ON QUANTUM ERGODICITY FOR LINEAR MAPS OF THE TORUS

PÄR KURLBERG AND ZEÉV RUDNICK

ABSTRACT. We prove a strong version of quantum ergodicity for linear hyperbolic maps of the torus ("cat maps"). We show that there is a density one sequence of integers so that as N tends to infinity along this sequence, all eigenfunctions of the quantum propagator at inverse Planck constant N are uniformly distributed.

A key step in the argument is to show that for a hyperbolic matrix in the modular group, there is a density one sequence of integers N for which its order (or period) modulo N is somewhat larger than $\sqrt{N}$.

1. INTRODUCTION

1.1. **Quantum ergodicity.** An important model for understanding the quantization of classically chaotic systems are *quantum maps*, and in particular the quantizations of linear automorphisms of the torus $\mathbf{T}^2$ ("cat maps"). Iterating such a map, we get a discrete dynamical system, well-known to be chaotic if the map is hyperbolic. A quantization of these "cat maps" was proposed by Hannay and Berry [9], see also [13, 4, 5]. In brief, this procedure restricts Planck's constant to be an inverse integer: $h = 1/N$, and the Hilbert space of states $\mathcal{H}_N$ is N-dimensional, in keeping with the intuition that each state occupies a Planck cell of volume $h = 1/N$ and the constraint that the total phase-space $\mathbf{T}^2$ has volume one. Classical observables (i.e. functions $f \in C^\infty(\mathbf{T}^2)$) give rise to operators $\mathrm{Op}_N(f)$ on $\mathcal{H}_N$. Given a linear automorphism A of the torus, its quantization is a unitary operator $U_N(A)$ on $\mathcal{H}_N$, called the quantum propagator, or "quantized cat map". The eigenfunctions of $U_N(A)$ play the rôle of energy eigenstates.

In this paper we will use the quantized cat map to illuminate one of the few rigorous results available on the semi-classical limit of eigenstates of classically chaotic systems, namely *Quantum Ergodicity* [17, 3, 20]. To formulate this notion, recall that if the classical dynamics are *ergodic*, then almost all trajectories of a particle cover the energy shell

Date: September 27, 1999.

Supported in part by a grant from the Israel Science Foundation.

uniformly. The intuition afforded by the "Correspondence Principle" leads one to look for an analogous statement about the semi-classical limit of expectation values of observables in an energy eigenstate. As formulated by Schnirelman [17], the corresponding assertion is that when the classical dynamics is *ergodic*, for almost all eigenstates the expectation values of observables converge to the phase-space average. For quantum maps, the form that this takes is the following ([2, 21, 22]): Fix an observable $f \in C^\infty(\mathbf{T}^2)$. Then for any orthonormal basis ψ_j of $\mathcal{H}_N$ consisting of eigenfunctions of $U_N(A)$, there is a subset $J(N) \subset \{1, 2, \dots, N\}$, with $\frac{\#J(N)}{N} \to 1$, so that for $j \in J(N)$ we have:

$$\langle \mathrm{Op}_N(f)\psi_j, \psi_j\rangle \to \int_{\mathbf{T}^2} f, \qquad \text{as } N \to \infty \tag{1.1}$$

This is a consequence, using positivity and a standard diagonalization argument, of the following estimate for the variance due to Zelditch [21]: Given $f \in C^\infty(\mathbf{T}^2)$, for any orthonormal basis ψ_j, $j = 1, \dots, N$ of of $\mathcal{H}_N$ consisting of eigenfunctions of $U_N(A)$, we have

$$\frac{1}{N}\sum_{j=1}^{N}\left|\langle \mathrm{Op}_N(f)\psi_j, \psi_j\rangle - \int_{\mathbf{T}^2} f\right|^2 \to 0 \tag{1.2}$$

Note that the result (1.2) does not guarantee that *all* eigenfunctions in $\mathcal{H}_N$ are equidistributed, even for one single value of N.

1.2. **Beyond quantum ergodicity.** In recent work [14], we have found that there is a commutative group of unitary operators on the state-space which commute with the quantized map and therefore act on its eigenspaces. We called these "Hecke operators", in analogy with the setting of the modular surface. We showed that the joint eigenfunctions of these and of $U_N(A)$ (which we called "Hecke eigenfunctions") are all equidistributed, that is (1.1) holds for any choice of Hecke eigenfunctions in $\mathcal{H}_N$.

Not all eigenfunctions of $U_N(A)$ are Hecke eigenfunctions. In fact, the Hecke eigenspaces have small dimension (at most $O(\log\log N)$), while the eigenspaces of $U_N(A)$ may have large dimension. In fact, the *mean* degeneracy is $N/\operatorname{ord}(A, N)$ where $\operatorname{ord}(A, N)$ the *order* (or period) of A modulo N, that is the least integer $k \geq 1$ for which $A^k = I \mod N$. It can be shown (see section 3.2) that the mean degeneracy can be as large as $N/\log N$ for arbitrarily large N. However, it is reasonable to expect that *all* eigenfunctions become equidistributed - that is we have quantum *unique* ergodicity.

In this paper, we show ergodicity of *all* eigenfunctions of $U_N(A)$ for almost all integers N:

Theorem 1. *Let A be a fixed cat map. There is a set of integers $\mathcal{N}^*$ of density one so that all eigenfunctions of $U_N(A)$ are equi-distributed, as $N \to \infty$, $N \in \mathcal{N}^*$.*

Previously, the only result giving an infinite set of N for which all eigenfunctions of $U_N(A)$ become equi-distributed is by Degli-Esposti, Graffi and Isola [5], which conditional on GRH give an infinite set of *primes*.

