_{1,\psi} &= \sum_{a \in M_k} \psi\big((k+1)a\big)\big\langle(k+1)a\big\rangle + \sum_{a \in M_k} \psi\big(-(k+1)a\big)\big\langle-(k+1)a\big\rangle \\
&= 2\sum_{a \in M_k} \psi\big((k+1)a\big)\big\langle(k+1)a\big\rangle - \psi(k+1)\sum_{a \in M_k} \psi(a)\ell \\
&= 2\psi(k+1)\Big(\sum_{a \in M_k} \psi(a)\langle a\rangle + \sum_{a \in M_k} \psi(a)\langle ka\rangle\Big) - \psi(k+1)\sum_{a \in M_k} \psi(a)\ell.
\end{aligned}
$$

Second, we have

$$(4.5)\,\ell B_{1,\psi} = \sum_{a \in M_k} \psi(a)\langle a\rangle - \sum_{a \in M_k} \psi(a)(\ell - \langle a\rangle) = 2\sum_{a \in M_k} \psi(a)\langle a\rangle - \sum_{a \in M_k} \psi(a)\ell.$$

---

[5]It is well known that $B_{1,\psi} \neq 0$, due to the Analytic Class number Formula (see (4.10) in the proof of Proposition 4.16).

Subtracting equation (4.5) $\psi(k+1)$ times from equation (4.4), we obtain

$$\big(1 - \psi(k+1)\big)\ell B_{1,\psi} = 2\psi(k+1) \sum_{a \in M_k} \psi(a)\langle ak \rangle = \frac{2\psi(k+1)}{\psi(k)} \sum_{a \in M_k} \psi(ak)\langle ak \rangle$$

$$= \frac{\psi(k+1)}{\psi(k)}\Big(\ell B_{1,\psi} + \psi(k) \sum_{a \in M_k} \psi(a)\ell\Big)$$

$$= \frac{\psi(k+1)}{\psi(k)}\ell B_{1,\psi} + \psi(k+1)\ell \sum_{a \in M_k} \psi(a).$$

This yields

$$\sum_{a \in M_k} \psi(a) = B_{1,\psi}\Big(\frac{1}{\psi(k+1)} - 1 - \frac{1}{\psi(k)}\Big). \qquad \blacksquare$$

Proposition 4.9 *For $\ell > 3$, $1 \le k \le \ell - 2$, and every odd divisor f of $\ell - 1$, the following statements are equivalent:*

(i) $\sum_{a \in M_k} \psi_0(a)^f = 0$, *where ψ_0 denotes a generator of $X(G)$;*

(ii) $k^{2f} + k^f + 1 \equiv 0 \pmod{\ell}$ *and* $(k+1)^f k^f \equiv -1 \pmod{\ell}$;

(iii) $H_f \subsetneq W_{k,f}$.

In this case, $k \in W_{k,f}$, $W_{k,f}$ is generated by H_f and k, and $|W_{k,f}| = 3f$.

Proof   Assume that (i) holds. By (4.3), we have that

$$(4.6) \qquad\qquad \frac{1}{\psi_0^f(k+1)} = 1 + \frac{1}{\psi_0^f(k)}.$$

But it is a trivial fact that if ω is a root of unity, then $\omega + 1$ is a root of unity if and only if ω is a primitive cubic root of unity. Thus, taking $\omega = 1/\psi_0^f(k)$, equation (4.6) is equivalent to the assertion that $\psi_0^f(k)$ is a primitive cubic root of unity and $\psi_0^f(k+1)\psi_0^f(-k) = 1$. The injectivity of ψ_0 implies (ii).

Now assume (ii). Note that $k, k^2 \notin H_f$ (otherwise $k^{2f} + k^f + 1 \equiv 3 \pmod{\ell}$), while $k^3 \in H_f$ (since $k^{3f} - 1 \equiv (k^f - 1)(k^{2f} + k^f + 1) \pmod{\ell}$). We will show that $k \in W_{k,f}$, equivalently by (4.2) that

$$(4.7) \qquad \ell[H_f][M_k^{-1}] = [H_f]([1] + [k] - [k+1])\Big(\sum_{a \in G}\langle a \rangle[-a^{-1}]\Big)$$

is invariant by multiplication by $[k]$. Observe that for every $b \in G$, we have

$$[H_f]([b] + [-b])\Big(\sum_{a \in G}\langle a \rangle[-a^{-1}]\Big) = [H_f]\Big(\ell \sum_{a \in G}[a]\Big) = f\ell \sum_{a \in G}[a].$$

Thus, taking $b = k+1$, the right-hand side of (4.7) is equal to

$$(4.8) \qquad [H_f]([1] + [k] + [-k-1])\Big(\sum_{a \in G}\langle a \rangle[-a^{-1}]\Big) - f\ell \sum_{a \in G}[a].$$

Observe that for every $a, b \in G$, we have $[a][H_f] = [b][H_f] \Leftrightarrow ab^{-1} \in H_f$. We claim that $k^2(-k-1)^{-1} \in H_f$. Indeed, first note that $(k+1)^{3f} \equiv -1 \pmod{\ell}$, and then

observe that

$$\left(k^2(-k-1)^{-1} \right)^f \equiv k^{2f}(k+1)^{2f} \equiv k^{3f} \equiv 1 \pmod{\ell}.$$

Thus, (4.8) is equal to

$$[H_f]\big([1] + [k] + [k^2] \big)\Big(\sum_{a \in G} \langle a \rangle [-a^{-1}] \Big) - f\ell \sum_{a \in G}[a]$$

for which it is clear that each of its two terms is invariant under multiplication by $[k]$.

Finally, assume (iii). For $w \in W_{k,f}$, one has, by definition,

$$[M_k^{-1}][H_f][w] = [M_k^{-1}][H_f].$$

Evaluating this equality at ψ_0^{-f}, we obtain that

$$\sum_{a \in M_k} \psi_0(a)^f = \Big(\sum_{a \in M_k} \psi_0(a)^f \Big) \psi_0(w^{-1})^f.$$

Hence, if $w \notin H_f$, then $\psi_0(w^{-1})^f \neq 1$, and $\sum_{a \in M_k} \psi_0(a)^f = 0$.

We still want to see that $|W_{k,f}| = 3f$ for an f as in the statement. Then $3f$ does not satisfy (ii), and thus by (iii) we have $W_{k,3f} = H_{3f}$. From the inclusions

$$H_f \subsetneqq W_{k,f} \subseteq W_{k,3f} = H_{3f},$$

we obtain that $W_{k,f} = H_{3f}$. ∎

Let $\mathcal{F}_0$ denote the set of (odd) divisors f of $\ell - 1$ such that $W_{k,f} = H_{3f}$ (or equivalently the set of odd divisors f such that any of the conditions (i), (ii), or (iii) of Proposition 4.9 hold).

Theorem 4.10   *For $\ell > 3$ and $1 \leq k \leq \ell - 2$, the following conditions are equivalent:*

(i) $\det(D_k) = 0$;

(ii)   *k is not a primitive cubic root of unity modulo ℓ and $\mathcal{F}_0$ is non-empty;*

(iii)   *if v_3 denotes the 3-adic valuation and ord denotes the order in G:*

      (a)   *k is not a primitive cubic root of unity modulo ℓ;*

      (b)   *$\operatorname{ord}(-k^2 - k)$ and $\operatorname{ord}(k)$ are odd;*

      (c)   *$v_3(\operatorname{ord}(k)) > v_3(\operatorname{ord}(-k^2 - k))$.*

In this case, $\mathcal{F}_0$ is exactly the set of odd divisors of $\ell - 1$ that are multiples of $N_k/3$ but not of N_k, where $N_k := \operatorname{lcm}(\operatorname{ord}(-k^2 - k), \operatorname{ord}(k))$, and thus $\operatorname{rk}(D_k) = \frac{\ell-1}{2}\left(1 - \frac{2}{N_k}\right)$.

