

Summary We prove equidistribution results for certain exponential sums that arise in the work of Kurlberg–Rudnick on "cat maps". We show (Theorems 1 and 2) that suitable normalizations of these sums behave like the traces of random matrices in $SU(2)$. We also show that as a suitable parameter varies, the corresponding sums are statistically independent (Theorems 3 and 4). The main tools are Deligne's Equidistribution Theorem, the Feit–Thompson Theorem, the Goursat–Kolchin–Ribet Theorem, and Laumon's Theorem of Stationary Phase.

Introduction, and Statement of Results

Fix a finite field k of **odd** characteristic p and cardinality q , a nontrivial \mathbb{C} -valued additive character ψ of k ,

$$\psi : (k, +) \rightarrow \mathbb{C}^\times,$$

and a nontrivial \mathbb{C} -valued multiplicative character of k^\times ,

$$\chi : (k, \times) \rightarrow \mathbb{C}^\times.$$

We extend χ to a function on all of k by defining $\chi(0) := 0$.

Kurlberg–Rudnick [Kur–Rud], in their study of "cat maps", encounter the \mathbb{C} -valued function $H(\psi, \chi)$ on k defined by

$$H(\psi, \chi)(t) := \sum_{x \text{ in } k} \psi(x^2 + tx)\chi(x).$$

It will be convenient to consider a "normalized" version $F(\psi, \chi)$ of this function. Denote by χ_{quad} the quadratic character of k^\times . Recall that for any nontrivial χ , the Gauss sum $G(\psi, \chi)$ is defined by

$$G(\psi, \chi) := \sum_{x \text{ in } k} \psi(x)\chi(x).$$

It is well known that $|G(\psi, \chi)| = \text{Sqrt}(q)$.

Denote by $A(\psi, \chi)$ the complex constant of absolute value q defined as the product

$$A(\psi, \chi) := \chi(-1/2)(-G(\psi, \chi))(-G(\psi, \chi_{\text{quad}})).$$

Choose a square root $B(\psi, \chi)$ of $1/A(\psi, \chi)$. With this choice, we define the \mathbb{C} -valued function $F(\psi, \chi)$ on k by

$$F(\psi, \chi)(t) := -H(\psi, \chi)(t)(\psi(t^2/8)B(\psi, \chi)).$$

Theorem 1 Notations as above, the function $F(\psi, \chi)$ on k takes real values which lie in the closed interval $[-2, 2]$.

For each t in k , denote by $\theta(\psi, \chi)(t)$ in $[0, \pi]$ the unique angle for which

$$F(\psi, \chi)(t) = 2\cos(\theta(\psi, \chi)(t)).$$

Denote by μ_{ST} the Sato–Tate measure $(2/\pi)\sin^2(\theta)d\theta$ on $[0, \pi]$. Denote by $\{S_n\}_{n \geq 1}$ the orthonormal basis of $L^2([0, \pi], \mu_{\text{ST}})$ given by

$$S_n(\theta) := \sin(n\theta)/\sin(\theta).$$

We interpret $[0, \pi]$ as the space of conjugacy classes in the group $\text{SU}(2)$, by mapping A in $\text{SU}(2)$ to the unique $\theta(A)$ in $[0, \pi]$ for which $\text{trace}(A) = 2\cos(\theta(A))$. Then the Sato–Tate measure becomes the measure induced on conjugacy classes by the (total mass one) Haar measure on $\text{SU}(2)$. The function $S_n(\theta)$ becomes the character of the unique n –dimensional irreducible representation of $\text{SU}(2)$. From this interpretation, and the representation theory of $\text{SU}(2)$, we see that $S_{n+1}(\theta)$ is a monic polynomial with integer coefficients P_n of degree n in $S_2(\theta) = 2\cos(\theta)$.

Moreover, the sequence $\{S_{n+1}\}_{n \geq 0}$ is obtained from the sequence $\{(2\cos(\theta))^n\}_{n \geq 0}$ by applying Gram–Schmid orthonormalization. The **Chebyshev polynomials of the second kind**, U_n , defined by

$$U_n(\cos(\theta)) = S_{n+1}(\theta),$$

are thus related to our P_n by

$$U_n(u) = P_n(2u).$$

The representation theoretic interpretation of the functions S_n shows that have the integration formula

$$\int_{[0, \pi]} S_n d\mu_{\text{ST}} = \delta_{n,1}.$$

So if we expand a continuous \mathbb{C} –valued function f on $[0, \pi]$ into its "representation–theoretic fourier series"

$$f = \sum_{n \geq 1} a_n S_n,$$

then its integral against Sato–Tate measure is given by

$$\int_{[0, \pi]} f d\mu_{\text{ST}} = a_1.$$

Interlude: review of equidistribution

We now recall some basic notions of equidistribution. Given a compact Hausdorff space X and a Borel probability measure μ on X , a sequence of Borel probability measures μ_i on X is said to converge "weak $*$ " to μ if for every continuous \mathbb{C} –valued function f on X , we have the integration formula

$$\int_X f d\mu = \lim_{i \rightarrow \infty} \int_X f d\mu_i.$$

If this integration formula holds for a set of test functions f_n whose finite \mathbb{C} –linear combinations are uniformly dense in the space of all continuous functions on X , then it holds for all continuous functions f .

In many applications, the measures μ_i arise as follows. For each i , one is given a nonempty finite set X_i , and a map $\theta_i : X_i \rightarrow X$

of sets. One takes for μ_i the average of the Dirac delta measures $\delta_{\theta_i(x)}$ as x runs over X_i :

$$\mu_i := (1/|X_i|) \sum_{x \text{ in } X_i} \delta_{\theta_i(x)}.$$

More concretely, for any continuous \mathbb{C} -valued function f on X ,

$$\int_X f d\mu_i = (1/|X_i|) \sum_{x \text{ in } X_i} f(\theta_i(x)).$$

In this situation, if the measures μ_i converge weak * to μ , we will say that the points $\theta_i(x)$, as x varies in X_i , are "approximately equidistributed" in X for the measure μ .