1.3. **Outline of the argument.** Our main tool in relating this result to more traditional themes of Number Theory is the following estimate for the fourth power moment of the expectation values, giving a condition in terms of the order of A modulo N:

Theorem 2. *There is a sequence of integers of density one so that for all observables $f \in C^\infty(\mathbf{T}^2)$ and any orthonormal basis $\{\psi_j\}_{j=1}^N$ of $\mathcal{H}_N$ consisting of eigenfunctions of $U_N(A)$ we have:*

$$\sum_{j=1}^N |\langle \mathrm{Op}_N(f)\psi_j, \psi_j\rangle - \int_{\mathbf{T}^2} f|^4 \ll \frac{N(\log N)^{14}}{\mathrm{ord}(A,N)^2}\,.$$

Thus for any subsequence of integers N such that

$$\frac{\mathrm{ord}(A,N)}{N^{1/2}(\log N)^7} \to \infty \tag{1.3}$$

(and satisfying an additional "genericity" assumption explained in section 4) we find that for all eigenfunctions of $U_N(A)$, $\langle \mathrm{Op}_N(f)\psi, \psi\rangle \to \int_{\mathbf{T}^2} f$ as $N \to \infty$.

Theorem 2 reduces the problem of quantum ergodicity to that of finding sequences of integers satisfying (1.3), a problem closely related to the classical Gauss-Artin problem of showing that any integer, other than ± 1 or a perfect square, is a primitive root modulo infinitely many primes. We show (Theorem 17) that there is some $\delta > 0$ for which there is a set of integers of density 1 so that

$$\mathrm{ord}(A,N) \gg N^{1/2} \exp((\log N)^\delta)\,.$$

This, combined with Theorem 2 gives Theorem 1.

To prove Theorem 17, we first show in Section 5 that on a set of density one, $\mathrm{ord}(A,N)$ is not much smaller than the product of the orders of A modulo prime divisors of N. Next, we deal with prime values of N. In Section 6 we show (Theorem 14) that given $1/2 < \eta < 3/5$, there is a set of primes of positive density $c(\eta) > 0$ so that

$\operatorname{ord}(A,p) \gg p^\eta$. We note that this is far short of the truth; by invoking the Generalized Riemann Hypothesis, one can show that for a set of primes of density one, we have $\operatorname{ord}(A,p) \gg p/\log p$ (c.f. [6]). In Section 7 we prove Theorem 17 by using Theorem 14 together with the elementary observation that for almost all primes p, $\operatorname{ord}(A,p) \geq p^{1/2}/\log p$.

As is apparent from this discussion, our result hinge on the condition (1.3) being satisfied; we can say nothing for N for which this condition fails, of which there are infinitely many examples. We consider it a fundamental problem to get results when $\operatorname{ord}(A,N)$ is smaller than $N^{1/2}$.

1.4. **Notation.** We will use the standard convention of analytic number theory: Thus $e(z)$ stands for $e^{2\pi i z}$, $f(x) \ll g(x)$ as $x \to \infty$ means that there is some $C > 0$ so that for x sufficiently large, $f(x) < Cg(x)$. Similarly, $f(x) \lesssim g(x)$ as $x \to \infty$ means $\limsup f(x)/g(x) \leq 1$. We will write $p^t || n$ if p^t divides n but p^{t+1} does not. We will denote by $\omega(N)$ the number of prime divisors of N.

2. Quantum mechanics on the torus

2.1. The Hilbert space of states. We review the basics of quantum mechanics on the torus $\mathbf{T}^2$, viewed as a phase space [9, 13, 4, 5], beginning with a description of the Hilbert space of states of such a system: We take state vectors to be distributions on the line which are periodic in both momentum and position representations: $\psi(q+1)=\psi(q)$, $[\mathcal{F}_h\psi](p+1)=[\mathcal{F}_h\psi](p)$, where $[\mathcal{F}_h\psi](p)=h^{-1/2}\int\psi(q)\,e(-pq/h)\,dq$. The space of such distributions is finite dimensional, of dimension precisely $N=1/h$, 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

$$\langle\phi,\psi\rangle=\frac{1}{N}\sum_{Q \bmod N}\phi(Q)\,\overline{\psi}(Q), \tag{2.1}$$

2.2. Observables. Next we construct quantum observables: A central role is played by the translation operators

$$[t_1\psi](Q)=\psi(Q+1)$$

and

$$[t_2\psi](Q)=e_N(Q)\,\psi(Q),$$

which may be viewed as the analogues of differentiation and multiplication (respectively) operators. In fact in terms of the usual translation operators on the line $\hat{q}\psi(q)=q\psi(q)$ and $\hat{p}\psi(q)=\frac{h}{2\pi i}\frac{d}{dq}\psi(q)$, they are given by $t_1=e(\hat{p})$, $t_2=e(\hat{q})$. In this context, Heisenberg's commutation relations read

$$t_1^a t_2^b=t_2^b t_1^a e_N(ab)\qquad\forall a,b\in\mathbf{Z}. \tag{2.2}$$

More generally, mixed translation operators are defined for $n=(n_1,n_2)\in\mathbf{Z}^2$ by

$$T_N(n)=e_N(\frac{n_1n_2}{2})t_2^{n_2}t_1^{n_1}.$$

These are unitary operators on $\mathcal{H}_N$, whose action on a wave-function $\psi\in L^2(\mathbf{Z}/N\mathbf{Z})$ is given by:

$$T_N(n)\psi(Q)=e^{\frac{i\pi n_1n_2}{N}}e(\frac{n_2Q}{N})\psi(Q+n_1) \tag{2.3}$$

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

$$T_N(n)^*=T_N(-n)\,. \tag{2.4}$$

As follows from the commutation relation (2.2), we have

$$T_N(m)\,T_N(n)=e_N(\frac{\omega(m,n)}{2})\,T_N(m+n) \tag{2.5}$$

where $\omega(m,n)$ is the symplectic form

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

For any smooth function $f \in \mathbf{C}^\infty(\mathbf{T}^2)$, define a *quantum observable* $\mathrm{Op}_N(f)$, called the *Weyl quantization* of f [7]

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

where $\widehat{f}(n)$ are the Fourier coefficients of f.

