

Matrix elements for the quantum cat map: fluctuations in short windows

This article has been downloaded from IOPscience. Please scroll down to see the full text article.

2007 Nonlinearity 20 2289

(<http://iopscience.iop.org/0951-7715/20/10/001>)

[The Table of Contents](#) and [more related content](#) is available

Download details:

IP Address: 132.66.41.185

The article was downloaded on 24/06/2008 at 14:11

Please note that [terms and conditions apply](#).

Matrix elements for the quantum cat map: fluctuations in short windows

Pär Kurlberg¹, Lior Rosenzweig² and Zeév Rudnick²

¹ Department of Mathematics, Royal Institute of Technology, SE-100 44 Stockholm, Sweden

² Raymond and Beverly Sackler School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel

E-mail: kurlberg@math.kth.se, rosenzwe@post.tau.ac.il and rudnick@post.tau.ac.il

Received 2 February 2007, in final form 27 July 2007

Published 22 August 2007

Online at stacks.iop.org/Non/20/2289

Recommended by S Nonnenmacher

Abstract

We study fluctuations of the matrix coefficients for the quantized cat map. We consider the sum of matrix coefficients corresponding to eigenstates whose eigenphases lie in a randomly chosen window, assuming that the length of the window shrinks with Planck's constant. We show that if the length of the window is smaller than the square root of Planck's constant, but larger than the separation between distinct eigenphases, then the variance of this sum is proportional to the length of the window, with a proportionality constant which coincides with the variance of the individual matrix elements corresponding to Hecke eigenfunctions.

Mathematics Subject Classification: 81Q50, 11L07, 11M36, 37D20, 37N20

1. Introduction

1.1. Background

Much effort has been expended in recent years to studying quantum wave functions of classically chaotic systems in the semiclassical limit. One well-known result is that the matrix elements of smooth observables concentrate around the classical average of the observable, at least in the mean square [4, 29, 33]; this is known as the 'quantum ergodicity theorem' and is valid in great generality. A harder problem, known as 'quantum unique ergodicity' (QUE), is the question whether *all* matrix elements converge to the classical average of the observable. This is expected to hold for any negatively curved surface [28], but unlike the case of quantum ergodicity, there are no general results available here. The only rigorous results available concern special arithmetic systems, namely cat maps and some special compact surfaces of

constant negative curvature, uniformized by unit groups of rational quaternion algebras. In these cases many quantum symmetries exist, and QUE is now known to hold for eigenfunctions of the desymmetrized system [17, 23]. The complexity of the problem increases as we increase the number of degrees of freedom and Kelmer [15] found systematic deviations from QUE for higher dimensional cat maps. Without incorporating the symmetries, QUE is violated for the two-dimensional cat map [9].

An important problem is to understand the rate of convergence to the classical average. It has been suggested by Feingold and Peres [10] that for generic systems with D degrees of freedom, the variance of the matrix elements about their mean decays with Planck's constant \hbar as \hbar^D , with a prefactor given in terms of the autocorrelation function of the classical observable. Several (non-rigorous) arguments were given for this by Eckhardt *et al* [8]. For an extensive numerical test of the Feingold–Peres conjecture, see Barnett [1]. Rigorous results towards this conjecture are only available for arithmetic systems—the modular domain [24, 32] and the cat map [20, 15]. In both cases arithmetic deviations from the conjecture are found.

Once one knows the variance, it is natural to believe that the *normalized* matrix elements fluctuate randomly about the mean. In this paper, we study the fluctuations of matrix elements of the quantized cat map, by studying the variance of *sums* of the matrix coefficients over randomly chosen energy windows. Our findings are that indeed there are considerable cancellations in these sums, consistent with a supposition that the signs of the normalized matrix elements behave randomly. We will describe the results in detail once we recall the model.

1.2. The quantum cat map

The quantized cat map is a model quantum system with chaotic classical analogue, first investigated by Hannay and Berry [12] and studied extensively since, see, e.g. [6, 9, 13, 17, 27]. While the classical system displays generic chaotic properties, the quantum system behaves non-generically in several aspects, such as the statistics of the eigenphases and the value distribution of the eigenfunctions [19].

We review some of the details of the system in a form suitable for our purposes, see, e.g. [6, 17, 27]. Let A be a linear hyperbolic toral automorphism, that is, $A \in SL_2(\mathbb{Z})$ is an integer unimodular matrix with distinct real eigenvalues. We assume $A \equiv I \pmod{2}$. Iterating the action of A on the torus $\mathbb{T} = \mathbb{R}^2/\mathbb{Z}^2$ gives a dynamical system, which is highly chaotic. The quantum mechanical system includes an integer $N \geq 1$, the inverse Planck constant (which we will take to be prime), an N -dimensional state space $\mathcal{H}_N \simeq L^2(\mathbb{Z}/N\mathbb{Z})$ and a unitary operator $U = U_N(A)$ on \mathcal{H}_N , which is the quantization A . Fix a smooth real-valued observable $f \in C^\infty(\mathbb{T})$, which we will assume to have zero mean: $\int_{\mathbb{T}} f(x) dx = 0$, and let $\text{Op}_N(f)$ be its quantization, which is a self-adjoint operator on \mathcal{H}_N . Let $\{\psi_j\}$ be an orthonormal basis of eigenstates for U with eigenvalues $\{e^{2\pi i\theta_j}\}$: $U\psi_j = e^{2\pi i\theta_j}\psi_j$ and $\langle \text{Op}_N(f)\psi_j, \psi_j \rangle$ the (diagonal) matrix elements.

Let $\text{ord}(A, N)$ be the least integer $r \geq 1$ for which $A^r \equiv I \pmod{N}$. When N is prime the distinct eigenphases θ_j are evenly spaced (with at most one exception) with spacing $1/\text{ord}(A, N)$, and in fact, the distinct eigenphases are all of the form $j/\text{ord}(A, N)$. The eigenspaces all have the same dimension (again with at most one exception) which is $(N \pm 1)/\text{ord}(A, N)$.

For fixed small $\epsilon > 0$, as $N \rightarrow \infty$ through a sequence of values such that $\text{ord}(A, N) > N^\epsilon$, QUE holds for this subsequence in the sense that *all* the matrix elements converge to the phase space average $\int_{\mathbb{T}} f(x) dx$ of the observable f [3, 18]. Note that this assumption on $\text{ord}(A, N)$ is valid for most values of N ; in fact $\text{ord}(A, N) > N^{1/2+o(1)}$ for almost all N , cf [18, lemma 15].

However, it should also be noted that ‘scars’ are found for values of N where $\text{ord}(A, N)$ is logarithmic in N , see [9].

To study the fluctuations of the matrix elements, we study the sums of diagonal matrix elements of $\text{Op}_N(f)$ over eigenphases lying in windows of length $1/L$ around θ , with θ chosen randomly. More generally we consider a window function, constructed by taking a fixed non-negative and even function $h \in L^2([-\frac{1}{2}, \frac{1}{2}])$ and setting $h_L(\theta) := \sum_{m \in \mathbb{Z}} h(L(\theta - m))$, which is periodic and localized in an interval of length $1/L$. We further normalize so that $\int_{-\infty}^{\infty} h(x)^2 dx = 1$, and hence $\int_0^1 h_L(\theta)^2 d\theta = 1/L$. Then set

$$P(\theta) := \sum_{j=1}^N h_L(\theta - \theta_j) \langle \text{Op}_N(f) \psi_j, \psi_j \rangle. \tag{1.1}$$

Note that $P(\theta)$ is independent of the choice of basis. If $f = g - g \circ A$ (where $g \circ A$ is defined by $(g \circ A)(x) = g(Ax)$) is a cocycle then, as follows from the ‘exact Egorov’s theorem’, all matrix elements $\langle \text{Op}_N(f) \psi_j, \psi_j \rangle = 0$ vanish and so $P(\theta) \equiv 0$ in this case.

