Astérisque

BENJI FISHER

# Equidistribution theorems (d'après P. Deligne et N. Katz)

*Astérisque*, tome 228 (1995), p. 69-79

<http://www.numdam.org/item?id=AST_1995__228__69_0>

© Société mathématique de France, 1995, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

*Article numérisé dans le cadre du programme*
*Numérisation de documents anciens mathématiques*
http://www.numdam.org/

# EQUIDISTRIBUTION THEOREMS

(d'après P. DELIGNE et N. KATZ)

Benji FISHER

## 1. INTRODUCTION

To fix ideas, let $p$ be a prime number, $\mathbb{F}_p$ the field with $p$ elements, and $K = \mathbb{F}_p(t)$. Let $K^{\text{sep}}$ be a separable closure of $K$ and $S$ a finite set of places of $K$. Let $l$ be a prime other than $p$ and consider a (continuous) representation

$$\rho\colon \operatorname{Gal}(K^{\text{sep}}/K) \longrightarrow \operatorname{GL}_n(\mathbb{Q}_l)$$

of the Galois group, unramified outside $S$. For places $v$ of $K$ outside $S$, we define (arithmetic) Frobenius elements $\phi_v$ in the Galois group $\operatorname{Gal}(K^{\text{sep}}/K)$ and consider

$$\operatorname{tr}_\rho(v) \stackrel{def}{=} \operatorname{tr}\bigl(\rho(\phi_v)\bigr),$$

the "trace of Frobenius," and

$$\det\bigl(T\operatorname{id} - \rho(\phi_v)\bigr),$$

the "characteristic polynomial of Frobenius." (Actually, $\phi_v$ is only defined up to conjugation, but this does not affect the trace and characteristic polynomial.)

For example, if $E$ is an elliptic curve over $K$ which has good reduction outside $S$ and if $T_l(E)$ is the Tate module of $E$ then we can take

$$\rho = \rho_l\colon \operatorname{Gal}(K^{\text{sep}}/K) \longrightarrow \operatorname{GL}\bigl(\mathbb{Q}_l \underset{\mathbb{Z}_l}{\otimes} T_l(E)\bigr).$$

It is well-known that

$$\det\bigl(T\operatorname{id} - \rho(\phi_v)\bigr) = T^2 - \operatorname{tr}_\rho(v)T + q_v;$$
$$\operatorname{tr}_\rho(v) = \alpha + \overline{\alpha} = 1 + q_v - \#E_v\bigl(\kappa(v)\bigr),$$

where $\kappa(v)$ is the residue field at $v$, $E_v$ is the (good) reduction of $E$ at $v$, $q_v = \#\kappa(v)$, and $\alpha$, $\overline{\alpha}$ are the eigenvalues of Frobenius. Furthermore, $\alpha$ and

1991 *Mathematics Subject Classification.* Primary 11L05; Secondary 11G25, 11L07, 14F20, 14G15.

$\overline{\alpha}$ are algebraic numbers; considered as complex numbers, $|\alpha| = |\overline{\alpha}| = \sqrt{q_v}$, whence the "error term" in $\#E_v(\kappa(v))$ is bounded:

$$\left|1 + q_v - \#E_v(\kappa(v))\right| = |\mathrm{tr}_\rho(v)| \leq 2\sqrt{q_v}.$$

The goal of this paper is to describe Deligne's equidistribution theorem in terms familiar to a number theorist. One application of this theorem is that the normalized "error terms"

$$\frac{\mathrm{tr}_\rho(v)}{\sqrt{q_v}} = \frac{1}{\sqrt{q_v}}\Big(1 + q_v - \#E_v(\kappa(v))\Big) \in [-2, 2]$$

are approximately equidistributed in the interval $[-2, 2]$ (assuming that $j(E) \in K = \mathbb{F}_p(t)$ does not lie in $\mathbb{F}_p$).

It takes some work to describe exactly what is meant by approximate equidistribution, but it is actually quite explicit. When giving explicit estimates, it is convenient to fix a power of $p$, say

$$q = p^r,$$

and to consider places $v$, weighted by $\deg(v) \stackrel{def}{=} [\kappa(v) : \mathbb{F}_p]$, such that $\kappa(v) \subseteq \mathbb{F}_q$. One consequence of Deligne's theorem is that (to continue the elliptic curve example)

$$\left|\frac{1}{N_r}\sum_v \deg(v)\frac{\mathrm{tr}\left(\rho(v)^{r/\deg(v)}\right)}{\sqrt{q}}\right| = O\left(\frac{1}{\sqrt{q}}\right) \text{ as } r \longrightarrow \infty,$$

where

$$N_r = \sum_v \deg(v)$$

and both sums are over $v \notin S$ such that $\deg(v)|r$. Note that most $v$ for which $\deg(v)|r$ actually satisfy $\deg(v) = r$. Thus $N_r$ is approximately $r$ times the number of places $v$ for which $\deg(v) = r$ and the quantity inside the absolute value signs is approximately the average of the normalized traces of Frobenius (or "error terms") for such $v$.