Given a state $\psi \in \mathcal{H}_N$, the *expectation value* of the observable f in the state ψ is defined to be $\langle \mathrm{Op}_N(f)\psi, \psi \rangle$.

2.3. **Cat maps.** To introduce dynamics, we consider a linear automorphism of the torus $A \in SL(2,\mathbf{Z})$. The iteration of A gives a (discrete) dynamical system, well-known to be chaotic if A is hyperbolic, that is $|\operatorname{tr} A| > 2$ (such a map is called a "cat map" in the physics literature).

If we further assume A is "quantizable", that is $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $ab \equiv cd \equiv 0 \mod 2$, then on can assign to A a unitary operator $U_N(A)$ on $\mathcal{H}_N$, the *quantum propagator*, whose iterates give the evolution of the quantum system, and characterized by the property (an analogue of "Egorov's theorem"):

$$U_N(A)^* \mathrm{Op}_N(f) U_N(A) = \mathrm{Op}_N(f \circ A) \tag{2.6}$$

This can be thought of as saying that the evolution of the quantum observable $\mathrm{Op}_N(f)$ follows the evolution $f \mapsto f \circ A$ of the classical observable f. That (2.6) holds *exactly* is a special feature of the linearity of the map A; for general maps, (2.6) is only expected to hold asymptotically as $N \to \infty$ (c.f. [15]).

The stationary states of the quantum system are given by the eigenfunctions ψ of $U_N(A)$. It is our goal to study the limiting expectation values $\langle \mathrm{Op}_N(f)\psi, \psi\rangle$ of observables in (normalized) eigenstates and show that outside a zero density set of N's, they all converge to the classical average $\int_{\mathbf{T}^2} f$ of the observable as $N \to \infty$.

3. The order of a matrix modulo N

3.1. Let $A \in SL(2,\mathbf{Z})$ be a hyperbolic matrix, that is $|\operatorname{tr}(A)| > 2$. The *order* (or period) $\operatorname{ord}(A,N)$ of the map A modulo N is the least integer $k \geq 0$ so that $A^k = I \mod N$. We begin to study the order of A modulo an arbitrary integer N, starting with some well-known generalities.

3.1.1. Firstly if M and N are co-prime then

$$\operatorname{ord}(A,MN) = \operatorname{lcm}(\operatorname{ord}(A,M), \operatorname{ord}(A,N))$$

and so if N has a prime factorization $N = \prod p_i^{k_i}$ then

$$\operatorname{ord}(A,N) = \operatorname{lcm}\{\operatorname{ord}(A,p_i^{k_i})\}$$

3.1.2. The eigenvalues ϵ, ϵ^{-1} of A generate a field extension $K = \mathbf{Q}(\epsilon)$, which is a real quadratic field since $\operatorname{tr}(A)^2 > 4$. We label them so that $|\epsilon| > 1$. Let

$$D_A = 4(\operatorname{tr}(A)^2 - 4)$$

so that $K = \mathbf{Q}(\sqrt{D_A})$. We denote by $\mathfrak{O}_K$ the ring of integers of K. The eigenvalues ϵ, ϵ^{-1} of A will be units in $\mathfrak{O}_K$. Adjoining ϵ to $\mathbf{Z}$ gives an *order* $\mathfrak{O} = \mathbf{Z}[\epsilon] \subseteq \mathfrak{O}_K$ in K. Then there is an $\mathfrak{O}$-ideal $I \subset \mathfrak{O}$ so that the action of ϵ 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 ϵ is precisely A (see [18] or [14]). The action of $\mathfrak{O}$ by multiplication on I gives us an embedding

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

so that $\gamma = x + y\epsilon \in \mathfrak{O}$ 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 one then γ corresponds to an element in $SL_2(\mathbf{Z})$

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

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

Denote by $\mathcal{C}_A(N)$ the group of norm one elements in $\mathfrak{O}/N\mathfrak{O}$:

$$\mathcal{C}_A(N) = \ker\left[\mathcal{N} : (\mathfrak{O}/N\mathfrak{O})^* \to (\mathbf{Z}/N\mathbf{Z})^*\right] .$$

This is a subgroup of $SL(2,\mathbf{Z}/N\mathbf{Z})$, containing the residues class of A modulo N.

The cardinality of $\mathcal{C}_A(N)$ can be computed via the Chinese Remainder Theorem from the cardinality at prime power arguments. To do so, define

$$\chi(p) = \begin{cases} +1, & p \text{ splits in } K \\ -1, & p \text{ inert in } K. \end{cases}$$

By quadratic reciprocity, χ is a Dirichlet character modulo D_A (not necessarily primitive). It can then be shown (see e.g. [14], Appendix B) that if p does not divide D_A, then

$$\#\mathcal{C}_A(p^k) = p^{k-1}(p-\chi(p)) \tag{3.1}$$

while for primes dividing D_A, there is some $c_A > 0$ so that

$$\#\mathcal{C}_A(p^k) \le c_A p^k \ . \tag{3.2}$$

As a consequence, we find that if p does not divide D_A, then the order of A modulo p divides $p-\chi(p)$, and more generally, for any prime power p^k, if p does not divide D_A then $\mathrm{ord}(A,p^k)$ divides $p^{k-1}(p-\chi(p))$.