In our applications below, (X, μ) will first be $([0, \pi], \mu_{\text{ST}})$, and the test functions will be the functions $S_n(\theta)$. Later (X, μ) will be the r -fold self product of $([0, \pi], \mu_{\text{ST}})$ with itself, and the test functions will be the r -fold products

$$S_{n_1, n_2, \dots, n_r}(\theta_1, \dots, \theta_r) = \prod_j S_{n_j}(\theta_j).$$

Thus, concretely, a sequence of Borel probability measures μ_i on $[0, \pi]$ converges weak * to the Sato–Tate measure μ_{ST} if and only if

$$\lim_{i \rightarrow \infty} \int_{[0, \pi]} S_n d\mu_i = 0, \text{ for each } n \geq 2.$$

[The point is that $\int_{[0, \pi]} S_n d\mu_{\text{ST}} = 0$ for $n \geq 2$, while S_1 is the constant function 1, and so each $\int_{[0, \pi]} S_1 d\mu_i$ and $\int_{[0, \pi]} S_1 d\mu_{\text{ST}}$ is 1.]

Similarly, for any $r \geq 1$, a sequence of Borel probability measures μ_i on $[0, \pi]^r$ converges weak * to the Sato–Tate measure $(\mu_{\text{ST}})^r$ if and only if for each r -tuple (n_1, \dots, n_r) of strictly positive integers with $\sum_j n_j \geq r+1$, we have

$$\lim_{i \rightarrow \infty} \int_{[0, \pi]^r} (\prod_j S_{n_j}(\theta_j)) d\mu_i = 0.$$

Return to Statement of Results

Given a finite field k of odd characteristic, and a pair (ψ, χ) as above, we view the formation of the angle $\theta(\psi, \chi)(t)$ as defining a map from k to $[0, \pi]$. We form the corresponding probability measure $\mu(k, \psi, \chi)$ on $[0, \pi]$, defined by

$$\mu(k, \psi, \chi) := (1/q) \sum_{t \text{ in } k} \delta_{\theta(\psi, \chi)(t)},$$

i.e. for any \mathbb{C} -valued continuous function f on $[0, \pi]$, we have

$$\int_{[0, \pi]} f d\mu(k, \psi, \chi) := (1/q) \sum_{t \text{ in } k} f(\theta(\psi, \chi)(t)).$$

Theorem 2 Take any sequence of data (k_i, ψ_i, χ_i) in which each k_i has characteristic at least 7, and in which $q_i := \text{Card}(k_i)$ is strictly increasing. Then the angles $\{\theta(\psi_i, \chi_i)(t)\}_{t \text{ in } k_i}$ are approximately equidistributed in the interval $[0, \pi]$ with respect to the Sato–Tate measure μ_{ST} , in the sense that as $i \rightarrow \infty$, the measures $\mu(k_i, \psi_i, \chi_i)$ tend weak * to the Sato–Tate measure μ_{ST} . More precisely, for any integer $n \geq 2$, and any datum (k, ψ, χ) with k of characteristic at least 7 we have the estimate

$$|\int_{[0, \pi]} S_n d\mu(k, \psi, \chi) - (1/q) \sum_{t \text{ in } k} S_n(\theta(\psi, \chi)(t))| \leq n/\text{Sqrt}(q).$$

Another way to state this last result is in terms of "semi–circle measure"

$$\mu_{\text{scir}} := (2/\pi)\text{Sqrt}(1 - u^2)du$$

on the closed interval $[-1, 1]$, which corresponds to Sato–Tate measure on $[0, \pi]$, via $u := \cos(\theta)$. By means of this change of variable, the functions $\{S_{n+1}(\theta)\}_{n \geq 0}$ become the Chebychev polynomials of the second kind $\{U_n(u)\}_{n \geq 0}$, and the measure $\mu(k, \psi, \chi)$ on $[0, \pi]$ becomes the measure $\nu(k, \psi, \chi)$ on $[-1, 1]$ defined by

$$\nu(k, \psi, \chi) := (1/q)\sum_{t \text{ in } k} \delta_{F(\psi, \chi)(t)/2},$$

i.e. for any \mathbb{C} -valued continuous function f on $[-1, 1]$, we have

$$\int_{[-1, 1]} f d\nu(k, \psi, \chi) := (1/q)\sum_{t \text{ in } k} f(F(\psi, \chi)(t)/2).$$

Theorem 2 bis Take any sequence of data (k_i, ψ_i, χ_i) in which each k_i has characteristic at least 7, and in which $q_i := \text{Card}(k_i)$ is strictly increasing. Then the real numbers $\{F(\psi, \chi)(t)/2\}_{t \text{ in } k}$ are approximately equidistributed in the interval $[-1, 1]$ with respect to the semicircle measure μ_{scir} , in the sense that as $i \rightarrow \infty$, the measures $\nu(k_i, \psi_i, \chi_i)$ tend weak * to the semicircle measure μ_{scir} . More precisely, for any integer $n \geq 1$, and any datum (k, ψ, χ) with k of characteristic at least 7, we have the estimate

$$\left| \int_{[-1, 1]} U_n d\nu(k, \psi, \chi) - \int_{[-1, 1]} U_n d\mu_{\text{scir}} \right| \leq (n+1)/\text{Sqrt}(q).$$

In the next theorem, we consider several χ 's simultaneously. Fix an integer $r \geq 1$. Given a finite field k of odd characteristic, a nontrivial additive character ψ of k , and r distinct nontrivial multiplicative characters $\chi_1, \chi_2, \dots, \chi_r$ of k^\times , we define a map from k to $[0, \pi]^r$ by

$$t \mapsto \theta(\psi, \chi\text{'s})(t) := (\theta(\psi, \chi_1)(t), \theta(\psi, \chi_2)(t), \dots, \theta(\psi, \chi_r)(t)).$$

We form the corresponding probability measure $\mu(k, \psi, \chi\text{'s})$ on $[0, \pi]^r$, defined by

$$\mu(k, \psi, \chi\text{'s}) := (1/q)\sum_{t \text{ in } k} \delta_{\theta(\psi, \chi\text{'s})(t)}$$

i.e. for any \mathbb{C} -valued continuous function f on $[0, \pi]^r$, we have

$$\int_{[0, \pi]^r} f d\mu(k, \psi, \chi\text{'s}) := (1/q)\sum_{t \text{ in } k} f(\theta(\psi, \chi\text{'s})(t)).$$