To be completely explicit, let $E$ be the curve given by the Weierstrass equation

$$E : y^2 = x^3 - tx^2 + t.$$

According to Tate's formulas ([7, §2] or [6, III.1]),

$$\Delta = 16t^2(4t^2 - 27); \quad j = \frac{256t^4}{4t^2 - 27},$$

so $E$ is elliptic and $j$ is not constant for $p > 2$. If $p = 3$ then $E$ has good reduction outside $S = \{0, \infty\}$ (and there is wild ramification at 0) and if $p > 3$ then $E$ has good reduction outside $S = \{0, \infty, \pm(27/4)^{1/2}\}$. For $p = 3$,

$$\left| \frac{1}{q-1} \sum_{v} \deg(v) \frac{\operatorname{tr}\left(\rho(v)^{r/\deg(v)}\right)}{\sqrt{q}} \right| \leq \frac{2\sqrt{q}}{q-1};$$

for $p > 3$, $N_r = q - 1 - \#\{x \in \mathbb{F}_q | x^2 = 27/4\}$ and the bound is $4/(\sqrt{q} - 1)$ or $4\sqrt{q}/N_r$.

There are several sections labeled **Translation**. These are intended to help the reader who wishes to consult sources written in the language of algebraic geometry rather than that of number theory. These sections can safely be skipped on a first reading.

## 2. Galois Groups

**Notation 2.1.** Let $K$ be a global field: that is, $K$ is a finite extension either of $\mathbb{Q}$ (the *unequal-characteristic* case or the *number-field* case) or of $\mathbb{F}_q(t)$, where $\mathbb{F}_q$ denotes the finite field with $q$ elements ($q$ a power of a prime $p$) and $t$ is an indeterminate (the *function-field* case or the *equal-characteristic* case). Deligne's equidistribution theorem applies only in the equal-characteristic case, but most of the ideas in this paper make sense in either context. Let $S$ be a finite set of places (equivalence classes of discrete valuations) of $K$. (Elements of $S$ are thought of as "bad primes" in the number-field case and as "points at infinity" in the function-field case.) Let $K_S^{\mathrm{ur}}$ be the maximal separable extension of $K$ which is unramified outside $S$; thus $K_S^{\mathrm{ur}}$ is the union (in a fixed algebraic closure of $K$) of all the finite, separable extensions $L/K$ which are unramified outside $S$. We will discuss representations of $\mathrm{Gal}(K_S^{\mathrm{ur}}/K)$, *i.e.*, representations of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ (where $K^{\mathrm{sep}}$ denotes a separable closure of $K$) which are unramified outside $S$.

**Remark 2.2.** $\mathrm{Gal}(K_S^{\mathrm{ur}}/K)$ can also be described as the inverse limit of $\mathrm{Gal}(L/K)$, where $L$ runs over the finite Galois extensions of $K$ which are unramified outside of $S$. Another description is as the quotient of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ by the closed, normal subgroup generated by the inertia groups $I_v$ for $v \notin S$. Note that, for $v \in S$, $I_v$ has *non*-trivial image in $\mathrm{Gal}(K_S^{\mathrm{ur}}/K)$.

**Translation 2.3.** If $K$ is a number-field, let $X = \operatorname{Spec} \mathcal{O}_K$; if $K$ is a function-field, let $X$ be the smooth, connected, projective curve with function field $K$. (*E.g.*, $X = \mathbb{P}^1_{\mathbb{F}_q}$ when $K = \mathbb{F}_q(t)$). In either case, let $U = X - S$. Then $\mathrm{Gal}(K_S^{\mathrm{ur}}/K)$ is called the **fundamental group** of $U$, denoted $\pi_1(U)$. It is a pro-finite group.

To be precise, this is the fundamental group of $U$ with the "base point" the choice of an algebraic closure of $K$; a different choice of base point would amount to applying an inner automorphism to $\pi_1(U)$, which is irrelevant for the purposes of this paper.

We will not try to justify calling this a "fundamental group". Suffice it to say that (a) there is such a justification; (b) there is a more general definition of which this is a special case; (c) this is an example of the ability of algebraic geometry to apply geometric notions to number theory; and (d) a similar definition, with $X$ a compact Riemann surface, $K$ the field of rational functions on $X$, and $U$ equal to $X$ with finitely many points removed, leads to $\pi_1(U)$ isomorphic to the profinite completion of the ordinary (topological) fundamental group of $U$ (with the isomorphism depending on the choice of base point).

## 3. Galois Representations

A representation of $\mathrm{Gal}(K_S^{\mathrm{ur}}/K)$ is the same as a representation of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ on which the inertia group $I_v$ acts trivially for $v \notin S$; *i.e.*, a Galois representation which is unramified outside $S$. We will consider $l$-adic representations; *i.e.*, representations over $\mathbb{Z}_l$, $\mathbb{Q}_l$, or finite extensions of $\mathbb{Q}_l$, where $l$ is a prime different from the residue characteristics of places $v$ for $v \notin S$. (In particular, if we refer to a representation over $\overline{\mathbb{Q}}_l$ then we really mean a representation over an unspecifed finite extension of $\mathbb{Q}_l$.) We are especially interested in the characters of representations, which we refer to as the **trace-functions** of the representations; and we evaluate these trace-functions at especially nice points:

**Definition 3.1.** Since $K$ is a global field, the residue fields $\kappa(v)$ (where $v$ is a place of $K$) are finite and so $\mathrm{Gal}\big(\kappa(v)^{\mathrm{sep}}/\kappa(v)\big) = \hat{\mathbb{Z}}\phi_v$, where $\phi_v$ is the (arithmetic) Frobenius automorphism $a \mapsto a^{\#\kappa(v)}$.