3.1.3. *An upper bound for* $\mathrm{ord}(A,N)$. Another consequence of (3.1), (3.2) is that for any integer $N=\prod p^{k_p}$,

$$\#\mathcal{C}_A(N) = \prod_p \#\mathcal{C}_A(p^{k_p}) \ll_A N\prod_{p|N}(1+\frac{1}{p}) \ll_A N\log\log N \ .$$

Thus, for any integer N, we have as an upper bound for the order

$$\mathrm{ord}(A,N) \ll N\log\log N \ . \tag{3.3}$$

3.2. **Making** $\mathrm{ord}(A,N)$ **small.** As for lower bounds on the order, it is easily seen that $\mathrm{ord}(A,N) \gg \log N$ for all N. In fact, this bound is sharp, as we claim:

Proposition 3. *There is an infinite sequence of integers* $\{N_k\}_{k=1}^\infty$ *for which* $\mathrm{ord}(A,N_k) \ll \log N_k$.

Proof. To explain the idea, recall first how to find integers n for which 2 has small order modulo n: The trick is to take $n_k = 2^k-1$, since then $2^k = 1 \mod n_k$, and so $\mathrm{ord}(2,n_k) \le k \sim \log n_k/\log 2$. To modifiy this idea to our context, assume for simplicity that the matrix A is "principal", that is the action of A on $\mathbf{Z}^2$ is equivalent to the action of the unit ϵ on the maximal order $\mathfrak{O}_K$ (in general we need an ideal in the order $\mathfrak{O}=\mathbf{Z}[\epsilon]$, see section 3.1.2). Then $A^k = I \mod N$ is *equivalent* to $\epsilon^k = 1 \mod N\mathfrak{O}_K$ (in general, only the implication $\Rightarrow$ is valid).

Factor $|\det(A^k-I)|$ as a product of prime powers:

$$|\det(A^k-I)| = \prod_S p^{\sigma_p}\prod_I p^{\iota_p}\prod_R p^{\rho_p}$$

where $\prod_S$ means the product over primes $p = \mathfrak{p}\bar{\mathfrak{p}}$ which split in $K = \mathbf{Q}(\epsilon)$, $\prod_I$ the product over inert primes and $\prod_R$ the product over the ramified primes $p = \mathfrak{p}^2$.

On the other hand, we have

$$\det(A^k - I) = \mathcal{N}(\epsilon^k - 1) = -\epsilon^{-k}(\epsilon^k - 1)^2 .$$

Write the ideal factorization of $\mathfrak{a}_k := (\epsilon^k - 1)\mathfrak{O}_K$ as

$$\mathfrak{a}_k = \prod_S \mathfrak{p}^{s'_p}\bar{\mathfrak{p}}^{s''_p} \prod_I p^{i_p} \prod_R \mathfrak{p}^{r_p} .$$

Since $\mathfrak{a}_k^2 = \det(A^k - I)\mathfrak{O}_K$, we get on comparing the prime exponents that

$$2s'_p = 2s''_p = \sigma_p, \qquad \iota_p = 2i_p, \qquad \rho_p = r_p .$$

Since σ_p is even, we can set

$$N_k := \prod_S p^{\sigma_p/2} \prod_I p^{i_p} \prod_R p^{[r_p/2]} .$$

Then

$$N_k \le |\det(A^k - I)| \le N_k^2 \delta$$

where $\delta = \prod_R p$ is the product of all ramified primes of K.

We have $\mathfrak{a}_k \subseteq N_k\mathfrak{O}_K$ and so $\epsilon^k = 1 \mod N_k\mathfrak{O}_K$, equivalently $A^k = I \mod N_k$. Thus we find

$$\operatorname{ord}(A, N_k) \le k \sim \frac{\log|\det(A^k - I)|}{\log \epsilon} \le \frac{\log N_k^2 \delta}{\log \epsilon} = \frac{2}{\log \epsilon} \log N_k + O(1)$$

and so $\operatorname{ord}(A, N_k) \ll \log N_k$ as required. $\square$

4. Large order of A implies equidistribution

4.1. In this section we give a relation between the order of the map A modulo N and the distribution of the eigenfunctions of the quantization $U_N(A)$. We start by relating the fourth power-moment of the expectation values $\langle T_N(n)\psi_i, \psi_i\rangle$, for ψ_i ranging over an orthonormal basis of $U_N(A)$-eigenfunctions, to the number of solutions of a certain equation modulo N.

Proposition 4. *Let $\{\psi_i\}_{i=1}^N$ be an orthonormal basis of eigenfunctions of $U_N(A)$. Then*

$$\sum_{i=1}^{N} |\langle T_N(n)\psi_i, \psi_i\rangle|^4 \leq \frac{N}{\operatorname{ord}(A,N)^4}\nu(N,n) \tag{4.1}$$

where $\nu(N,n)$ is the number of solutions of the congruence

$$n(A^i - A^j + A^k - A^l) \equiv 0 \mod N, \qquad 1 \leq i,j,k,l \leq \operatorname{ord}(A,N)$$

Proof. Let

$$D(n) = \frac{1}{\operatorname{ord}(A,N)} \sum_{i=1}^{\operatorname{ord}(A,N)} T_N(nA^i),$$

and let t_{ij} be the matrix coefficients of $T_N(n)$ expressed in terms of the basis $\{\psi_i\}_{i=1}^N$. From (2.6) we have that

$$T_N(nA^i) = U_N^*(A)T_N(n)U_N^*(A)$$

and by assumption $U_N(A)\psi_i = \lambda_i\psi_i$ for λ_i a root of unity. Thus, if $\{D_{ij}\}_{i,j=1}^N$ are the matrix coefficients of D in terms of the basis $\{\psi_i\}_{i=1}^N$, then

$$D_{ij} = \begin{cases} t_{ij} & \text{if } \lambda_i = \lambda_j, \\ 0 & \text{otherwise.} \end{cases} \tag{4.2}$$

If we denote by $\{v_i\}_{i=1}^N$ the column vectors of D, then the (k,k)-entry of $(D^*D)^2$ is

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

and since $|\langle v_k, v_k\rangle| = \sum_i |D_{ki}|^2$ we get

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

Substituting the definition of D and using (2.4) and (2.5), we see that $(D^*D)^2$ is given by $\operatorname{ord}(A,N)^{-4}$ times a sum, ranging over $1 \leq$