The expected value of $P(\theta)$, when we pick θ randomly and uniformly in the unit interval, is

$$\int_0^1 P(\theta) d\theta = 0,$$

since we assume that $\int_{\mathbb{T}} f(x) dx = 0$. (Strictly speaking, for f smooth we only have $\int_0^1 P(\theta) d\theta = O_{f,R}(N^{-R})$ for all $R > 0$, see section 3.1 for more details.)

We will study the variance of $P(\theta)$. To describe it, we introduce the quadratic form associated with the matrix A by

$$Q(x) = \omega(x, xA),$$

where $\omega(x, y) = x_1 y_2 - x_2 y_1$ is the standard symplectic form. If the Fourier expansion³ of the observable is $f(x) = \sum_{k \in \mathbb{Z}^2} \hat{f}(k) e(kx)$, where in what follows we abbreviate $e(z) := e^{2\pi i z}$, set

$$C_{\text{arith}}(f) := \sum_{\substack{k, k' \in \mathbb{Z}^2 \\ Q(k) = Q(k')}} (-1)^{k_1 k_2 + k'_1 k'_2} \hat{f}(k) \overline{\hat{f}(k')}. \tag{1.2}$$

1.3. Results

We can now formulate our main result.

Theorem 1.1. *Fix $f \in C^\infty(\mathbb{T}^2)$ of zero mean. Consider any sequence of primes N for which $\text{ord}(A, N)/\sqrt{N} \rightarrow \infty$. Assume that $L < 2\text{ord}(A, N)$. Then as $N \rightarrow \infty$,*

$$\text{Var}(P) = \frac{1}{L} C_{\text{arith}}(f) + O\left(\frac{\sqrt{N}}{L^2}\right).$$

It is easy to check that $C_{\text{arith}}(f)$ vanishes if $f = g - g \circ A$ is a cocycle. In that case $P = 0$ so theorem 1.1 has no content. In the case $C_{\text{arith}}(f) \neq 0$, if we further assume $L/\sqrt{N} \rightarrow \infty$ we get the following corollary.

Corollary 1.2. *Under the assumptions of theorem 1.1, if $C_{\text{arith}}(f) \neq 0$, and $L/\sqrt{N} \rightarrow \infty$ then, as $N \rightarrow \infty$,*

$$\text{Var}(P) \sim \frac{C_{\text{arith}}(f)}{L}.$$

³ With $k = (k_1, k_2)$, $\hat{f}(k) := \int_0^1 \int_0^1 f(x_1, x_2) e^{-2\pi i(k_1 x_1 + k_2 x_2)} dx_1 dx_2$.

The prefactor $C_{\text{arith}}(f)$ coincides with the asymptotic variance of the normalized matrix elements of $\text{Op}_N(f)$ when computed in the Hecke basis [20]. To explain this, note that if $1/L$ is smaller than the minimal separation between distinct eigenphases, that is if $L > \text{ord}(A, N)$, then from definition (1.1) we get

$$\int_0^1 P(\theta)^2 d\theta = \frac{1}{L} \sum_{j=1}^{\text{ord}(A, N)} \left| \sum_{k: \theta_k = \frac{j}{\text{ord}(A, N)}} \langle \text{Op}_N(f) \psi_k, \psi_k \rangle \right|^2, \quad (1.3)$$

the inner sum being over an orthonormal basis of the eigenspace corresponding to a given eigenphase. In particular, once L exceeds $\text{ord}(A, N)$, the dependence of $P(\theta)$ on L is essentially trivial, and thus we may (and shall) restrict $L < 2\text{ord}(A, N)$. If in addition we have $\text{ord}(A, N) = N \pm 1$, then (almost) all the inner sums in (1.3) collapse to a single term, and thus we find that when $\text{ord}(A, N) = N \pm 1$ is maximal and $L > N + 1$, then

$$\int_0^1 P(\theta)^2 d\theta = \frac{1}{L} \sum_{j=1}^N |\langle \text{Op}_N(f) \psi_j, \psi_j \rangle|^2 + O\left(\frac{1}{NL}\right).$$

Thus we recover the variance of the individual matrix elements (a trick used by Berry [2]), which in turn was shown to be $C_{\text{arith}}(f)$ in [20].

For comparison of our results with those expected of *generic* quantum chaotic systems, consider the case where we take A to be a nonlinear perturbation of a cat map, the perturbation sufficiently small so that the map remains hyperbolic [25]. The resulting system is expected to have generic spectral statistics (depending on the symmetries of the map) [14, 25]. Arguing as in [5, 8] one then expects that the variance of $P(\theta)$ in this case is asymptotic to $(1/L)C_{\text{gen}}(f)$, where

$$C_{\text{gen}}(f) = \sum_{t=-\infty}^{\infty} \int_{\mathbb{T}} (f \circ A^t)(x) f(x) dx \quad (1.4)$$

is the classical autocorrelation function. To compare with the arithmetic variance $C_{\text{arith}}(f)$ in (1.2), note that when A is *linear*, we may write (1.4) in terms of the Fourier expansion of the observable f as

$$C_{\text{gen}}(f) = \sum_{\substack{k, k' \in \mathbb{Z}^2 \\ k' \sim k}} (-1)^{k_1 k_2 + k'_1 k'_2} \hat{f}(k) \overline{\hat{f}(k')},$$

where the sum $k' \sim k$ is over pairs of frequencies which lie in the same A -orbit: $k' = kA^t$ for some integer t . This condition implies the condition $Q(k') = Q(k)$ which enters in sum (1.2) for the arithmetic variance $C_{\text{arith}}(f)$ (and also implies that $(-1)^{k_1 k_2 + k'_1 k'_2} = 1$).

1.4. About the proof

As we explain in section 3, the variance of P can be written as

$$\text{Var}(P) = \frac{1}{L^2} \sum_{t \in \mathbb{Z} - \{0\}} \hat{h}\left(\frac{t}{L}\right)^2 |\text{tr}\{\text{Op}_N(f)U^{-t}\}|^2. \quad (1.5)$$

One approach to evaluating (1.5), used in [8], is to use a trace formula expressing $\text{tr}\{\text{Op}_N(f)U^t\}$ as a sum over periodic orbits of the map A with certain phases, where the number of summands grows exponentially in t . This gives $\text{Var}(P)$ as a sum over pairs of periodic orbits. The averaging over θ produces a sum over ‘diagonal’ pairs where the phases

cancel and the remaining pairs. The obvious diagonal pairs consist of equal orbits and give the generic answer $C_{\text{gen}}(f)$. To reproduce the correct answer $C_{\text{arith}}(f)$ in this case requires identifying another diagonal family and showing that the contribution of the remaining pairs is negligible. We have not been able to do that.

