Vol. 103, No. 1 DUKE MATHEMATICAL JOURNAL © 2000

HECKE THEORY AND EQUIDISTRIBUTION FOR THE QUANTIZATION OF LINEAR MAPS OF THE TORUS

PÄR KURLBERG AND ZEÉV RUDNICK

1. Introduction

1.1. Background. One of the key issues of "Quantum Chaos" is the nature of the semiclassical limit of eigenstates of classically chaotic systems. When the classical system is given by the geodesic flow on a compact Riemannian manifold M (or rather, on its cotangent bundle), one can formulate the problem as follows: The quantum Hamiltonian is, in suitable units, represented by the positive Laplacian $-\Delta$ on M. To measure the distribution of its eigenstates, we start with a (smooth) classical observable, that is, a (smooth) function on the unit cotangent bundle S^*M; via some choice of quantization from symbols to pseudodifferential operators, we form its quantization $\operatorname{Op}(f)$. This is a zero-order pseudodifferential operator with principal symbol f. The expectation value of $\operatorname{Op}(f)$ in the eigenstate ψ is $\langle \operatorname{Op}(f)\psi, \psi\rangle$.

Let ψ_j be a sequence of normalized eigenfunctions: $\Delta\psi_j + \lambda_j\psi_j = 0$, $\int_M |\psi_j|^2 = 1$. The problem then is to understand the possible limits as $\lambda_j \to \infty$ of the distributions

$$f \in C^\infty(S^*M) \longmapsto \big\langle \operatorname{Op}(f)\psi_j, \psi_j\big\rangle. \tag{1.1}$$

In the case where the geodesic flow is chaotic, it is assumed that the eigenfunctions are random, for instance, in the sense that the expectation values converge as $\lambda_j \to \infty$ to the average of f with respect to Liouville measure on S^*M. The validity of this for almost all eigenmodes if the classical flow is ergodic (so a very weak notion of chaos!) is asserted by Schnirelman's theorem [21],[1] a fact sometimes referred to as quantum ergodicity. The case where there are no exceptional subsequences is called "quantum unique ergodicity" (QUE). Its validity seems to be a very difficult problem, which is to date unsolved in any case where the dynamics are truly chaotic (see, however, Marklof and Rudnick [16], where QUE is proved for an ergodic, though nonmixing, model case).

1.2. Cat maps. In order to shed some light on the validity of QUE, we look at a "toy model" of the situation—the quantization of linear hyperbolic automorphisms

Received 22 June 1999. Revision received 25 August 1999.

2000 *Mathematics Subject Classification*. Primary 81Q50; Secondary 11F27.

Authors' work partially supported by Israel Science Foundation grant number 192/96 and the US-Israel Binational Science Foundation grant number 97-00157. Kurlberg's work partially supported by the European Commission-Training and Mobility of Researchers network "Algebraic Lie Representations" EC-contract number ERB FMRX-CT97-0100.

[1] See Zelditch [24] and de Verdiere [5] for proofs.

of the 2-dimensional torus $\mathbf{T}^2$. Here the phase space $\mathbf{T}^2$ is compact, and instead of a Hamiltonian flow, we consider the discrete time dynamics generated by the iterations of a single map $A \in \mathrm{SL}(2, \mathbf{Z})$. If A is hyperbolic, that is, $|\operatorname{tr} A| > 2$, then this map is a paradigm of chaotic dynamics. Such maps are sometimes called *cat maps* in the physics literature. A quantization of these cat maps was proposed by Hannay and Berry [9] and elaborated in [6], [7], [12], [13], and [25]. We review this in some detail in Sections 2 and 3. In particular, the admissible values of Planck's constant are inverse integers $h = 1/N$, and the Hilbert space of states $\mathcal{H}_N \simeq L^2(\mathbf{Z}/N\mathbf{Z})$ of the quantum system is finite-dimensional, of dimension $N = h^{-1}$. To every classical observable $f \in C^\infty(\mathbf{T}^2)$, we associate an operator $\mathrm{Op}_N(f)$ on $\mathcal{H}_N$, the corresponding quantum observable. The quantization of the cat map is a unitary operator $U_N(A)$ on $\mathcal{H}_N$, the quantum propagator, unique up to a phase factor, characterized by an exact version of Egorov's theorem[2]

$$U_N(A)^{-1}\,\mathrm{Op}_N(f)U_N(A) = \mathrm{Op}_N(f \circ A), \quad \forall f \in C^\infty\big(\mathbf{T}^2\big). \tag{1.2}$$

The eigenvectors ϕ of the quantum propagator $U_N(A)$ are the analogues of the eigenmodes of the Laplacian, and to study their concentration properties, one forms the distributions

$$f \longmapsto \big\langle \mathrm{Op}_N(f)\phi, \phi\big\rangle.$$

In particular, we want to understand the quantum limits as $N \to \infty$. An analogue of Schnirelman's theorem in this setting was proven in [3] and [25]. We would like to know if QUE holds, that is, if the only quantum limit is the uniform measure on $\mathbf{T}^2$.

The spectrum of the quantum propagator $U_N(A)$ has degeneracies, which renders the study of possible quantum limits difficult. The degeneracies are systematic and are inversely related to the order of $A \bmod 2N$. Degli Esposti, Graffi, and Isola [7] showed that if, instead of looking at all integer values of N, one restricts to the sparse subsequence consisting of primes for which the degeneracies are bounded,[3] and, moreover, split in the quadratic extension of the rationals containing the eigenvalues of A, then the only limit is indeed the uniform measure.

Our first goal in this paper is to show that the degeneracies are coupled to the existence of quantum symmetries. There is a commutative group of unitary operators on $\mathcal{H}_N$ that commute with $U_N(A)$ and therefore act on each eigenspace of $U_N(A)$. We call these *Hecke operators* in analogy with the setting of the modular surface[4] (see [10], [15], [20]). We may thus consider eigenfunctions of the desymmetrized

[2] This exact version of Egorov's theorem is very special and is a consequence of the map being linear.

[3] It is an open problem to show that there are infinitely many primes where the degeneracy is bounded. This is known, assuming the generalized Riemann hypothesis, which, in fact, guarantees that a positive proportion of the primes satisfy the assumption.

[4] A notable difference between our setting and the modular surface is that in the latter one expects few, if any, degeneracies.

quantum map, that is, eigenstates of both $U_N(A)$ and of all the Hecke operators. We call these Hecke eigenfunctions. Our second goal is to show that these become equidistributed with respect to Liouville measure, that is, the expectation values of quantum observables in Hecke eigenstates converge to the classical phase-space average of the observable.

1.3. Results. We turn to a detailed description of our results. We first carry out a systematic study of the quantum propagator. We define $U_N(A)$ so that it only depends on the remainder of $A \bmod 2N$ and satisfies (1.2). One gets a projective representation $A \mapsto U_N(A)$ of the subgroup of quantizable elements in the finite modular group $\mathrm{SL}(2, \mathbf{Z}/2N\mathbf{Z})$. In Section 4, we explain that it can be made into an ordinary representation if we further restrict to the subgroup $\Gamma(4, 2N)$ given by $g = I \bmod 4$ for N even, $g = I \bmod 2$ for N odd. Thus, for $A, B \in \Gamma(4, 2N)$, we have $U_N(AB) = U_N(A)U_N(B)$. Consequently, if $AB = BA \bmod 2N$, then their propagators commute. This is the basic principle that we use to form the Hecke operators.

Fix a hyperbolic matrix A, which we further assume lies in the congruence subgroup

$$\Gamma(4) = \left\{ g \in \mathrm{SL}(2, \mathbf{Z}) : g = I \bmod 4 \right\}$$

so that its reduction modulo $2N$ lies in $\Gamma(4, 2N)$ for all N. To find matrices commuting with A modulo $2N$, we use the connection with the theory of real quadratic fields (see Section 5). If α is an eigenvalue of A, form $\mathfrak{O} = \mathbf{Z}[\alpha]$, which is an order in the real quadratic field $K = \mathbf{Q}(\alpha)$. There is an $\mathfrak{O}$-ideal I so that the action of α on I by multiplication has A as its matrix in a suitable basis. Thus the action of $\mathfrak{O}$ on I by multiplication gives us an embedding $\iota : \mathfrak{O} \hookrightarrow \mathrm{Mat}_2(\mathbf{Z})$ and induces a map $\iota : \mathfrak{O}/2N\mathfrak{O} \to \mathrm{Mat}_2(\mathbf{Z}/2N\mathbf{Z})$. Under this map, the images of elements $\beta \in \mathfrak{O}/2N\mathfrak{O}$ whose Galois norm is $1 \bmod 2N$ lie in $\mathrm{SL}(2, \mathbf{Z}/2N\mathbf{Z})$ and commute with A modulo $2N$. If we further require that $\beta = 1 \bmod 4\mathfrak{O}$, then we get a group of commuting matrices $\iota(\beta) \in \Gamma(4, 2N)$, whose quantum propagators $U_N(\iota(\beta))$ commute with $U_N(A)$ and with each other. These are our Hecke operators.

Since the Hecke operators commute with $U_N(A)$, they act on its eigenspaces, and since they commute with each other, there is a basis of $\mathcal{H}_N$ consisting of joint eigenfunctions of $U_N(A)$ and the Hecke operators, whose elements we call Hecke eigenfunctions. Our main theorem is the following:

THEOREM 1. *Let $A \in \Gamma(4)$ be a hyperbolic matrix, and let $f \in C^\infty(\mathbf{T}^2)$ be a smooth observable. Then for all normalized Hecke eigenfunctions $\phi \in \mathcal{H}_N$ of $U_N(A)$, the expectation values $\langle \mathrm{Op}_N(f)\phi, \phi \rangle$ converge to the phase-space average of f as $N \to \infty$. Moreover, for all $\epsilon > 0$, we have*

$$\left\langle \mathrm{Op}_N(f)\phi, \phi \right\rangle = \int_{\mathbf{T}^2} f(x)\,dx + O_{f,\epsilon}\left(N^{-1/4+\epsilon}\right), \quad \textit{as } N \longrightarrow \infty.$$

Remark 1.1. It is easy to extend Theorem 1 to give similar results for matrix elements of $\mathrm{Op}_N(f)$. When N is such that the degeneracies in the spectrum of $U_N(A)$

are sufficiently small, this implies, as in [7], that the expectation values of $\mathrm{Op}_N(f)$ in all eigenstates converge to $\int_{\mathbf{T}^2} f(x)dx$.

Remark 1.2. The exponent of $1/4$ in our theorem is certainly not optimal, and more likely the correct exponent is $1/2$. That is the exponent given in [7], where the problem is reduced to one-variable exponential sums, which can be estimated using Weil's theorem—the Riemann hypothesis for a curve over a finite field.

What we in fact show (see Theorem 9) is that if ϕ_i, $i = 1, \dots, N$ is an orthonormal basis of $\mathcal{H}_N$ consisting of Hecke eigenfunctions, then

$$\sum_{i=1}^{N} \left| \langle \mathrm{Op}_N(f)\phi_i, \phi_i\rangle - \int_{\mathbf{T}^2} f(x)\,dx \right|^4 \ll N^{-1+\epsilon},$$

from which we deduce Theorem 1 by taking an orthonormal basis with $\phi_1 = \phi$ and omitting all but one term on the left-hand side. If all terms on the left-hand side are of roughly the same size, then we would expect this to give the exponent $1/2$.

The proof of Theorem 1 is reduced to a counting problem in Section 6. This in turn comes down to counting solutions of the congruence

$$\beta_1 - \beta_2 + \beta_3 - \beta_4 = 0 \bmod N\mathfrak{O}$$

in norm-one elements $\beta_i \in \mathfrak{O}/N\mathfrak{O}$. The number of such norm-one elements is $O(N^{1+\epsilon})$ (see Lemma 8), and since this equation has three degrees of freedom, the trivial bound of the number of solutions is $O(N^{3+\epsilon})$, $\forall\epsilon > 0$. To get any result in Theorem 1, we need to show that the number of solutions is $O(N^{3-\delta})$ for some $\delta > 0$, that is, any saving over the trivial bound would do. This is accomplished in Section 7, where we show that the number of solutions is $O(N^{2+\epsilon})$, the optimal bound.