$i, j, k, l \leq \operatorname{ord}(A, N)$, of terms

$$T_N(nA^i)T_N(-nA^j)T_N(nA^k)T_N(-nA^l) = \gamma_{i,j,k,l}T_N(n(A^i - A^j + A^k + A^l))$$

where $\gamma_{i,j,k,l}$ has absolute value one. Now take the trace; as follows from (2.3) (see Lemma 4 in [14]), the absolute value of the trace of $T_N(n)$ equals N if $n \equiv (0,0) \mod N$, zero otherwise. The result now follows by taking absolute values and summing over all i, j, k, l. (For more details, see section 6.2 in [14].) $\square$

4.2. **A counting problem.** In order to make use of Proposition 4 we must bound the number of solutions to

$$n(A^i - A^j + A^k - A^l) \equiv 0 \mod N, \quad 1 \leq i, j, k, l \leq \operatorname{ord}(A, N).$$

We will show that there are essentially only *trivial* solutions of this equation, i.e.

$$(A^i, A^k) = (A^j, A^l), \quad (A^i, A^k) = (A^l, A^k), \quad \text{or } (A^i, A^j) = (-A^k, -A^l),$$

where the third possibility only happens if there exists t such that $A^t = -I$. In terms of the exponents i, j, k, l this means that

$$(i, k) = (j, l), \quad (i, k) = (l, k), \quad \text{or } (i, j) = (t - k, t - l), \tag{4.3}$$

where equality is to be interpreted as equality modulo the order of A.

4.2.1. *The prime case.* Here we assume $N = p$ is prime.

Lemma 5. *Assume that nA and n are linearly independent modulo p, and that the eigenvalues of A are distinct modulo p. Then there are at most $3\operatorname{ord}(A, p)^2$ solutions of*

$$n(A^i - A^j + A^k - A^l) \equiv 0 \mod p, \ 1 \leq i, j, k, l \leq \operatorname{ord}(A, p) \tag{4.4}$$

Proof. Let K be the real quadratic field containing the eigenvalues of A, and let K_p be the residue class field at the prime p, i.e., $K_p = \mathfrak{O}_K/P$ where P is a prime of K lying above p. K_p has cardinality p if p splits in K, or p^2 if p is inert. We may diagonalize the reduction of A modulo p over the field K_p. In the eigenvector basis we have $A' = \begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{pmatrix}$ and $n' = (n_1', n_2')$, where the assumption of linear independence modulo p implies that both $n_1', n_2' \neq 0$ (in K_p.) Thus (4.4) is equivalent to the following two equations over K_p:

$$\begin{aligned} \epsilon^i - \epsilon^j + \epsilon^k - \epsilon^l &= 0 \\ \epsilon^{-i} - \epsilon^{-j} + \epsilon^{-k} - \epsilon^{-l} &= 0 \end{aligned} \tag{4.5}$$

which in turn (see lemma 15 in [14]) is equivalent to

$$\begin{aligned} \epsilon^l &= \epsilon^i - \epsilon^j + \epsilon^k \\ (\epsilon^k - \epsilon^i)(\epsilon^k - \epsilon^j)&(\epsilon^i + \epsilon^j) = 0 \end{aligned} \tag{4.6}$$

Hence l is determined by the triple (i, j, k). Dividing by ϵ^k and letting $i' = i - k$ and $j' = j - k$ we rewrite the second equation as

$$(1 - \epsilon^{i'})(1 - \epsilon^{j'})(\epsilon^{i'} + \epsilon^{j'}) = 0, \quad 1 \le i', j' \le \operatorname{ord}(A, p) \tag{4.7}$$

If the first (or second) factor equals zero then $\operatorname{ord}(A,p) \mid i'$ (or j') since the order of ϵ in $K_p^\times$ equals $\operatorname{ord}(A, p)$. If the third factor is zero then $\operatorname{ord}(A,p) \mid i' - j' - t$ where $\epsilon^t = -1$. In each case this leaves $\operatorname{ord}(A, p)$ possibilities for the pair (i', j'), and since k is unconstrained the total number of solutions is at most $3 \operatorname{ord}(A, p)^2$. □

Remark: The condition of linear independence mod p in lemma 5 is satisfied for all but finitely many primes. In fact, if we let

$$M = \begin{pmatrix} n_1 & n_2 \\ m_1 & m_2 \end{pmatrix}$$

where $n = (n_1, n_2)$ and $nA = (m_1, m_2)$, then the condition of linear dependence is equivalent to $p \mid \det M$. Now $\det M$ is a *nonzero* integer, because A has no rational eigenvectors. We also note that if the independence condition is not satisfied then trivially there are at most $\operatorname{ord}(A,p)^4$ solutions to (4.4).

Lemma 6. *Let N be square free and coprime to $D_A = 4(\operatorname{tr}(A)^2 - 4)$. Assume further that nA and n are linearly independent modulo p for all $p \mid N$. Then there are at most $3^{\omega(N)} \operatorname{ord}(A, N)^2$ solutions of*

$$n(A^i - A^j + A^k - A^l) \equiv 0 \mod N, \quad 1 \le i, j, k, l \le \operatorname{ord}(A, N). \tag{4.8}$$

Proof. Let (i, j, k, l) be a solution to (4.8). If $p \mid N$ then (4.8) holds with N replaced by p. Arguing as in lemma 5 one of the three factors in (4.7) must be zero, and the vanishing factor determines which one of the three equations in (4.3) that (i, j, k, l) must satisfy modulo $\operatorname{ord}(A, p)$. For example, if the first factor in (4.7) is zero, then $(i, j) \equiv (k, l) \mod \operatorname{ord}(A, p)$.