Let $\overline{v}$ be any lift of $v$ to $K^{\mathrm{sep}}$ and let $D_{\overline{v}}$ and $I_{\overline{v}}$ denote the decomposition and inertia groups at $\overline{v}$. (Of course, when we write $I_v$, as we did above, we really mean $I_{\overline{v}}$ for some such $\overline{v}$.) Recall that

$$(*) \qquad \hat{\mathbb{Z}}\phi_v = \mathrm{Gal}(\kappa(v)^{\mathrm{sep}}/\kappa(v)) \xrightarrow{\sim} D_{\overline{v}}/I_{\overline{v}} \subseteq \mathrm{Gal}(K^{\mathrm{sep}}/K)/I_{\overline{v}};$$

thus if $v \notin S$ ($v$ is a "good prime") there is a map $\hat{\mathbb{Z}}\phi_v \longrightarrow \mathrm{Gal}\big(K_S^{\mathrm{ur}}/K\big)$, which depends on the choice of $\overline{v}$. By abuse of notation, the image of $\phi_v$ (or the conjugacy class of this image, which is independent of the choice of $\overline{v}$) is denoted $\phi_v \in \mathrm{Gal}\big(K_S^{\mathrm{ur}}/K\big)$; it is called the **Frobenius element** at $v$. Given a representation $\rho$ of $\mathrm{Gal}\big(K_S^{\mathrm{ur}}/K\big)$ and a place $v \notin S$, there is a well-defined "trace of Frobenius" $\mathrm{tr}_\rho(v) = \mathrm{tr}\big(\rho(\phi_v)\big)$ and "characteristic polynomial

of Frobenius" $\det(T\,\mathrm{id} - \rho(\phi_v))$. If $V$ is the representation space of $\rho$ then we often write $\mathrm{tr}(\phi_v|V)$ for $\mathrm{tr}(\rho(\phi_v))$ and $\det(T\,\mathrm{id} - \phi_v|V)$ for $\det(T\,\mathrm{id} - \rho(\phi_v))$.

**Translation 3.2.** Algebraic geometers usually work with the **geometric Frobenius** element $\mathrm{Fr}_v = {\phi_v}^{-1} \in \mathrm{Gal}(\kappa(v)^{\mathrm{sep}}/\kappa(v))$. In terms of the geometric Frobenius $\mathrm{Fr}_v$, one considers the characteristic polynomial $\det(\mathrm{id} - T\,\mathrm{Fr}_v\,|V)$. It has the same roots as $\det(T\,\mathrm{id} - \phi_v|V)$.

Let $\mathbb{F}_q$ be a finite field and $x \in U(\mathbb{F}_q)$ an $\mathbb{F}_q$-valued point of $U$ which lies over $v$. *I.e.*, let $x\colon \mathrm{Spec}\,\mathbb{F}_q \longrightarrow U$ factor through $\mathrm{Spec}\,\kappa(v) \longrightarrow U$. Then $\pi_1(\mathrm{Spec}\,\mathbb{F}_q) = \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) = \hat{\mathbb{Z}}\,\mathrm{Fr}_{\mathbb{F}_q}$, where $\mathrm{Fr}_{\mathbb{F}_q}$ denotes the inverse of $a \mapsto a^q$, and $x$ induces a map $\pi_1(\mathrm{Spec}\,\mathbb{F}_q) \longrightarrow \pi_1(U)$. If $\mathbb{F}_q = \kappa(v)$ then this is the same map as $(*)$ above. The image of $\mathrm{Fr}_{\mathbb{F}_q}$ under this map is denoted $\mathrm{Fr}_x$ or $\mathrm{Fr}_{\mathbb{F}_q,x}$. The map

$$\pi_1(\mathrm{Spec}\,\mathbb{F}_q) \longrightarrow \pi_1(\mathrm{Spec}\,\kappa(v)) = \mathrm{Gal}(\kappa(v)^{\mathrm{sep}}/\kappa(v))$$

takes $\mathrm{Fr}_{\mathbb{F}_q}$ to ${\mathrm{Fr}_v}^{[\mathbb{F}_q:\kappa(v)]}$ and so $\mathrm{Fr}_x = {\mathrm{Fr}_v}^{[\mathbb{F}_q:\kappa(v)]} \in \pi_1(U)$.