Acknowledgments. We thank J. Bernstein, D. Kazhdan, J. Keating, J. Marklof, F. Mezzadri, P. Sarnak, and S. Zelditch for helpful discussions concerning various points in the paper.

2. Background on quantization of maps. In this paper, we consider the quantization of linear (orientation-preserving) automorphisms of the torus $\mathbf{T}^2 = \mathbf{R}^2/\mathbf{Z}^2$, that is, elements of the modular group $\mathrm{SL}(2, \mathbf{Z})$, which for the most part are assumed to be hyperbolic (known as cat maps in some of the literature). For this, we first review a procedure (one of several) for quantization of maps.

The first to quantize the cat map were Hannay and Berry [9]. We follow in part an approach by means of representation theory that was developed by Knabe [13] and Degli Esposti, Graffi, and Isola [6] and [7]. See also [3], [12], and [25] for other approaches.

2.1. The quantization procedure. We start by describing some desiderata for a quantization procedure for a symplectic map A of a phase space. In the literature it is customary to distinguish two components of the quantization procedure—a kinematic component and a dynamical one.

In the kinematic component, one constructs a Hilbert space $\mathcal{H}_h$ of states of the quantum system and an algebra of operators on the space—the algebra of quantum observables.[5] Smooth functions f on the classical phase space of the system (that is, classical observables) are mapped to members $\mathrm{Op}_h(f)$ of this algebra. To make the connection with the classical system, it is required that in the limit $h \to 0$, the commutator of the quantization of two observables f, g reproduce the quantization of their Poisson bracket $\{f, g\} = \sum_j (\partial f/\partial p_j)(\partial g/\partial q_j) - (\partial f/\partial q_j)(\partial g/\partial p_j)$:

$$\frac{i}{\hbar}\big[\mathrm{Op}_h(f), \mathrm{Op}_h(g)\big] - \mathrm{Op}_h(\{f, g\}) \xrightarrow[h\to 0]{} 0. \tag{2.1}$$

(We do not specify the sense of convergence.)

The dynamical part of quantization amounts to prescribing a discrete time evolution of the algebra of quantum observables, that is, a unitary map $U_h(A)$ of $\mathcal{H}_h$, that reproduces the classical map A in the limit $h \to 0$ in the sense that

$$U_h(A)^{-1}\,\mathrm{Op}_h(f)U_h(A) - \mathrm{Op}_h(f \circ A) \xrightarrow[h\to 0]{} 0. \tag{2.2}$$

(This is the analogue of Egorov's theorem.)

In our case, the classical phase space is the torus $\mathbf{T}^2$. The classical observables are smooth functions on $\mathbf{T}^2$. We find that Planck's constant h is restricted to be an inverse integer: $h = 1/N$, $N \geq 1$. The state-space $\mathcal{H}_h$ is $\mathcal{H}_N = L^2(\mathbf{Z}/N\mathbf{Z})$. To each observable $f \in C^\infty(\mathbf{T}^2)$, we assign, by an analogue of Weyl quantization, an operator $\mathrm{Op}_N(f)$ on $\mathcal{H}_N$ so that (2.1) holds where convergence is in the space of $N \times N$ matrices. The dynamics are given by a linear map $A \in \mathrm{SL}(2, \mathbf{Z})$ so that $x = \binom{p}{q} \in \mathbf{T}^2 \mapsto Ax$ is a symplectic map of the torus. Given an observable $f \in C^\infty(\mathbf{T}^2)$, the classical evolution defined by A is $f \mapsto f \circ A$, where $f \circ A(x) = f(Ax)$. It turns out that for a certain subset of matrices A, there is a unitary map $U_N(A)$ on $L^2(\mathbf{Z}/N\mathbf{Z})$ so that an exact form of (2.2) holds:

$$U_N(A)^{-1}\,\mathrm{Op}_N(f)U_N(A) = \mathrm{Op}_N(f \circ A), \quad \forall f \in C^\infty\big(\mathbf{T}^2\big).$$

This is our discrete time evolution.

We describe these procedures in detail below.

2.2. Kinematics: The space of states.

2.2. Kinematics: The space of states. As the Hilbert space of states, we take distributions $\psi(q)$ on the line $\mathbf{R}$ that are periodic in both the position and the momentum representation. As is well known, this restricts Planck's constant to take only inverse integer values. We review the argument: recall that the momentum representation of a wave-function ψ is

$$\mathcal{F}_h\psi(p) = \frac{1}{\sqrt{h}}\int_{-\infty}^{\infty}\psi(q)e^{-2\pi i qp/h}\,dq.$$

[5] h stands for Planck's constant.

We then require

$$\psi(q+1)=\psi(q), \qquad \mathcal{F}_h\psi(p+1)=\mathcal{F}_h\psi(p)$$

(one may just require that this hold up to a phase). From periodicity in the position representation, we get

$$\psi(q)=\sum_{n\in\mathbf{Z}} c_n e(nq),$$

where

$$e(z):=e^{2\pi i z}.$$

In the momentum representation, that is, applying $\mathcal{F}_h$, we get

$$\mathcal{F}_h\psi(p)=\sqrt{h}\sum_{n\in\mathbf{Z}} c_n\delta(p-nh).$$

Now, in order that $\mathcal{F}_h\psi(p+1)=\mathcal{F}_h\psi(p)$, we clearly need $1/h\in\mathbf{Z}$, that is, for some integer $N\geq 1$, that

$$h=\frac{1}{N}.$$

In that case, we also need

$$c_{n+N}=c_n.$$

Thus, we find that $h=1/N$ and the space of states is finite dimensional, of dimension $N=1/h$, and consists of periodic point-masses at the coordinates $q=Q/N$, $Q\in\mathbf{Z}$. We may then identify $\mathcal{H}_N$ with the N-dimensional vector space $L^2(\mathbf{Z}/N\mathbf{Z})$, with the inner product $\langle\cdot,\cdot\rangle$ defined by

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

2.3. Quantizing observables. Next we construct quantum observables: for a free particle on the line, we would take as the basic observables the position and momentum operators

$$\hat{q}\psi(q):=q\psi(q), \qquad \hat{p}\psi(q):=\frac{\hbar}{i}\frac{d\psi}{dq}(q)$$

($\hbar=h/2\pi$). For our periodic phase space, we take the basic observables to be $e(\hat{q})=e^{2\pi i\hat{q}}$ and $e(\hat{p})$, which correspond to the phase space translations

$$e(\hat{q})\psi(q)=e(q)\psi(q), \qquad e(\hat{p})\psi(q)=\psi(q+h).$$

Corresponding to the commutation relation

$$[\hat{q},\hat{p}]=i\hbar=-\frac{h}{2\pi i},$$

we find that

$$e(\hat{q})e(\hat{p}) = e^{-2\pi i h} e(\hat{p})e(\hat{q}).$$

Writing

$$t_1 := e(\hat{p}), \qquad t_2 := e(\hat{q})$$

(so that $t_2 t_1 = e^{-2\pi i h} t_1 t_2$), we put, for $n = (n_1, n_2) \in \mathbf{Z}^2$,

$$T_N(n) := e^{i\pi n_1 n_2/N} t_2^{n_2} t_1^{n_1}. \tag{2.3}$$

Their action on a wave function $\psi \in L^2(\mathbf{Z}/N\mathbf{Z})$ is

$$T_N(n)\psi(Q) = e^{i\pi n_1 n_2/N} e\left(\frac{n_2 Q}{N}\right)\psi(Q + n_1). \tag{2.4}$$

These are clearly of period $2N$ in n:

$$T_N(n + 2Nm) = T_N(n), \quad n, m \in \mathbf{Z}^2.$$

The adjoint of $T_N(n)$ is given by

$$T_N(n)^* = T_N(-n). \tag{2.5}$$

They also satisfy

$$T_N(m)T_N(n) = e^{i\pi\omega(m,n)/N} T_N(m+n), \tag{2.6}$$

where

$$\omega(m,n) = m_1 n_2 - m_2 n_1.$$

Now we can finally construct quantum observables. For any smooth classical observable $f \in C^\infty(\mathbf{T}^2)$ with Fourier expansion

$$f(x) = \sum_{n \in \mathbf{Z}^2} f_n e(n \cdot x), \quad x = \begin{pmatrix} p \\ q \end{pmatrix} \in \mathbf{T}^2,$$

we define its quantization $\mathrm{Op}_N(f)$ as

$$\mathrm{Op}_N(f) := \sum_{n \in \mathbf{Z}^2} f_n T_N(n).$$

The verification of (2.1) is an easy calculation using (2.6).

2.4. The Heisenberg group. We now digress to connect this construction to the representation theory of a certain Heisenberg group H_{2N}.

For vectors $x = (x_1, x_2)$, $y = (y_1, y_2)$, define $\omega(x, y) := x_1 y_2 - x_2 y_1$. This is a nondegenerate symplectic form. The Heisenberg group H_{2N} is defined to be the set $(\mathbf{Z}/2N\mathbf{Z})^2 \times \mathbf{Z}/2N\mathbf{Z}$ with multiplication

$$(x, z) \cdot (x', z') := \big(x + x', z + z' + \omega(x, x')\big).$$

This is at odds with the standard convention where one multiplies ω by $1/2$, but is essential for us because 2 is not invertible in $\mathbf{Z}/2N\mathbf{Z}$.

It is useful to record various facts about the multiplication in H_{2N}: the inverse of (x, z) is

$$(x, z)^{-1} = (-x, -z). \tag{2.7}$$

The commutator of two elements is given by

$$(x, z)(x', z')(x, z)^{-1}(x', z')^{-1} = \big(0, 2\omega(x, x')\big). \tag{2.8}$$

From this commutator identity and the fact that ω is nondegenerate, we immediately find the following lemma.

Lemma 2. *The center of H_{2N} is $(N\mathbf{Z}/2N\mathbf{Z})^2 \times \mathbf{Z}/2N\mathbf{Z}$, that is,*

$$\mathrm{Cent}(H_{2N}) = \big\{(N\epsilon, N\eta, z) : \epsilon, \eta = 0, 1,\ z \in \mathbf{Z}/2N\mathbf{Z}\big\}.$$

We define a representation of H_{2N} on $L^2(\mathbf{Z}/N\mathbf{Z})$ by setting

$$\pi(n, z) = e\left(\frac{z}{2N}\right) T_N(n).$$

From the relation (2.6), it follows that $\pi(h)\pi(h') = \pi(hh')$, that is, we do indeed get a representation.

The center of H_{2N} then acts via the character χ given by

$$\chi(x_0, y_0, z) = e\left(\frac{z + x_0 y_0}{2N}\right)$$

(that is, $\pi(x_0, y_0, z) = \chi(x_0, y_0, z) I$).

The basic facts about π and the representation theory of H_{2N} are covered in the following proposition.

Proposition 3. (i) *All irreducible representations of H_{2N} have dimension at most N.*

(ii) *The representation π is irreducible and is the unique, irreducible N-dimensional representation with central character χ.*

We omit the details of the proof; the main point (which is easy to verify from the definitions) is the following lemma.

LEMMA 4. *The trace of $T_N(n)$ is given by*

$$\left|\operatorname{tr} T_N(n)\right| = \begin{cases} N, & \text{if } n \equiv (0,0) \bmod N, \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Let $\phi_i = \sqrt{N}\delta_i$ where δ_i is the Dirac delta function supported at i, so that $\{\phi_i\}_{i=1}^N$ is an orthonormal basis of $L^2(\mathbf{Z}/N\mathbf{Z})$. Then

$$\operatorname{tr} T_N(n) = \sum_{i=1}^{N} \left\langle T_N(n)\phi_i, \phi_i \right\rangle,$$

and by equation (2.4),

$$\begin{aligned} T_N(n)\phi_i(Q) &= e\left(\frac{n_1n_2+2n_2Q}{2N}\right)\phi_i(Q+n_1) \\ &= e\left(\frac{n_1n_2+2n_2Q}{2N}\right)\phi_{i-n_1}(Q) \\ &= e\left(\frac{-n_1n_2+2n_2i}{2N}\right)\phi_{i-n_1}(Q). \end{aligned}$$

Therefore, $\operatorname{tr} T_N(n) = 0$ unless $n_1 \equiv 0 \bmod N$, in which case,

$$\sum_{i=1}^{N} \left\langle T_N(n)\phi_i, \phi_i \right\rangle = e\left(\frac{-n_1n_2}{2N}\right) \sum_{i=1}^{N} e\left(\frac{n_2 i}{N}\right).$$

The result now follows since $\sum_{i=1}^N e(n_2 i/N)$ equals N if $n_2 \equiv 0 \bmod N$, and is zero otherwise. □

2.5. Description of π as an induced representation. Let Y be the subgroup of elements

$$Y = \left\{(x_0, y, z) : y, z \in \mathbf{Z}/2N\mathbf{Z},\ x_0 \in N\mathbf{Z}/2N\mathbf{Z}\right\}.$$

It is easily seen to be a normal, maximal abelian subgroup, of index N, containing the center. For $(x_0, y, z) \in Y$, set

$$\tau(x_0, y, z) := e\left(\frac{z + x_0 y}{2N}\right).$$

This is a character of Y (we need to use $2x_0 \equiv 0 \bmod 2N$ in verifying this), restricting to the character $\chi(x_0, y_0, z) = e(z + x_0y_0/2N)$ of the center.