Now, the group generated by A modulo N is cyclic and isomorphic to $\oplus_{q \in Q} \mathbf{Z}/q^{a_q}\mathbf{Z}$ where the q's are *distinct* primes. We will denote the $\mathbf{Z}/q^{a_q}\mathbf{Z}$ component of i by i_q and similarly for j, k, l. Since $\operatorname{ord}(A, N)$ is equal to the least common multiple of $\{\operatorname{ord}(A,p)\}_{p \mid N}$ there exists for each $q \in Q$ at least one prime $p \mid N$ such that $q^{a_q} \parallel \operatorname{ord}(A, p)$.

Claim: if (i,j,k,l) is a solution to (4.8) then (i_q,j_q,k_q,l_q) satisfies one of the equations in (4.3). The reason is as follows: there is a prime $p \mid N$ such that $q^{a_q} \parallel \operatorname{ord}(A,p)$, thus one of the equations in (4.3) is satisfied modulo $\operatorname{ord}(A,p)$. Since $q^{a_q} \parallel \operatorname{ord}(A,p)$ this implies that (i_q,j_q,k_q,l_q) satisfies one of the equations in (4.3). (Note in particular that this leaves q^{2a_q} possibilities for (i_q,j_q,k_q,l_q) if we specify one of the equations in (4.3) to be satisfied). Now, to each $p \mid N$ there are 3 different types of trivial solutions, and since (i_q,j_q,k_q,l_q) must satisfy one of the possibilities in (4.3) for all $q \in Q$, we obtain that there are at most

$$3^{\omega(N)} \prod_{q \in Q} q^{2a_q} = 3^{\omega(N)} \operatorname{ord}(A,N)^2$$

solutions to (4.8). □

In our applications the hypothesis of linear independence might not hold for all $p \mid N$. However, we have the following

Lemma 7. *Let N be square free. Then there are at most*

$$O_A\left(|n|_2^{8+\epsilon} 3^{\omega(N)} \operatorname{ord}(A,N)^2\right)$$

solutions to

(4.9)
$$n(A^i - A^j + A^k - A^l) \equiv 0 \mod N, \quad 1 \le i,j,k,l \le \operatorname{ord}(A,N).$$

Proof. By the remark after lemma 5, linear dependence modulo p holds if and only if $p \mid \det M$, where $|\det M| \ll_A |n|_2^2$. Let

$$N' = \frac{N}{\gcd(D_A \det M, N)}.$$

Then the hypothesis in lemma 6 is satisfied for N', leaving $3^{\omega(N')} \operatorname{ord}(A,N')^2$ possible values for (i,j,k,l) modulo $\operatorname{ord}(A,N')$. Now, an element in $\mathbf{Z}/\operatorname{ord}(A,N')\mathbf{Z}$ has exactly $\frac{\operatorname{ord}(A,N)}{\operatorname{ord}(A,N')}$ preimages in $\mathbf{Z} \cap [1, \operatorname{ord}(A,N)]$. Hence there are at most

$$3^{\omega(N')} \operatorname{ord}(A,N')^2 \left(\frac{\operatorname{ord}(A,N)}{\operatorname{ord}(A,N')}\right)^4$$

solutions to (4.9). Since

$$|\det(M)| \ll_A |n|_2^2$$

we get that

$$\frac{N}{N'} = \gcd(D_A \det M, N) \le D_A \det M \ll_A |n|_2^2.$$

Finally noting that since N is square-free,

$\operatorname{ord}(A,N) = \operatorname{lcm}(\operatorname{ord}(A,N'), \operatorname{ord}(A,N/N')) \le \operatorname{ord}(A,N')\cdot\operatorname{ord}(A,N/N')$

we find (by (3.3)) that

$$\frac{\operatorname{ord}(A,N)}{\operatorname{ord}(A,N')} \le \operatorname{ord}(A,N/N') \ll \left(\frac{N}{N'}\right)^{1+\epsilon}$$

for all $\epsilon > 0$, and we are done. □

4.3. **Conclusion.**

Proposition 8. *There exists a density-one sequence S of integers such that if $n \neq 0$ and $N \in S$ then*

$$\sum_{i=1}^{N} |\langle T_N(n)\psi_i, \psi_i\rangle|^4 \ll |n|_2^{8+\epsilon} \frac{N(\log N)^{14}}{\operatorname{ord}(A,N)^2}$$

Proof. Let S be the set of integers of the form $N = ds^2$, where d is square free, $s \le \log N$, and $\omega(N) \le 3/2 \log\log N$. By Lemmas 21 and 22, S has density one.

For $N = ds^2 \in S$, we wish to bound the number of solutions to

$$n(A^i - A^j + A^k - A^l) = 0 \bmod N, \quad 1 \le i,j,k,l \le \operatorname{ord}(A,N) \tag{4.10}$$

Since N is not square free we cannot apply lemma 7 directly. For $N = ds^2$, d square-free, we further decompose $d = d_1 \gcd(d,s)$, so that d_1 and $N/d_1 = \gcd(d,s)s^2$ are coprime.

Given $t \in \mathbf{Z}$ there are exactly $\frac{\operatorname{ord}(A,N)}{\operatorname{ord}(A,d_1)}$ solutions to $A^i \equiv A^t \mod d_1$ if $i \in \mathbf{Z} \cap [1, \operatorname{ord}(A,N)]$. Thus, a solution of

$$n(A^i - A^j + A^k - A^l) = 0 \bmod d_1, \quad 1 \le i,j,k,l \le \operatorname{ord}(A,d_1) \tag{4.11}$$

lifts to at most $(\operatorname{ord}(A,N)/\operatorname{ord}(A,d_1))^4$ solutions for which $1 \le i,j,k,l \le \operatorname{ord}(A,N)$. This, together with lemma 7 applied to (4.11) gives there are at most

$$\left(\frac{\operatorname{ord}(A,N)}{\operatorname{ord}(A,d_1)}\right)^4 |n|_2^{8+\epsilon} 3^{\omega(d_1)} \operatorname{ord}(A,d_1)^2$$

solutions to (4.10).