Proof   If $\det(D_k) = 0$, then by Proposition 4.5, there exists an odd divisor f of $\ell - 1$ such that Proposition 4.9(i) holds. Moreover, k cannot be a primitive cubic root of unity, since Proposition 4.9(ii) would not then hold.

If k is not a primitive cubic root of unity, then $n_k = 1$ by Lemma 2.7. Then if $\mathcal{F}_0$ is non-empty, Proposition 4.9(i) implies that $\det(D_k) = 0$ by Proposition 4.5.

Note that the two equations of Proposition 4.9(ii) can be replaced by the following three:

$$(4.9) \qquad k^f \not\equiv 1 \pmod{\ell}, \qquad k^{3f} \equiv 1 \pmod{\ell}, \qquad (-k^2 - k)^f \equiv 1 \pmod{\ell}.$$

Clearly, there exists an odd divisor f of $\ell - 1$ satisfying (4.9) if and only if (a), (b), and (c) hold. Moreover, in this case, an odd divisor f verifies (4.9) if and only if f is an odd multiple of

$$f_0 := \mathrm{lcm}\Big(\mathrm{ord}(-k^2 - k), \frac{\mathrm{ord}(k)}{3} \Big)$$

that is not a multiple of $3f_0$. Since the set of such f's is in bijection with the set

$$\Big\{ 1 \le m \le \frac{\ell - 1}{f_0} \ \Big| \ (m, 6) = 1 \Big\},$$

the number of such f's is $\frac{\ell - 1}{3f_0} = \frac{\ell - 1}{N_k}$. But by Proposition 4.7, this number is precisely $\dim(\mathrm{Ker}(D_k))$. ∎

The following result tells us that the rank of D_k is "asymptotically non-degenerate".

Proposition 4.11 *For ℓ prime, we have*

$$\lim_{\substack{\ell \to \infty \\ 1 \le k \le \ell - 2}} \frac{\mathrm{rk}(D_k)}{r_k} = 1.$$

Proof When ℓ is non-degenerate, the quotient $\mathrm{rk}(D_k)/r_k = 1$, and there is nothing to prove. Since when (ℓ, k) is degenerate, one has $r_k = \frac{\ell - 1}{2}$, by Theorem 4.10 it is enough to show that $N_k \to \infty$ when $\ell \to \infty$ (the existence of infinitely many degenerate primes is ensured by Remark 3.4). Given an integer $N_0 > 0$, we want to show that there exists a prime $\ell_0 > 0$ such that for every $\ell > \ell_0$ and every $1 \le k \le \ell - 2$, one has that $N_k > N_0$. This immediately follows from the claim that for every N_0, the set S_{N_0} of degenerate primes ℓ such that $N_0 = N_k$ for some $1 \le k \le \ell - 2$ has finite cardinality. Indeed, set $f := N_0/3$ and define the polynomials

$$p_f(x) := x^{2f} + x^f + 1, \qquad q_f(x) := \frac{(x+1)^f x^f + 1}{x^2 + x + 1} \in \mathbb{Z}[x].$$

Clearly, S_{N_0} is a subset of the set of primes dividing the resultant R_{N_0} of $p_f(x)$ and $q_f(x)$, and therefore it suffices to show that R_{N_0} is nonzero. This may be deduced from the fact that the roots of $p_f(x)$ are unrepeated roots of unity, whereas $q_f(x)$ has neither double roots nor roots of finite order. ∎

Remark 4.12 We claim that $N_k \ge 27$. This implies that

$$\mathrm{rk}(D_k) \ge \frac{25}{27} \cdot \frac{\ell - 1}{2},$$

which is a slightly better bound than the one computed in [Mai89]. This bound is sharp, since $N_k = 27$ for $\ell = 271$ and $k = 32$. Recalling the notation of the previous proof, to show that $N_k \ge 27$, it is enough to observe that $S_9 = S_{15} = S_{21} = \varnothing$. This follows from the fact that

$$R_9 = 3^4, \qquad R_{15} = 5^{10}, \qquad R_{21} = 7^{16},$$

and none of 3, 5, or 7 is degenerate. Note that $R_{27} = 3^{16} \cdot 271^6$ and thus $S_{27} = \{271\}$.

We will say that a divisor f of $\ell - 1$ is a k-degenerate residue degree if $\det(D_{k,f}) = 0$ and that f is non-k-degenerate otherwise (however, to simplify the terminology, we will drop the k from now on). By Lemma 4.4, if f is even, then f is degenerate. For a degenerate pair (ℓ, k), let $\mathcal{F}_1$ denote the set of odd divisors f of $\ell - 1$ such that $v_3(f) \geq v_3(N_k)$.

Proposition 4.13   *Let f be an odd divisor of $\ell - 1$.*

(i)   *If (ℓ, k) is degenerate, then f is a non-degenerate residue degree if and only if $f \in \mathcal{F}_0 \cup \mathcal{F}_1$. Moreover, in the case where $f \in \mathcal{F}_1$ we have $W_{k,f} = H_f$, whereas in the case where $f \in \mathcal{F}_0$ we have $W_{k,f} = H_{3f}$. If f is degenerate, then $W_{k,f} = H_f$.*

(ii)   *If (ℓ, k) is non-degenerate, then f is non-degenerate. Moreover, $W_{k,f} = H_{3f}$ if k is a primitive cubic root of unity and $v_3(f) = 0$, and $W_{k,f} = H_f$ otherwise.*

Proof   To shorten notation, let us write Σ_f for $\sum_{a \in M_k} \psi_0(a)^f$. Assume that (ℓ, k) is degenerate. If $f \in \mathcal{F}_1$, then no multiple of f lies in $\mathcal{F}_0$. Thus, $W_{k,f} = H_f$ and $\Sigma_{f'} \neq 0$ for every multiple f' of f. Then Proposition 4.5 yields $\det(D_{k,f}) \neq 0$. If $f \in \mathcal{F}_0$, then $W_{k,f} = H_{3f}$. Since $\Sigma_{f'} \neq 0$ for every multiple f' of $3f$, Proposition 4.5 yields $\det(D_{k,f}) \neq 0$. If $f \notin \mathcal{F}_0 \cup \mathcal{F}_1$, then $v_3(f) < v_3(N_k)$ and f is not a multiple of $N_k/3$. Since $f \notin \mathcal{F}_0$, we have $W_{k,f} = H_f$. Note that there exists a multiple f' of f in $\mathcal{F}_0$. Then Proposition 4.5 yields $\det(D_{k,f}) = 0$.

Assume that (ℓ, k) is non-degenerate. Let f be an odd divisor of $\ell - 1$. If k is not a primitive cubic root of unity, then W_k is trivial. Then by Proposition 4.5, $\det(D_k) \neq 0$ implies that f is non-degenerate. In this case, $W_{k,f} = H_f$. Suppose now that k is a primitive cubic root of unity. If $v_3(f) > 0$, then $W_{k,f} = H_f$ and for every multiple f' of f we have $\Sigma_{f'} \neq 0$. Thus, f is non-degenerate. If $v_3(f) = 0$, then $W_{k,f} = H_{3f}$ and for every multiple f' of $3f$ we have $\Sigma_{f'} \neq 0$. Thus, f is also non-degenerate. ∎

The characterization of *non-degenerate residue degree* and the description of $n_{k,f}$ given in the introduction follow from the previous proposition.