We consider the induced representation $\operatorname{Ind}_Y^{H_{2N}} \tau$ of the Heisenberg group. The basic model for it is the space of functions $\Phi : H_{2N} \to \mathbf{C}$ satisfying $\Phi(ah) = \tau(a)\Phi(h)$ for $a \in Y$, $h \in H_{2N}$. The action of the group is by right multiplication

$h\Phi(h') := \Phi(h'h)$. By restricting to the subgroup $X = \{(x,0,0)\}$, we can realize this induced representation as functions on $\mathbf{Z}/2N\mathbf{Z}$ that are N-periodic (since the element $(N,0,0)$ lies in $X \cap Y$). We can identify this space of functions with $L^2(\mathbf{Z}/N\mathbf{Z})$.

Let us compute the action of a group element $h = (x,y,z) \in H_{2N}$ in this model. For this we need to write $(x',0,0)\cdot h$ as $a\cdot(x'',0,0)$, $a \in Y$. The relevant identity is

$$(x',0,0)(x,y,z) = \bigl(0,y,z+xy+2x'y\bigr)(x'+x,0,0).$$

Thus, the element $h = (x,y,z)$ acts as

$$h\phi(x') = e\biggl(\frac{z+xy+2x'y}{2N}\biggr)\phi(x'+x).$$

In particular, $(x,0,0)$ acts as translation by x and $(0,y,0)$ as a multiplication operator $\phi(x') \mapsto e(x'y/N)\phi(x')$. The center acts by the character $(x_0,y_0,z) \mapsto e(z+x_0y_0/2N)$. These show that π coincides with the induced representation $\operatorname{Ind}_Y^{H_{2N}}\tau$.

3. Dynamics: Quantized cat maps. We now show how to assign to (certain) linear automorphisms A of the torus $\mathbf{T}^2$, a unitary operator $U_N(A)$ on $L^2(\mathbf{Z}/N\mathbf{Z})$ that satisfies the following statement: for all observables $f \in C^\infty(\mathbf{T}^2)$,

$$U_N(A)^{-1}\operatorname{Op}_N(f)U_N(A) = \operatorname{Op}_N(f\circ A).$$

The finite modular group $\mathrm{SL}(2,\mathbf{Z}/2N\mathbf{Z})$ acts by automorphisms on the Heisenberg groups H_{2N} via $(x,z)^A := (xA,z)$, $A \in \mathrm{SL}(2,\mathbf{Z}/2N\mathbf{Z})$. That this is indeed an automorphism (i.e., $(h_1h_2)^A = h_1^Ah_2^A$) follows from A preserving the symplectic form ω. Moreover, we have $(h^A)^B = h^{AB}$. Composing the representation π of H_{2N} with A gives a new representation $\pi^A(h) := \pi(h^A)$, which is clearly still an irreducible N-dimensional representation. Its central character χ^A can be easily computed as follows: if $x_0, y_0 \in N\mathbf{Z}/2N\mathbf{Z}$ and $(x_1,y_1) = (x_0,y_0)A$, then χ^A is given by

$$\chi^A(x_0,y_0,z) = \chi\bigl((x_0,y_0)A,z\bigr) = e\biggl(\frac{z+x_1y_1}{2N}\biggr).$$

This is the same character as χ if and only if $x_1y_1 \equiv x_0y_0 \bmod 2N$ for all $x_0, y_0 \in N\mathbf{Z}/2N\mathbf{Z}$. Writing $A = \bigl(\begin{smallmatrix} a & b\\ c & d\end{smallmatrix}\bigr)$ and $x_0 = N\epsilon$, $y_0 = N\eta$, $\epsilon,\eta \in \mathbf{Z}/2\mathbf{Z}$, this is equivalent to requiring

$$N\bigl(ab\epsilon^2 + cd\eta^2\bigr) \equiv 0 \bmod 2, \quad \forall\epsilon,\eta \in \mathbf{Z}/2\mathbf{Z},$$

or

$$Nab \equiv Ncd \equiv 0 \bmod 2.$$

This is only a restriction if N is odd and is satisfied by the elements of the theta group

$$\Gamma_\theta(2N) = \left\{\begin{pmatrix} a & b\\ c & d\end{pmatrix} \in \mathrm{SL}(2,\mathbf{Z}/2N\mathbf{Z}) : ab \equiv cd \equiv 0 \bmod 2\right\}.$$

Therefore, if $A \in \Gamma_\theta(2N)$, we get a unitarily equivalent representation π^A of H_{2N}. Thus, there is a unitary map $U_N(A)$, the quantum propagator associated to A, so that

$$\pi\left(h^A\right) = U_N(A)^{-1}\pi(h)U_N(A), \quad \forall h \in H_{2N}.$$

In particular, we find

$$U_N(A)^{-1}T_N(n)U_N(A) = T_N(nA), \tag{3.1}$$

and consequently, for all observables $f \in C^\infty(\mathbf{T}^2)$,

$$\mathrm{Op}_N(f \circ A) = U_N(A)^{-1}\,\mathrm{Op}_N(f)U_N(A). \tag{3.2}$$

Now for any quantizable element $A \in \mathrm{SL}(2,\mathbf{Z})$ (that is, $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $ab \equiv cd \equiv 0 \bmod 2$), we define the quantum propagator (or quantized cat map) to be $U_N(\bar{A})$ where $\bar{A} \in \mathrm{SL}(2,\mathbf{Z}/2N\mathbf{Z})$ is the reduction of A modulo $2N$. Thus, by its construction, $U_N(A)$ only depends on the reduction $A \bmod 2N$. (This is a difference from the construction in Hannay and Berry [9].)

4. Multiplicativity. The quantum propagators $U_N(A)$ are uniquely defined up to a phase factor, because of the irreducibility of π (Schur's lemma). Thus, they define a projective representation of $\Gamma_\theta(2N)$; that is,

$$U_N(AB) = e^{i\phi_N(A,B)}U_N(A)U_N(B) \quad A, B \in \Gamma_\theta(2N).$$

Define the subgroup

$$\Gamma(4,2N) = \left\{ g \in \mathrm{SL}(2,\mathbf{Z}/2N\mathbf{Z}) : \begin{cases} g = I \bmod 4, & (N \text{ even}) \\ g = I \bmod 2, & (N \text{ odd}) \end{cases} \right\}.$$

The goal of this section is to show that there is a choice of phases for the propagators $U_N(A)$ so that on the subgroup $\Gamma(4,2N)$, the map $A \mapsto U_N(A)$ is a homomorphism.

THEOREM 5. *There is a choice of quantum propagators so that*

$$U_N(AB) = U_N(A)U_N(B), \quad A, B \in \Gamma(4,2N).$$

As a consequence, we find the following corollary.

COROLLARY 6. *If $A, B \in \Gamma(4,2N)$ commute $\bmod 2N$, then their propagators also commute: $U_N(A)U_N(B) = U_N(B)U_N(A)$.*

Theorem 5 is essentially known in various guises and arose out of the study of theta functions and the Weil representation. One form is due to Kubota [14] (see also [8]). There are also treatments purely at the finite level [1] and [18]. Since Corollary 6 is absolutely crucial to our work, and we did not find a good reference for the exact form that we need, we sketch a proof (or more precisely, a verification) of Theorem 5. We wish to note that Theorem 5 is a priori more subtle than Corollary 6, since once we know that there is some choice of phases for which Corollary 6 holds, then it holds for all choices; this is not the case with Theorem 5.[6]

4.1. Reduction to prime powers. Factor $2N = \prod_p p^{k_p} = 2^k \prod_{p>2} p^{k_p} = 2^k M$, with M odd. The Chinese remainder theorem gives an isomorphism

$$\mathbf{Z}/2N\mathbf{Z} \simeq \prod_p \mathbf{Z}/p^{k_p}\mathbf{Z},$$

given by

$$x \longmapsto \big(x \bmod p^{k_p}\big)_p$$

with inverse

$$\big(x_p \bmod p^{k_p}\big)_p \longmapsto \sum \frac{2N}{p^{k_p}} r_p x_p \bmod 2N,$$

where r_p is the inverse of $2N/p^{k_p}$ modulo p^{k_p}. Correspondingly, we have a bijection

$$L^2(\mathbf{Z}/2N\mathbf{Z}) \simeq \bigotimes_p L^2\big(\mathbf{Z}/p^{k_p}\mathbf{Z}\big).$$

We define the phase space translations $T^{(p)}$ on $L^2(\mathbf{Z}/p^{k_p}\mathbf{Z})$ as in (2.4) by

$$T^{(p)}(n)\psi(Q) = e\left(\frac{r_p(n_1n_2+2n_2Q)}{p^{k_p}}\right)\psi(Q+n_1).$$

It is then a simple matter to see that $T_N(n) = \otimes_p T^{(p)}(n)$, that is, if $\psi = \otimes_p \psi_p \in \bigotimes_p L^2(\mathbf{Z}/p^{k_p}\mathbf{Z})$ is decomposable, then

$$T_N(n)\psi(Q) = \prod_p T^{(p)}(n)\psi\big(Q \bmod p^{k_p}\big).$$

This allows us to express the quantum propagators $U_N(A)$ as tensor products. Indeed, if we already have propagators $U^{(p)}(A)$ that satisfy

$$U^{(p)}(A)^{-1}T^{(p)}(n)U^{(p)}(A) = T^{(p)}(nA), \tag{4.1}$$

we then set

$$U_N(A) := \otimes U^{(p)}(A), \tag{4.2}$$

which still satisfies

$$U_N(A)^{-1}T_N(n)U_N(A) = T_N(nA)$$

[6] We thank Jon Keating for emphasizing this point to us.

for all $n \in \mathbf{Z}^2$, and therefore $U_N(A)$ coincides up to a phase with any other map satisfying this.

We use this procedure to define $U_N(A)$ (that is, choose a phase) so that U_N is an honest representation of a subgroup $\Gamma(4, 2N)$ of $\mathrm{SL}(2, \mathbf{Z}/2N\mathbf{Z})$, not merely a projective representation. From the factorization property (4.2), it follows that it is enough to show that $U^{(p)}$ is a representation of $\mathrm{SL}(2, \mathbf{Z}/p^{k_p}\mathbf{Z})$ when $p > 2$ is odd, and of $\Gamma(4, 2^k)$ if $N = 2^{k-1}M$ is even.

4.2. Gauss sums. We need some preliminary information on Gauss sums. We define normalized Gauss sums

$$S_r\big(a, p^k\big) = \frac{1}{\sqrt{p^k}} \sum_{x \bmod p^k} e\left(\frac{-rax^2}{p^k}\right). \tag{4.3}$$

For p odd, these are fourth roots of unity. To describe them, define for $t \in (\mathbf{Z}/p^k\mathbf{Z})^*$,

$$\Lambda_{r,p^k}(t) = \frac{S_r\big(t, p^k\big)}{S_r\big(1, p^k\big)}.$$

Note that if $t = t_1^2 \in (\mathbf{Z}/p^k\mathbf{Z})^*$ is a square, then $\Lambda_{r,p^k}(t) = 1$, since from (4.3) we find after the change of variables $x_1 = t_1 x$ that $S_r(t, p^k) = S_r(1, p^k)$.