Clearly $\omega(d_1) \le \omega(N)$, $\operatorname{ord}(A,d_1) \le \operatorname{ord}(A,N)$, and since d_1, N/d_1 are coprime, with $N/d_1 \le s^3$, we have

$$\frac{\operatorname{ord}(A,N)}{\operatorname{ord}(A,d_1)} \le \operatorname{ord}(A, \frac{N}{d_1}) \ll (\frac{N}{d_1})^{1+\epsilon} \le s^{3(1+\epsilon)}$$

for all $\epsilon > 0$ (by (3.3)). Hence the number $\nu(N,n)$ of solutions of (4.10) is bounded by

$$\nu(N,n) \ll |n|_2^{8+\epsilon} s^{12+\epsilon} 3^{\omega(N)} \operatorname{ord}(A,N)^2 . \tag{4.12}$$

Thus we find that for $N \in S$ the number of solutions of (4.10) is bounded by

$$|n|_2^{8+\epsilon} (\log N)^{12+\epsilon} 3^{3/2 \log\log N} \operatorname{ord}(A,N)^2 \ll |n|_2^{8+\epsilon} (\log N)^{14} \operatorname{ord}(A,N)^2$$

and consequently we see from Proposition 4 that

$$\sum_{i=1}^{N} |\langle T_N(n)\psi_i, \psi_i\rangle|^4 \leq |n|_2^{8+\epsilon} \frac{N(\log N)^{14}}{\operatorname{ord}(A,N)^2}$$

as required. □

By a routine argument (see [14]) we get:

Corollary 9. *There is a density one sequence of integers N so that for all observables $f \in C^\infty(\mathbf{T}^2)$, we have*

$$\sum_{j=1}^{N} |\langle \operatorname{Op}_N(f)\psi_j, \psi_j\rangle - \int_{\mathbf{T}^2} f|^4 \ll_f \frac{N(\log N)^{14}}{\operatorname{ord}(A,N)^2}$$

This reduces the proof of Theorem 1 to showing that for a sequence of density one of integers, $\operatorname{ord}(A,N)$ grows faster than $N^{1/2}(\log N)^7$ as $N \to \infty$. We will do this in Section 7 (Theorem 17).

5. Relating the order of A modulo integers to the order modulo primes

Our goal in this section is to show (Proposition 11) that for a set of density one of integers N, $\operatorname{ord}(A,N)$ is not much smaller than the product of $\operatorname{ord}(A,p)$ over prime divisors p of N.

5.1. For a set of positive integers $\mathcal{M}=\{m_1,\dots,m_k\}$, define

$$\mathcal{L}(\mathcal{M})=\frac{\prod_{j=1}^k m_j}{\operatorname{lcm}\{m_1,\dots,m_k\}}$$

Then $\mathcal{L}(\mathcal{M})$ is a positive integer, $\mathcal{L}(\{m\})=1$ and $\mathcal{L}(\{m_1,m_2\})=\gcd(m_1,m_2)$.

From the definition, a prime ℓ divides $\mathcal{L}(m_1,\dots,m_k)$ if and only if there are two distinct indices $i\neq j$ so that ℓ divides both m_i and m_j.

Lemma 10. *Let $\mathcal{M}=\{m_1,\dots,m_k\}$, $\mathcal{N}=\{n_1,\dots,n_k\}$ and suppose that $m_j\mid n_j$, $1\le j\le k$. Then $\mathcal{L}(\mathcal{M})$ divides $\mathcal{L}(\mathcal{N})$. In particular,*

$$\operatorname{lcm}\{m_1,\dots,m_k\}\ge\frac{\prod_j m_j}{\mathcal{L}(\mathcal{N})}\ .$$

Proof. Factor $m_j=\prod_i p_i^{\alpha_{ij}}$, $n_j=\prod_i p_i^{\alpha_{ij}+\beta_{ij}}$ with $\alpha_{ij},\beta_{ij}\ge 0$. Then $\mathcal{L}(\mathcal{M})=\prod_i p_i^{\mu_i}$, $\mathcal{L}(\mathcal{N})=\prod_i p_i^{\nu_i}$ where

$$\mu_i=\sum_{j=1}^k\alpha_{ij}-\max_{1\le j\le k}\alpha_{ij},$$

$$\nu_i=\sum_{j=1}^k(\alpha_{ij}+\beta_{ij})-\max_{1\le j\le k}(\alpha_{ij}+\beta_{ij})\ .$$

Thus the Lemma reduces to the following easily verified inequality: For any non-negative reals $a_j,b_j\ge 0$, $1\le j\le k$, we have

$$\sum_j a_j-\max_j a_j\le\sum_j(a_j+b_j)-\max_j\{a_j+b_j\}\ .$$

□

5.2. We need to apply these considerations to bounding $\operatorname{ord}(A,N)$. Given an integer N, we will write $N=ds^2$ with d square-free, and further decompose $d=d_0\gcd(d,D_A)$, so that $d_0=d_0(N)$ is square-free and co-prime to D_A.

Now define

$$L(N)=\mathcal{L}(\{p-\chi(p):p\mid d_0(N)\})\tag{5.1}$$

Since $d_0 \mid N$, we have

$$\operatorname{ord}(A,N) \geq \operatorname{ord}(A,d_0) = \operatorname{lcm}(\{\operatorname{ord}(A,p) : p \mid d_0\})$$

Moreover, for $p \mid d_0$ we have $\operatorname{ord}(A,p) \mid p - \chi(p)$ and so by Lemma 10 we find

$$\operatorname{lcm}(\{\operatorname{ord}(A,p) : p \mid d_0\}) \geq \frac{\prod_{p \mid d_0} \operatorname{ord}(A,P)}{L(N)}$$

and thus

$$\operatorname{ord}(A,N) \geq \frac{\prod_{p \mid d_0} \operatorname{ord}(A,P)}{L(N)} \tag{5.2}$$

We will show (Proposition 11) that for almost all $N \leq x$, we have $L(N) \leq \exp(3(\log\log x)^4)$ and consequently we get as the main result of this section:

Proposition 11. *For almost all $N \leq x$,*

$$\operatorname{ord}(A,N) \geq \frac{\prod_{p \mid d_0} \operatorname{ord}(A,p)}{\exp(3(\log\log x)^4)}$$

where d_0 is given by writing $N = ds^2$, with $d = d_0 \gcd(d, D_A)$ square-free.