Instead, we use a different formula for $\text{trOp}_N(f)U^{-t}$, based on a formula for the quantum propagator $U_N(A)$ introduced by Kelmer [15] and an expansion in Fourier modes of f to rewrite (1.5) as a double sum over Fourier modes

$$\text{Var}(P) \sim \frac{1}{L^2} \sum_{k,k'} (-1)^{k_1 k_2 + k'_1 k'_2} \hat{f}(k) \overline{\hat{f}(k')} S(k, k'),$$

where $S(k, k')$ is a certain incomplete exponential sum, which is trivial for pairs of frequencies with $Q(k) = Q(k')$. These pairs of frequencies give the main term of $C_{\text{arith}}(f)/L$; this is our new diagonal approximation, ‘dual’ in a sense to the standard one using periodic orbits. To handle the off-diagonal terms, it suffices to give a non-trivial bound for the exponential sum $S(k, k')$ when $Q(k) \neq Q(k')$. Using a standard completion technique, we reduce it to giving a bound for a certain complete exponential sum. When N is a ‘split’ prime, that is, if A is diagonalizable modulo N , the required bound is a standard result of the Riemann hypothesis for function fields (proved by Weil). For the remaining ‘inert’ primes, the required bound was recently established by Gurevich and Hadani [11]. In the appendix, we will give a different proof that only requires Weil’s original methods [30].

2. Prerequisites on cat maps and their quantization

2.1. The quadratic form associated with A

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ be hyperbolic and assume that $A \equiv I \pmod{2}$. Then A preserves the standard symplectic form

$$\omega(x, y) := x_1 y_2 - x_2 y_1,$$

and thus A also preserves the quadratic form

$$Q(x) := \omega(x, xA) = bx_1^2 + (d - a)x_1 x_2 - cx_2^2, \tag{2.1}$$

which has discriminant $\text{disc}(Q) = (\text{tr } A)^2 - 4$ (which is even since $A \equiv I \pmod{2}$).

Lemma 2.1. *Let N be an odd prime, and let $A \in SL_2(\mathbb{Z})$ so that $(\text{tr } A)^2 - 4 \not\equiv 0 \pmod{N}$. Then the space of binary quadratic forms preserved by A is one-dimensional.*

Proof. Passing if necessary to a quadratic extension \mathbb{F} of the base field $\mathbb{Z}/N\mathbb{Z}$ over which A is diagonalizable, as we may by our assumption on N , consider the action of A on 2×2 matrices over \mathbb{F} via $M \mapsto A^T M A$ (where A^T is the transpose of A). The decomposition of the space of matrices to a direct sum of the one-dimensional space of skew-symmetric and the three-dimensional space Sym^2 of symmetric matrices (identified with quadratic forms) is preserved by A .

Let λ^\pm be the eigenvalues of A . Since N is coprime to $\text{tr}(A)^2 - 4$, $A \not\equiv \pm I \pmod{N}$ and in particular $\lambda \neq \pm 1$. Let $v_\pm \neq 0$ be the corresponding eigenvectors: $v_\pm A = \lambda^\pm v_\pm$ (note that our vectors are row vectors). Then the matrices $v_\pm^T v_\pm$ are four eigenvectors for the action of A on 2×2 matrices, with eigenvalues $\lambda^2, 1, 1, \lambda^{-2}$. The skew symmetric matrices are fixed by A and hence the eigenvalues of A on Sym^2 are $\lambda^2, 1, \lambda^{-2}$. The 1-eigenspace corresponds to binary quadratic forms which are preserved by A . Since $\lambda \neq \pm 1$, we find that the 1-eigenspace is one dimensional, proving the claim. \square

Thus we find that if N is coprime to $\text{disc}(Q)$, then any binary quadratic form preserved by A is a multiple of Q modulo N .

2.2. Hecke operators

Let N be a prime not dividing $\text{disc}(Q) = (\text{tr } A)^2 - 4$. In [17] we described a commutative algebraic group $\mathcal{C}_A(N) \subset SL_2(\mathbb{Z}/N\mathbb{Z})$, containing A , which in the case at hand is the centralizer of A in $SL_2(\mathbb{Z}/N\mathbb{Z})$ and coincides with the special orthogonal group of the quadratic form Q given in (2.1) over the field $\mathbb{Z}/N\mathbb{Z}$. The group $\mathcal{C}_A(N)$ is isomorphic to either the multiplicative group of the field $(\mathbb{Z}/N\mathbb{Z})^*$ (the ‘split’ case) or the norm-one elements in a quadratic extension of $\mathbb{Z}/N\mathbb{Z}$ (the ‘inert’ case). Thus $\mathcal{C}_A(N)$ has order $N - 1$ or $N + 1$, respectively. Note that if $g \in \mathcal{C}_A(N)$ and $g \neq 1$, then the matrix $g - 1$ is invertible.

2.3. Some other invariant quadratic forms

As examples of quadratic forms over $\mathbb{Z}/N\mathbb{Z}$ preserved by A , consider for $g \in \mathcal{C}_A(N)$, $g \neq 1$,

$$q(x; g) := \omega(x(g - 1)^{-1}, x(g - 1)^{-1}g).$$

Note that $q(\bullet, g) = 0$ if $g = -I \pmod{N}$.

Lemma 2.2. *If $g \not\equiv \pm I \pmod{N}$ then $q(\bullet; g)$ is a non-zero multiple of Q .*

Proof. By lemma 2.1 it suffices to show that $q(\bullet; g)$ is preserved by A and is non-zero. It is preserved by A since A preserves ω and commutes with both g and $(g - I)^{-1}$. By lemma 2.1, $q(\bullet; g)$ is thus a multiple of the form Q . We claim that the multiple is non-zero mod N . To see this, it suffices to see that $q(\bullet; g)$ is not identically zero. If this were the case, then since ω is non-degenerate and $g - I$ invertible, we would have that yg is a scalar multiple of y for all vectors y , which necessarily forces g to be a scalar matrix. Since $\det g = 1$, we must therefore have $g = \pm I \pmod{N}$, contradicting our assumption. \square

2.4. Computing $Q(x)$ and $q(x; g)$

Choose a generator g_0 of the cyclic group $\mathcal{C}_A(N)$. Passing if necessary to a quadratic extension of $\mathbb{Z}/N\mathbb{Z}$, write $x = x_+ + x_-$, where x_{\pm} are eigenvectors of g_0 , hence of g and of A , with $x_{\pm}g = \lambda^{\pm 1}x_{\pm}$, $x_{\pm}A = \lambda_A^{\pm 1}x_{\pm}$ ($\lambda_A \neq \pm 1$ if N is coprime to $\text{disc}(Q) = (\text{tr } a)^2 - 4$). Then

$$\begin{aligned} Q(x) &= \omega(x, xA) = \omega(x_+ + x_-, \lambda_A x_+ + \lambda_A^{-1} x_-) \\ &= (\lambda_A - \lambda_A^{-1})\omega(x_-, x_+). \end{aligned}$$