For p odd, Λ_{r,p^k} is given in terms of the Legendre symbol as

$$\Lambda_{r,p^k}(t) = \left(\frac{t}{p}\right)^k$$

and is a character of $(\mathbf{Z}/p^k\mathbf{Z})^*$:

$$\Lambda_{r,p^k}(tt') = \Lambda_{r,p^k}(t)\Lambda_{r,p^k}(t').$$

When $p = 2$, we have

$$\Lambda_{r,2^k}(t) = \left(\frac{-2^k}{t}\right) i^{-r(\bar{t}^2-1)/8},$$

where $\bar{t}$ is the smallest positive residue of $t \bmod 4$. In that case, it is not quite a character of the whole multiplicative group of $\mathbf{Z}/2^k\mathbf{Z}$, but instead satisfies

$$\Lambda_{r,2^k}(tt') = (t, t')_2 \Lambda_{r,2^k}(t)\Lambda_{r,2^k}(t'), \tag{4.4}$$

where $(t, t')_2$ is the Hilbert symbol. In particular, if $t, t' = 1 \bmod 4$, then the Hilbert symbol is trivial, and so we get a character of the subgroup $\{t = 1 \bmod 4\} \subset (\mathbf{Z}/2^k\mathbf{Z})^*$ (this is relevant for $k \geq 2$) given simply by

$$\Lambda_{r,2^k}(t) = \begin{cases} 1, & t = 1 \bmod 8, \\ (-1)^k, & t = 5 \bmod 8. \end{cases}$$

For p odd, we also need to know the normalized Gauss sum (4.3) when $t = -1$, in which case, we have

$$S_r\bigl(-1, p^k\bigr) = \begin{cases} 1, & k \text{ even}, \\ \epsilon(p)\left(\dfrac{r}{p}\right), & k \text{ odd}, \end{cases}$$

where

$$\epsilon(p) = \begin{cases} 1, & p = 1 \bmod 4, \\ i, & p = 3 \bmod 4. \end{cases}$$

4.3. p odd. We describe how to define $U^{(p)}$ on $\mathrm{SL}(2, \mathbf{Z}/p^k\mathbf{Z})$ so that it gives a representation (see Nobs [18] for details). This group is generated by the matrices

$$\begin{pmatrix} 1 & b \\ & 1 \end{pmatrix}, \qquad \begin{pmatrix} t & \\ & t^{-1} \end{pmatrix}, \qquad \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}, \tag{4.5}$$

and so it suffices to specify $U^{(p)}$ on such matrices, provided we preserve all relations between them. This is done by the formulas

$$U^{(p)} \begin{pmatrix} 1 & b \\ & 1 \end{pmatrix} \psi(x) = e\left(\frac{rbx^2}{p^k}\right)\psi(x), \tag{4.6}$$

$$U^{(p)} \begin{pmatrix} t & \\ & t^{-1} \end{pmatrix} \psi(x) = \Lambda_{r,p^k}(t)\psi(tx), \tag{4.7}$$

$$U^{(p)} \begin{pmatrix} & 1 \\ -1 & \end{pmatrix} \psi(x) = S_r\bigl(-1, p^k\bigr) \frac{1}{\sqrt{p^k}} \sum_{y \bmod p^k} \psi(y) e\left(\frac{2rxy}{p^k}\right). \tag{4.8}$$

It is easy to check that these satisfy (4.1). To see a verification that this prescription does indeed give a consistent definition (that is, that all relations between the generators (4.5) are satisfied), see, for example, [18]. Once we have this, then we get $U^{(p)}(AB) = U^{(p)}(A)U^{(p)}(B)$ automatically.

Remark 4.1. It is in fact the case that any projective representation of $\mathrm{SL}(2, \mathbf{Z}/p^k\mathbf{Z})$, p odd, can be modified to give a representation (and more generally, $\mathrm{SL}(2, \mathbf{Z}/m\mathbf{Z})$ if $m \neq 0 \bmod 4$)—this is due to Schur [22] when $k = 1$. See [17] and [2] for the general case.

4.4. $p = 2$. Here we restrict to the subgroup $\Gamma(4, 2^k)$, $k \geq 2$. The literature in this case is harder to come by, so we include complete proofs. We start by describing generators and relations for this group. More generally, let p be any prime and let $k \geq 2$. Let

$$\Gamma\bigl(p^2, p^k\bigr) := \bigl\{g \in \mathrm{SL}\bigl(2, \mathbf{Z}/p^k\mathbf{Z}\bigr) : g = I \bmod p^2\bigr\}.$$

LEMMA 7. *$\Gamma(p^2, p^k)$ has a presentation with generators $u_+(x)$, $u_-(y)$, $s(t)$, where $x, y, t \in \mathbf{Z}/p^k\mathbf{Z}$, $x, y \equiv 0 \bmod p^2$, $t \equiv 1 \bmod p^2$, and relations*

$$u_+(x)u_+(x') = u_+(x+x'), \tag{4.9}$$

$$u_-(y)u_-(y') = u_-(y+y'), \tag{4.10}$$

$$s(t)s(t') = s(tt'), \tag{4.11}$$

$$s(t)u_+(x)s(t)^{-1} = u_+\bigl(t^2x\bigr), \tag{4.12}$$

$$s(t)u_-(y)s(t)^{-1} = u_-\bigl(t^{-2}y\bigr), \tag{4.13}$$

$$s(d)u_+(a)u_-(b) = u_-\bigl(d^{-1}b\bigr)u_+(da), \quad d := (1+ab)^{-1}. \tag{4.14}$$

Proof. Let G be the abstract group with the above presentation. We get a map Ψ from G into $\Gamma(p^2, p^k)$ by taking

$$\Psi : u_+(x) \longmapsto \begin{pmatrix} 1 & x \\ & 1 \end{pmatrix}, \qquad u_-(y) \longmapsto \begin{pmatrix} 1 & \\ y & 1 \end{pmatrix}, \qquad s(t) \longmapsto \begin{pmatrix} t & \\ & t^{-1} \end{pmatrix}.$$

We verify that the relations hold in $\mathrm{SL}(2, \mathbf{Z}/p^k\mathbf{Z})$ so that Ψ is a homomorphism. Next, note that we have a Bruhat decomposition for $\Gamma(p^2, p^k)$: every element can be uniquely written in the form

$$\gamma = \begin{pmatrix} t & \\ & t^{-1} \end{pmatrix} \begin{pmatrix} 1 & x \\ & 1 \end{pmatrix} \begin{pmatrix} 1 & \\ y & 1 \end{pmatrix},$$

which follows from the formula

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \gamma = \begin{pmatrix} d^{-1} & \\ & d \end{pmatrix} \begin{pmatrix} 1 & bd \\ & 1 \end{pmatrix} \begin{pmatrix} 1 & \\ c/d & 1 \end{pmatrix}$$

(note that since $d = 1 \bmod p^2$, it is particularly invertible). This implies that the map Ψ is surjective. To see that Ψ is an isomorphism, it suffices to show that every element of the abstract group G can also be written in the form $g = s(t)u_+(x)u_-(y)$, since then by the uniqueness of the decomposition in $\Gamma(p^2, p^k)$, Ψ is also one-to-one.

With the aid of the first five relations, every word $W \in G$ can be written as a product:

$$W = s(t_1)u_+(x_1)u_-(y_1) \cdot \ldots \cdot s(t_n)u_+(x_n)u_-(y_n),$$

for some $n \geq 1$. We prove by induction on n that we can write $W = s(t)u_+(x)u_-(y)$ for $x, y = 0 \bmod p^2$, $t = 1 \bmod p^2$. When $n = 1$, this holds trivially, and for $n > 1$, we use the relations (4.13) and (4.14) to write

$$u_-(y_{n-1})s(t_n)u_+(x_n) = s(t_n)u_-\bigl(t_n^2 y_{n-1}\bigr)u_+(x_n) = s(t_n)s(t')u_+(x')u_-(y'),$$

and so

$$\begin{aligned} W &= s(t_1)u_+(x_1)u_-(y_1)\cdots s(t_{n-1})u_+(x_{n-1})s(t_n)s(t')u_+(x')u_-(y')u_-(y_n)\\ &= s(t_1)u_+(x_1)u_-(y_1)\cdots s(t'_{n-1})u_+(x''_{n-1})u_-(y''_{n-1}) \end{aligned}$$

after a further application of the first five relations. The result now follows by induction. □

We now specify the propagators $U^{(2)}(A)$ for the generators: for

$$\begin{pmatrix} 1 & a \\ & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} t & \\ & t^{-1} \end{pmatrix},$$

they are given by the same formulas (4.6) and (4.7). For the matrices

$$\begin{pmatrix} 1 & \\ b & 1 \end{pmatrix} = \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}^{-1} \begin{pmatrix} 1 & -b \\ & 1 \end{pmatrix} \begin{pmatrix} & 1 \\ -1 & \end{pmatrix},$$

we conjugate (4.6) by an analogue of the Fourier transform (4.8) and define

$$U^{(2)} \begin{pmatrix} 1 & \\ b & 1 \end{pmatrix} \psi(x) = \sum_{y \bmod 2^k} \psi(y) \frac{1}{2^k} \sum_{z \bmod 2^k} e\left(\frac{r\big(-bz^2 + 2z(y-x)\big)}{2^k} \right). \tag{4.15}$$

To show that this defines a representation, we have to check that all the relations of Lemma 7 are satisfied. The first five are fairly straightforward, bearing in mind that Λ is a character of the multiplicative group of residues $t = 1 \bmod 4$ (see (4.4)). The last relation (4.14) requires verifying an identity of Gauss sums: unwinding the action of the right and left-hand sides in (4.14), we must show that

$$\begin{aligned} &\Lambda(d) \sum_{z \bmod 2^k} \sum_{y \bmod 2^k} \psi(y) e\left(\frac{r}{2^k} \big(2yz - bz^2 - 2dxz + ad^2x^2 \big) \right) \\ &\quad = \sum_{z \bmod 2^k} \sum_{y \bmod 2^k} \psi(y) e\left(\frac{r}{2^k} \big(2yz - d^{-1}bz^2 - 2xz + ady^2 \big) \right). \end{aligned}$$

Now $d \equiv 1 \bmod 16$ implies that $\Lambda(d) = 1$ since d is then a square modulo 2^k, and if the identity is to hold for all ψ and all values of x, we obtain that for all x, y,

$$\begin{aligned} &\sum_{z \bmod 2^k} e\left(\frac{r}{2^k} \big(-bz^2 + 2z(y-dx) + ad^2x^2 \big) \right) \\ &\quad = \sum_{z \bmod 2^k} e\left(\frac{r}{2^k} \big(-d^{-1}bz^2 + 2z(y-x) + ady^2 \big) \right). \end{aligned} \tag{4.16}$$

We verify this in Appendix A.

5. Hecke operators. We now introduce a commutative group of unitary operators on $L^2(\mathbf{Z}/N\mathbf{Z})$ that commute with $U_N(A)$. For this, we have to bring in the theory of quadratic fields (see [19] for a survey in connection to cat maps).

5.1. Integral matrices and quadratic fields. Let $A \in \mathrm{SL}_2(\mathbf{Z})$ be a hyperbolic matrix: $|\operatorname{tr} A| > 2$. The eigenvalues α, α^{-1} of A generate a field extension $K = \mathbf{Q}(\alpha)$, which is a real quadratic field since $\operatorname{tr}(A)^2 > 4$. We denote by $\mathfrak{O}_K$ the ring of integers of K. The eigenvalues α, α^{-1} of A are units in $\mathfrak{O}_K$. Adjoining α to $\mathbf{Z}$ gives an order $\mathfrak{O} = \mathbf{Z}[\alpha] \subseteq \mathfrak{O}_K$ in K. We claim that there is an $\mathfrak{O}$-ideal $I \subset \mathfrak{O}$ so that the action of α by multiplication on I is equivalent to the action of A on $\mathbf{Z}^2$, in the sense that there is a basis of I with respect to which the matrix of α is precisely A.

The construction is as follows (refer to [23]): since α is an eigenvalue of A, there is a vector $v = (v_1, v_2)$ such that $vA = \alpha v$ and $v \in \mathfrak{O}^2$. Let $I := \mathbf{Z}[v_1, v_2] \subset \mathfrak{O}$. Then I is in an $\mathfrak{O}$-ideal, and the matrix of α acting on I by multiplication in the basis v_1, v_2 is precisely A.