Example 4.14   If $(\ell, k) = (67, 6)$, then $\det(D_k) = 0$. Since $N_k = 33$, we have that $\det(D_{k,3})$, $\det(D_{k,11})$, and $\det(D_{k,33})$ are nonzero; that is, 3, 11, and 33 are non-degenerate residue degrees. Similarly, if $(\ell, k) = (163, 10)$, then $\det(D_k) = 0$, but $\det(D_{k,27})$ and $\det(D_{k,81})$ are nonzero, since $N_k = 81$.

Remark 4.15   In Proposition 4.13, we have characterized the divisors f of $\ell - 1$ for which $\det(D_{k,f})$ vanishes. It is easy to see that, in this case,

$$\operatorname{rk}(D_{k,f}) = \frac{\ell - 1}{2f}\left(1 - \frac{2f}{N_{k,f}}\right),$$

where $N_{k,f} := \operatorname{lcm}(\operatorname{ord}(-k^2 - k), \operatorname{ord}(k), f)$.

Finally, we would like to give formulas of $\det(D_{k,f})$ in terms of the relative class number (for $k = 1$, similar formulas are given in [Haz90, SS95, Doh94]).

Proposition 4.16   *Let f be an odd divisor of $\ell - 1$. Set $F_{k,f} := F^{W_{k,f}}$, let $\omega_{k,f}$ be the number of roots of unity contained in $F_{k,f}$, and let $h^-_{k,f}$ be the relative class number*

of $F_{k,f}$. *One has*

$$\det(D_{k,f}) = \frac{h_{k,f}^- P_{k,f}}{\omega_{k,f}} \left(\frac{f}{n_{k,f}} \right)^{r_{k,f}}, \quad \text{where} \quad P_{k,f} := \prod_{\psi \in X_{k,f}^-(G)} \left(\frac{1}{\psi(k+1)} - 1 - \frac{1}{\psi(k)} \right).$$

Proof Since f is odd, $F_{k,f}$ is a CM field and the Analytic Class Number Formula (ACNF) states that

$$(4.10) \qquad\qquad h_{k,f}^- = \omega_{k,f} \prod_{\psi \in X^-(\mathrm{Gal}(F_{k,f}/\mathbb{Q}))} \frac{-1}{2} B_{1,\psi}$$

(see [Lan78]). Since $X(\mathrm{Gal}(F_{k,f}/\mathbb{Q})) \simeq X^-(G/W_{k,f}) = X_{k,f}^-(G)$, we obtain the statement combining ACNF with (4.3) and Proposition 4.5. ∎

Remark 4.17   One can show that the rank of the image of Φ_k^* is the dimension of the Mumford-Tate group of $A_k := \mathrm{Jac}(\mathcal{C}_k)$ (see [Yu15]). One thus has that $\mathrm{rk}(D_k) = \dim \mathrm{Hg}(A_k)$. For $1 \le k, k' \le \ell - 1$, let $A_{k,k'} := \mathrm{Jac}(\mathcal{C}_k) \times \mathrm{Jac}(\mathcal{C}_{k'})$ and one has analogously that $\dim \mathrm{Hg}(A_{k,k'}) = \mathrm{rk}(D_k | D_{k'}) \le \frac{\ell-1}{2}$. If we choose k, k' in order that A_k and $A_{k'}$ are nonisogenous and of non-degenerate type (we can do this in virtue of Theorems 2.3 and 4.10), this yields an example in which

$$\mathrm{Hg}(A_{k,k'}) \subsetneq \mathrm{Hg}(A_k) \times \mathrm{Hg}(A_{k'}), \qquad \mathrm{L}(A_{k,k'}) = \mathrm{L}(A_k) \times \mathrm{L}(A_{k'}).$$

In particular, the Algebraic Sato–Tate Conjecture, which holds for A_k (resp. $A_{k'}$) taking the algebraic group $\mathrm{TL}(A_k)$ (resp. $\mathrm{TL}(A_{k'})$), does not hold for $A_{k,k'}$ taking the algebraic group $\mathrm{TL}(A_{k,k'})$.

5   Computing Distributions Explicitly

As mentioned in Section 4, the results of Section 3 suffice to determine the distributions of the coefficients of the normalized local factors attached to $\mathcal{C}_k$ when (ℓ, k) is non-degenerate. Nonetheless, in this section we will present an alternative direct method to compute them, which works independently. It is based on an accurate description of the local factors $L_p(\mathcal{C}_k, T)$, and we emphasize that it can be applied without the necessity of computing the Sato–Tate group. We will compute distributions restricting to primes of a fixed residue degree in F. We encounter a curious phenomenon: even in the cases in which the pair (ℓ, k) is degenerate, the method of this section permits one to describe the distributions once one restricts to either even or non-degenerate residue degrees (*i.e.,* the necessarily odd residue degrees f such that $\det(D_{k,f}) \ne 0$).

5.1   Local Factors of $\mathrm{Jac}(\mathcal{C}_k)$

We will describe the local factors of $\mathrm{Jac}(\mathcal{C}_k)$ in terms of the subgroup $W_{k,f} \subseteq G$, where f is a divisor of $\ell - 1$.

Lemma 5.1   *Let $\mathfrak{p}$ be a prime of F of residue degree $f \mid \ell - 1$ and coprime to ℓ. For any $a \in G$, we have*

$$W_{k,f} = \left\{ w \in G \mid {}^{\sigma_w}(J_{(ka,a)}(\mathfrak{p})) = J_{(ka,a)}(\mathfrak{p}) \right\}.$$

Proof   By [Gon99, Lemma 3.2], the right-hand side of the above equation coincides with

$$\left\{ w \in G \mid {}^{\sigma_w}(J_{(ka,a)}(\mathfrak{p})\mathcal{O}_F) = J_{(ka,a)}(\mathfrak{p})\mathcal{O}_F \right\}.$$

Now the lemma follows from

$$
{}^{\sigma_w}(J_{(ka,a)}(\mathfrak{p})\mathcal{O}_F) = J_{(ka,a)}(\mathfrak{p})\mathcal{O}_F \iff \prod_{j \in G/H_f} {}^{\sigma_j}\mathfrak{p}^{E_{k,f}(-aj^{-1})}
$$

$$
= \prod_{j \in G/H_f} {}^{\sigma_j}\mathfrak{p}^{E_{k,f}(-waj^{-1})}. \qquad \blacksquare
$$

Proposition 5.2   *Let $p \neq \ell$ be a prime of residue degree f in F. For any prime $\mathfrak{p}$ of F lying over p, one has*

$$L_p(\mathcal{C}_k, T) = \prod_{a \in G/W_{k,f}} \left(1 - J_{(ka,a)}(\mathfrak{p}) T^f \right)^{\frac{n_{k,f}}{f}}.$$

Proof   In terms of local factors, Lemma 2.10 states

$$L_p(\mathcal{C}_k, T)^{\ell-1} = L_{\mathfrak{p}}\left((\mathcal{C}_k)_F, T^f \right)^{\frac{\ell-1}{f}}.$$

But, by Lemma 5.1, we have

$$L_{\mathfrak{p}}((\mathcal{C}_k)_F, T^f)^{\frac{\ell-1}{f}} = \prod_{a \in G/W_{k,f}} \left(1 - J_{(ka,a)}(\mathfrak{p}) T^f \right)^{n_{k,f}\frac{\ell-1}{f}}.$$

Since $L_p(\mathcal{C}_k, T)$ and $\prod_{a \in G/W_{k,f}}(1 - J_{(ka,a)}(\mathfrak{p}) T^f)^{\frac{n_{k,f}}{f}}$ both have constant term equal to 1, the proposition follows. $\blacksquare$

From the previous proposition, we can deduce an alternative proof of a lemma of [GR78].