Theorem 3 Fix $r \geq 1$. Take any sequence of data $(k_i, \psi_i, \chi_i\text{'s})$ in which each k_i has characteristic at least 7, and in which $q_i := \text{Card}(k_i)$ is strictly increasing. Then the r -tuples of angles

$$\{\theta(\psi_i, \chi_i\text{'s})(t)\}_{t \text{ in } k_i}$$

are approximately equidistributed in $[0, \pi]^r$ with respect to $(\mu_{\text{ST}})^r$, in the sense that as $i \rightarrow \infty$, the measures $\mu(k_i, \psi_i, \chi_i\text{'s})$ tend weak * to $(\mu_{\text{ST}})^r$. More precisely, for any r tuple of strictly positive integers (n_1, n_2, \dots, n_r) with $\sum_j n_j \geq r+1$, and any datum $(k, \psi, \chi\text{'s})$ with k of characteristic at least 7, we have the estimate

$$\int_{[0, \pi]^F} S_{n_1, n_2, \dots, n_r} d\mu(k, \psi, \chi's) = |(1/q) \sum_{t \in k} S_{n_1, n_2, \dots, n_r}(\theta(\psi, \chi's)(t))| \leq (\prod_i n_i) / \text{Sqrt}(q).$$

In terms of semicircle measure, the measure $(\mu_{ST})^F$ on $[0, \pi]^F$ becomes the measure $(\mu_{\text{scir}})^F$ on $[-1, 1]^F$, the test functions

$$S_{n_1 + 1, \dots, n_r + 1}(\theta_1, \dots, \theta_r)$$

become the functions

$$U_{n_1, \dots, n_r}(\theta's) := \prod_j U_{n_j}(u_j).$$

The measures

$$\mu(k, \psi, \chi's) := (1/q) \sum_{t \in k} \delta_{\theta(\psi, \chi's)(t)}$$

on $[0, \pi]^F$ become the measures

$$\nu(k, \psi, \chi's) := (1/q) \sum_{t \in k} \delta_{F(\psi, \chi's)(t)/2}$$

on $[-1, 1]^F$.

Theorem 3 bis Fix $r \geq 1$. Take any sequence of data $(k_i, \psi_i, \chi_i's)$ in which each k_i has characteristic at least 7, and in which $q_i := \text{Card}(k_i)$ is strictly increasing. Then the r -tuples in $[-1, 1]^F$

$$\{F(\psi, \chi's)(t)/2\}_{t \in k}$$

are approximately equidistributed in $[-1, 1]^F$ with respect to $(\mu_{\text{scir}})^F$, in the sense that as $i \rightarrow \infty$, the measures $\nu(k_i, \psi_i, \chi_i's)$ tend weak * to $(\mu_{\text{scir}})^F$. More precisely, for any nonzero r -tuple of nonnegative integers (n_1, n_2, \dots, n_r) , we have the estimate

$$\begin{aligned} \int_{[-1, 1]^F} U_{n_1, n_2, \dots, n_r} d\nu(k, \psi, \chi's) &= |(1/q) \sum_{t \in k} U_{n_1, n_2, \dots, n_r}(F(\psi, \chi's)(t)/2)| \\ &\leq (\prod_i (n_i + 1)) / \text{Sqrt}(q). \end{aligned}$$

Here is a strengthening of Theorem 3, where we vary not just χ but the pair (ψ, χ) . Given ψ and χ , we denote by $\bar{\psi}$ and $\bar{\chi}$ the complex conjugate characters

$$\begin{aligned} \bar{\psi}(x) &:= \psi(-x) = 1/\psi(x), \\ \bar{\chi}(x) &:= \chi(x^{-1}) = 1/\chi(x). \end{aligned}$$

Fix an integer $r \geq 1$. Given a finite field k of odd characteristic, suppose we are given r pairs

$$\{(\psi_i, \chi_i)\}_{i=1 \text{ to } r}$$

each consisting of a non-trivial additive character ψ_i and a nontrivial multiplicative character χ_i .

Suppose that for all $i \neq j$, we have

$$(\psi_i, \chi_i) \neq (\psi_j, \chi_j), \text{ and } (\psi_i, \chi_i) \neq (\bar{\psi}_j, \bar{\chi}_j).$$

[Equivalently, the (ψ_i, χ_i) and their complex conjugates form $2r$ distinct pairs.] We define a map

from k to $[0, \pi]^F$ by

$$t \mapsto \theta(\psi's, \chi's)(t) := (\theta(\psi_1, \chi_1)(t), \theta(\psi_2, \chi_2)(t), \dots, \theta(\psi_r, \chi_r)(t)).$$

We form the corresponding probability measure $\mu(k, \psi's, \chi's)$ on $[0, \pi]^r$, defined by

$$\mu(k, \psi, \chi's) := (1/q) \sum_{t \in k} \delta_{\theta(\psi's, \chi's)(t)}$$

i.e. for any \mathbb{C} -valued continuous function f on $[0, \pi]$, we have

$$\int_{[0, \pi]^r} f d\mu(k, \psi, \chi's) := (1/q) \sum_{t \in k} f(\theta(\psi's, \chi's)(t)).$$

Theorem 4 Fix $r \geq 1$. Take any sequence of data $(k_i, \psi_i's, \chi_i's)$ as above (i.e. we are given r distinct pairs $(\psi_{i_j}, \chi_{i_j})_{j=1 \text{ to } r}$ which together with their complex conjugates form $2r$ distinct pairs) in which each k_i has characteristic at least 7, and in which $q_i := \text{Card}(k_i)$ is strictly increasing. Then the r -tuples of angles

$$\{\theta(\psi_i's, \chi_i's)(t)\}_{t \in k_i}$$

are approximately equidistributed in $[0, \pi]^r$ with respect to $(\mu_{\text{ST}})^r$, in the sense that as $i \rightarrow \infty$, the measures $\mu(k_i, \psi_i, \chi_i's)$ tend weak * to $(\mu_{\text{ST}})^r$. More precisely, for any r tuple of strictly positive integers (n_1, n_2, \dots, n_r) with $\sum_j n_j \geq r+1$, and any datum $(k, \psi's, \chi's)$ with k of characteristic at least 7, we have the estimate

$$\begin{aligned} & \left| \int_{[0, \pi]^r} S_{n_1, n_2, \dots, n_r} d\mu(k, \psi's, \chi's) \right. \\ & \left. - (1/q) \sum_{t \in k} S_{n_1, n_2, \dots, n_r}(\theta(\psi's, \chi's)(t)) \right| \leq (\prod_i n_i) / \text{Sqrt}(q). \end{aligned}$$

Remark Theorem 3 is the special case of Theorem 4 in which all the ψ_i are equal to a single ψ [The point is that $\psi \neq \bar{\psi}$, because the characteristic p is odd.]