Likewise,

$$\begin{aligned} q(x; g) &= \omega(x(g - I)^{-1}, x(g - I)^{-1}g) \\ &= \omega\left(\frac{1}{\lambda - 1}x_+ + \frac{1}{\lambda^{-1} - 1}x_-, \frac{\lambda}{\lambda - 1}x_+ + \frac{\lambda^{-1}}{\lambda^{-1} - 1}x_-\right) \\ &= \frac{\lambda - \lambda^{-1}}{(\lambda - 1)(\lambda^{-1} - 1)}\omega(x_-, x_+). \end{aligned}$$

In particular we find

$$q(x; g) = Q(x) \frac{\lambda - \lambda^{-1}}{\lambda_A - \lambda_A^{-1}} \frac{1}{(\lambda - 1)(\lambda^{-1} - 1)} = \frac{Q(x)}{\lambda_A - \lambda_A^{-1}} \frac{1 + \lambda}{1 - \lambda}. \quad (2.2)$$

2.5. Quantum mechanics on the torus

We recall the basic facts of quantum mechanics on the torus which we need in the paper, see [17, 27] for further details. Planck’s constant is restricted to be an inverse integer $1/N$, and the Hilbert space of states \mathcal{H}_N is N -dimensional, which is identified with $L^2(\mathbb{Z}/N\mathbb{Z})$ with the inner product given by

$$\langle \phi, \psi \rangle := \frac{1}{N} \sum_{Q \bmod N} \phi(Q) \overline{\psi(Q)}.$$

Classical observables, that is, real-valued functions $f \in C^\infty(\mathbb{T})$, give rise to quantum observables, that is, self-adjoint operators $\text{Op}_N(f)$ on \mathcal{H}_N . To define these, one starts with translation operators: for $n = (n_1, n_2) \in \mathbb{Z}^2$ let $T_N(n)$ be the unitary operator on \mathcal{H}_N whose action on a wave-function $\psi \in \mathcal{H}_N$ is

$$T_N(n)\psi(Q) = e^{\frac{i\pi n_1 n_2}{N}} e\left(\frac{n_2 Q}{N}\right) \psi(Q + n_1).$$

For any smooth function $f \in C^\infty(\mathbb{T})$, define $\text{Op}_N(f)$ by

$$\text{Op}_N(f) := \sum_{n \in \mathbb{Z}^2} \hat{f}(n) T_N(n),$$

where $\hat{f}(n)$ are the Fourier coefficients of f . The trace of $\text{Op}_N(f)$ is

$$\text{tr}\{\text{Op}_N(f)\} = N \int_{\mathbb{T}} f(x) dx + O_f(N^{-\infty}), \tag{2.3}$$

where the term $O_f(N^{-\infty})$ is one that is bounded by N^{-R} for any $R > 0$, the implied constant depending on f and R .

2.6. A formula for the quantum propagator

For any $B \in SL_2(\mathbb{Z})$, $B \equiv I \pmod{2}$, the quantum propagator $U_N(B)$ is a unitary map of \mathcal{H}_N satisfying Egorov’s formula

$$U_N(B)^* \text{Op}_N(f) U_N(B) = \text{Op}_N(f \circ B)$$

for all observables $f \in C^\infty(\mathbb{T})$. This property defines the propagator only up to a phase, which will be of no interest to us.

A useful formula for the propagator, known in the context of the Weil representation (cf [26]), and introduced for cat maps by Kelmer [15], is the following: for any $B \in SL_2(\mathbb{Z})$ and N odd, the quantum propagator $U_N(B)$ is given by

$$U_N(B) = \frac{1}{N|\ker_N(B - I)|^{1/2}} \sum_{n \in (\mathbb{Z}/N\mathbb{Z})^2} e\left(\frac{\omega(n, nB)}{2N}\right) T_N(n(I - B)),$$

where $\ker_N(B - I)$ denotes the kernel of the map $B - I$ on $\mathbb{Z}^2/N\mathbb{Z}^2$. We apply this when N is a prime not dividing⁴ $\text{disc}(Q)$, $B = A^t$ (where A^t is the t th power of A) so that $A^t \not\equiv I \pmod{N}$. Note that $|\ker_N(A^t - I)| = 1$ since in the group $\mathcal{C}_A(N)$, if $g \neq 1$, then the matrix $g - 1$ is invertible. Thus

$$U_N(A^t) = \frac{1}{N} \sum_{n \in (\mathbb{Z}/N\mathbb{Z})^2} e\left(\frac{\omega(n, nA^t)}{2N}\right) T_N(n(I - A^t)). \tag{2.4}$$

⁴ Since $A \equiv I \pmod{2}$, $\text{disc}(Q)$ is even and hence such N is odd.

Lemma 2.3. *Let $A \in SL_2(\mathbb{Z})$ be hyperbolic and assume that $A \equiv I \pmod{2}$. Then for any prime N not dividing $\text{disc}(Q)$ and integer t such that $A^t \not\equiv I \pmod{N}$, we have*

$$\text{tr}\{\text{Op}_N(f)U_N(A^t)\} = \sum_k (-1)^{k_1 k_2} \hat{f}(k) e\left(\frac{\bar{2}q(k; A^t)}{N}\right),$$

where $\bar{2}$ is the inverse of $2 \pmod{N}$.

Proof. It suffices to show that

$$\text{tr}\{T_N(k)U(A^t)\} = (-1)^{k_1 k_2} e\left(\frac{\bar{2}\omega(n, nA^t)}{N}\right), \tag{2.5}$$

where n is such that $k = n(A^t - I) \pmod{N}$. Using (2.4) we find

$$\text{tr}\{T_N(k)U_N(A^t)\} = \frac{1}{N} \sum_{n \in (\mathbb{Z}/N\mathbb{Z})^2} e\left(\frac{\omega(n, nA^t)}{2N}\right) \text{tr}\{T_N(k)T_N(n(I - A^t))\}.$$

As is easy to see from the definition (see lemma 4 and (2.6) in [17])

$$\text{tr}\{T_N(n)T_N(m)\} = \begin{cases} (-1)^{m_1 m_2 + n_1 n_2} N & \text{if } n \equiv -m \pmod{N}, \\ 0 & \text{otherwise.} \end{cases}$$

Thus $\text{tr}\{T_N(k)T_N(n(I - A^t))\} = (-1)^{k_1 k_2} N$ if $k = -n(I - A^t) \pmod{N}$ and 0 otherwise. Now if $A^t \not\equiv I \pmod{N}$, such n as above exists and is unique since $A^t - I$ is invertible. Therefore

$$\text{tr}\{T_N(k)U(A^t)\} = (-1)^{k_1 k_2} e\left(\frac{\omega(n, nA^t)}{2N}\right). \tag{2.6}$$

Now if b is an even integer and N is odd then $e(\frac{b}{2N}) = e(\frac{\bar{2}b}{N})$. Applying this to (2.6) with $b = \omega(n, nA^t)$ which is even since $A \equiv I \pmod{2}$, we end up with formula (2.5). \square

3. Proof of theorem 1.1

3.1. A formula for the variance

Fix a non-negative, even, test function h , supported in $[-\frac{1}{2}, \frac{1}{2}]$ and normalized so that $\int_{-\infty}^{\infty} h(x)^2 dx = 1$. Set

$$h_L(x) := \sum_{k \in \mathbb{Z}} h(L(x - k)),$$

which is then a periodic function, localized on the scale of $1/L$, and $\int_0^1 h_L(\theta)^2 d\theta = 1/L$. The Fourier expansion of h_L is (in the L^2 sense)

$$h_L(x) = \frac{1}{L} \sum_{t \in \mathbb{Z}} \hat{h}\left(\frac{t}{L}\right) e(tx),$$

where $\hat{h}(y) = \int_{-\infty}^{\infty} h(x)e(-xy) dx$.