Corollary 5.3 (see [GR78, Lemma 1.1])   *If $p \neq \ell$ is a prime of even residue degree f in F, we have that*

$$L_p(\mathcal{C}_k, T) = (1 + p^{\frac{f}{2}} T^f)^{\frac{\ell-1}{f}}.$$

Proof   By Lemma 4.4, if f is even, then $W_{k,f} = G$. Therefore, by Proposition 5.2, it suffices to show that $J_{(k,1)}(\mathfrak{p}) = -p^{f/2}$. Since $-1 \in H_f \subseteq W_{k,f}$, we have that $J_{(k,1)}(\mathfrak{p})$ is fixed by complex conjugation and thus real. Then $\|J_{(k,1)}(\mathfrak{p})\| = p^f$, leaves the two possibilities $J_{(k,1)}(\mathfrak{p}) = \varepsilon p^{f/2}$, with $\varepsilon = \pm 1$. To solve the ambiguity, we will compute the number of $\mathbb{F}_{p^f}$-rational points of

$$\mathcal{C}_k : v^\ell = u(u+1)^{\ell-k-1}.$$

One the one hand, this number is

$$|\mathcal{C}_k(\mathbb{F}_{p^f})| = 1 + p^f - \varepsilon p^{\frac{f}{2}} (\ell - 1).$$

On the other hand, the number of $\mathbb{F}_{p^f}$-rational points is $\equiv 3 \pmod{\ell}$. Indeed for any $u_0 \neq 0, -1$, there are ℓ possibilities for an affine point of the form (u_0, v); there are the two affine points $(0, 0)$ and $(-1, 0)$, and there is the point at infinity. Since $p^{\frac{f}{2}} \equiv -1 \pmod{\ell}$, we obtain $3 \equiv 2 - \varepsilon \pmod{\ell}$, which yields $\varepsilon = -1$. ∎

Recall that $F_{k,f}$ is the subfield of F fixed by $W_{k,f}$. Let $I_{F_{k,f}}(\ell)$ denote the group of fractional ideals of $F_{k,f}$ that are coprime to ℓ. Consider the map

$$\Psi_{(ka,a),f} \colon I_{F_{k,f}}(\ell) \longrightarrow F_{k,f}^*, \qquad \Psi_{(ka,a),f}(\mathfrak{P}) := \prod_{w \in W_{k,f}} J_{(wka,wa)}(\mathfrak{P}\mathcal{O}_F).$$

Proposition 5.4 *The homomorphism* $\Psi_{(ka,a),f}$ *is a Grössencharacter of infinity type*

$$\sum_{j \in G/W_{k,f}} \frac{n_{k,f}^2}{f} E_{k,f}(-aj^{-1})[j] \in \mathbb{Z}[G/W_{k,f}]$$

and weight $n_{k,f}^2$. *If* $n_{k,f} > 1$, *the conductor of* $\Psi_{(ka,a),f}$ *is* $\mathfrak{l}$, *where* $\mathfrak{l}$ *is the prime of* $F_{k,f}$ *lying above* ℓ. *For every prime* $\mathfrak{P} \in I_{F_{k,f}}(\ell)$, *one has*

$$(5.1) \qquad \Psi_{(ka,a),f}(\mathfrak{P})\mathcal{O}_{F_{k,f}} = \prod_{t \in G/W_{k,f}} \sigma_t(\mathfrak{P})^{\frac{n_{k,f}^2}{f} E_{k,f}(-at^{-1})}.$$

Moreover, for every prime $\mathfrak{p} \in I_F(\ell)$ *of residue degree* f *and* $\mathfrak{P} := \mathfrak{p} \cap \mathcal{O}_{F_{k,f}}$, *one has*

$$\Psi_{(ka,a),f}(\mathfrak{P}) = J_{(ka,a)}(\mathfrak{p})^{\frac{n_{k,f}^2}{f}}.$$

Proof For $\alpha \in F_{k,f}^*$ such that $\alpha \equiv^{\times} 1 \pmod{\ell^2}$, by (2.4), we have

$$\Psi_{(ka,a),f}(\alpha\mathcal{O}_{F_{k,f}}) = \prod_{w \in W_{k,f}} \prod_{t \in G} \sigma_t(\alpha)^{E_k(-wat^{-1})} = \prod_{t \in G} \sigma_t(\alpha)^{\frac{n_{k,f}}{f} E_{k,f}(-at^{-1})}$$

$$= \prod_{t \in G/W_{k,f}} \sigma_t(\alpha)^{\frac{n_{k,f}^2}{f} E_{k,f}(-at^{-1})}.$$

Equality (5.1) follows from a similar calculation. To compute the weight, use

$$\frac{n_{k,f}^2}{f} E_{k,f}(a) + \frac{n_{k,f}^2}{f} E_{k,f}(-a) = n_{k,f}^2.$$

If $\mathfrak{p} \in I_F(\ell)$ has residue degree f and $\mathfrak{P} := \mathfrak{p} \cap \mathcal{O}_{F_{k,f}}$, then by definition of $W_{k,f}$, we have

$$\Psi_{(ka,a),f}(\mathfrak{P}) = \prod_{w \in W_{k,f}} \sigma_w J_{(ka,a)}(\mathfrak{P}\mathcal{O}_F) = \prod_{w \in W_{k,f}} J_{(ka,a)}(\mathfrak{p})^{\frac{n_{k,f}}{f}} = J_{(ka,a)}(\mathfrak{p})^{\frac{n_{k,f}^2}{f}}.$$

Since $(1 - \zeta_\ell)^2 \mathcal{O}_F$ is a modulus for $J_{(ka,a)}$ (see §2.2) and $\mathfrak{l}\mathcal{O}_F = (1 - \zeta_\ell)^{n_{k,f}}\mathcal{O}_F$, we have that $\mathfrak{l}$ is a modulus for $\Psi_{(ka,a),f}$ if $n_{k,f} > 1$. ∎

Theorem 5.5 *Let f be an (odd) divisor of $\ell - 1$ such that $\det(D_{k,f}) \neq 0$. Let $\{\mathfrak{p}_i\}_{i \geq 1}$ be an ordering by norm of the primes of F of residue degree f. Set*

$$(5.2) \qquad v_{\mathfrak{p}_i} = \left(\frac{J_{(ka_1,a_1)}(\mathfrak{p}_i)}{\sqrt{N\mathfrak{p}_i}}, \ldots, \frac{J_{(ka_{r_{k,f}},a_{r_{k,f}})}(\mathfrak{p}_i)}{\sqrt{N\mathfrak{p}_i}} \right),$$

where $a_1, \ldots, a_{r_{k,f}}$ is a system of representatives of $M_k/W_{k,f}$. Then the sequence $\{v_{\mathfrak{p}_i}\}_{i \geq 1}$ is equidistributed over $\mathrm{U}(1) \times \overset{r_{k,f}}{\cdots} \times \mathrm{U}(1)$.