In terms of semicircle measure, the measures

$$\mu(k, \psi's, \chi's) := (1/q) \sum_{t \in k} \delta_{\theta(\psi, \chi's)(t)}$$

on $[0, \pi]^r$ become the measures

$$\nu(k, \psi's, \chi's) := (1/q) \sum_{t \in k} \delta_{F(\psi's, \chi's)(t)/2}$$

on $[-1, 1]^r$.

The statement of Theorem 4 becomes

Theorem 4 bis Fix $r \geq 1$. Take any sequence of data $(k_i, \psi_i's, \chi_i's)$ as above (i.e. we are given r distinct pairs $(\psi_{i_j}, \chi_{i_j})_{j=1 \text{ to } r}$ which together with their complex conjugates form $2r$ distinct pairs) in which each k_i has characteristic at least 7, and in which $q_i := \text{Card}(k_i)$ is strictly increasing. Then the r -tuples in $[-1, 1]^r$,

$$\{F(\psi's, \chi's)(t)/2\}_{t \in k_i}$$

are approximately equidistributed in the r -fold product $[-1, 1]^r$ with respect to the r -fold product

measure $(\mu_{\text{Scir}})^r$ in the sense that as $i \rightarrow \infty$, the measures $\mu(k_i, \psi_i, \chi_i$'s) tend weak * to $(\mu_{\text{Scir}})^r$. More precisely, for any nonzero r -tuple of nonnegative integers (n_1, n_2, \dots, n_r) , we have the estimate

$$\begin{aligned} & \int_{|t| \leq 1} |U_{n_1, n_2, \dots, n_r}(k, \psi$$
's, χ 's)| \\ &= (1/q) \sum_{t \in k} U_{n_1, n_2, \dots, n_r}(F(\psi's, χ 's)(t)/2) \\ &\leq (\prod_i (n_i + 1))/\text{Sqrt}(q) \end{aligned}

Proofs of the theorems

Let us fix the finite field $k = \mathbb{F}_q$. For any pair (ψ, χ) consisting of a nontrivial additive character ψ and a nontrivial multiplicative character χ , both ψ and χ take values in the field $\mathbb{Q}(\xi_p, \xi_{q-1})$, viewed as a subfield of \mathbb{C} . The quantity $A(\psi, \chi)$ is an algebraic integer in $\mathbb{Q}(\xi_p, \xi_{q-1})$, which is a unit outside of p . If we adjoin to $\mathbb{Q}(\xi_p, \xi_{q-1})$ the square roots $B(\psi, \chi)$ of the $1/A(\psi, \chi)$ for all the finitely many such pairs (ψ, χ) , we get a finite extension F/\mathbb{Q} inside \mathbb{C} , in which the $B(\psi_i, \chi_i)$ are algebraic numbers, and units outside of p . The functions $H(\psi, \chi)$ and $F(\psi, \chi)$ take values in the number field K .

Now pick a prime number $\ell \neq p$, an algebraic closure $\bar{\mathbb{Q}}_\ell$ of the field \mathbb{Q}_ℓ of ℓ -adic numbers, and an embedding of the number field F into $\bar{\mathbb{Q}}_\ell$. Extend this embedding to a field isomorphism $\mathbb{C} \cong \bar{\mathbb{Q}}_\ell$. By means of this isomorphism, we may and will view the characters ψ and χ , and the functions $H(\psi, \chi)$ and $F(\psi, \chi)$, as taking values in $\bar{\mathbb{Q}}_\ell$. The quantity $B(\psi, \chi)$ is an ℓ -adic unit in $\bar{\mathbb{Q}}_\ell$.

On the affine line $\mathbb{A}^1 \otimes k$, we have the Artin–Schreier sheaf \mathcal{L}_ψ and the (extension by zero across 0 of) the Kummer sheaf \mathcal{L}_χ . The $\bar{\mathbb{Q}}_\ell$ -sheaf $\mathcal{L}_{\psi(x^2)} \otimes \mathcal{L}_{\chi(x)}$ on $\mathbb{A}^1 \otimes k$ is lisse on $\mathbb{G}_m \otimes k$ of rank one, and it vanishes at $x=0$. Its naive Fourier Transform $\text{NFT}_\psi(\mathcal{L}_{\psi(x^2)} \otimes \mathcal{L}_{\chi(x)})$, cf. [Ka–GKM, 8.2], will be denoted $\mathcal{H}(\psi, \chi)$:

$$\mathcal{H}(\psi, \chi) := \text{NFT}_\psi(\mathcal{L}_{\psi(x^2)} \otimes \mathcal{L}_{\chi(x)}).$$

Because $\mathcal{L}_{\psi(x^2)} \otimes \mathcal{L}_{\chi(x)}$ is a geometrically irreducible middle extension on \mathbb{A}^1 which is pure of weight zero, lisse of rank one on \mathbb{G}_m , ramified but tame at 0 and with Swan conductor 2 at ∞ , its naive Fourier Transform $\mathcal{H}(\psi, \chi)$ is a lisse $\bar{\mathbb{Q}}_\ell$ -sheaf of rank 2 on \mathbb{A}^1 , which is geometrically irreducible and pure of weight one. Its trace function is given as follows. For a finite extension E/k , denote by ψ_E (resp. χ_E) the nontrivial character of E obtained by composing ψ (resp. χ) with the relative trace $\text{Trace}_{E/k}$ (resp. the relative norm $\text{Norm}_{E/k}$). For any point t in $E = \mathbb{A}^1(E)$, we have

$$\text{Trace}(\text{Frob}_{t,E} | \mathcal{H}(\psi, \chi)) = -\sum_{x \in E} \psi_E(x^2 + tx)\chi_E(x).$$

In particular, for t in k , we have

$$\text{Trace}(\text{Frob}_{t,k} | \mathcal{H}(\psi, \chi)) = -H(\psi, \chi)(t).$$

Now define a second geometrically irreducible lisse $\bar{\mathbb{Q}}_\ell$ -sheaf of rank 2 on $\mathbb{A}^1 \otimes k$, $\mathcal{F}(\psi, \chi)$, now pure of weight zero, to be the following twist of $\mathcal{H}(\psi, \chi)$:

$$\mathcal{F}(\psi, \chi) := \mathcal{H}(\psi, \chi) \otimes \mathcal{L}_{\psi(t^2/8)} \otimes \mathcal{B}(\psi, \chi)^{\deg}.$$