Remark 5.1. It is easy to check that the above construction sets up a bijection between $\mathrm{GL}_2(\mathbf{Z})$-conjugacy classes of elements in $\mathrm{SL}_2(\mathbf{Z})$ with eigenvalues α, α^{-1} and ideal classes in the order $\mathfrak{O}$. (Recall that two ideals, I_1, I_2; are said to be in the same ideal class if there exist nonzero $a, b \in \mathfrak{O}$ so that $aI_1 = bI_2$.)

In the same way, the action of $\mathfrak{O}$ by multiplication on I gives us an embedding

$$\iota : \mathfrak{O} \hookrightarrow \mathrm{Mat}_2(\mathbf{Z})$$

so that $\gamma = x + y\alpha \in \mathfrak{O}$ corresponds to $xI + yA$. Moreover, the determinant of $xI + yA$ equals $\mathcal{N}(\gamma) = \gamma\bar{\gamma}$, where $\mathcal{N} : K \to \mathbf{Q}$ is the Galois norm. In particular, if $\gamma \in \mathfrak{O}$ has norm 1, then γ corresponds to an element in $\mathrm{SL}_2(\mathbf{Z})$, and if in addition $\gamma \equiv 1 \bmod 4\mathfrak{O}$, then γ corresponds to an element in $\Gamma(4)$.

5.2. Hecke operators. Given an integer $M \geq 1$, the embedding $\iota : \mathfrak{O} \hookrightarrow \mathrm{Mat}_2(\mathbf{Z})$ induces a map $\iota_M : \mathfrak{O}/M\mathfrak{O} \to \mathrm{Mat}_2(\mathbf{Z}/M\mathbf{Z})$, and the norm $\mathcal{N} : K \to \mathbf{Q}$ gives a well-defined map

$$\mathcal{N} : \mathfrak{O}/M\mathfrak{O} \longrightarrow \mathbf{Z}/M\mathbf{Z}.$$

We let $\mathscr{C}_A(M)$ be the group of norm-one elements in $\mathfrak{O}/M\mathfrak{O}$:

$$\mathscr{C}_A(M) = \ker\big[\mathcal{N} : (\mathfrak{O}/M\mathfrak{O})^* \longrightarrow (\mathbf{Z}/M\mathbf{Z})^*\big].$$

Similarly, replacing the order $\mathfrak{O}$ by the maximal order $\mathfrak{O}_K$, we set

$$\mathscr{C}_K(M) = \ker\big[\mathcal{N} : (\mathfrak{O}_K/M\mathfrak{O}_K)^* \longrightarrow (\mathbf{Z}/M\mathbf{Z})^*\big]$$

to be the norm-one elements in $\mathfrak{O}_K/M\mathfrak{O}_K$.

If $M = 2N$ is even, we set $\mathscr{C}_A^\theta(M)$ to be the elements of $\mathscr{C}_A(2N)$ that are congruent to 1 modulo $4\mathfrak{O}$ (resp., $2\mathfrak{O}$) if N is even (resp., odd). For M odd, we set $\mathscr{C}_A^\theta(M) = \mathscr{C}_A(M)$.

By construction, the image of $\mathcal{C}_A^\theta(2N)$ in $\mathrm{Mat}_2(\mathbf{Z}/2N\mathbf{Z})$ lies in $\Gamma(4,2N)$. Since α commutes with all elements in $\mathcal{C}_A^\theta(2N)$, we see that A commutes, modulo $2N$, with the elements in $\iota(\mathcal{C}_A^\theta(2N))$. Thus, by Corollary 6, the quantizations $U_N(\iota(\beta))$ of $\beta \in \mathcal{C}_A^\theta(2N)$ commute with $U_N(A)$ and with each other. We call these Hecke operators.

We need to know the number of Hecke operators.

LEMMA 8. *The number of elements of $\mathcal{C}_A^\theta(2N)$ satisfies*

$$N^{1-\epsilon} \ll \left|\mathcal{C}_A^\theta(2N)\right| \ll N^{1+\epsilon}, \quad \forall \epsilon > 0.$$

Proof. Since the reduction map $\mathfrak{O} \to \mathfrak{O}/4\mathfrak{O}$ has image of size 4^2, $\mathcal{C}_A^\theta(2N)$ has bounded index in $\mathcal{C}_A(2N)$. The inclusion $\mathfrak{O} \subset \mathfrak{O}_K$ induces a map $\mathfrak{O}/M\mathfrak{O} \to \mathfrak{O}_K/M\mathfrak{O}_K$, which has kernel and cokernel of size at most $[\mathfrak{O}_K : \mathfrak{O}]$, independent of M. Therefore, the induced map $\mathcal{C}_A(M) \to \mathcal{C}_K(M)$ on norm-one elements also has bounded kernel and cokernel. Thus, it suffices to prove the lemma in the case of the maximal order $\mathfrak{O}_K$. By the Chinese remainder theorem, it suffices to prove it in the case of prime powers, which is given in Appendix B by Lemma 19. □

5.3. Hecke eigenfunctions. The Hecke operators $U_N(\iota(\beta))$, $\beta \in \mathcal{C}_A^\theta(2N)$, commute with each other and with $U_N(A)$. Therefore, the eigenspaces of the unitary map $U_N(A)$ break up into joint eigenspaces of the Hecke operators. Such a joint eigenfunction we call a Hecke eigenfunction. In other words, there exist an orthonormal basis $\{\phi_i\}$ of $L^2(\mathbf{Z}/N\mathbf{Z})$ and characters λ_i of $\mathcal{C}_A^\theta(2N)$ such that ϕ_i are eigenfunctions of $U_N(A)$ and

$$U_N\bigl(\iota(\beta)\bigr)\phi_i = \lambda_i(\beta)\phi_i, \quad \forall \beta \in \mathcal{C}_A^\theta(2N).$$

We call such a basis of $L^2(\mathbf{Z}/N\mathbf{Z})$ a Hecke basis.

6. Ergodicity of Hecke eigenfunctions. In the next two sections, we show that if $\phi \in L^2(\mathbf{Z}/N\mathbf{Z})$ is a normalized Hecke eigenfunction, then the expectation values $\langle \mathrm{Op}_N(f)\phi, \phi\rangle$ converge to the classical phase-space average $\int_{\mathbf{T}^2} f$ for all smooth observables (see Theorem 1). In fact, we show something stronger.

THEOREM 9. *Let $\phi_i \in L^2(\mathbf{Z}/N\mathbf{Z})$, $i = 1, \dots, N$ be any orthonormal basis of Hecke eigenfunctions of $U_N(A)$. Then*

$$\sum_{i=1}^{N} \left| \bigl\langle \mathrm{Op}_N(f)\phi_i, \phi_i \bigr\rangle - \int_{\mathbf{T}^2} f(x)\, dx \right|^4 \ll_{f,\epsilon} N^{-1+\epsilon}.$$

6.1. Proof of Theorem 9. To prove this theorem, it suffices to prove it for the basic observables $f(x) = e(nx)$, $0 \neq n \in \mathbf{Z}^2$, that is, to show that the following theorem holds.

THEOREM 10. *Let $0 \neq n \in \mathbf{Z}^2$, and let $\phi_i \in L^2(\mathbf{Z}/N\mathbf{Z})$, $i = 1, \dots, N$ be any orthonormal basis of Hecke eigenfunctions of $U_N(A)$. Then*

$$\sum_{i=1}^{N} \left|\left\langle T_N(n)\phi_i, \phi_i \right\rangle\right|^4 \ll_\epsilon |n|^{16} N^{-1+\epsilon}, \quad N \longrightarrow \infty.$$

The proof of Theorem 9 from Theorem 10 is easy using the rapid decay of the Fourier coefficients of f. Indeed, write $f(x) = \sum_{n \in \mathbf{Z}^2} \widehat{f}(n) e(nx)$, so that $\mathrm{Op}_N(f) = \sum_{n \in \mathbf{Z}^2} \widehat{f}(n) T_N(n)$. Therefore,

$$\sum_{i=1}^{N} \left| \left\langle \mathrm{Op}_N(f)\phi_i^N, \phi_i^N \right\rangle - \int_{\mathbf{T}^2} f(x)\,dx \right|^4$$

$$= \sum_{i=1}^{N} \left| \sum_{0 \neq n \in \mathbf{Z}^2} \widehat{f}(n) \left\langle T_N(n)\phi_i, \phi_i \right\rangle \right|^4 \leq \sum_{i=1}^{N} \sum_{n_1, \dots, n_4 \neq 0} \prod_{k=1}^{4} \left| \widehat{f}(n_k) \left\langle T_N(n_k)\phi_i, \phi_i \right\rangle \right|.$$

For notational convenience, we write

$$t_i(n) := \left|\left\langle T_N(n)\phi_i, \phi_i \right\rangle\right|.$$

Now interchange the order of summation and apply Cauchy-Schwartz twice. For fixed n_1, n_2, n_3, n_4,

$$\sum_{i=1}^{N} t_i(n_1) t_i(n_2) t_i(n_3) t_i(n_4)$$

$$\leq \left(\sum_{i=1}^{N} \left(t_i(n_1) t_i(n_2) \right)^2 \right)^{1/2} \left(\sum_{i=1}^{N} \left(t_i(n_3) t_i(n_4) \right)^2 \right)^{1/2} \leq \prod_{k=1}^{4} \left(\sum_{i=1}^{N} t_i(n_k)^4 \right)^{1/4}.$$

Now use Theorem 10. For $n_k \neq 0$,

$$\left(\sum_{i=1}^{N} t_i(n_k)^4 \right)^{1/4} \ll |n_k|^4 N^{-1/4+\epsilon},$$

and so we get

$$\sum_{i=1}^{N} t_i(n_1) t_i(n_2) t_i(n_3) t_i(n_4) \ll N^{-1+\epsilon'} \prod_{k=1}^{4} |n_k|^4.$$

Now sum over all possible $n_k \neq 0$ to find

$$\sum_{i=1}^{N} \left| \left\langle \mathrm{Op}_N(f)\phi_i, \phi_i \right\rangle - \int_{\mathbf{T}^2} f(x)\,dx \right|^4 \ll N^{-1+\epsilon} \left(\sum_{n \neq 0} \widehat{f}(n) |n|^4 \right)^4,$$

which proves Theorem 9. □

6.2. Reduction to a counting problem. We first reduce Theorem 10 to a counting problem.

Proposition 11. *Fix $0 \neq n = \iota(\nu) \in \mathbf{Z}^2$, $\nu \in I$. Then for any Hecke basis of eigenfunctions ϕ_i,*

$$\sum_{i=1}^{N} \left|\left\langle T_N(n)\phi_i, \phi_i\right\rangle\right|^4 \\ \leq \frac{N}{\left|\mathscr{C}_A^\theta(2N)\right|^4} \#\left\{\beta_i \in \mathscr{C}_A^\theta(2N) : \nu\left(\beta_1 - \beta_2 + \beta_3 - \beta_4\right) = 0 \bmod NI\right\}.$$

In order to prove Proposition 11, we define for $n = \iota(\nu)$, $0 \neq \nu \in I$,

$$D = D(n) = \frac{1}{\left|\mathscr{C}_A^\theta(2N)\right|} \sum_{\beta \in \mathscr{C}_A^\theta(2N)} U_N\left(\iota(\beta)\right)^{-1} T_N(n) U_N\left(\iota(\beta)\right).$$

If (t_{ij}) is the matrix coefficients of $T_N(n)$ expressed in the eigenvector basis $\{\phi_k\}$ so that $t_{ij} = \langle T_N(n)\phi_i, \phi_j\rangle$, then we see that

$$D_{ij} = \frac{1}{\left|\mathscr{C}_A^\theta(2N)\right|} \sum_{\beta \in \mathscr{C}_A^\theta(2n)} \lambda_i(\beta)\overline{\lambda_j(\beta)} t_{ij}.$$

Since the sum of a nontrivial character over all elements in a group vanishes, we have

$$D_{ij} = \begin{cases} t_{ij}, & \text{if } \lambda_i = \lambda_j, \\ 0, & \text{otherwise.} \end{cases} \tag{6.1}$$

Lemma 12. *With D defined as above, we have*

$$\sum_{\lambda_i = \lambda_j} |t_{ij}|^4 \leq \operatorname{tr}\left((D^* D)^2\right).$$