Proof Observe that replacing $v_{\mathfrak{p}_i}$ by

$$v'_{\mathfrak{p}_i} = \left(\frac{J_{(ka_1,a_1)}(\mathfrak{p}_i)^{\frac{n_{k,f}^2}{f}}}{\sqrt{N\mathfrak{p}_i}^{\frac{n_{k,f}^2}{f}}}, \ldots, \frac{J_{(ka_{r_{k,f}},a_{r_{k,f}})}(\mathfrak{p}_i)^{\frac{n_{k,f}^2}{f}}}{\sqrt{N\mathfrak{p}_i}^{\frac{n_{k,f}^2}{f}}} \right)$$

in the statement of the theorem yields an equivalent statement. Set $\mathfrak{P}_i := \mathfrak{p}_i \cap \mathcal{O}_{F_{k,f}}$. By Proposition 5.4, the tuple $v'_{\mathfrak{p}_i}$ is exactly

$$\left(\frac{\Psi_{(ka_1,a_1),f}(\mathfrak{P}_i)}{\sqrt{N\mathfrak{P}_i}^{n_{k,f}^2}}, \ldots, \frac{\Psi_{(ka_{r_{k,f}},a_{r_{k,f}}),f}(\mathfrak{P}_i)}{\sqrt{N\mathfrak{P}_i}^{n_{k,f}^2}} \right).$$

Let us now make a change of notation: $\{\mathfrak{P}_i\}_{i \geq 1}$ is an ordering by norm of all of the primes of $F_{k,f}$. Let $\mathrm{Frob}_{\mathfrak{P}_i} \in \mathrm{Gal}(F/F_{k,f})$ be the relative Frobenius at $\mathfrak{P}_i$. Then the theorem follows from the claim that the sequence

$$\left\{ \left(\frac{\Psi_{(ka_1,a_1),f}(\mathfrak{P}_i)}{\sqrt{N\mathfrak{P}_i}^{n_{k,f}^2}}, \ldots, \frac{\Psi_{(ka_{r_{k,f}},a_{r_{k,f}}),f}(\mathfrak{P}_i)}{\sqrt{N\mathfrak{P}_i}^{n_{k,f}^2}}, \mathrm{Frob}_{\mathfrak{P}_i} \right) \right\}_{i \geq 1}$$

is equidistributed over $\mathrm{U}(1) \times \overset{r_{k,f}}{\cdots} \times \mathrm{U}(1) \times \mathrm{Gal}(F/F_{k,f})$. For $(b_1, \ldots, b_{r_{k,f}}) \in \mathbb{Z}^{r_{k,f}}$ and $\chi \in \mathrm{Gal}(F/F_{k,r})$, let us write

$$\Psi := \Psi_{(ka_1,a_1),f}^{b_1} \cdot \ldots \cdot \Psi_{(ka_{r_{k,f}},a_{r_{k,f}}),f}^{b_{r_{k,f}}} \chi.$$

By Theorem 3.12, we have to show that

$$\prod_{i \geq 1} \left(1 - \frac{\Psi(\mathfrak{P}_i)}{\sqrt{N\mathfrak{P}_i}^{(b_1 + \cdots + b_{r_{k,f}})n_{k,f}^2}} N\mathfrak{P}_i^{-s} \right)^{-1}$$

is holomorphic and nonvanishing for $\mathfrak{R}(s) \geq 1$, unless χ is trivial and all the b_i's are zero. Artin reciprocity guarantees the existence of an ideal $\mathfrak{c}$ of $F_{k,f}$ (divisible by precisely the primes that ramify in F) such that for all $\alpha \in F_{k,f}^*$ satisfying $\alpha \equiv^{\times} 1 \pmod{\mathfrak{c}}$, $\chi(\alpha \mathcal{O}_{F_{k,f}}) = 1$. This means that Ψ is again a Grössencharacter,[6] and by Hecke's result all we have to check is that it is not trivial unless χ is trivial and all the b_i's are zero. Suppose that Ψ is trivial and write $B := (b_1 + \cdots + b_{r_{k,f}})n_{k,f}^2/2$. Then

---

[6]At this point the importance of Proposition 5.4 becomes apparent. It permits to reduce an equidistribution problem about eigenvalues of Grössencharacters of the field F to an equidistribution problem about eigenvalues of Grössencharacters of the field $F_{k,f}$, where the primes of residue degree f can be detected by means of another Grössencharacter.

reindexing the b_j's on the set $M_k/W_{k,f}$, for every prime $\mathfrak{P}$ of $\mathcal{O}_{F_{k,f}}$ with $\mathrm{Frob}_{\mathfrak{P}} = 1$, equation (5.1) implies

$$\mathcal{O}_{F_{k,f}} = \Psi(\mathfrak{P})\mathcal{O}_{F_{k,f}} = \prod_{j \in M_k/W_{k,f}} \prod_{t \in G/W_{k,f}} \sigma_t(\mathfrak{P})^{b_j \frac{n_{k,f}^2}{f} E_{k,f}(-t^{-1}j) - B}.$$

It follows from Artin's Theorem (applied to the set of characters on the monoid generated by prime ideals $\mathfrak{P}$ of $\mathcal{O}_{F_{k,f}}$ with $\mathrm{Frob}_{\mathfrak{P}} = 1$) that for every $t \in G/W_{k,f}$, one has

$$\sum_{j \in M_k/W_{k,f}} b_j E_{k,f}(-t^{-1}j) - \frac{Bf}{n_{k,f}^2} = 0.$$

Since $\det(D_{k,f}) \neq 0$, all the b_j's are zero. Then $\Psi = \chi$, and χ is also trivial. ∎

We can now deduce Theorem 1.3.

Proof of Theorem 1.3 Let $\{p_i\}_{i \geq 1}$ be the ordering by size of the rational primes of residue degree f in F, and define the assignment

$$\{p_i\}_{i \geq 1} \longrightarrow \mathrm{U}(1) \times \overset{r_{k,f}}{\cdots} \times \mathrm{U}(1) \overset{\mathrm{proj}}{\longrightarrow} [-2,2]^{r_{k,f}}/\mathfrak{S}_{r_{k,f}},$$
$$p_i \longmapsto \nu_{\mathfrak{p}_i} \longmapsto \left(s_1(\mathfrak{p}_i), \dots, s_{r_{k,f}}(\mathfrak{p}_i)\right),$$

where $\nu_{\mathfrak{p}_i}$ is as in (5.2), $\mathfrak{p}_i$ is any prime of F lying over p_i, and

$$s_j(p_i) = -\frac{J_{(ka_j,a_j)}(\mathfrak{p}_i)}{\sqrt{N\mathfrak{p}_i}} - \frac{\overline{J_{(ka_j,a_j)}(\overline{\mathfrak{p}}_i)}}{\sqrt{N\mathfrak{p}_i}}.$$

Note that this assignment is independent of the choice of $\mathfrak{p}_i$ over p_i. By Proposition 5.2, we have

$$L_{p_i}(\mathcal{C}_k, T/\sqrt{p_i}) = \prod_{j=1}^{r_{k,f}} \left(1 + s_j(p_i)T^f + T^{2f}\right)^{\frac{n_{k,f}}{f}}.$$

Observe that the image of the Haar measure of $\mathrm{U}(1) \times \overset{r_{k,f}}{\cdots} \times \mathrm{U}(1)$ on $[-2,2]^{r_{k,f}}/\mathfrak{S}_{r_{k,f}}$ by the map proj is

$$\prod_{i=1}^{r_{k,f}} \frac{1}{\pi} \frac{dx_i}{\sqrt{4 - x_i^2}}.$$

One concludes by applying Theorem 5.5. ∎

5.2 Explicit Distributions

For every $p \nmid \ell$, define $a_i(p)$, for $i = 0, \dots, \ell - 1$, to be the ith coefficient of the *normalized* local factor of $\mathcal{C}_k$ at p

$$L_p(\mathcal{C}_k, T/\sqrt{p}) := \sum_{i=0}^{\ell-1} a_i(p) T^i.$$

Note that $a_i(p) \in I_i := \left[-\binom{\ell-1}{i}, \binom{\ell-1}{i}\right]$ and that $a_i(p) = a_{\ell-1-i}(p)$. Let a_i denote the sequence $\{a_i(p)\}_{p \nmid \ell}$, where the primes are ordered by size. In this section, from Theorem 1.3, we will describe how to compute, in the case where (ℓ, k) is non-degenerate, the measure μ_i over I_i with respect to which a_i is equidistributed for $i = 0, \dots, \frac{\ell-1}{2}$.