For any finite extension E/k , and any point t in E , we have

$$\begin{aligned} & \text{Trace}(\text{Frob}_{t,E} \mid \mathcal{F}(\psi, \chi)) \\ &= (\text{Trace}(\text{Frob}_{t,k} \mid \mathcal{H}(\psi, \chi)) \psi_E(t^2/8) \mathcal{B}(\psi, \chi)^{\deg(E/k)}). \end{aligned}$$

In particular, for t in k , we have

$$\text{Trace}(\text{Frob}_{t,k} \mid \mathcal{F}(\psi, \chi)) = F(\psi, \chi)(t).$$

Lemma 1 The lisse rank two sheaf $\mathcal{F}(\psi, \chi)$ on $\mathbb{A}^1 \otimes k$ has trivial determinant. Equivalently, the determinant of the lisse rank two sheaf $\mathcal{H}(\psi, \chi)$ on $\mathbb{A}^1 \otimes k$ is given by

$$\det(\mathcal{H}(\psi, \chi)) \cong \mathcal{L}_{\psi(-t^2/4)} \otimes \mathcal{A}(\psi, \chi)^{\deg}.$$

proof By Chebotarov, it suffices to prove that for any finite extension E/k , and for any t in E , we have

$$\det(\text{Frob}_{t,E} \mid \mathcal{H}(\psi, \chi)) = \mathcal{L}_{\psi_E(-t^2/4)} \otimes \mathcal{A}(\psi, \chi)^{\deg(E/k)}.$$

By the Hasse–Davenport theorem, the Gauss sum $G(\psi_E, \chi_E)$ over E is related to the Gauss sum $G(\psi, \chi)$ over k by

$$(-G(\psi_E, \chi_E)) = (-G(\psi, \chi))^{\deg(E/k)}.$$

In view of the definition of $\mathcal{A}(\psi, \chi)$, we have

$$\mathcal{A}(\psi_E, \chi_E) = \mathcal{A}(\psi, \chi)^{\deg(E/k)}.$$

So it is the same to prove

$$\det(\text{Frob}_{t,E} \mid \mathcal{H}(\psi_E, \chi_E)) = \mathcal{L}_{\psi_E(-t^2/4)} \otimes \mathcal{A}(\psi_E, \chi_E).$$

So we are reduced to proving universally that for any t in k , we have

$$\det(\text{Frob}_{t,k} \mid \mathcal{H}(\psi, \chi)) = \mathcal{L}_{\psi(-t^2/4)} \otimes \mathcal{A}(\psi, \chi).$$

For this we use the classical Hasse–Davenport argument, cf. [Ka–MG, p. 53]. From the definition of $\mathcal{H}(\psi, \chi)$ as a naive Fourier Transform, we have

$$\begin{aligned} & \det(1 - \text{TFrob}_{t,k} \mid \mathcal{H}(\psi, \chi)) \\ &= \det(1 - \text{TFrob}_k \mid H^1_c(\mathbb{G}_m \otimes \bar{k}, \mathcal{L}_{\psi(x^2 + tx)} \otimes \mathcal{L}_{\chi(x)})) \end{aligned}$$

As this H^1_c is the only nonvanishing cohomology group, the Lefschetz Trace formula expresses the L–function on $\mathbb{G}_m \otimes k$ with coefficients in $\mathcal{L}_{\psi(x^2 + tx)} \otimes \mathcal{L}_{\chi(x)}$ as

$$\begin{aligned} & L(\mathbb{G}_m \otimes k, \mathcal{L}_{\psi(x^2 + tx)} \otimes \mathcal{L}_{\chi(x)})(T) \\ &= \det(1 - \text{TFrob}_k \mid H^1_c(\mathbb{G}_m \otimes \bar{k}, \mathcal{L}_{\psi(x^2 + tx)} \otimes \mathcal{L}_{\chi(x)})). \end{aligned}$$

Because this H^1_c has dimension 2, we obtain the determinant in question as the coefficient of T^2 in the power series expansion of the L–function:

$$\begin{aligned} & \det(\text{Frob}_{t,k} | \mathcal{H}(\psi, \chi)) \\ &= \text{coef. of } T^2 \text{ in } L(\mathbb{G}_m^{\otimes k}, \mathcal{L}_{\psi(x^2 + tx)} \otimes \mathcal{L}_{\chi(x)})(T). \end{aligned}$$

From the additive expression of this abelian L–function as a sum over all effective divisors on $\mathbb{G}_m^{\otimes k}$, i.e. over all monic polynomials in $k[X]$ with nonzero constant term, we see that for any integer $d \geq 1$, the coefficient of T^d is

$$\sum_{\text{monic } f \text{ of deg. } d, f(0) \neq 0} \psi(\sum_{\text{roots } \alpha \text{ of } f} (\alpha^2 + t\alpha)) \chi(\prod_{\text{roots } \alpha \text{ of } f} (\alpha))$$

Denote by $S_1(f)$ and by $N_1(f)$ the elementary and the Newton symmetric functions of the roots of f . Then the coefficient of T^d is

$$\sum_{\text{monic } f \text{ of deg. } d, f(0) \neq 0} \psi(N_2(f) + tS_1(f)) \chi(S_d(f)).$$

The expression of N_2 in terms of S_1 and S_2 is

$$N_2 = (S_1)^2 - 2S_2.$$

So all in all we find that the coefficient of T^d is

$$\sum_{\text{monic } f \text{ of deg. } d, f(0) \neq 0} \psi((S_1(f))^2 + tS_1(f) - 2S_2(f)) \chi(S_d(f)).$$

Now a monic f of degree d with $f(0) \neq 0$ is precisely given by its coefficients, which are the elementary symmetric functions of its roots:

$$f(X) = X^d - S_1(f)X^{d-1} + S_2(f)X^{d-2} + \dots + (-1)^d S_d(f).$$

So we may write the coefficient of T^d as

$$\sum_{s_1, s_2, \dots, s_d \text{ in } k, s_d \neq 0} \psi(s_1^2 + ts_1 - 2s_2) \chi(s_d).$$

This expression shows that for $d > 2$ the coefficient of T^d vanishes (because the sum of $\chi(s_d)$ over nonzero s_d vanishes), as it must. The coefficient of T^2 is

$$\begin{aligned} & \sum_{s_1, s_2 \text{ in } k, s_2 \neq 0} \psi((s_1^2 + ts_1 - 2s_2) \chi(s_2)) \\ &= (\sum_{s_1 \text{ in } k} \psi(s_1^2 + ts_1)) (\sum_{s_2 \text{ in } k^\times} \psi(-2s_2) \chi(s_2)). \end{aligned}$$