Let N be a prime which does not divide $\text{disc}(Q) = (\text{tr } A)^2 - 4$. Let

$$P(\theta) := \sum_j h_L(\theta - \theta_j) \langle \text{Op}_N(f)\psi_j, \psi_j \rangle,$$

which is a sum of matrix elements on a window of size $1/L$ around θ . Then, in the L^2 sense, and with $U = U_N(A)$, we have

$$P(\theta) = \frac{1}{L} \sum_{t \in \mathbb{Z}} e(t\theta) \hat{h}\left(\frac{t}{L}\right) \text{tr}\{\text{Op}_N(f)U^{-t}\}. \tag{3.1}$$

(Note that $|\text{tr}\{\text{Op}_N(f)U^{-t}\}|$ is uniformly bounded in t .) The mean value of $P(\theta)$ is

$$\int_0^1 P(\theta) \, d\theta = \frac{1}{L} \hat{h}(0) \text{tr}\{\text{Op}_N(f)\} = O_f(N^{-\infty})$$

according to (2.3). Thus the variance can be written as

$$\text{Var}(P) = \frac{1}{L^2} \sum_{t \in \mathbb{Z} - \{0\}} \hat{h}\left(\frac{t}{L}\right)^2 |\text{tr}\{\text{Op}_N(f)U^{-t}\}|^2. \tag{3.2}$$

3.2. Computing the variance

Let $\text{ord}(A, N)$ be the least integer $r \geq 1$ so that $A^r \equiv I \pmod N$. It is a divisor of $|\mathcal{C}_A(N)|$, that is, of either $N - 1$ or $N + 1$. We will rewrite (3.2) as

$$\text{Var}(P) = \frac{1}{L^2} \sum_{\tau \pmod{\text{ord}(A, N)}} \Gamma(\tau) |\text{tr}\{\text{Op}_N(f)U^{-\tau}\}|^2, \tag{3.3}$$

where

$$\Gamma(\tau) = \sum_{\substack{t \in \mathbb{Z} - \{0\} \\ t \equiv \tau \pmod{\text{ord}(A, N)}}} \hat{h}\left(\frac{t}{L}\right)^2. \tag{3.4}$$

We may omit the term $\tau \equiv 0 \pmod{\text{ord}(A, N)}$ from the sum (3.3) at the cost of introducing an error of $O(N^{-\infty})$, since then $\text{tr}\{\text{Op}_N(f)U^{-\tau}\} = \text{tr}\{\text{Op}_N(f)\} = O(N^{-\infty})$ while $|\Gamma(\tau)| \ll L$.

Now we use lemma 2.3 to rewrite $\text{tr}\{\text{Op}_N(f)U_N(A^t)\}$, where we replace $U_N(A^t)$ by $U_N(A)^t$ after introducing a phase (which can be ignored as we are taking absolute values) and replacing t by $-t$ in (3.2), as we may since h is even. The result is that

$$\text{Var}(P) = \frac{1}{L^2} \sum_{k, k'} (-1)^{k_1 k_2 + k'_1 k'_2} \hat{f}(k) \overline{\hat{f}(k')} S(k, k') + O(N^{-\infty}), \tag{3.5}$$

where, in the notation of section 2.3, we have

$$S(k, k') = \sum_{t \not\equiv 0 \pmod{\text{ord}(A, N)}} \Gamma(t) e\left(\frac{\bar{2}(q(k; A^t) - q(k'; A^t))}{N}\right). \tag{3.6}$$

We have $|S(k, k')| \ll NL$ since $|\Gamma(t)| \ll L$. Thus we may, using rapid decay of the Fourier coefficients $\hat{f}(k)$, truncate the sum (3.5) at frequencies at most $N^{1/4}$ to get

$$\text{Var}(P) = \frac{1}{L^2} \sum_{|k|, |k'| < N^{1/4}} (-1)^{k_1 k_2 + k'_1 k'_2} \hat{f}(k) \overline{\hat{f}(k')} S(k, k') + O(N^{-\infty}). \tag{3.7}$$

3.3. Diagonal terms

The sum $S(k, k')$ is trivial if the phase difference $q(k; A^t) - q(k'; A^t)$ vanishes mod N for all t . By lemma 2.2, this happens if and only if we have $Q(k) \equiv Q(k') \pmod N$. For the frequencies appearing in (3.7), we have $|Q(k)|, |Q(k')| \ll \sqrt{N}$ by Cauchy–Schwartz, and

hence the congruence $Q(k) \equiv Q(k') \pmod N$ forces that this latter condition becomes an equality $Q(k) = Q(k')$.

These ‘diagonal’ pairs of frequencies with $Q(k) = Q(k')$ give a contribution of

$$\frac{1}{L^2} \sum_{Q(k)=Q(k')} (-1)^{k_1 k_2 + k'_1 k'_2} \widehat{f}(k) \overline{\widehat{f}(k')} \sum_{t \neq 0 \pmod{\text{ord}(A, N)}} \Gamma(t)$$

(we may drop the condition $|k|, |k'| < N^{1/4}$ at a cost of $O(N^{-\infty})$). We claim that

$$\sum_{t \neq 0 \pmod{\text{ord}(A, N)}} \Gamma(t) = L + O(1).$$

To see this, write

$$\sum_{\substack{t \pmod{\text{ord}(A, N)} \\ t \neq 0 \pmod{\text{ord}(A, N)}}} \Gamma(t) = \sum_{t \in \mathbb{Z}} \widehat{h}\left(\frac{t}{L}\right)^2 - \sum_{j \in \mathbb{Z}} \widehat{h}\left(\frac{\text{ord}(A, N)}{L} j\right)^2.$$

Now

$$\sum_{t \in \mathbb{Z}} \widehat{h}\left(\frac{t}{L}\right)^2 = L^2 \int_0^1 h_L(\theta)^2 d\theta = L$$

and

$$\sum_{j \in \mathbb{Z}} \widehat{h}\left(\frac{\text{ord}(A, N)}{L} j\right)^2 = O(1)$$

since $L < 2\text{ord}(A, N)$. Thus the pairs of frequencies with $Q(k) = Q(k')$ give a total contribution of

$$\frac{1}{L} C_{\text{arith}}(f) + O\left(\frac{1}{L^2}\right). \tag{3.8}$$

3.4. Off-diagonal terms

For the remaining pairs of frequencies, where $Q(k) \neq Q(k')$, the sum $S(k, k')$ is a certain incomplete exponential sum.

Proposition 3.1. *If $Q(k) \neq Q(k')$ then*

$$|S(k, k')| \ll \sqrt{N}.$$

Assuming we have this, the off-diagonal pairs will then contribute at most $O(\sqrt{N}/L^2)$. Thus in combination with (3.8) we get

$$\text{Var}(P) = \frac{C_{\text{arith}}(f)}{L} + O\left(\frac{\sqrt{N}}{L^2}\right),$$

which gives theorem 1.1.