Let $a_{i,f}$ be the subsequence of a_i made up of those $a_i(p)$ such that p has residue degree f in F. Denote by $\mu_{i,f}$ the measure over I_i with respect to which $a_{i,f}$ is equidistributed. Then

$$\mu_i = \sum_{1 \le f \mid \ell-1} \frac{\phi(f)}{\ell-1} \mu_{i,f} \quad \text{and} \quad M_n[\mu_i] = \sum_{1 \le f \mid \ell-1} \frac{\phi(f)}{\ell-1} M_n[\mu_{i,f}],$$

where ϕ is the Euler function, and $M_n[\mu_i]$ (resp. $M_n[\mu_{i,f}]$) stands for the n-th moment of μ_i (resp. $\mu_{i,f}$). We now show how to compute $\mu_{i,f}$ and $M_n[\mu_{i,f}]$ when f is even or non-degenerate (this covers the case (ℓ, k) non-degenerate).

Case f even. For $p \ne \ell$ with residue degree f in F, Corollary 5.3 implies that if $i \equiv 0 \pmod{f}$, then

$$a_i(p) = \binom{\ell-1/f}{\ell-1-i/f} \quad \text{and thus} \quad M_n[\mu_{i,f}] = \binom{\ell-1/f}{\ell-1-i/f}^n.$$

If $i \not\equiv 0 \pmod{f}$, then $a_i(p) = 0$ and $M_n[\mu_{i,f}] = 0$. Note that this is independent of (k, ℓ) being degenerate.

Case f non-degenerate. Using Theorem 1.3, it is a straightforward computation to obtain the first moments $M_n[\mu_{i,f}]$. In Table 2 we have listed the first moments $M_n[\mu_i]$ for some non-degenerate pairs (ℓ, k).

6   Examples and Numerical Data

6.1   Examples

In Table 1 we show $\mathrm{ST}(\mathrm{Jac}(\mathcal{C}_k))$ for several non-degenerate pairs (ℓ, k). We also write the set M_k, the subgroup W_k of G, and a generator g of G. We use the following notation. We denote by U a random element in the connected component $\mathrm{ST}(\mathrm{Jac}(\mathcal{C}_k))^0$ and by γ a generator of the group of components. For $u_i \in \mathrm{U}(1)$, write

$$U_i := \begin{pmatrix} u_i & 0 \\ 0 & \overline{u}_i \end{pmatrix}.$$

We denote the characteristic polynomial of a random element in $\mathrm{ST}(\mathrm{Jac}(\mathcal{C}_k))^0 \gamma^i$ by $P_{\gamma^i}(T)$, and write $s_i := u_i + \overline{u}_i$. For every nontrivial divisor d of $\ell-1$, in Table 1 we show $P_{\gamma^i}(T)$, for some γ^i having order d. For the case $d = 1$, it is clear that

$$P_{\gamma^{\ell-1}}(T) = \Big(\prod_{i=1}^{r_k} (T^2 + s_i T + 1) \Big)^{n_k}.$$

Table 1: Some Sato–Tate groups $\mathrm{ST}(\mathrm{Jac}(\mathcal{C}_k))$.

(ℓ, k)	M_k	W_k	g	$\{g, \ldots, g^{\frac{\ell-1}{2}} \mid g^{\frac{\ell-1}{2}}, \ldots, g^{\ell-1}\}$
$(5,2)$	$\{1,3\}$	$\{1\}$	2	$\{\mathbf{2},4 \mid \mathbf{3},1\}$

$$\gamma = \begin{pmatrix} 0 & I_2 \\ J_2 & 0 \end{pmatrix} \qquad U = \begin{pmatrix} U_1 & 0 \\ 0 & U_2 \end{pmatrix}$$
$$P_{\gamma^2}(T) = (T^2+1)^2, \qquad P_\gamma(T) = T^4+1$$

(ℓ, k)	M_k	W_k	g	
$(7,2)$	$\{1,2,4\}$	$\{1,2,4\}$	3	$\{\mathbf{3},\mathbf{2},6 \mid \mathbf{4},5,1\}$

$$\gamma = \begin{pmatrix} 0 & J_2 & 0 \\ 0 & 0 & J_2 \\ J_2 & 0 & 0 \end{pmatrix} \qquad U = \begin{pmatrix} U_1 & 0 & 0 \\ 0 & U_1 & 0 \\ 0 & 0 & U_1 \end{pmatrix}$$
$$P_{\gamma^3}(T) = (T^2+1)^3, \quad P_{\gamma^2}(T) = T^6 + (u_1^3 + \overline{u}_1^3)T^3 + 1, \quad P_\gamma(T) = T^6+1$$

(ℓ, k)	M_k	W_k	g	
$(7,3)$	$\{1,3,5\}$	$\{1\}$	3	$\{\mathbf{3},2,6 \mid \mathbf{4},5,1\}$

$$\gamma = \begin{pmatrix} 0 & J_2 & 0 \\ 0 & 0 & I_2 \\ I_2 & 0 & 0 \end{pmatrix} \qquad U = \begin{pmatrix} U_1 & 0 & 0 \\ 0 & U_2 & 0 \\ 0 & 0 & U_3 \end{pmatrix}$$
$$P_{\gamma^3}(T) = (T^2+1)^3, \quad P_{\gamma^2}(T) = T^6 + (u_1 u_2 \overline{u}_3 + \overline{u}_1 \overline{u}_2 u_3)T^3 + 1, \quad P_\gamma(T) = T^6+1$$

(ℓ, k)	M_k	W_k	g	
$(11,1)$	$\{1,2,3,4,5\}$	$\{1\}$	2	$\{\mathbf{2},4,\mathbf{8},5,10 \mid 9,7,3,6,1\}$

$$\gamma = \begin{pmatrix} 0 & I_2 & 0 & 0 & 0 \\ 0 & 0 & J_2 & 0 & 0 \\ 0 & 0 & 0 & J_2 & 0 \\ 0 & 0 & 0 & 0 & J_2 \\ I_2 & 0 & 0 & 0 & 0 \end{pmatrix} \qquad U = \begin{pmatrix} U_1 & 0 & 0 & 0 & 0 \\ 0 & U_2 & 0 & 0 & 0 \\ 0 & 0 & U_3 & 0 & 0 \\ 0 & 0 & 0 & U_4 & 0 \\ 0 & 0 & 0 & 0 & U_5 \end{pmatrix}$$
$$P_{\gamma^5}(T) = (T^2+1)^5, \quad P_{\gamma^2}(T) = T^{10} + (u_1 \overline{u}_2 \overline{u}_3 \overline{u}_4 \overline{u}_5 + \overline{u}_1 u_2 u_3 u_4 u_5)T^5 + 1,$$
$$P_\gamma(T) = T^{10}+1$$