The second factor is $\chi(-1/2)G(\psi, \chi)$, and the first factor is

$$\begin{aligned} \sum_{s_1 \text{ in } k} \psi(s_1^2 + ts_1) &= \sum_{s_1 \text{ in } k} \psi((s_1 + t/2)^2 - t^2/4) \\ &= \psi(-t^2/4) \sum_{s \text{ in } k} \psi(s^2) \\ &= \psi(-t^2/4) G(\psi, \chi_{\text{quad}}). \end{aligned}$$

Putting this all together, we find that $\det(\text{Frob}_{t,k} | \mathcal{H}(\psi, \chi))$, the coefficient of T^2 in the L function, is indeed equal to

$$\chi(-1/2)G(\psi, \chi) \psi(-t^2/4)G(\psi, \chi_{\text{quad}}) = \psi(-t^2/4)A(\psi, \chi),$$

as asserted. QED

Lemma 2 For $p \geq 7$, the lisse rank two sheaf $\mathcal{F}(\psi, \chi)$ on $\mathbb{A}^1 \otimes \mathbb{k}$ has geometric monodromy group G_{geom} equal to $\text{SL}(2)$, and under the ℓ -adic representation ρ of $\pi_1 := \pi_1(\mathbb{A}^1 \otimes \mathbb{k})$ corresponding to $\mathcal{F}(\psi, \chi)$, we have $\rho(\pi_1) \subset G_{\text{geom}}(\overline{\mathbb{Q}}_\ell)$.

proof We have already proven that $\mathcal{F}(\psi, \chi)$ has trivial determinant, so we trivially have the inclusions

$$\rho(\pi_1) \subset \text{SL}(2)(\overline{\mathbb{Q}}_\ell)$$

and

$$G_{\text{geom}} \subset \text{SL}(2).$$

So it remains only to prove that G_{geom} contains $\text{SL}(2)$. As the sheaf $\mathcal{F}(\psi, \chi)$ is geometrically irreducible and starts life on $\mathbb{A}^1 \otimes \mathbb{k}$, its G_{geom} is a semisimple subgroup of $\text{GL}(2)$. So its identity component $(G_{\text{geom}})^0$, being a connected semisimple subgroup of $\text{GL}(2)$, is either the group $\text{SL}(2)$, or it is the trivial group. So either G_{geom} contains $\text{SL}(2)$, or G_{geom} is a finite irreducible subgroup Γ of $\text{GL}(2, \overline{\mathbb{Q}}_\ell)$. For $p \geq 7$, the second case cannot occur, thanks to the $n = 2$ case of the Feit–Thompson theorem [F–T]: for any $n \geq 2$, any finite subgroup Γ of $\text{GL}(n, \overline{\mathbb{Q}}_\ell)$ and any prime $p > 2n+1$, any p -Sylow subgroup Γ_1 of Γ is both normal and abelian. Our Γ is a finite quotient of $\pi_1(\mathbb{A}^1 \otimes \overline{\mathbb{k}})$, so it has no nontrivial quotients of order prime to p . The quotient Γ/Γ_1 is prime to p , hence trivial, and hence $\Gamma = \Gamma_1$. Then Γ is abelian, which is impossible since it is an irreducible subgroup of $\text{GL}(2, \overline{\mathbb{Q}}_\ell)$. QED

Lemma 3 Let (ψ_i, χ_i) for $i=1,2$ be two pairs, each consisting of a nontrivial additive character ψ_i and a nontrivial multiplicative character χ_i . Put $\mathcal{F}_i := \mathcal{F}(\psi_i, \chi_i)$. Suppose that $(\psi_1, \chi_1) \neq (\psi_2, \chi_2)$ and that $(\psi_1, \chi_1) \neq (\overline{\psi_2}, \overline{\chi_2})$. Then for any lisse rank one $\overline{\mathbb{Q}}_\ell$ -sheaf L on $\mathbb{A}^1 \otimes \overline{\mathbb{k}}$, the sheaves $L \otimes \mathcal{F}_1$ and \mathcal{F}_2 are not geometrically isomorphic (i.e., isomorphic as lisse $\overline{\mathbb{Q}}_\ell$ -sheaves on $\mathbb{A}^1 \otimes \overline{\mathbb{k}}$) and the sheaves $L \otimes \mathcal{F}_1$ and $(\mathcal{F}_2)^\vee$ are not geometrically isomorphic.

proof Since \mathcal{F}_2 has $G_{\text{geom}} = \text{SL}(2)$, \mathcal{F}_2 is geometrically self-dual, so it suffices to show that $L \otimes \mathcal{F}_1$ and \mathcal{F}_2 are not geometrically isomorphic. Since \mathcal{F}_1 is a twist of $\mathcal{H}_1 := \mathcal{H}(\psi_1, \chi_1)$ by a lisse rank one sheaf, it suffices to show that for any lisse rank one $\overline{\mathbb{Q}}_\ell$ -sheaf L on $\mathbb{A}^1 \otimes \overline{\mathbb{k}}$, the sheaves $L \otimes \mathcal{H}_1$ and \mathcal{H}_2 are not geometrically isomorphic.

If L is tame at ∞ , then L , being lisse on $\mathbb{A}^1 \otimes \overline{\mathbb{k}}$, is trivial. So in this case we must show that \mathcal{H}_1 is not geometrically isomorphic to \mathcal{H}_2 . We know that $\det(\mathcal{H}_1) = \mathcal{L}_{\psi_1(-2/4)}$. So if $\psi_1 \neq \psi_2$, then \mathcal{H}_1 and \mathcal{H}_2 have non-isomorphic determinants. Indeed, if $\psi_1 \neq \psi_2$, then there exists an

$\alpha \neq 1$ in k^\times for which $\psi_1(x) = \psi_2(\alpha x)$, and so

$$\det(\mathcal{H}_1) \otimes (\det(\mathcal{H}_2))^\vee \cong \mathcal{L}_{\psi_1}((\alpha-1)t^2/4)$$

is geometrically nontrivial, because it has Swan conductor two at ∞ .