To prove proposition 3.1, we will need the following result.

Lemma 3.2. *Let $k, k' \in \mathbb{Z}^2$, $Q(k) \neq Q(k')$. Define*

$$E_A(j) = \sum_{0 \neq t \pmod{\text{ord}(A, n)}} e\left(\frac{jt}{\text{ord}(A, N)}\right) e\left(\frac{\tilde{2}(q(k; A^t) - q(k'; A^t))}{N}\right). \tag{3.9}$$

Then for all j ,

$$|E_A(j)| \leq 2\sqrt{N}.$$

Proof. For each multiplicative character χ of $\mathcal{C}_A(N)$, define the complete sum

$$E(\chi) := \sum_{1 \neq y \in \mathcal{C}_A(N)} \chi(y) e\left(\frac{\bar{2}(q(k; y) - q(k'; y))}{N}\right). \tag{3.10}$$

By [appendix A](#), for each character χ of $\mathcal{C}_A(N)$ we have

$$|E(\chi)| \leq 2\sqrt{N}. \tag{3.11}$$

Let $r = (|\mathcal{C}_A(N)|)/(\text{ord}(A, N))$. Choose a generator A_0 of $\mathcal{C}_A(N)$ such that $A = A_0^r \pmod N$. Define a character χ_1 of $\mathcal{C}_A(N)$ by setting $\chi_1(A_0) = e(1/|\mathcal{C}_A(N)|)$. Then

$$\chi_1(A^t) = e\left(\frac{\tau}{\text{ord}(A, N)}\right).$$

We may write the indicator function of the subgroup of $\mathcal{C}_A(N)$ generated by A as

$$\mathbf{1}_A(y) = \frac{1}{r} \sum_{\substack{\theta \in \widehat{\mathcal{C}_A(N)} \\ \theta(A) = 1}} \theta(y),$$

where the sum runs over all r characters of $\mathcal{C}_A(N)$ which are trivial on A . Then we may rewrite $E_A(j)$ in terms of the complete sums [\(3.10\)](#) as

$$E_A(j) = \frac{1}{r} \sum_{\substack{\theta \in \widehat{\mathcal{C}_A(N)} \\ \theta(A) = 1}} E(\chi_1^j \theta). \tag{3.12}$$

Now using the estimate [\(3.11\)](#) gives $|E_A(j)| \leq 2\sqrt{N}$. □

Proof of proposition 3.1. Let $k, k' \in \mathbb{Z}^2$, $Q(k) \neq Q(k')$. Recall definition [\(3.6\)](#)

$$S(k, k') = \sum_{t \neq 0 \pmod{\text{ord}(A, N)}} \Gamma(t) e\left(\frac{\bar{2}(q(k; A^t) - q(k'; A^t))}{N}\right).$$

Expanding

$$\Gamma(\tau) = \sum_{j \pmod{\text{ord}(A, N)}} \gamma(j) e\left(\frac{j\tau}{\text{ord}(A, N)}\right), \tag{3.13}$$

we get

$$S(k, k') = \sum_{j \pmod{\text{ord}(A, N)}} \gamma(j) E_A(j),$$

where $E_A(j)$ is given in [\(3.9\)](#).

According to lemma [3.2](#), if $Q(k) \neq Q(k')$ then

$$|S(k, k')| \leq 2\sqrt{N} \sum_{j \pmod{\text{ord}(A, N)}} |\gamma(j)|,$$

and so it remains to show that $\sum_j |\gamma(j)| = O(1)$.

We first note that $\gamma(j) \geq 0$ so we may ignore the absolute value signs: indeed, from definitions [\(3.4\)](#) and [\(3.13\)](#) we see that

$$\gamma(j) = \frac{L^2}{\text{ord}(A, N)} \int_0^1 h_L(\theta) h_L\left(\theta + \frac{j}{\text{ord}(A, N)}\right) d\theta,$$

which is non-negative since $h_L \geq 0$.

Thus we have

$$\sum_j |\gamma(j)| = \sum_j \gamma(j) = \Gamma(0),$$

and by definition,

$$\Gamma(0) = \sum_{m \in \mathbb{Z} - \{0\}} \hat{h} \left(\frac{\text{ord}(A, N)}{L} m \right)^2,$$

which is bounded since $L < 2\text{ord}(A, N)$. \square

Acknowledgments

The authors thank Dubi Kelmer for several helpful comments and the referees for several suggestions for improving the presentation. PK was partially supported by a grant from the Göran Gustafsson Foundation, the Royal Swedish Academy of Sciences and the Swedish Research Council. LR and ZR were supported by The Israel Science Foundation (grant no 925/06).

Appendix A. An estimate for a character sum

In this appendix we give a proof for the bound $|E(\chi)| \leq 2\sqrt{N}$ stated in (3.11) for the character sum $E(\chi)$ defined in (3.10). This bound is not new; as we explain below, in the ‘split’ case it follows immediately from Weil’s bound [30]. In the ‘inert’ case, the sum appears in the work of Gurevich and Hadani [11] who discovered that the matrix coefficients of $T_N(k)$ in the Hecke basis can be written as

$$\frac{1}{\mathcal{C}_A(N)} \sum_{B \in \mathcal{C}_A(N)} \chi(B) \text{tr}\{T_N(k)U_N(B)\},$$

and hence by (2.2), the matrix elements can be expressed in terms of the sum $E(\chi)$. Gurevich and Hadani invoke the full force of Deligne’s Weil II paper [7] to give the bound (3.11). However, to make the paper more self-contained and perhaps also of independent interest, we will give another proof that only requires Weil’s original methods [30], together with some class field theory. Following Li [21, 22], we express the exponential sum in terms of a certain idèle class character sum (over degree one places) and then derive the bound from the Riemann hypothesis for curves. (The same argument was used in [16] in a similar context.)

Appendix A.1. $E(\chi)$ as a character sum

Using (2.2) we can write $E(\chi)$ as follows: in the split case, where the matrix A is diagonalizable over $\mathbb{Z}/N\mathbb{Z}$ then

$$E(\chi) = \sum_{0,1 \neq x \in \mathbb{Z}/N\mathbb{Z}} \chi(x) \psi \left(\frac{1+x}{1-x} \right),$$

where χ is a multiplicative character and ψ a non-trivial additive character of $\mathbb{Z}/N\mathbb{Z}$. If $\chi \equiv \mathbf{1}$ is trivial then $E(\mathbf{1}) = -\psi(1) - \psi(-1)$ so $|E(\mathbf{1})| \leq 2$. For $\chi \neq \mathbf{1}$, the bound $|E(\chi)| \leq 2\sqrt{N}$ follows from Weil’s 1948 result [30] (cf [22, chapter 6, theorem 3]).

In the inert case, let \mathbb{F} be a quadratic extension of $\mathbb{Z}/N\mathbb{Z}$, $H \subset \mathbb{F}^\times$ the group of elements of norm one, ψ a non-trivial additive character of $\mathbb{Z}/N\mathbb{Z}$ and χ a multiplicative character of H . Let $\lambda_A \in H$, $\lambda_A \neq \pm 1$. Then by (2.2)

$$E(\chi) = \sum_{1 \neq x \in H} \chi(x) \psi \left(\frac{1}{\lambda_A - \lambda_A^{-1}} \frac{1+x}{1-x} \right).$$

If the multiplicative character $\chi \equiv \mathbf{1}$ is trivial, then $E(\mathbf{1}) = 0$, since $x \mapsto (1/(\lambda_A - \lambda_A^{-1}))((1+x)/(1-x))$ is a bijection of $H \setminus \{1\}$ with $\mathbb{Z}/N\mathbb{Z}$. From now on assume $\chi \neq \mathbf{1}$ is non-trivial.