(ℓ, k)	M_k	W_k	g	
$(13,2)$	$\{1,2,3,4,7,8\}$	$\{1\}$	2	$\{\mathbf{2},4,\mathbf{8},\mathbf{3},\mathbf{6},12 \mid 11,9,5,10,7,1\}$

$$\gamma = \begin{pmatrix} 0 & I_2 & 0 & 0 & 0 & 0 \\ 0 & 0 & I_2 & 0 & 0 & 0 \\ 0 & 0 & 0 & I_2 & 0 & 0 \\ 0 & 0 & 0 & 0 & J_2 & 0 \\ 0 & 0 & 0 & 0 & 0 & I_2 \\ I_2 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \qquad U = \begin{pmatrix} U_1 & 0 & 0 & 0 & 0 & 0 \\ 0 & U_2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & U_4 & 0 & 0 \\ 0 & 0 & 0 & 0 & U_5 & 0 \\ 0 & 0 & 0 & 0 & 0 & U_6 \end{pmatrix}$$
$$P_{\gamma^6}(T) = (T^2+1)^6,$$
$$P_{\gamma^4}(T) = (T^6 + (u_1 \overline{u}_3 \overline{u}_5 + \overline{u}_1 u_3 u_5)T^3 + 1)(T^6 + (u_2 \overline{u}_4 \overline{u}_6 + \overline{u}_2 u_4 u_6)T^3 + 1),$$
$$P_{\gamma^3}(T) = (T^4+1)^3, \quad P_{\gamma^2}(T) = (T^6+1)^2, \quad P_\gamma(T) = T^{12}+1$$

(ℓ, k)	M_k	W_k	g	
$(13,3)$	$\{1,2,3,5,6,9\}$	$\{1,3,9\}$	2	$\{\mathbf{2},4,\mathbf{8},\mathbf{3},\mathbf{6},12 \mid 11,\mathbf{9},5,10,7,1\}$

$$\gamma = \begin{pmatrix} 0 & J_2 & 0 & 0 & 0 & 0 \\ 0 & 0 & I_2 & 0 & 0 & 0 \\ 0 & 0 & 0 & J_2 & 0 & 0 \\ 0 & 0 & 0 & 0 & I_2 & 0 \\ 0 & 0 & 0 & 0 & 0 & J_2 \\ I_2 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \qquad U = \begin{pmatrix} U_1 & 0 & 0 & 0 & 0 & 0 \\ 0 & U_2 & 0 & 0 & 0 & 0 \\ 0 & 0 & U_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & U_2 & 0 & 0 \\ 0 & 0 & 0 & 0 & U_1 & 0 \\ 0 & 0 & 0 & 0 & 0 & U_2 \end{pmatrix}$$
$$P_{\gamma^6}(T) = (T^2+1)^6, \quad P_{\gamma^4}(T) = (T^6 + (u_1^3 + \overline{u}_1^3)T^3 + 1)(T^6 + (u_2^3 + \overline{u}_2^3)T^3 + 1),$$
$$P_{\gamma^3}(T) = (T^4+1)^3, \quad P_{\gamma^2}(T) = (T^6+1)^2, \quad P_\gamma(T) = T^{12}+1$$

Table 2: First moments of the measures μ_i. For i and n odd, $M_n[\mu_i] = 0$, and we do not write these moments on the table.

(ℓ, k)	$M_2[\mu_1]$	$M_4[\mu_1]$	$M_6[\mu_1]$	$M_8[\mu_1]$
$(5, 2)$	1	9	100	1225
$(7, 2)$	3	81	2430	76545
$(7, 3)$	1	15	310	7455
$(11, 1)$	1	27	1090	55195
$(13, 2)$	1	33	1660	106785
$(13, 3)$	3	243	24300	2679075
(ℓ, k)	$M_1[\mu_2]$	$M_2[\mu_2]$	$M_3[\mu_2]$	$M_4[\mu_2]$
$(5, 2)$	1	3	10	41
$(7, 2)$	2	18	207	2646
$(7, 3)$	1	5	35	321
$(11, 1)$	1	9	133	2873
$(13, 2)$	1	11	206	5781
$(13, 3)$	2	60	2610	130842
(ℓ, k)	$M_2[\mu_3]$	$M_4[\mu_3]$	$M_6[\mu_3]$	$M_8[\mu_3]$
$(7, 2)$	28	7860	2575810	893661020
$(7, 3)$	6	822	184860	48884710
$(11, 1)$	24	73176	406662720	2941907232600
$(13, 2)$	39	287391	4433856900	93962238664175
$(13, 3)$	487	12209463	398722297600	14560811533839655
(ℓ, k)	$M_1[\mu_4]$	$M_2[\mu_4]$	$M_3[\mu_4]$	$M_4[\mu_4]$
$(11, 1)$	1	54	4588	497236
$(13, 2)$	3	139	20267	4480911
$(13, 3)$	10	2142	712107	266575698
(ℓ, k)	$M_2[\mu_5]$	$M_4[\mu_5]$	$M_6[\mu_5]$	$M_8[\mu_5]$
$(11, 1)$	72	934332	22782049800	725020102732940
$(13, 2)$	236	22587768	4493470904960	1230243879356591400
$(13, 3)$	5004	1604318076	675819691911360	319107416394892272084
(ℓ, k)	$M_1[\mu_6]$	$M_2[\mu_6]$	$M_3[\mu_6]$	$M_4[\mu_6]$
$(13, 2)$	4	334	93100	38562182
$(13, 3)$	16	6678	4147390	2893450202

Table 3: Some moment statistics of normalized traces for $x = 2^{27}$.

(ℓ, k)	$M_{1,x}$	$M_{2,x}$	$M_{3,x}$	$M_{4,x}$	$M_{5,x}$	$M_{6,x}$	$M_{7,x}$	$M_{8,x}$
$(5, 2)$	-0.000	1.010	-0.002	9.084	-0.030	100.877	-0.366	1235.171
$(7, 2)$	-0.000	2.999	-0.000	80.984	-0.009	2429.414	0.674	76523.229
$(7, 3)$	0.000	0.999	0.000	14.979	0.011	309.265	0.722	7428.375
$(11, 1)$	-0.000	0.999	-0.007	26.907	-0.203	1080.500	-3.930	54274.737
$(13, 2)$	-0.000	1.001	0.004	32.948	0.376	1646.380	43.571	104860.429
$(13, 3)$	-0.000	3.002	-0.026	243.122	-2.262	24306.084	-199.309	2679022.039

6.2 Numerical Data

Recall the notation of Subsection 5.2, for which a_1 denotes the sequence of normalized Frobenius traces of Jac$(\mathcal{C}_k)$ and μ_1 the measure on $I_1 = \left[-\binom{\ell-1}{2}, \binom{\ell-1}{2} \right]$ attached to it. For $x \gg 0$, let

$$M_{n,x} := \frac{1}{\pi(x)} \sum_{p \le x} \left(\frac{|\mathcal{C}_k(\mathbb{F}_p)| - p - 1}{\sqrt{p}} \right)^n,$$

where $\pi(x)$ denotes the number of primes of good reduction p for $\mathcal{C}_k$ such that $p \le x$. Theorem 3.14 implies that, for every $n \ge 0$, we have

$$\mathrm{M}_n[\mu_1] = \lim_{x \to \infty} M_{n,x}.$$

In Table 2, we display the first values of $\mathrm{M}_n[\mu_i]$, for $1 \le i \le 6$ and even $2 \le n \le 8$, following the procedure described in Subsection 5.2. In Table 3 we show the first values of $M_{n,x}$ for $x = 2^{27}$.

Acknowledgments   Thanks to Santiago Molina for helpful discussions, to Anna Somoza and Joan Sánchez for computer assistance in the elaboration of Table 3, and to the referee for helpful suggestions.