We next recover χ_i from \mathcal{H}_i . For this, we recall that

$$\mathcal{H}_i := \text{NFT}(\mathcal{L}_{\psi_i}(x^2) \otimes \mathcal{L}_{\chi_i}(x)).$$

Laumon's stationary phase decomposition [Lau–TF] of $\mathcal{H}_i(\infty)$ ($:= \mathcal{H}_i$ as a representation of the inertia group $I(\infty)$) has the form

$$\mathcal{H}_i(\infty) = \mathcal{L}_{\chi_i}^- \oplus \mathcal{M}_i$$

with \mathcal{M}_i a one–dimensional representation of $I(\infty)$ of Swan conductor two. [In the notation of [Ka–ESDE, 7.4.1],

$$\mathcal{L}_{\chi_i}^- = \text{FTloc}(0, \infty)(\mathcal{L}_{\psi_i}(x^2) \otimes \mathcal{L}_{\chi_i}(x)),$$

$$\mathcal{M}_i = \text{FTloc}(\infty, \infty)(\mathcal{L}_{\psi_i}(x^2) \otimes \mathcal{L}_{\chi_i}(x)).]$$

Looking at the determinant of $\mathcal{H}_i(\infty)$, we see that the above decomposition of $\mathcal{H}_i(\infty)$ is

$$\begin{aligned} \mathcal{H}_i(\infty) &\cong \mathcal{L}_{\chi_i}^- \oplus \mathcal{L}_{\chi_i} \otimes \det(\mathcal{H}_i) \\ &\cong \mathcal{L}_{\chi_i}^- \oplus \mathcal{L}_{\chi_i} \otimes \mathcal{L}_{\psi_i}(-t^2/4). \end{aligned}$$

Thus we recover χ_i from \mathcal{H}_i from looking at the tame part of $\mathcal{H}_i(\infty)$.

So $\chi_1 \neq \chi_2$, then \mathcal{H}_1 cannot be geometrically isomorphic to \mathcal{H}_2 .

Thus, if either $\psi_1 \neq \psi_2$, or if $\chi_1 \neq \chi_2$, then \mathcal{H}_1 is not geometrically isomorphic to \mathcal{H}_2 .

Suppose now that L is not tame at ∞ , but that $L \otimes \mathcal{H}_1 \cong \mathcal{H}_2$ geometrically. Looking at $I(\infty)$ representations, we have

$$L \otimes \mathcal{H}_1(\infty) \cong L \otimes \mathcal{L}_{\chi_1}^- \oplus L \otimes \mathcal{L}_{\chi_1} \otimes \mathcal{L}_{\psi_1}(-t^2/4)$$

while

$$\mathcal{H}_2(\infty) \cong \mathcal{L}_{\chi_2}^- \oplus \mathcal{L}_{\chi_2} \otimes \mathcal{L}_{\psi_2}(-t^2/4).$$

There is at most one decomposition of a two–dimensional $I(\infty)$ representation as the sum of a tame character and of a nontame character. Since L is not tame at ∞ , $L \otimes \mathcal{L}_{\chi_1}^-$ is not tame at ∞ . So in

matching the terms, we must have

$$L \otimes \mathcal{L}_{\chi_1}^- \cong \mathcal{L}_{\chi_2} \otimes \mathcal{L}_{\psi_2}(-t^2/4),$$

i.e.,

$$L \otimes \mathcal{L}_{\psi_2}(t^2/4) \cong \mathcal{L}_{\chi_2} \otimes \mathcal{L}_{\chi_1}$$

as $I(\infty)$ –representation. Thus $L \otimes \mathcal{L}_{\psi_2}(t^2/4)$ is tame at ∞ . As $L \otimes \mathcal{L}_{\psi_2}(t^2/4)$ is lisse on $\mathbb{A}^1_{\bar{k}}$, it is trivial. Thus we get

$$L \cong \mathcal{L}_{\psi_2(-t^2/4)}, \text{ and } \chi_1 = \bar{\chi}_2.$$

Interchanging the indices and repeating the argument, we get

$$L^\vee \cong \mathcal{L}_{\psi_1(-t^2/4)}.$$

Thus we have $\mathcal{L}_{\psi_2(-t^2/4)} \cong \mathcal{L}_{\psi_1(t^2/4)}$. From this we conclude that $\psi_1 = \bar{\psi}_2$. So if L is not tame, the existence of a geometric isomorphism $L \otimes \mathcal{H}_1 \cong \mathcal{H}_2$ implies that $(\psi_1, \chi_1) = (\bar{\psi}_2, \bar{\chi}_2)$. QED

Lemma 4 For any pair (ψ, χ) consisting of a nontrivial additive character ψ and a nontrivial multiplicative character χ , the lisse sheaf $\mathcal{F} := \mathcal{F}(\psi, \chi)$ as $I(\infty)$ –representation is the direct sum of two inverse characters, each of Swan conductor two:

$$\mathcal{F}(\infty) \cong \mathcal{L}_{\bar{\chi}} \otimes \mathcal{L}_{\psi(t^2/8)} \oplus \mathcal{L}_{\chi} \otimes \mathcal{L}_{\psi(-t^2/8)}.$$

proof Indeed, we have seen that $\mathcal{H} := \mathcal{H}(\psi, \chi)$ as $I(\infty)$ –representation is given by

$$\begin{aligned} \mathcal{H}(\infty) &\cong \mathcal{L}_{\bar{\chi}} \oplus \mathcal{L}_{\chi} \otimes \det(\mathcal{H}) \\ &\cong \mathcal{L}_{\bar{\chi}} \oplus \mathcal{L}_{\chi} \otimes \mathcal{L}_{\psi(-t^2/4)}. \end{aligned}$$

Therefore \mathcal{F} , being an α^{deg} twist of $\mathcal{F} \otimes \mathcal{L}_{\psi(t^2/8)}$, has $I(\infty)$ –representation given by

$$\mathcal{F}(\infty) \cong \mathcal{L}_{\bar{\chi}} \otimes \mathcal{L}_{\psi(t^2/8)} \oplus \mathcal{L}_{\chi} \otimes \mathcal{L}_{\psi(-t^2/8)}. \text{ QED}$$

Lemma 5 Fix an integer $r \geq 1$. Suppose that the characteristic p of k is at least 7. Suppose we are given r pairs $\{(\psi_i, \chi_i)\}_{i=1}^r$, each consisting of a non–trivial additive character ψ_i and a nontrivial multiplicative character χ_i . Suppose that for all $i \neq j$, we have

$$(\psi_i, \chi_i) \neq (\psi_j, \chi_j), \text{ and } (\psi_i, \chi_i) \neq (\bar{\psi}_j, \bar{\chi}_j).$$