Take a quadratic non-residue $D \pmod N$ and let \sqrt{D} be a root of $X^2 - D$ in \mathbb{F} . We may write each element $1 \neq x \in H$ uniquely as

$$x = \frac{t - \sqrt{D}}{t + \sqrt{D}},$$

where $t \in \mathbb{Z}/N\mathbb{Z}$. In particular we have $\lambda_A = (t_0 - \sqrt{D})/(t_0 + \sqrt{D})$ with $t_0 \neq 0$ since $\lambda_A \neq \pm 1$. Then for $x \neq 1$,

$$\frac{1}{\lambda_A - \lambda_A^{-1}} \frac{1+x}{1-x} = \frac{D - t_0^2}{4t_0 D} \cdot t$$

and so

$$E(\chi) = \sum_{t \in \mathbb{Z}/N\mathbb{Z}} \chi \left(\frac{t - \sqrt{D}}{t + \sqrt{D}} \right) \psi \left(\frac{D - t_0^2}{4t_0 D} \cdot t \right).$$

Arguing as in [22, chapter 6], we will construct idèle class characters $\tilde{\nu}, \tilde{\psi}$ of the function field $\mathbb{Z}/N\mathbb{Z}(X)$, of finite order, satisfying the following.

(i) The conductors of $\tilde{\psi}$ and $\tilde{\nu}$ are

$$\text{cond}(\tilde{\psi}) = 2\infty, \quad \text{cond}(\tilde{\nu}) = (w),$$

where w is the degree two place of $\mathbb{Z}/N\mathbb{Z}(X)$ corresponding to the irreducible polynomial $X^2 - D$. In particular the product $\tilde{\psi}\tilde{\nu}$ is unramified at all finite degree one places $v \neq \infty$.

(ii) Their values at a uniformizer π_v for the degree one place v corresponding to the polynomial $X + t$ are

$$\tilde{\psi}(\pi_v) = \psi \left(\frac{D - t_0^2}{4t_0 D} \cdot t \right), \quad \tilde{\nu}(\pi_v) = \chi \left(\frac{t - \sqrt{D}}{t + \sqrt{D}} \right).$$

Thus we can write $E(\chi)$ as a sum over degree one places $v \neq \infty$ of $\mathbb{Z}/N\mathbb{Z}[X]$:

$$E(\chi) = \sum_{\substack{\text{deg}(v) = 1 \\ v \neq \infty}} (\tilde{\nu}\tilde{\psi})(\pi_v).$$

Class field theory and the Riemann hypothesis for curves over a function field give (see [22, corollary 3 of chapter 6])

$$|E(\chi)| \leq (\text{deg cond}(\tilde{\psi}\tilde{\nu}) - 2)\sqrt{N}.$$

Since the conductor of the product $\tilde{\nu}\tilde{\psi}$ is $2\infty + w$, which has degree 4, we get

$$|E(\chi)| \leq 2\sqrt{N}$$

as claimed.

Appendix A.2. Construction of idèle class characters

We describe the construction of idèle class characters of the function field $K = \mathbb{Z}/N\mathbb{Z}(X)$. See [22, 31] for background.

Given a place v of K , let K_v denote the completion of K with respect to the topology induced by v , and let $U_v = \{\alpha \in K_v : |\alpha|_v = 1\}$ be the v -adic units of K_v . Let $\mathcal{P}_v = \{\alpha \in K_v : |\alpha|_v < 1\}$ be the maximal ideal and denote by π_v a uniformizer. In particular for the infinite place we may take $\pi_\infty = X^{-1}$.

Let I_K be idèle group of K . I_K admits a product decomposition $I_K = K^\times \cdot (\prod_{v \neq \infty} U_v \times K_\infty^\times)$, with $(\prod_{v \neq \infty} U_v \times K_\infty^\times) \cap K^\times = (\mathbb{Z}/N\mathbb{Z})^\times$. The idèle class group is

$$I_K/K^\times \simeq \left(K_\infty^\times \times \prod_{v \neq \infty} U_v \right) / (\mathbb{Z}/N\mathbb{Z})^\times.$$

Appendix A.2.1. Constructing $\tilde{\psi}$. Given a non-trivial additive character ψ_0 of $\mathbb{Z}/N\mathbb{Z}$, we will define an idèle class character $\tilde{\psi}$ of finite order such that for the degree one place v corresponding to the polynomial $X + t$ we have

$$\tilde{\psi}(\pi_v) = \psi_0(t).$$

We first define $\tilde{\psi}$ on U_∞ by setting

$$\tilde{\psi} \left(a + bX^{-1} + \sum_{n \geq 2} c_n X^{-n} \right) = \psi_0(-b/a)$$

so that we get a character of $U_\infty/((\mathbb{Z}/N\mathbb{Z})^\times(1 + \mathcal{P}_\infty^2))$. Since K_∞^\times equals $\langle X^n \rangle_{n \in \mathbb{Z}} \times U_\infty$, we may extend $\tilde{\psi}$ to a character of K_∞^\times by declaring $\tilde{\psi}_\infty(X) = 1$. Extend $\tilde{\psi}$ to $\prod_{v \neq \infty} U_v \times K_\infty^\times$ by letting $\tilde{\psi}$ be trivial on $\prod_{v \neq \infty} U_v$. Since $(\prod_{v \neq \infty} U_v \times K_\infty^\times) \cap K^\times = (\mathbb{Z}/N\mathbb{Z})^\times$ and $\tilde{\psi}$ is trivial on $(\mathbb{Z}/N\mathbb{Z})^\times$, $\tilde{\psi}$ can be regarded as a character of the idèle class group I_K/K^\times .

The conductor of $\tilde{\psi}$ is $2 \cdot \infty$, since $\tilde{\psi}|_{U_v}$ is trivial for $v \neq \infty$ and $\tilde{\psi}|_{1+\mathcal{P}_\infty}$ is non-trivial.