**Example 3.3.** Let $E$ be an elliptic curve over $K$, as in the introduction (except that now $K$ can be any global field). Fix a prime number $l$. Let $S$ be the set of all places at which $E$ has bad reduction or which have residue characteristic $l$. Let $\rho = \rho_l$ be the representation of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ on the Tate module $V_l = \mathbb{Q}_l \underset{\mathbb{Z}_l}{\otimes} T_l(E)$. By the criterion of Néron-Ogg-Shafarevich ([7, Theorem 4] or [6, III.7]), $\rho$ is unramified outside $S$. At a place $v \notin S$, $T_l(E) \cong T_l(E_v)$, where $E_v$ is the (good) reduction of $E$ at $v$, by [7, Theorem 4] or [6, III.7 and VII.3]. Thus by [7, §5] or [6, V.1] the characteristic polynomial of Frobenius at $v$ is

$$\det(T\,\mathrm{id} - \rho(\phi_v)) = (T - \alpha_v)(T - \overline{\alpha_v}) = T^2 - a_v T + q_v,$$

where $q_v = \#\kappa(v)$ and $a_v = \mathrm{tr}_\rho(v) = 1 + q_v - \#E_v(\kappa(v))$.

**Example 3.4 (Function-field case).** Let $K = \mathbb{F}_q(t)$. Let $\psi$ be a non-trivial additive character of $\mathbb{F}_q$; for example, $\psi(a) = \exp(2\pi i\,\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(a)/p) = {\zeta_p}^{\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(a)}$. Let $\chi$ be a multiplicative character of $\mathbb{F}_q$; even the case where $\chi$ is the trivial character is interesting. Let $\alpha$ be a solution to $\alpha^q - \alpha = t$ and let $\beta$ be a solution to $\beta^{q-1} = t$. Then the Artin-Schreier extension $\mathbb{F}_q(\alpha)/\mathbb{F}_q(t)$ gives a map

$$\mathrm{Gal}(\mathbb{F}_q(t)^{\mathrm{sep}}/\mathbb{F}_q(t)) \longrightarrow\!\!\!\!\rightarrow \mathrm{Gal}(\mathbb{F}_q(\alpha)/\mathbb{F}_q(t)) \xrightarrow{\sim} \mathbb{F}_q \xrightarrow{\psi} \mathbb{Z}[\zeta_p]^\times,$$

where $\zeta_p$ is a primitive root of unity of order $p$, the characteristic of $\mathbb{F}_q$. Considering $\mathbb{Z}[\zeta_p]^\times \subseteq {\overline{\mathbb{Q}}_l}^\times$, we get a one-dimensional $l$-adic representation $\rho_\psi$;

we denote its representation space by $\mathcal{L}_\psi$. Similarly, the Kummer extension $\mathbb{F}_q(\beta)/\mathbb{F}_q(t)$ gives a map

$$\mathrm{Gal}\big(\mathbb{F}_q(t)^{\mathrm{sep}}/\mathbb{F}_q(t)\big) \longrightarrow\!\!\!\!\rightarrow \mathrm{Gal}\big(\mathbb{F}_q(\beta)/\mathbb{F}_q(t)\big) \xrightarrow{\sim} {\mathbb{F}_q}^{\times} \xrightarrow{\chi} \mathbb{Z}[\zeta_{q-1}]^{\times},$$

and a representation $\rho_\chi$ on a one-dimensional space $\mathcal{L}_\chi$.

It is not hard to see that $\mathcal{L}_\psi$ is unramified outside $\{\infty\}$ and that $\mathcal{L}_\chi$ is unramified outside $\{0,\infty\}$. With a little work, one can also see that if $v \neq \infty$ extends to a place $\overline{v}$ of $\overline{\mathbb{F}_q}(t)$ and $t-a$ is a generator of the maximal ideal of $\overline{v}$ then

$$\mathrm{tr}(\phi_v|\mathcal{L}_\psi) = \psi\big(\mathrm{tr}_{\mathbb{F}_q[a]/\mathbb{F}_q}(a)\big).$$

Similarly, if $v \notin \{0,\infty\}$ then

$$\mathrm{tr}(\phi_v|\mathcal{L}_\chi) = \chi\big(\mathrm{N}_{\mathbb{F}_q[a]/\mathbb{F}_q}(a)\big).$$

**Translation 3.5.** The notation here is non-standard. Usually, one defines $\mathcal{L}_\psi$ and $\mathcal{L}_\chi$ to be what is here called $\mathcal{L}_{\overline{\psi}}$ and $\mathcal{L}_{\overline{\chi}}$, so that the above formulas hold with $\phi_v$ replaced with $\mathrm{Fr}_v$. $\mathcal{L}_\psi$ is a one-dimensional representation of $\pi_1(\mathbb{A}^1{}_{\mathbb{F}_q})$ and $\mathcal{L}_\chi$ is a one-dimensional representation of $\pi_1(\mathbb{G}_{m,\mathbb{F}_q})$, where $\mathbb{A}^1 = \mathbb{P}^1 - \{\infty\}$ and $\mathbb{G}_m = \mathbb{A}^1 - \{0\}$. Any $a \in \mathbb{F}_{q^r}$ can be considered as an element of $\mathbb{A}^1(\mathbb{F}_{q^r})$, *i.e.*, as a map $\mathrm{Spec}\,\mathbb{F}_{q^r} \longrightarrow \mathbb{A}^1$, or as a map $\mathbb{F}_q[t] \longrightarrow \mathbb{F}_{q^r}$. If $\mathfrak{p}$ denotes the kernel of $\mathbb{F}_q[t] \longrightarrow \mathbb{F}_{q^r}$ and $v$ denotes the place corresponding to $\mathfrak{p}$ then we have the situation described above. Let $\mathrm{Fr}_{\mathbb{F}_{q^r},a} = {\mathrm{Fr}_v}^{r/\deg(v)}$. Then, using standard notation,