For each $i = 1$ to r , put

$$\mathcal{F}_i := \mathcal{F}(\psi_i, \chi_i),$$

and denote by

$$\rho_i : \pi_1(\mathbb{A}^{1 \otimes k}) \rightarrow \text{SL}(2, \bar{\mathbb{Q}}_\ell)$$

the ℓ –adic representation which \mathcal{F}_i "is". Consider the lisse $\bar{\mathbb{Q}}_\ell$ –sheaf \mathcal{G} on $\mathbb{A}^{1 \otimes k}$, defined as the direct sum

$$\mathcal{G} := \bigoplus_{i=1}^r \mathcal{F}_i.$$

Denote by

$$\rho := \bigoplus_{i=1}^r \rho_i : \pi_1(\mathbb{A}^{1 \otimes k}) \rightarrow \prod_{i=1}^r \text{SL}(2, \bar{\mathbb{Q}}_\ell)$$

the ℓ –adic representation which \mathcal{G} "is". Then the group G_{geom} for \mathcal{G} is the largest possible, namely $\prod_{i=1}^r \text{SL}(2)$.

proof By Lemma 2, the geometric monodromy group G_i of each \mathcal{F}_i is $\text{SL}(2)$. So the geometric monodromy group G for \mathcal{G} is a closed subgroup of $\prod_{i=1}^r G_i$ which maps onto each factor. By the Goursat–Kolchin–Ribet theorem [Ka–ESDE, 1.8.2], it results from Lemma 3 that $G^{0, \text{der}}$ is the

full product $\prod_{i=1}^r G_i^{0,\text{der}}$. Since each G_i is $SL(2)$, $G^{0,\text{der}}$ is the full product $\prod_{i=1}^r SL(2)$. Since G is in any case a subgroup of this product, we have $G = \prod_{i=1}^r SL(2)$. QED

Theorem 4 now result immediately from Deligne's Equidistribution Theorem [De–Weil II, 3.5], cf. [Ka–GKM, 3.6, 3.6.3], [Ka–Sar, 9.2.5, 9.2.6], applied to the sheaf \mathcal{G} of Lemma 5. A maximal compact subgroup K of $\prod_{i=1}^r SL(2, \mathbb{C})$ is the product group $\prod_{i=1}^r SU(2)$. Its space of conjugacy classes is the product space $[0, \pi]^r$, with measure the r –fold self–product of the Sato–Tate measure μ_{ST} . Its irreducible representations are precisely the tensor products of irreducible representations of the factors. For the i 'th factor $SU(2)$, denote by $\text{std}(i)$ its standard two–dimensional representation. There is one irreducible representation of the i 'th factor of each dimension $n \geq 1$, given by $\text{Symm}^{n-1}(\text{std}(i))$. Its character is the function $S_n(\theta)$. So the **nontrivial** irreducible representations of the product group

$$\prod_{i=1}^r SU(2)$$

are the tensor products

$$\otimes_{i=1}^r \text{Symm}^{n_i-1}(\text{std}(i))$$

with all $n_i \geq 1$ and at least one $n_i > 1$. This representation has dimension $\prod_{i=1}^r n_i$. Its character is $\prod_{i=1}^r S_{n_i}(\theta_i)$.

The sheaf \mathcal{G} of Lemma 5 has all its ∞ –slopes equal to two. For each point t in k , the image $\rho(\text{Frob}_{t,k})^{\text{ss}}$ in $\prod_{i=1}^r SL(2, \bar{\mathbb{Q}}_\ell)$, when viewed in $\prod_{i=1}^r SL(2, \mathbb{C})$ via the chosen field isomorphism of $\bar{\mathbb{Q}}_\ell$ with \mathbb{C} , is conjugate in $\prod_{i=1}^r SL(2, \mathbb{C})$ to an element of $K = \prod_{i=1}^r SU(2)$, which is itself well–defined up to conjugacy in K . The resulting conjugacy class is none other than the r –tuple

$$(\theta(\psi_1, \chi_1)(t), \theta(\psi_2, \chi_2)(t), \dots, \theta(\psi_r, \chi_r)(t)).$$

So Theorem 4 is just Deligne's Equidistribution Theorem applied to \mathcal{G} . The "more precisely" estimate results from [Ka–GKM, 3.6.3] and the fact that \mathcal{G} is lisse on \mathbb{A}^1 and has highest ∞ –slope two.

In more concrete terms, each $F(\psi_i, \chi_i)(t)$ is the trace of of a conjugacy class in $SU(2)$, hence is real and lies in $[-2, 2]$. This gives Theorem 1. Theorem 2 is the special case $r=1$ of Theorem 4, and Theorem 3 is the special case "all ψ_i equal" of Theorem 4.

References

[De–Weil II] Deligne, P., La conjecture de Weil II, Pub. Math. I.H.E.S. 52 (1981), 313–428.

[F–T] Feit, W., and Thompson, J., On groups which have a faithful representation of degree less than $(p-1)/2$, Pacific Math. J. 4 (1961), 1257–1262.

[Ka–ESDE] Katz, N., *Exponential sums and differential equations*, Annals of Math. Study 124, Princeton Univ. Press, 1990.

[Ka–GKM] Katz, N., *Gauss sums, Kloosterman sums, and monodromy groups*, Annals of Math. Study 116, Princeton Univ. Press, 1988.

[Ka–MG] Katz, N., On the monodromy groups attached to certain families of exponential sums, Duke Math. J. 54 No. 1 (1987), 41–56.

[Ka–Sar] Katz, N., and Sarnak, P., *Random Matrices, Frobenius Eigenvalues, and Monodromy*, A.M.S. Colloquium Publications 45, 1999.

[Kol] Kolchin, E., Algebraic groups and algebraic independence, Amer. J. Math. 90 (1968), 1151–1164.

[Kur–Rud] Kurlberg, P., and Rudnick, Z., Value distribution for eigenfunctions of desymmetrized quantum maps, preprint, December, 2000.

[Lau–TF] Laumon, G., Transformation de Fourier, constantes d'équations fonctionnelles et conjecture de Weil, Pub. Math. I.H.E.S. 65 (1987), 131–210.

[Ri] Ribet, K., Galois action on division points of abelian varieties with real multiplication, Amer. J. Math. 98 (1976), 751–805.