Proof. Let $D = (d_{ij}) = (v_i)$ where the v_i's are the column vectors of D. Examining the (k, k)-entry of $(D^*D)^2$, we get

$$\left((D^* D)^2\right)_{kk} = \sum_i \langle v_i, v_k\rangle\langle v_k, v_i\rangle = \sum_i \left|\langle v_i, v_k\rangle\right|^2,$$

and hence,

$$\operatorname{tr}\left((D^* D)^2\right) \geq \sum_k \left|\langle v_k, v_k\rangle\right|^2 \geq \sum_{i,j} |d_{ij}|^4.$$

The result now follows from (6.1). □

LEMMA 13. *We have*

$$\operatorname{tr}\big((D^*D)^2\big) \le \frac{N}{\big|\mathscr{C}_A^\theta(2N)\big|^4}\Big|\big\{\beta_i \in \mathscr{C}_A^\theta(2N) : \nu(\beta_1-\beta_2+\beta_3-\beta_4) \equiv 0 \bmod NI\big\}\Big|.$$

Proof. Recall that by (3.1), since $n \cdot \iota(\beta) = \iota(\nu\beta)$ for $\beta \in \mathfrak{O}$, $n = \iota(\nu)$,

$$U_N\big(\iota(\beta)\big)^{-1} T_N(n) U_N\big(\iota(\beta)\big) = T_N\big(\iota(\nu\beta)\big).$$

Also note that $T_N(w)^* = T_N(-w)$ for all w by (2.5). Substituting the definition of D and expanding, we see that $(D^*D)^2$ is given by $1/|\mathscr{C}_A^\theta(2N)|^4$ times a sum, ranging over all $\beta_1, \beta_2, \beta_3, \beta_4 \in \mathscr{C}_A^\theta(2N)$, of terms

$$\begin{aligned} &T_N\big(\iota(\nu\beta_1)\big)T_N\big(-\iota(\nu\beta_2)\big)T_N\big(\iota(\nu\beta_3)\big)T_N\big(-\iota(\nu\beta_4)\big) \\ &\qquad = \gamma(\beta_1,\beta_2,\beta_3,\beta_4) T_N\Big(\iota\big(\nu(\beta_1-\beta_2+\beta_3-\beta_4)\big)\Big), \end{aligned}$$

where $\gamma(\beta_1,\beta_2,\beta_3,\beta_4)$ has absolute value 1 (see (2.6)). Now take the trace; by Lemma 4, the absolute value of the trace of $T_N(n)$ equals N if $n \equiv (0,0) \bmod N$, and equals zero otherwise. The result now follows by taking absolute values and summing over all $\beta_1, \beta_2, \beta_3, \beta_4 \in \mathscr{C}_A^\theta(2N)$. □

It remains to estimate the number of solutions of

$$\nu(\beta_1-\beta_2+\beta_3-\beta_4) \equiv 0 \bmod NI, \quad \beta_i \in \mathscr{C}_A^\theta(2N). \tag{6.2}$$

PROPOSITION 14. *The number of solutions to (6.2) is bounded by $O(|\mathcal{N}(\nu)|^8 N^{2+\epsilon})$.*

6.3. Proof of Theorem 10: Conclusion. By Proposition 11, we need a suitable upper bound for the number of solutions of (6.2) and a lower bound for the number of elements of $\mathscr{C}_A^\theta(2N)$. By Proposition 14, the number of solutions is at most $|\mathcal{N}(\nu)|^8 N^{2+\epsilon}$. Note that $|\mathcal{N}(\nu)| \ll |n|^2$. From Lemma 8, we obtain that $|\mathscr{C}_A^\theta(2N)| \gg N^{1-\epsilon}$ and the result follows.

7. Counting solutions.

In this section, we prove Proposition 14.

7.1. A reduction. Since $NI \subseteq N\mathfrak{O} \subseteq N\mathfrak{O}_K$, the number of solutions to (6.2) is bounded by the number of solutions to

$$\nu\big(\beta_1-\beta_2+\beta_3-\beta_4\big) \in N\mathfrak{O}_K, \quad \beta_i \in \mathscr{C}_A^\theta(2N).$$

Moreover, at the cost of increasing slightly the number of solutions, we may omit the parity condition on β_i, replacing $\mathscr{C}_A^\theta(2N)$ by $\mathscr{C}_A(2N)$.

The inclusion $\mathfrak{O} \subset \mathfrak{O}_K$ induces a map $\mathfrak{O}/M\mathfrak{O} \to \mathfrak{O}_K/M\mathfrak{O}_K$, which has kernel and cokernel of size at most $[\mathfrak{O}_K : \mathfrak{O}]$, independent of M. Therefore, the induced map

$$\begin{aligned} \mathscr{C}_A(M) = \ker\big[(\mathfrak{O}/M\mathfrak{O})^* \longrightarrow (\mathbf{Z}/M\mathbf{Z})^*\big] &\longrightarrow \mathscr{C}_K(M) \\ &= \ker\big[(\mathfrak{O}_K/M\mathfrak{O}_K)^* \longrightarrow (\mathbf{Z}/M\mathbf{Z})^*\big] \end{aligned}$$

on norm-one elements also has bounded kernel and cokernel. Thus, up to a bounded factor (depending on A but not on N or ν), the number of solutions to (6.2) is bounded by the number of solutions of

$$\nu\big(\beta_1-\beta_2+\beta_3-\beta_4\big)=0 \bmod N\mathfrak{O}_K, \quad \beta_i\in\mathscr{C}_K(2N). \tag{7.1}$$

At the cost of increasing the number of solutions, we multiply (7.1) by the Galois conjugate $\bar{\nu}$ to get

$$\mathcal{N}(\nu)\big(\beta_1-\beta_2+\beta_3-\beta_4\big)=0 \bmod N\mathfrak{O}_K, \quad \beta_i\in\mathscr{C}_K(2N).$$

Setting

$$N'=\frac{N}{\gcd(N,\mathcal{N}(\nu))},$$

this equation is equivalent to

$$\beta_1-\beta_2+\beta_3-\beta_4=0 \bmod N'\mathfrak{O}_K, \quad \beta_i\in\mathscr{C}_K(2N). \tag{7.2}$$

Next, note that the reduction map $\mathfrak{O}_K/rs\mathfrak{O}_K\to\mathfrak{O}_K/r\mathfrak{O}_K$ has kernel $r\mathfrak{O}_K/rs\mathfrak{O}_K \simeq \mathfrak{O}_K/s\mathfrak{O}_K$ of size s^2, and so the induced map on norm-one elements $\mathscr{C}_K(rs)\to\mathscr{C}_K(r)$ has kernel of order at most s^2. (This is crude, but sufficient for our purposes.) Thus, the reduction map $\mathscr{C}_K(2N)\to\mathscr{C}_K(N')$ has kernel of size at most $4\gcd(N,\mathcal{N}(\nu))^2\le 4|\mathcal{N}(\nu)|^2$. Therefore, the number of solutions of (7.2) is bounded by $(4|\mathcal{N}(\nu)|^2)^4$ times the number of solutions of the equation

$$\beta_1-\beta_2+\beta_3-\beta_4=0 \bmod N'\mathfrak{O}_K, \quad \beta_i\in\mathscr{C}_K(N'). \tag{7.3}$$

Equation (7.3) is invariant under Galois conjugation, and we obtain a second equation (note that $\bar{\beta}=\beta^{-1}$ since $\mathcal{N}(\beta)=1 \bmod N'$):

$$\beta_1^{-1}-\beta_2^{-1}+\beta_3^{-1}-\beta_4^{-1}\equiv 0 \bmod N'\mathfrak{O}_K. \tag{7.4}$$

7.2. A transformation. We thus have a system of equations (7.3) and (7.4), which we transform using the following lemma.

Lemma 15. *If x,y,z,w are invertible, then the system of equations*

$$\begin{cases} x+y=z+w \\ x^{-1}+y^{-1}=z^{-1}+w^{-1}\end{cases}$$

is equivalent to the system

$$\begin{cases} (z-x)(z-y)(x+y)=0 \\ w=x+y-z.\end{cases}$$

Proof. From the second equation, we get

$$\frac{x+y}{xy}=\frac{z+w}{zw},$$

or

$$(x+y)zw=(z+w)xy.$$

The first equation gives us that $w=x+y-z$; inserting it in $(x+y)zw=(z+w)xy$, we get

$$(x+y)z(x+y-z)=(x+y)xy$$

or

$$0=(x+y)\big(zx+zy-z^2-xy\big)=-(z-x)(z-y)(x+y). \qquad \square$$

Thus, by Lemma 15, the system of equations (7.3) and (7.4) is equivalent to the system

$$(\beta_3-\beta_1)(\beta_3-\beta_2)(\beta_1+\beta_2)\equiv 0 \bmod N'\mathfrak{O}_K, \tag{7.5}$$

$$\beta_4\equiv\beta_1-\beta_2+\beta_3 \bmod N'\mathfrak{O}_K, \tag{7.6}$$

with $\beta_i\in\mathscr{C}_K(N')$.

Since β_4 is determined by β_1,β_2,β_3, we may ignore (7.6) (at the cost of increasing the number of solutions, since being in $\mathscr{C}_K(N')$ is a nonempty condition). Multiplying equation (7.5) by β_3^{-3} and letting $\beta_i'=\beta_i/\beta_3$, we obtain

$$\big(1-\beta_1'\big)\big(1-\beta_2'\big)\big(\beta_1'+\beta_2'\big)\equiv 0 \bmod N'\mathfrak{O}_K. \tag{7.7}$$

Since β_3 is arbitrary, the number of solutions of (7.5) is bounded by $|\mathscr{C}_K(N')|$ times the number of solutions in $\beta_1',\beta_2'\in\mathscr{C}_K(N')$ to (7.7).

7.3. Prime powers. By the Chinese remainder theorem, the number of solutions to (7.7) is multiplicative, and we may concentrate on the prime power case. Thus, we need to count the solutions to the equation

$$\big(1-\beta_1'\big)\big(1-\beta_2'\big)\big(\beta_1'+\beta_2'\big)\equiv 0 \bmod p^k\mathfrak{O}_K \tag{7.8}$$

with $\beta_i'\in\mathfrak{O}_K/p^k\mathfrak{O}_K$, $\mathcal{N}(\beta_i')=1 \bmod p^k$.

We first recall some properties of primes in quadratic extensions: let $P|p$ be a prime in $\mathfrak{O}_K$ lying above p, and let e denote the ramification index, that is, the largest integer e such that $P^e|p\mathfrak{O}_K$. Since K is quadratic, $e\in\{1,2\}$ and $e=1$ for all but finitely many primes p. If $e=2$, then p is said to be ramified. If $e=1$, then p is called unramified, and one of two things can happen: either $p\mathfrak{O}_K=P$ is still a prime ideal, in which case p is said to be inert, or $p\mathfrak{O}_K=P\overline{P}$, in which case p is said to split.

Now, fix a prime p with ramification index e, be it 1 or 2. The norm map $\mathcal{N} : \mathfrak{O}_K \to \mathbf{Z}$ gives a well-defined homomorphism:

$$\left(\mathfrak{O}_K / P^{ek}\right)^{\times} \longrightarrow \left(\mathbf{Z}/p^k\right)^{\times}.$$

We let

$$\left(\mathfrak{O}_K / P^{ek}\right)^{1}$$

be the kernel of this map, that is, the group of norm-one elements. For $l \leq ek$, we let

$$\left(\left(1+P^l\right)/\left(1+P^{ek}\right)\right)^1$$

be the norm-one elements in the subgroup $(1+P^l)/(1+P^{ek})$; these are precisely the norm-one elements that reduce to 1 modulo P^l.

LEMMA 16. *There is a constant $c > 1$ so that the number of solutions of (7.8) is at most ckp^k.*

Proof. Equation (7.8) is invariant under Galois conjugation; therefore, its solutions in $\mathfrak{O}_K/p^k\mathfrak{O}_K$ correspond bijectively to solutions $\beta_i' \in \mathfrak{O}_K/P^{ek}$, $\mathcal{N}(\beta_i') = 1 \bmod p^k$ (this is, of course, only an issue in the split case where $\mathfrak{O}_K/p^k\mathfrak{O}_K \simeq \mathfrak{O}_K/P^k \times \mathfrak{O}_K/\overline{P}^k$). Thus, we need to count solutions of

$$\left(1-\beta_1'\right)\left(1-\beta_2'\right)\left(\beta_1'+\beta_2'\right) \equiv 0 \bmod P^{ek} \tag{7.9}$$

with $\beta_i' \in \mathfrak{O}_K/P^{ek}$, $\mathcal{N}(\beta_i') = 1 \bmod p^k$.