$$\begin{aligned} &\big(\forall a \in \mathbb{F}_{q^r} = \mathbb{A}^1(\mathbb{F}_{q^r})\big) \quad \mathrm{tr}\big(\mathrm{Fr}_a\,|\mathcal{L}_\psi\big) = \psi\big(\mathrm{tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(a)\big); \\ &\big(\forall a \in {\mathbb{F}_{q^r}}^{\times} = \mathbb{G}_m(\mathbb{F}_{q^r})\big) \quad \mathrm{tr}\big(\mathrm{Fr}_a\,|\mathcal{L}_\chi\big) = \chi\big(\mathrm{N}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(a)\big). \end{aligned}$$

**Remarks 3.6.** Various algebraic manipulations can be done on the level of representations. For example, $\mathrm{tr}_{\rho\oplus\sigma} = \mathrm{tr}_\rho + \mathrm{tr}_\sigma$ and $\mathrm{tr}_{\rho\otimes\sigma} = \mathrm{tr}_\rho \cdot \mathrm{tr}_\sigma$. In some cases, it is also possible to define convolutions. In particular, (generalized) Kloosterman sums can be dealt with in this setting: given a non-trivial additive character $\psi$ and arbitrary multiplicative characters $\chi_1, \ldots, \chi_n$ of ${\mathbb{F}_q}^{\times}$, there is a representation $\mathcal{K}$ of $\mathrm{Gal}\big(K_S^{\mathrm{ur}}/K\big)$ $(S = \{0,\infty\})$, obtained by convolving $\mathcal{L}_\psi \otimes \mathcal{L}_{\chi_i}$ $(i = 1, 2, \ldots, n)$, so that

$$\mathrm{tr}\big(\phi_v \mid \mathcal{K}\big) = (-1)^{n-1} \sum_{u_1 \ldots u_n = a} \psi(u_1 + \cdots + u_n)\chi_1(u_1)\ldots\chi_n(u_n),$$

where the sum is over $n$-tuples in $\mathbb{F}_q[a]$ with product $a$ and where $\psi$ and the $\chi_i$ are extended to $\mathbb{F}_q[a]$ by trace and norm. Taking $n = 2$ and both $\chi_1$ and $\chi_2$ to be the trivial character, we get the ordinary Kloosterman sum. For details, see [3, Chapter 5] and [5, §8.1].

## 4. EQUIDISTRIBUTION

Deligne's theorem applies only to the function-field case, to which we will restrict after a few more definitions.

**Definition 4.1.** Let $\rho$ be a representation of $\mathrm{Gal}(K_S^{\mathrm{ur}}/K)$ on a vector space $V$. The (arithmetic) **monodromy group** of $\rho$, denoted $G_{\mathrm{arith}}$, is the Zariski-closure of the image of $\rho$ in $\mathrm{GL}(V)$. In the function-field case, the **geometric monodromy group** of $\rho$, denoted $G_{\mathrm{geom}}$, is the monodromy group of $\rho \mid \mathrm{Gal}(K_S^{\mathrm{ur}}/K\overline{\mathbb{F}_q})$, *i.e.*, the Zariski-closure of $\rho\Big(\mathrm{Gal}(K_S^{\mathrm{ur}}/K\overline{\mathbb{F}_q})\Big)$ in $\mathrm{GL}(V)$.

**Example 4.2.** If $\rho$ is the representation of $\mathrm{Gal}(K_S^{\mathrm{ur}}/K)$ on the Tate module of an elliptic curve in the function-field case then $G_{\mathrm{geom}} = \mathrm{SL}(2)$ according to [2, Lemme 3.5.5], unless $j$ is a constant. (This is why we assumed $j \notin \mathbb{F}_p$ in the Introduction.)

**Translation 4.3.** Recall that $\mathrm{Gal}(K_S^{\mathrm{ur}}/K) = \pi_1(U)$, where $U$ is the curve $X - S$. We also have

$$\mathrm{Gal}(K_S^{\mathrm{ur}}/K\overline{\mathbb{F}_q}) = \pi_1^{\mathrm{geom}}(U) \stackrel{def}{=} \pi_1\big(U \underset{\mathbb{F}_q}{\otimes} \overline{\mathbb{F}_q}\big) \subseteq \pi_1(U).$$

For example, if $U = \mathbb{A}^1{}_{\mathbb{F}_q}$ then $U \underset{\mathbb{F}_q}{\otimes} \overline{\mathbb{F}_q} = \mathbb{A}^1{}_{\overline{\mathbb{F}_q}}$.