Finally, the value of $\tilde{\psi}$ at the uniformizer π_v for a degree one place v corresponding to the polynomial $X + t$ equals

$$\begin{aligned} \tilde{\psi}_v(\pi_v) &= \tilde{\psi}_\infty \left(\frac{1}{X+t} \right) = \tilde{\psi}_\infty(X \cdot (1+tX^{-1}))^{-1} \\ &= \tilde{\psi}_\infty(1+tX^{-1})^{-1} = \psi_0(-t)^{-1} = \psi_0(t). \end{aligned}$$

Appendix A.2.2. Constructing $\tilde{\nu}$. Given a multiplicative character χ of the group H of norm one elements of \mathbb{F} , we define an idèle class character $\tilde{\nu}$ of finite order so that

$$\tilde{\nu}(\pi_v) = \chi \left(\frac{t - \sqrt{D}}{t + \sqrt{D}} \right)$$

if v is the degree one place corresponding to the polynomial $X + t$ (see [22, chapter 6, proof of theorem 6]): denote by w the degree two place corresponding to the irreducible polynomial $X^2 - D$. Then $U_w/(1 + \mathcal{P}_w) \simeq \mathbb{F}^\times$ via the map induced by $X \mapsto \sqrt{D}$. If σ is the Galois involution of \mathbb{F} , then the map $x \mapsto \sigma(x)/x$ gives an isomorphism of $\mathbb{F}^\times/(\mathbb{Z}/N\mathbb{Z})^\times$ to the group $H \subset \mathbb{F}^\times$ of norm-one elements. Thus we get a homomorphism

$$\Phi : U_w \rightarrow U_w/((\mathbb{Z}/N\mathbb{Z})^\times \cdot (1 + \mathcal{P}_w)) \simeq H.$$

We define a character \tilde{v}_w of U_w by

$$\tilde{v}_w(u) := \chi^{-1}(\Phi(u)),$$

which is trivial on $(\mathbb{Z}/N\mathbb{Z})^\times(1 + \mathcal{P}_w)$. Extend it to a character \tilde{v} of $\prod_{v \neq \infty} U_v \times K_\infty^\times$ by having \tilde{v}_v trivial if $v \neq w$. Since \tilde{v} is trivial on $(\mathbb{Z}/N\mathbb{Z})^\times = (\prod_{v \neq \infty} U_v \times K_\infty^\times) \cap K^\times$, \tilde{v} gives a character of the idèle class group I_K/K^\times .

If χ is non-trivial, then the conductor of \tilde{v} is w . By construction, for a degree one place v corresponding to the polynomial $X + t$, we have

$$\tilde{v}(\pi_v) = \tilde{v}_w\left(\frac{1}{X+t}\right) = \chi(\Phi(X+t)) = \chi\left(\frac{\sigma(\sqrt{D}+t)}{\sqrt{D}+t}\right) = \chi\left(\frac{t-\sqrt{D}}{t+\sqrt{D}}\right).$$

References

- [1] Barnett A H 2006 Asymptotic rate of quantum ergodicity in chaotic Euclidean billiards *Commun. Pure Appl. Math.* **59** 1457–88
- [2] Berry M V 1985 Semiclassical theory of spectral rigidity *Proc. R. Soc. Lond. Ser. A* **400** 229–51
- [3] Bourgain J 2007 A remark on quantum ergodicity for cat maps *Geometric Aspects of Functional Analysis, Papers from the Israel Seminar (GAFA) (2004–2005) (Lecture Notes in Mathematics vol 1910)* ed V D Milman and G Schechtman (Berlin: Springer)
- [4] Colin de Verdière Y 1985 Ergodicité et fonctions propres du Laplacien *Commun. Math. Phys.* **102** 497–502
- [5] de Carvalho T O, Keating J P and Robbins J M 1998 Fluctuations in quantum expectation values for chaotic systems with broken time-reversal symmetry *J. Phys. A: Math. Gen.* **31** 5631–40
- [6] Degli Esposti M, Graffi S and Isola S 1995 Classical limit of the quantized hyperbolic toral automorphisms *Commun. Math. Phys.* **167** 471–507
- [7] Deligne P 1981 La conjecture de Weil II *Publ. Math. Inst. Hautes Etudes Sci.* **52** 313–428
- [8] Eckhardt B, Fishman S, Keating J P, Agam O, Main J and Müller K 1995 Approach to ergodicity in quantum wave functions *Phys. Rev. E* **52** 5893–903
- [9] Faure F, Nonnenmacher S and De Bievre S 2003 Scarred eigenstates for quantum cat maps of minimal periods *Commun. Math. Phys.* **239** 449–92
- [10] Feingold M and Peres A 1986 Distribution of matrix elements of chaotic systems *Phys. Rev. A* **34** 591–5
- [11] Gurevich S and Hadani R 2006 Proof of the Kurlberg–Rudnick rate conjecture *C. R. Math. Acad. Sci. Paris* **342** 69–72
- [12] Hannay J H and Berry M V 1980 Quantization of linear maps on the torus—Fresnel diffraction by a periodic grating *Physica D* **1** 267–91
- [13] Keating J P 1991 The cat maps: quantum mechanics and classical motion *Nonlinearity* **4** 309–41
- [14] Keating J P and Mezzadri F 2000 Pseudo-symmetries of Anosov maps and spectral statistics *Nonlinearity* **13** 747–75
- [15] Kelmer D 2007 Arithmetic quantum unique ergodicity for symplectic linear maps of the multidimensional torus *Ann. Math.* at press (*Preprint math-ph/0510079*)
- [16] Kurlberg P 2007 Bounds on supremum norms for Hecke eigenfunctions of quantized cat maps *Ann. Henri Poincaré* **8** 75–89
- [17] Kurlberg P and Rudnick Z 2000 Hecke theory and equidistribution for the quantization of linear maps of the torus *Duke Math. J.* **103** 47–78
- [18] Kurlberg P and Rudnick Z 2001 On quantum ergodicity for linear maps of the torus *Commun. Math. Phys.* **222** 201–27
- [19] Kurlberg P and Rudnick Z 2001 Value distribution for eigenfunctions of desymmetrized quantum maps *Int. Math. Res. Not.* **18** 995–1002
- [20] Kurlberg P and Rudnick Z 2005 On the distribution of matrix elements for the quantum cat map *Ann. Math.* **161** 489–507
- [21] Winnie Li W C 1992 Character sums and abelian Ramanujan graphs *J. Number Theory* **41** 199–217
- [22] Winnie Li W C 1996 *Number Theory with Applications (Series on University Mathematics vol 7)* (River Edge, NJ: World Scientific)
- [23] Lindenstrauss E 2006 Invariant measures and arithmetic quantum unique ergodicity *Ann. Math. (2)* **163** 165–219
- [24] Luo W and Sarnak P 2004 Quantum variance for Hecke eigenforms *Ann. Sci. École Norm. Sup. (4)* **37** 769–99
- [25] Basilio de Matos M and Ozorio de Almeida A M 1995 Quantization of Anosov maps *Ann. Phys.* **237** 46–65

- [26] Mœglin C, Vignéras M F and Waldspurger J L 1987 *Correspondances de Howe sur un corps p -adique* (Lecture Notes in Mathematics vol 1291) (Berlin: Springer)
- [27] Rudnick Z 2005 The arithmetic theory of quantum maps *Proc. NATO Advanced Study Institute (Montreal, 2005)*
- [28] Rudnick Z and Sarnak P 1994 The behavior of eigenstates of arithmetic hyperbolic manifolds *Commun. Math. Phys.* **161** 195–213
- [29] Schnirelman A I 1974 Ergodic properties of eigenfunctions *Usp. Mat. Nauk* **29** 181–2
- [30] Weil A 1948 On some exponential sums *Proc. Natl Acad. Sci. USA* **34** 204–7
- [31] Weil A 1974 *Basic Number Theory* 3rd edn (*Die Grundlehren der Mathematischen Wissenschaften* Band 144) (Berlin: Springer)
- [32] Zhao P *PhD Thesis* Ohio State University (in preparation)
- [33] Zelditch S 1987 Uniform distribution of eigenfunctions on compact hyperbolic surfaces *Duke Math. J.* **55** 919–41