We first assume that p is odd. Since $\beta_1' \equiv \beta_2' \equiv 1 \bmod P$ implies that $\beta_1' + \beta_2' \equiv 2 \not\equiv 0 \bmod P$, we see that at most two of the factors in (7.9) can be congruent to zero modulo P. Moreover, we may assume that the third factor is nonzero by multiplying by a suitable β and permuting the variables. (Of course, we must then compensate by multiplying the number of solutions by $\binom{3}{2}$.) Now if the product is zero modulo P^{ek}, then there is some $0 \leq n \leq ek$ such that one factor is zero modulo P^n and the other is zero modulo P^{ek-n}. Thus, the number of solutions to (7.9) equals

$$\binom{3}{2}\sum_{n=1}^{ek-1}\left|\left(\left(1+P^n\right)/\left(1+P^{ek}\right)\right)^1\right| \times \left|\left(\left(1+P^{ek-n}\right)/\left(1+P^{ek}\right)\right)^1\right| + 2\left|\left(\mathfrak{O}_K/P^{ek}\right)^1\right|.$$

Using Lemma 20, we obtain

$$\left|\left(\left(1+P^n\right)/\left(1+P^{ek}\right)\right)^1\right| \times \left|\left(\left(1+P^{ek-n}\right)/\left(1+P^{ek}\right)\right)^1\right| \leq p^{k+e-1},$$

and by Lemma 19, we obtain

$$\left|\left(\mathfrak{O}_K/P^{ek}\right)^1\right| \leq 2(p+1)p^{k-1}.$$

Hence, for p odd, the total number of solutions to (7.9) is bounded by

$$4(p+1)p^{k-1}+3(ek-1)p^{e-1}p^k \ll kp^k$$

(since $e=1$ for all but finitely many primes).

If $p=2$, it is no longer true that only two factors can be zero modulo P. However, $\beta_1 \equiv \beta_2 \equiv 1 \bmod P^{e+1}$ implies that $\beta_1+\beta_2 \equiv 2 \bmod P^{e+1}$. Since $2\mathfrak{O}_K = P^e$, we see that if two factors are zero modulo P^{e+1}, then the third factor can be congruent to 0 at most modulo P^e. We may thus bound the number of solutions by counting the number of ways the product of two factors can be equal to zero modulo P^{ek-e}. This we can do as we did for odd primes, and we obtain the same bound as before, except that we lose an additional factor of at most

$$\left|\left((1+P^{ek-e})/(1+P^{ek})\right)^1\right|^4 \ll 2^{O(e)} = O(1).$$

This proves Lemma 16. □

7.4. Proof of Proposition 14. By multiplying over all primes, we see from Lemma 16 that the number of solutions of equation (7.7) is $O((N')^{1+\epsilon})$. Therefore, we see that the number of solutions of (7.5) is $O((N')^{2+\epsilon})$ since $|\mathscr{C}_K(N')| \ll (N')^{1+\epsilon}$ by Lemma 19. This gives a bound for the solutions of (7.3), and multiplying by $|\mathcal{N}(\nu)|^8$ gives a bound for the number of solutions of (7.2). In turn, by the reasoning in Section 7.1, we get a bound of $O(|\mathcal{N}(\nu)|^8 N^{2+\epsilon})$ on the solutions of (6.2).

Appendices

Appendix A. An identity of Gauss sums. For Section 4, we need to prove (4.16). To prove it we need a lemma about Gauss sums. Given an integer x, we define its *dyadic valuation*, $v(x)$, by $x = 2^{v(x)}x_0$, where x_0 is an odd integer. Let

$$G(b,c) = \sum_{z \bmod 2^k} e\left(\frac{r}{2^k}\left(-bz^2+2cz\right)\right).$$

Lemma 17. *If $v(c) < v(b) < k$, then*

$$G(b,c) = \begin{cases} 2^k, & \textit{if } v(b)=k-1 \textit{ and } v(c)=k-2, \\ 0, & \textit{otherwise.} \end{cases}$$

Proof. We may write

$$G(b,c) = \sum_{z \bmod 2^k} e\left(\frac{2cr}{2^k}\left(-\beta z^2+z\right)\right),$$

where β is an integer satisfying $2c\beta \equiv b \bmod 2^k$. Let $n = k-1-v(c)$; it is the smallest integer n such that $e((2cr/2^k)x) = 1$ for all $x \equiv 0 \bmod 2^n$.

First, assume that $n > 1$. Let $\epsilon = \epsilon_0 2^{n-1}$ be such that $e((2cr/2^k)\epsilon) \neq 1$. Making the change of variables $z \to z+\epsilon$, we see that

$$G(b,c) = \sum_{z \bmod 2^k} e\left(\frac{2cr}{2^k}\left(-\beta\left(z^2+2\epsilon z+\epsilon^2\right)+z+\epsilon\right)\right) = G(b,c)e\left(\frac{2cr}{2^k}\epsilon\right)$$

since $2\epsilon z+\epsilon^2 \equiv 0 \bmod 2^n$. But $e((2cr/2^k)\epsilon) \neq 1$, and therefore, $G(b,c) = 0$.

If $n \leq 1$, then as $n = k-1-v(c)$ and $v(c) < v(b) < k$, we must have $n = 1$, $v(c) = k-2$, and $v(b) = k-1$. Hence, $\beta \equiv 1 \bmod 2$. Moreover, if $n = 1$, we must have $e(2crx/2^k) = e(x/2)$. Thus

$$G(b,c) = \sum_{z \bmod 2^k} e\left(\frac{z^2+z}{2}\right) = 2^k$$

since $z^2+z \equiv 0 \bmod 2$ for all z. □

Proposition 18. *The following equality holds for all x, y:*

$$\sum_{z \bmod 2^k} e\left(\frac{r}{2^k}\left(-bz^2+2z(y-dx)+ad^2x^2\right)\right)$$
$$= \sum_{z \bmod 2^k} e\left(\frac{r}{2^k}\left(-d^{-1}bz^2+2z(y-x)+ady^2\right)\right).$$

Proof. The case $v(b) \geq k$, that is, $b \equiv 0 \bmod 2^k$, implies that $d \equiv 1 \bmod 2^k$ and the equality holds trivially. We may thus assume that $v(b) < k$.

We begin by noting that since $y-dx = d(d^{-1}y-x) = d(y-x+aby)$, we see that $v(y-x) < v(b)$ implies that $v(y-dx) < v(b)$; putting $x' = d^{-1}x$, we see that the converse holds, and hence, $v(y-x) < v(b)$ if and only if $v(y-dx) < v(b)$.

First case: $v(y-x) < v(b)$. Putting $c = y-x$, $c = y-dx$, respectively, and applying Lemma 17, we see that both sides are zero except when $v(c) = k-2$ and $v(b) = k-1$. For the exceptional case, we note that $v(b) = k-1$ implies that $d^{-1} = 1+ab \equiv 1 \bmod 2^k$, and the same holds for d. Moreover, $v(c) = k-2$ means that $x \equiv y \bmod 2^{k-2}$, and since $4 \mid a$, we see that

$$\text{LHS} = 2^k e\left(\frac{r}{2^k}ad^2x^2\right) = 2^k e\left(\frac{r}{2^k}ady^2\right) = \text{RHS}.$$

Second case: $v(y-x) \geq v(b)$. As remarked above, this means that $v(y-dx) \geq v(b)$. We may thus complete the squares inside the exponentials, and we get

$$\text{LHS} = \sum_{z \bmod 2^k} e\left(\frac{r}{2^k}\left(-b\left(z-\frac{y-dx}{b}\right)^2+\frac{(y-dx)^2}{b}+ad^2x^2\right)\right)$$

and

$$\text{RHS} = \sum_{z \bmod 2^k} e\left(\frac{r}{2^k}\left(-d^{-1}b\left(z - \frac{d(y-x)}{b}\right)^2 + \frac{d(y-x)^2}{b} + ady^2\right)\right).$$

After changing variables and taking constants outside, we get

$$\text{LHS} = e\left(\frac{r}{2^k}\left(\frac{(y-dx)^2}{b} + ad^2x^2\right)\right) \sum_{z \bmod 2^k} e\left(\frac{r}{2^k}\left(-bz^2\right)\right)$$

and

$$\text{RHS} = e\left(\frac{r}{2^k}\left(\frac{d(y-x)^2}{b} + ady^2\right)\right) \sum_{z \bmod 2^k} e\left(\frac{r}{2^k}\left(-d^{-1}bz^2\right)\right).$$

Now, $d \equiv 1 \bmod 16$ means that d is a square modulo 2^k. Changing variables by $z \to \sqrt{d}z$ in the second sum, we see that the sums are equal, and we are left to prove that

$$e\left(\frac{r}{2^k}\left(\frac{(y-dx)^2}{b} + ad^2x^2\right)\right) = e\left(\frac{r}{2^k}\left(\frac{d(y-x)^2}{b} + ady^2\right)\right).$$

This follows from the equality

$$\frac{(y-dx)^2}{b} + ad^2x^2 = \frac{d(y-x)^2}{b} + ady^2.$$

Collecting terms, it is equivalent to

$$\begin{aligned} 0 &= ad\left(y^2 - dx^2\right) + b^{-1}\left(dy^2 + dx^2 - 2dxy - y^2 - d^2x^2 + 2dxy\right) \\ &= ad\left(y^2 - dx^2\right) + b^{-1}\left(y^2(d-1) + x^2\left(d - d^2\right)\right) \\ &= ad\left(y^2 - dx^2\right) + (d-1)b^{-1}\left(y^2 - dx^2\right), \end{aligned}$$

which follows from the identity

$$ad + \frac{(d-1)}{b} = d\left(a + \frac{1-1/d}{b}\right) = d\left(a + \frac{1-(1+ab)}{b}\right) = d\left(a - \frac{ab}{b}\right) = 0. \qquad \square$$

Appendix B. Counting norm-one elements. Let e be the ramification index of a prime p in $\mathfrak{O}_K$, that is, the largest integer such that $P^e \mid p\mathfrak{O}_K$, where $P \subset \mathfrak{O}_K$ is any prime ideal dividing $p\mathfrak{O}_K$. Since K is quadratic, $e \in \{1, 2\}$. If $e = 2$, then p is said to be ramified. If $e = 1$, then p is called unramified, and one of two things can happen: either $p\mathfrak{O}_K = P$, in which case p is said to be inert, or $p\mathfrak{O}_K = P\overline{P}$, in which case p is said to be split.

Now fix a prime p with ramification index e, be it 1 or 2. The norm map

$$\mathcal{N} : \mathfrak{O}_K \longrightarrow \mathbf{Z}$$

descends modulo p^k and gives a homomorphism

$$\left(\mathfrak{O}_K / P^{ek}\right)^\times \longrightarrow \left(\mathbf{Z}/p^k\right)^\times.$$

We let $(\mathfrak{O}_K / P^{ek})^1$ be the kernel of this map, that is, the group of norm-one elements. For $l \leq ek$, we let

$$\left((1+P^l)\big/(1+P^{ek})\right)^1$$

be the norm-one elements in the subgroup $(1+P^l)/(1+P^{ek})$; these are precisely the norm-one elements that reduce to 1 modulo P^l.

LEMMA 19. *We have*

$$\left|\left(\mathfrak{O}_K / P^{ek}\right)^1\right| = \begin{cases} (p-1)p^{k-1}, & \text{if } p \text{ is split,} \\ (p+1)p^{k-1}, & \text{if } p \text{ is inert,} \\ 2p^k, & \text{if } p \text{ is ramified.} \end{cases}$$

Proof. Recall first from class field theory [4] that the index (in $\mathbf{Z}_p^\times$) of the image of the units in the p-adic completion of $\mathfrak{O}_K$ under the norm map equals the ramification index e. We split the proof into three parts.