**Remarks 4.4.** It is often convenient to think of $\mathrm{GL}(V)$ as an algebraic group. When $V$ is a vector space over $\mathbb{Q}_l$ or a finite extension of $\mathbb{Q}_l$, one can think of $\mathrm{GL}(V)$ as an $l$-adic Lie group; or one can imbed $\overline{\mathbb{Q}}_l \hookrightarrow \mathbb{C}$ and think of it as a complex Lie group. Usually, one can work in whichever context one is most comfortable; the representation theory is the same in any of these contexts.

**Definition 4.5.** A representation $\rho$ is **pure of weight 0** if, for all $v \notin S$ and all eigenvalues $\alpha$ of $\rho(\phi_v)$, $|\alpha| = 1$ for all *Archimedian* absolute values $|\cdot|$.

**Example 4.6.** There is a "twisted" Kloosterman representation, denoted $\mathcal{K}\big(\frac{1-n}{2}\big)$, such that

$$\mathrm{tr}\big(\phi_v \mid \mathcal{K}\big(\tfrac{1-n}{2}\big)\big) = q_v{}^{(1-n)/2}\,\mathrm{tr}\big(\phi_v \mid \mathcal{K}\big).$$

This twisted Kloosterman representation is pure of weight 0.

**Translation 4.7.** Normally, one defines a representation $\mathcal{F}$ such that $\mathrm{tr}\big(\mathrm{Fr}_v \mid \mathcal{F}\big)$ gives the Kloosterman sum. This $\mathcal{F}$ is the dual (contragradient) representation of $\mathcal{K}$: $\mathcal{F} = \mathcal{K}^\vee$. The relation between the normalized (weight-0) representations is $\mathcal{F}\big(\frac{n-1}{2}\big) = \mathcal{K}\big(\frac{1-n}{2}\big)^\vee$.

Let $\rho\colon \mathrm{Gal}(K_S^{\mathrm{ur}}/K) \longrightarrow \mathrm{GL}(V)$ be an $l$-adic representation which is pure of weight 0 and let $G = G_{\mathrm{arith}}$ be its (arithmetic) monodromy group, thought of as a *complex* Lie group. (*I.e.*, fix a complex imbedding of $\overline{\mathbb{Q}}_l$, or of an appropriate finite extension of $\mathbb{Q}_l$ if you do not like the axiom of choice, and let $G$ denote the group of $\mathbb{C}$-valued points of $G_{\mathrm{arith}}$.) Let $\Gamma$ be a maximal compact subgroup of $G$. For any $v \notin S$, $\rho(\phi_v)$ has all eigenvalues of absolute value 1 since $\rho$ is pure of weight 0. Thus if $\rho(\phi_v)^{\mathrm{s/s}}$ denotes its semisimple part, in the sense of (multiplicative) Jordan decomposition, then the closure of the subgroup generated by $\rho(\phi_v)^{\mathrm{s/s}}$ is compact, and so some conjugate of $\rho(\phi_v)^{\mathrm{s/s}}$ lies in $\Gamma$.

Of course, $\phi_v$ is only defined up to conjugation in $G$. Since $G$ and $\Gamma$ have the "same" representations, and characters of representations separate conjugacy classes, $\rho(\phi_v)^{\mathrm{s/s}}$ gives a well-defined element $\theta(v) \in \Gamma^\natural$, where $\Gamma^\natural$ denotes the set of conjugacy classes of $\Gamma$. Since $\Gamma$ is a compact group, we can consider Haar measure on $\Gamma$ (normalized to have total mass 1) and its direct image, which will be denoted $\mu^\natural$, on $\Gamma^\natural$.

We are now ready to state Deligne's equidistribution theorem. Our statement follows [3, Theorem 3.6]; see also [2, Thèoréme 3.5.3].

**Theorem 4.8 (Deligne).** *Let $\rho\colon \mathrm{Gal}(K_S^{ur}/K) \longrightarrow \mathrm{GL}(V)$ be an $l$-adic representation which is pure of weight 0. Assume that $G_{\mathrm{geom}} = G_{\mathrm{arith}} = G$. Then as $v$ runs over the places of $K$, $v \notin S$, the conjugacy classes $\theta(v)$ corresponding to $\rho(\phi_v)^{\mathrm{s/s}}$ are approximately equidistributed in $\Gamma^\natural$ with respect to $\mu^\natural$, the direct image of Haar measure. More precisely: for any non-trivial, irreducible, complex representation $\Lambda$ of $\Gamma$ (or of $G$) and any $r$,*

$$\left| \frac{1}{N_r} \sum_v \deg(v) \operatorname{tr} \Lambda\big(\theta(v)^{r/\deg(v)}\big) \right| = O\left( \frac{\dim \Lambda}{q^{r/2}} \right),$$

*where $N_r = \sum_v \deg(v)$ and both sums are over places $v \notin S$ such that $\deg(v) \mid r$. The bounds implicit in the $O$ can be made explicit.*