References

[BGK03] G. Banaszak, W. Gajda, P. Krasoń, *On Galois representations for abelian varieties with real and complex multiplications*. J. Number Theory **100**(2003), no. 1, 117–132. http://dx.doi.org/10.1016/S0022-314X(02)00121-X

[BK15] G. Banaszak and K. S. Kedlaya, *An algebraic Sato–Tate group and Sato–Tate conjecture*. Indiana Univ. Math. J. **64**(2015), no. 1, 245–274.   http://dx.doi.org/10.1512/iumj.2015.64.5438

[Brü04] L. Brünjes, *Forms of Fermat equations and their zeta functions*. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2004.   http://dx.doi.org/10.1142/9789812561800

[Del82] P. Deligne, *Hodge cycles on abelian varieties*. In: Hodge cycles, motives, and Shimura varieties, Lecture Notes in Math., 900, Springer, 1982, pp. 9–100.

[Doh94] K. Dohmae, *Demjanenko matrix for imaginary Abelian fields of odd conductors*. Proc. Japan Acad. Ser. A Math. Sci. **70**(1994), no. 9, 292–294.   http://dx.doi.org/10.3792/pjaa.70.292

[Fit15] F. Fité, *Equidistribution, L-functions and Sato–Tate groups*. Contemp. Math. **649**(2015), 63–88.

[FKRS12] F. Fité, K. S. Kedlaya, V. Rotger, A. V. Sutherland, *Sato–Tate distributions and Galois endomorphism modules in genus* 2. Compositio Math. **148**(2012), no. 5, 1390–1442. http://dx.doi.org/10.1112/S0010437X12000279

[FS14] F. Fité and A.V. Sutherland, *Sato–Tate distributions of twists of $y^2 = x^5 - x$ and $y^2 = x^6 + 1$.* Algebra Number Theory **8**(2014), no. 3, 543–585.   http://dx.doi.org/10.2140/ant.2014.8.543

[FS16] F. Fité and I. E. Shparlinski, *On the singularity of the Demjanenko matrix of quotients of Fermat curves*. Proc. Amer. Math. Soc. **144**(2016), no. 1, 55–63. http://dx.doi.org/10.1090/proc12717

[Gon99] J. González, *Fermat Jacobians of prime degree over finite fields*. Canad. Math. Bull. **42**(1999), no. 1, 78–86.   http://dx.doi.org/10.4153/CMB-1999-009-7

[Gre80] R. Greenberg, *On the Jacobian variety of some algebraic curves*. Compositio Math. **42**(1980/81), no. 3, 345–359.

[Gro78] B. H. Gross, *On the periods of Abelian integrals and a formula of Chowla and Selberg*. Invent. Math. **45**(1978), no. 2, 193–211.   http://dx.doi.org/10.1007/BF01390273

[GR78] B. H. Gross and D. E. Rohrlich, *Some results on the Mordell-Weil group of the Jacobian of the Fermat curve*. Invent. Math. **44**(1978), no. 3, 201–224. http://dx.doi.org/10.1007/BF01403161

[Has55] H. Hasse, *Zetafunktion und L-Funktionen zu einem arithmetischen Funktionenkörper vom Fermatschen Typus*. Abh. Deutsch. Akad. Wiss. Berlin. Kl. Math. Nat. **1954**(1954), no. 4.

[Haz90]   F. Hazama, *Demjanenko matrix, class number, and Hodge group*. J. Number Theory **34**(1990), no. 2, 174–177.   http://dx.doi.org/10.1016/0022-314X(90)90147-J

[Hec20]   E. Hecke, *Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen*. Math. Z. **6**(1920), no. 1–2, 11–51.   http://dx.doi.org/10.1007/BF01202991

[Joh13]   C. Johansson, *On the Sato–Tate conjecture for non-generic abelian surfaces, with an Appendix by Francesc Fité*. To appear in Trans. Amer. Math. Soc.   arxiv:1307.6478

[KR78]   N. Koblitz and D. Rohrlich, *Simple factors in the Jacobian of a Fermat curve*. Canad. J. Math. **30**(1978), no. 6, 1183–1205.   http://dx.doi.org/10.4153/CJM-1978-099-6

[KS09]   K. S. Kedlaya and A. V. Sutherland, *Hyperelliptic curves, L-polynomials, and random matrices*. In: Arithmetic, geometry, cryptography, and coding theory, Contemp. Math., 487, American Mathematical Society, Providence, RI, 119–162.
http://dx.doi.org/10.1090/conm/487/09529

[Kub65]   T. Kubota, *On the field extension by complex multiplication*. Trans. Amer. Math. Soc. **118**(1965), 113–122.   http://dx.doi.org/10.1090/S0002-9947-1965-0190144-8

[Lan78]   S. Lang, *Cyclotomic fields*. Graduate Texts in Mathematics, 59, Springer-Verlag, New York-Heidelberg- Berlin, 1978.

[Leo62]   H. W. Leopoldt, *Zur Arithmetik in Abelschen Körper*. J. Reine Angew. Math. **209**(1962), 54–71.

[Mai89]   L. Mai, *Lower Bounds for the ranks of CM types*. J. Number Theory **32**(1989), no. 2, 192–202.   http://dx.doi.org/10.1016/0022-314X(89)90025-5

[Rib80]   K. A. Ribet, *Division fields of abelian varieties with complex multiplication*. Abelian functions and transcendental numbers (Colloq., École Polytech., Palaiseau, 1979), Mém. Soc. Math. France (N.S.), **1980/81**, no. 2, pp. 75–94.

[Ser68]   J.-P. Serre, *Abelian ℓ-adic representations and elliptic curves*. Research Notes in Mathematics, 7, A K Peters, Wellesley, MA, 1998.

[Ser77]   _____, *Linear representations of finite groups*. Graduate Texts in Mathematics, 42, Springer-Verlag, New York-Heidelberg, 1977.

[Ser12]   _____, *Lectures on $N_X(p)$*. Chapman & Hall/CRC Research Notes in Mathematics, 11, CRC Press, Boca Raton, FL, 2012.

[SS95]   J. W. Sands and W. Schwartz, *A Demjanenko matrix for abelian fields of prime power conductor*. J. Number Theory **52**(1995), no. 1, 85–97.
http://dx.doi.org/10.1006/jnth.1995.1057

[ST61]   G. Shimura and Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*. The Mathematical Society of Japan, Tokyo, 1961.

[Sti90]   L. Stickelberger, *Über eine Verallgemeinerung der Kreistheilung*. Math. Ann. **37**(1890), no. 3, 321–367.   http://dx.doi.org/10.1007/BF01721360

[Tan96]   S. G. Tankaeev, *On the Mumford-Tate conjecture for abelian varieties*. Algebraic geometry 4, J. Math Sci. **81**(1996), no. 3, 2719–2737.   http://dx.doi.org/10.1007/BF02362337

[Wei52]   A. Weil, *Jacobi sums as "Grössencharaktere"*. Trans. Amer. Math. Soc. **73**(1952), 487–495.

[Yu15]   C.-F. Yu, *A note on the Mumford-Tate conjecture for CM abelian varieties*. Taiwanese J. Math. **19**(2015), no. 4, 1073–1084.

Institut für Experimentelle Mathematik/Fakultät für Mathematik, Universität Duisburg-Essen, D-45127 Essen, Germany
e-mail: francesc.fite@gmail.com

Departament de Matemàtica Aplicada IV, Universitat Politècnica de Catalunya, Av. Víctor Balaguer s/n., E-08800 Vilanova i la Geltrú, Catalonia
e-mail: josepg@ma4.upc.edu

Departament de Matemàtica Aplicada II, Universitat Politècnica de Catalunya, Edifici Omega-Campus Nord, Jordi Girona 1-3, E-08034 Barcelona, Catalonia
e-mail: joan.carles.lario@upc.edu