The split case. If p splits in K, then $p\mathfrak{O}_K = P_1 P_2$ where P_1, P_2 are prime ideals in $\mathfrak{O}_K$, and where $P_2 = \overline{P_1}$. The map $x \to \bar{x}$ gives an isomorphism between $\mathfrak{O}_K / P_1^k$ and $\mathfrak{O}_K / P_2^k$. This, together with the Chinese remainder theorem, gives

$$\mathfrak{O}_K \big/ p^k \mathfrak{O}_K \simeq \mathfrak{O}_K \big/ P_1^k \times \mathfrak{O}_K \big/ P_2^k \simeq \mathfrak{O}_K \big/ P_1^k \times \mathfrak{O}_K \big/ P_1^k,$$

where $x \in \mathfrak{O}_K / p^k \mathfrak{O}_K$ is mapped to $(x, \bar{x}) \in \mathfrak{O}_K / P_1^k \times \mathfrak{O}_K / P_1^k$. Furthermore, $\mathfrak{O}_K / P_1^k \simeq \mathbf{Z}/p^k\mathbf{Z}$, and therefore,

$$\mathfrak{O}_K \big/ p^k \mathfrak{O}_K \simeq \mathbf{Z}\big/p^k\mathbf{Z} \times \mathbf{Z}\big/p^k\mathbf{Z}. \tag{B.1}$$

Under this isomorphism, Galois conjugation maps $(x, y) \in \mathbf{Z}/p^k\mathbf{Z} \times \mathbf{Z}/p^k\mathbf{Z}$ to (y, x). Thus the natural embedding of $\mathbf{Z}/p^k\mathbf{Z}$ in $\mathfrak{O}_K / p^k \mathfrak{O}_K \simeq \mathbf{Z}/p^k\mathbf{Z} \times \mathbf{Z}/p^k\mathbf{Z}$ consists of elements of the form (x, x) and the image of (x, y) under the norm map is (xy, xy). Hence, the norm-one elements in $\mathfrak{O}_K / p^k \mathfrak{O}_K$ correspond to elements of the form $(x, y) \in \mathbf{Z}/p^k\mathbf{Z} \times \mathbf{Z}/p^k\mathbf{Z}$ such that $xy = 1$, and the number of such elements is $(p-1)p^{k-1}$.

The inert case. Here $e = 1$ and the local norm map is onto $\mathbf{Z}_p^\times$. Reducing modulo p, we get an exact sequence

$$1 \longrightarrow (\mathfrak{O}_K/P^k)^1 \longrightarrow (\mathfrak{O}_K/P^k)^\times \longrightarrow (\mathbf{Z}/p^k)^\times \longrightarrow 1.$$

Hence,

$$\left|(\mathfrak{O}_K/P^k)^1\right| = \frac{\left|(\mathfrak{O}_K/P^k)^\times\right|}{\left|(\mathbf{Z}/p^k)^\times\right|} = (p+1)p^{k-1}.$$

The ramified case. Here the image of the norm map in $\mathbf{Z}_p^\times$ is of index 2, and thus the image of the norm in $(\mathbf{Z}/p^k)^\times$ has cardinality $(p-1)p^{k-1}/2$. Consequently,

$$\left|(\mathfrak{O}_K/P^{ek})^1\right| = 2\frac{\left|(\mathfrak{O}_K/P^{ek})^\times\right|}{(p-1)p^{k-1}}.$$

Now

$$\left|(\mathfrak{O}_K/P^{ek})^\times\right| = \left|(\mathfrak{O}_K/P)^\times\right| \times \left|(1+P)/(1+P^{ek})\right| = (p-1)p^{ek-1},$$

and since $e=2$, we get

$$\left|(\mathfrak{O}_K/P^{ek})^1\right| = 2\frac{(p-1)p^{2k-1}}{(p-1)p^{k-1}} = 2p^k. \qquad \square$$

We also need to know the number of norm-one elements that reduce to 1 modulo P^l.

Lemma 20. *We have*

$$\left|\left((1+P^l)/(1+P^{ek})\right)^1\right| = \begin{cases} p^{k-l}, & \textit{if } p \textit{ is split or inert,} \\ K_p \times p^{k+\lceil l/2 \rceil - l}, & \textit{if } p \textit{ is ramified,} \end{cases}$$

where $K_p = 1$ if p is odd, and $K_2 = 1$ or 2.

Proof. The split case. From the previous discussion of the isomorphism in (B.1), we see that norm-one elements congruent to 1 modulo P_1^l correspond to elements $(x, x^{-1}) \in \mathbf{Z}/p^k\mathbf{Z} \times \mathbf{Z}/p^k\mathbf{Z}$, such that $x \equiv 1 \bmod p^l$. The number of such elements is $|(1+p^l)/(1+p^k)| = p^{k-l}$.

The inert case. If p is odd, then $x \to x^2$ is an automorphism of $(1+P^l)/(1+P^k)$ since the order of the group is odd. Thus, the norm is locally onto in the sense that the map

$$\mathcal{N} : (1+P^l)/(1+P^k) \longrightarrow (1+p^l)/(1+p^k)$$

is onto.

If p is even (and inert), then squaring is not an automorphism as $(1+x)^2 = 1+2x+x^2$. However, $1+p^l \subset 1+P^l$ and squaring maps $(1+p^l)/(1+p^k)$ onto $(1+p^{l+1})/(1+p^k)$. Thus,

$$(1+p^{l+1})/(1+p^k) \subset \mathcal{N}\left((1+P^l)/(1+P^k)\right),$$

which shows that the image of the norms must be either $(1+p^{l+1})/(1+p^k)$ or $(1+p^l)/(1+p^k)$. (There are no subgroups in between!) We show that the former holds; since 2 is unramified, the discriminant of K is odd and $\mathfrak{O}_K = \mathbf{Z}[1+\sqrt{d_k}/2]$. Hence, $\operatorname{tr}(\mathfrak{O}_K) = \mathbf{Z}$, and there exists $x \in \mathfrak{O}_K$ with odd trace. Now

$$\mathcal{N}\big(1+p^k x\big) = 1 + p^k \operatorname{tr}(x) + p^{2k}\mathcal{N}(x)$$

shows that the image must be $(1+p^l)/(1+p^k)$.

Thus, whether p is even or odd, the norm map is locally onto, and hence,

$$\left|\big((1+P^l)/(1+P^k)\big)^1\right| = \frac{\left|\big((1+P^l)/(1+P^k)\big)^\times\right|}{\left|\big((1+p^l)/(1+p^k)\big)^\times\right|} = p^{k-l}.$$

The ramified case. First, we note that

$$\mathcal{N}\big((1+P^l)/(1+P^{ek})\big) \subset \big(1+p^{\lceil l/2\rceil}\big)/\big(1+p^k\big). \tag{B.2}$$

Arguing as before that squares are in the image of the norm, we see that equality holds for p odd, and we obtain

$$\begin{aligned}&\left|\big((1+P^l)/(1+P^{ek})\big)^1\right| \\ &\qquad = \frac{\left|\big((1+P^l)/(1+P^{ek})\big)^\times\right|}{\left|\big((1+p^{\lceil l/2\rceil})/(1+p^k)\big)^\times\right|} = \frac{\left|\mathfrak{O}_K/P\right|^{2k-l}}{p^{k-\lceil l/2\rceil}} = \frac{p^{2k-l}}{p^{k-\lceil l/2\rceil}} = p^{k+\lceil l/2\rceil-l}.\end{aligned}$$

For p even, the squaring argument shows that

$$\big(1+p^{\lceil l/2\rceil+1}\big)/\big(1+p^k\big) \subset \mathcal{N}\big((1+P^l)/(1+P^{ek})\big),$$

which gives a lower bound on the image. This gives the same result as for the odd case, except for a factor of 2. □

References

[1] R. Balian and C. Itzykson, *Observations sur la mécanique finie*, C. R. Acad. Sci. Paris Sér. I Math. **303** (1986), 773–778.

[2] F. R. Beyl, *The Schur Multiplicator of* $\mathrm{SL}(2,\mathbf{Z}/m\mathbf{Z})$ *and the congruence subgroup property*, Math. Z. **191** (1986), 23–42.

[3] A. Bouzouina and S. De Bièvre, *Equipartition of the eigenfunctions of quantized ergodic maps on the torus*, Comm. Math. Phys. **178** (1996), 83–105.

[4] J. W. S. Cassels and A. Frohlich, eds., *Algebraic Number Theory*, Proceedings of an instructional conference organized by the London Mathematical Society (University of Sussex, Brighton, 1965), Thompson, Washington, 1967.

[5] Y. Colin de Verdière, *Ergodicité et fonctions propres du laplacien*, Comm. Math. Phys. **102** (1985), 497–502.

[6] M. Degli Esposti, *Quantization of the orientation preserving automorphisms of the torus*, Ann. Inst. H. Poincaré **58** (1993), 323–341.

[7] M. Degli Esposti, S. Graffi, and S. Isola, *Classical limit of the quantized hyperbolic toral automorphisms*, Comm. Math. Phys. **167** (1995), 471–507.

[8] S. Gelbart, *Weil's Representation and the Spectrum of the Metaplectic Group*, Lecture Notes in Math. **530**, Springer, Berlin, 1976.

[9] J. H. Hannay and M. V. Berry, *Quantization of linear maps on a torus-Fresnel diffraction by a periodic grating*, Phys. D **1** (1980), 267–290.

[10] D. Jakobson, *Quantum unique ergodicity for Eisenstein series on* $\mathrm{PSL}_2(\mathbf{Z})\backslash\mathrm{PSL}_2(\mathbf{R})$, Ann. Inst. Fourier (Grenoble) **44** (1994), 1477–1504.

[11] J. P. Keating, *The cat maps: quantum mechanics and classical motion*, Nonlinearity **4** (1991), 309–341.

[12] S. Klimek, A. Lésniewski, N. Maitra, and R. Rubin, *Ergodic properties of quantized toral automorphisms*, J. Math. Phys. **38** (1997), 67–83.

[13] S. Knabe, *On the quantisation of Arnold's cat*, J. Phys. A **23** (1990), 2013–2025.

[14] T. Kubota, *On automorphic functions and the reciprocity law in a number field*, Lectures in Mathematics (Department of Mathematics, Kyoto University) **2**, Kinokuniya, Tokyo, 1969.

[15] W. Luo and P. Sarnak, *Quantum ergodicity of eigenfunctions on* $\mathrm{PSL}_2(\mathbf{Z})\backslash\mathbf{H}^2$, Inst. Hautes Études Sci. Publ. Math. **81** (1995), 207–237.

[16] J. Marklof and Z. Rudnick, *Quantum unique ergodicity for parabolic maps*, to appear in Geom. Funct. Analysis.

[17] J. Mennicke, *On Ihara's modular group*, Invent. Math. **4** (1967), 202–228.

[18] A. Nobs, *Die irreduziblen Darstellungen der Gruppen* $\mathrm{SL}_2(\mathbf{Z}_p)$*, insbesondere* $\mathrm{SL}_2(\mathbf{Z}_2)$*. I*, Comment. Math. Helv. **51** (1976), 465–489.

[19] I. Percival and F. Vivaldi, *Arithmetical properties of strongly chaotic motions*, Phys. D **25** (1987), 105–130.

[20] Z. Rudnick and P. Sarnak, *The behaviour of eigenstates of arithmetic hyperbolic manifolds*, Comm. Math. Phys. **161** (1994), 195–213.

[21] A. Schnirelman, *Ergodic properties of eigenfunctions*, Uspekhi Math. Nauk **29** (1974), 181–182.

[22] I. Schur, *Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen*, J. Reine Angew. Math. **132** (1907), 85–137.

[23] O. Taussky, "Connections between algebraic number theory and integral matrices", appendix to *A Classical Invitation to Algebraic Numbers and Class Fields*, by H. Cohn, Universitext, Springer, New York, 1978.

[24] S. Zelditch, *Uniform distribution of eigenfunctions on compact hyperbolic surfaces*, Duke Math. J. **55** (1987), 919–941.

[25] ———, *Index and dynamics of quantized contact transformations*, Ann. Inst. Fourier (Grenoble) **47** (1997), 305–363.

Kurlberg: Raymond and Beverly Sackler School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel; Current: Department of Mathematics, University of Georgia, Athens, Georgia 30602, USA; kurlberg@math.uga.edu

Rudnick: Raymond and Beverly Sackler School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel; rudnick@math.tau.ac.il