**Remarks 4.9.** (1) It should be clear what a power of $\theta(v) \in \Gamma^\natural$ means.
(2) The concrete example at the end of the introduction was obtained by taking $\Lambda$ to be the standard two-dimensional representation of $G = \mathrm{SL}(2)$. The power of $p$ in the denominator appears because the standard representation on the Tate module must be twisted to make it pure of weight 0. Getting explicit bounds for $p = 3$ involves some calculation because of wild ramification. For calculating explicit bounds, see [3, equation 3.6.3].
(3) Estimates for sums over $v \notin S$ such that $\deg(v) = r$ or $\deg(v) \leq r$ follow from the estimate given above. (*Cf* the remarks made in the Introduction.)
(4) If a set $\mathcal{S}$ of points in $\Gamma^\natural$ is perfectly equidistributed with respect to $\mu^\natural$ then

averaging a continuous function over $\mathcal{S}$ is the same as integrating with respect to $\mu^\natural$. Any continuous function on $\Gamma^\natural$ can be uniformly approximated by a linear combination of irreducible characters, so $\mathcal{S}$ is equidistributed if the average over $\mathcal{S}$ of $\mathrm{tr} \circ \Lambda$ is 0 for all non-trivial, irreducible, complex representations $\Lambda$. This is the sense in which this is an equidistribution theorem.

**Corollary 4.10.** *When Deligne's theorem applies,* $\{\mathrm{tr}\,\rho(\phi_v)\} = \{\mathrm{tr}_\rho(v)\}$ *is (approximately) equidistributed in* $\mathrm{tr}(\Gamma)$ *with respect to the direct image of Haar measure.*

**Remark 4.11.** The condition $G_{\mathrm{geom}} = G_{\mathrm{arith}}$ is rather mysterious. This author does not even know whether it holds for $\rho \oplus \sigma$ or for $\rho \otimes \sigma$ given that it holds for $\rho$ and for $\sigma$. Katz has shown that it holds for a twisted Kloosterman representation $\mathcal{K}(\alpha)$ by showing that $G_{\mathrm{geom}}$ is "as large as possible." Here $\alpha \in \overline{\mathbb{Q}}_l^{\times}$ is an $l$-adic unit and $\mathcal{K}(\alpha) = \mathcal{K} \otimes \overline{\mathbb{Q}}_l(\alpha)$, where $\overline{\mathbb{Q}}_l(\alpha)$ denotes the one-dimensional representation on which $\mathrm{Fr}_v$ acts as multiplication by $\alpha$. More precisely, $G_{\mathrm{geom}} \triangleleft G_{\mathrm{arith}}$ and Katz shows that the normalizer of $G_{\mathrm{geom}}$ in $\mathrm{GL}(n)$ is (scalars)$G_{\mathrm{geom}}$; the existence of such an $\alpha$ follows. Thus Deligne's theorem and its corollary apply, so the (generalized) Kloosterman sums for a given $\mathbb{F}_q$ are (approximately) equidistributed.

**Theorem 4.12 (Katz).** *Assume that* $p > 2n+1$ *and that* $(\chi_1, \ldots, \chi_n)$ *is not* Kummer-induced. *Then the connected component* $G_{\mathrm{geom}}(\mathcal{K})^0$ *is "as large as possible": it is either* $\mathrm{SL}(n)$ *or* $\mathrm{SO}(n)$ *or* $\mathrm{Sp}(n)$. *In the* SO *case,* $G_{\mathrm{geom}}(\mathcal{K})$ *is not contained in* (scalars) $\mathrm{SO}(n)$. *Furthermore, there is an* $l$*-adic unit* $\alpha \in \overline{\mathbb{Q}}_l^{\times}$ *such that twisted Kloosterman representation* $\mathcal{K}(\alpha)$ *is pure of weight* 0 *and has* $G_{\mathrm{geom}} = G_{\mathrm{arith}}$.

For completeness' sake, we give

**Definition 4.13.** An $n$-tuple $(\chi_1, \ldots, \chi_n)$ of multiplicative characters is **Kummer-induced** if there exists a non-trivial multiplicative character $\Lambda$ such that $(\Lambda\chi_1, \ldots, \Lambda\chi_n)$ is a permutation of $(\chi_1, \ldots, \chi_n)$.

**Remarks 4.14.** By $\mathrm{Sp}(n)$ we mean the subgroup of $\mathrm{SL}(n)$ which many would call $\mathrm{Sp}(n/2)$. Note that $(\mathbf{1}, \ldots, \mathbf{1})$ is *not* Kummer-induced. In this case, the condition $p > 2n+1$ is not necessary: for $p > 2$, $G_{\mathrm{geom}}$ is either $\mathrm{SL}(n)$ (if $n$ is odd) or $\mathrm{Sp}(n)$ (if $n$ is even), whereas for $p = 2$, $G_{\mathrm{geom}}$ is either $\mathrm{SO}(n)$ (if $n$ is odd) or $\mathrm{Sp}(n)$ (if $n$ is even), except that $G_{\mathrm{geom}}$ is the exceptional Lie group $G_2$ for $p = 2$, $n = 7$. This is [3, Theorem 11.1]; the above Theorem is [4, Theorem 13 and Corollary 16].

## 5. Explicit Statements for Elliptic Curves

**Notation 5.1.** Let $K$ be a function field of genus $g$ over a finite field $\mathbb{F}_q$ and $E/K$ an elliptic curve with good reduction outside of $S$ (a finite set of places). For $v \notin S$ (a place of good reduction) let $\deg(v)$ be the degree of $v$, *i.e.*, the degree of the residue field $\kappa(v)$ at $v$ over the ground field $\mathbb{F}_q$; and define $\theta(v)$ by

$$1 + q^{\deg(v)} - \#E_v\big(\kappa(v)\big) = 2\sqrt{q^{\deg(v)}}\cos\theta(v);$$

also, if $r$ is a multiple of $\deg(v)$, let $\theta_r(v) \stackrel{def}{=} \big(r/\deg(v)\big)\theta(v)$. Finally, let $l$ be a prime other than the characteristic of $K$ and let $T_l(E)$ denote the Tate module of $E$.

**Remark 5.2.** Suppose a matrix $A \in \mathrm{SU}(2)$ acts on a two-dimensional complex vector space $V$ with eigenvalues $e^{\pm i\theta}$. (For our purposes, $V$ will be $T_l(E) \otimes \mathbb{C}$.) Recall that the irreducible representations of $\mathrm{SU}(2)$ are given by the symmetric powers $\mathrm{Sym}^n(V)$ $(n = 0, 1, 2, \dots)$. Then $A$ acts on $\mathrm{Sym}^n(V)$ with eigenvalues $e^{ji\theta}e^{-ki\theta}$ $(j + k = n)$ and one can check that the trace of $A$ on $\mathrm{Sym}^n(V)$ is $\sin(n+1)\theta/\sin\theta$.

With the above notation, the explicit form of Deligne's theorem is that

$$\Big|\sum_v \deg(v)\frac{\sin(n+1)\theta_r(v)}{\sin\theta_r(v)}\Big| \le (n+1)h_n\sqrt{q^r}.$$

(The sum is over places $v \notin S$ such that $\deg(v) \mid r$.) The not-quite-constant $h_n$ is given by

$$h_n = 2g - 2 + \#S + \sum_{v\in S}\frac{1}{n+1}\,\mathrm{Sw}_v\big(\mathrm{Sym}^n T_l(E)\big).$$

Here $\mathrm{Sw}_v$ denotes the Swan conductor, a measure of wild ramification (*i.e.*, a measure of the action of higher ramification groups on the given representation). In particular,

- If $p > 3$ then there is no wild ramification, so $h_n = 2g - 2 + \#S$, independent of $n$.
- If $n = 1$ then, in the notation of [Sil, Appendix C, §16], the Swan conductor of the Tate module is given by

  $$\mathrm{Sw}_v\big(T_l(E)\big) = \delta_v = f_v - 2 = \mathrm{ord}_v\big(\mathcal{D}_{E/K}\big) - 1 - m_v,$$

  where $f_v$ is the exponent of the conductor at $v$, $\mathcal{D}_{E/K}$ is the minimal discriminant of $E/K$, and $m_v$ is the number of irreducible components

(ignoring multiplicities) of the fiber at $v$ of the Néron model of $E$. Thus

$$2h_1\sqrt{q^r} = [2(2g-2+\#S)+\delta_v]\sqrt{q^r}.$$

- In general, $\frac{1}{n+1}\mathrm{Sw}_v(\mathrm{Sym}^n T_l(E))$ is at most the largest *break* of $T_l(E)$ at $v$, which is at most the Swan conductor (since the Swan conductor is the sum of the breaks). Thus

$$h_n \leq 2g-2+\#S+\sum_{v\in S}\delta_v.$$

**Remark 5.3.** References to the Swan conductor are somewhat scattered. Besides the reference to [Sil] already mentioned (and the references therein), one should consult [Ka-1, Chapter 1] and Chapter 19 of Serre's *Linear Representations of Finite Groups.*

## References


1. Pierre DELIGNE, Applications de la Formule des Traces aux Sommes Trigonometriques, in *Cohomologie Etale* (SGA $4\frac{1}{2}$), Springer Lecture Notes in Mathematics **569**, New York, 1977.
2. ———, La conjecture de Weil. II, *Publ. Math. IHES* **52** (1981) 313–428.
3. Nicholas M. KATZ, *Gauss Sums, Kloosterman Sums, and Monodromy Groups*, Princeton University Press, Princeton, 1988.
4. ———, On the Monodromy Groups Attached to Certain Families of Exponential Sums, *Duke Math. J.* **54** No. 1, (1987) 41–56.
5. ———, *Exponential Sums and Differential Equations*, Princeton University Press, Princeton, 1990.
6. Joseph H. SILVERMAN, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.
7. John T. TATE, The Arithmetic of Elliptic Curves, *Inventiones Math.* **23** (1974) pp. 179–206.



Benji FISHER
Mathematics Department
Columbia University
New York, NY 10027
benji@math.columbia.edu