5.3. For $x \gg 1$, we set $z = z(x) = (\log\log x)^3$. We say that an integer is *z-smooth* if it has no prime divisors larger than z.

Lemma 12. *For almost all $N \leq x$ (that is for all but $O(x/\log\log x)$), $L(N)$ is z-smooth.*

Proof. Suppose that $L(N)$ is divisible by a prime $\ell > z$. From the definition of $L(N)$, this implies that there are two distinct prime divisors q_1, q_2 of $d_0(N)$ so that ℓ divides $q_i - \chi(q_i)$, $i = 1,2$. In particular, $\ell \leq x^{1/2}$. Thus we find two distinct primes such that

$$q_1 q_2 \mid N \quad \text{and} \quad q_i = \pm 1 \mod \ell, \quad i = 1,2 \tag{5.3}$$

For fixed q_1, q_2 the number of $N \leq x$ divisible by $q_1 q_2$ is $[x/q_1 q_2]$. Thus for fixed ℓ, the number of $N \leq x$ satisfying (5.3) is at most

$$\sum_{q_1, q_2 = \pm 1 \mod \ell} \frac{x}{q_1 q_2} \leq x \left(\sum_{q = \pm 1 \mod \ell} \frac{1}{q} \right)^2$$

By Brun-Titchmarsh (Lemma 23 - recall $\ell \leq x^{1/2}$), this is bounded (up to constant factor) by $x(\log\log x/\ell)^2$. Summing over all primes $\ell > z$, we find that the number of integers $N \le x$ such that $L(N)$ is divisible by some prime $\ell > z$ is at most

$$x(\log\log x)^2 \sum_{\ell > z} \frac{1}{\ell^2} \ll \frac{x(\log\log x)^2}{z} \ll \frac{x}{\log\log x}$$

$\square$

Proposition 13. *For almost all integers $N \le x$ we have*

$$L(N) \le \exp(3(\log\log x)^4)\ .$$

Proof. By Lemma 12 we may assume that $L(N)$ is z-smooth, with $z = (\log\log x)^3$. For $p \mid d_0(N)$, write the z-smooth part of $p - \chi(p)$ as $f_p s_p^2$, with f_p square-free. Set

$$S_N = \max_{p \mid d_0} s_p\ .$$

Note that since f_p is square-free and z-smooth, it divides the product of all primes $q \le z$. Thus for $z \gg 1$ we have:

$$f_p \le \prod_{q \le z} q \le e^{3z/2}\ .$$

Since $L(N)$ is z-smooth and divides $\prod_{p \mid d_0}(p - \chi(p))$, it also divides the product $\prod_{p \mid d_0} f_p s_p^2$. Thus

$$L(N) \le \prod_{p \mid d_0} f_p s_p^2 \le \prod_{p \mid d_0} e^{3z/2} S^2 \le (e^{\frac{3}{2}z} S^2)^{\omega(N)}$$

or

$$\frac{\log L(N)}{\omega(N)} - \frac{3}{2} z \le \log S_N^2 \tag{5.4}$$

Now for almost all $N \le x$ we have (Lemma 22)

$$\omega(N) < \frac{3}{2} \log\log x \tag{5.5}$$

and so by (5.4) if $L(N)$ is large, so is S_N. Specifically, if $\log L(N) > 3z \log\log x = 3(\log\log x)^4$ then by (5.4), (5.5), we find

$$\log S_N^2 > z/2 = (\log\log x)^3/2$$

We will show that this fails for almost all $N \le x$ and thus prove the Proposition.

To estimate the number of $N \le x$ for which $\log S_N^2 > z/2 = (\log\log x)^3/2$, recall that by the definition of S_N there is some prime q dividing d_0 (and hence dividing N) so that the z-smooth part of $q - \chi(q)$ is $f_q s_q^2$ and $S_N = s_q$ (in particular if $N \le x$ then $S_N \le x^{1/2}$). Thus there is a prime $q \mid N$ for which $q = \pm 1 \mod S^2$.

Given q there are at most $[x/q]$ integers $N \leq x$ divisible by q, and hence the total number of $N \leq x$ with $\log S_N^2 > z/2$ is at most

$$\sum_{\exp(z/4)<S<x^{1/2}} \sum_{\substack{q=\pm 1 \mod S^2 \\ q \leq x}} \frac{x}{q}$$

By Lemma 23 we have for fixed $S < x^{1/2}$

$$\sum_{\substack{q=\pm 1 \mod S^2 \\ q \leq x}} \frac{x}{q} \ll \frac{x \log\log x}{S^2}$$

and summing over $S > e^{z/4}$ gives at most

$$x \log\log x \sum_{S>\exp(z/4)} \frac{1}{S^2} \ll \frac{x \log\log x}{\exp(z/4)}$$

Thus the number of $N \leq x$ for which $\log S_N^2 > z/2 = (\log\log x)^3/2$ is at most

$$\frac{x \log\log x}{e^{z/4}} \ll x \log\log x \exp(-\frac{1}{4}(\log\log x)^3) = o(x)$$

and we are done. $\square$

6. Large order for primes

In this section we show that $\operatorname{ord}(A,p)$ is large for a positive proportion of primes. Our main result here is:

Theorem 14. *Let $1/2 < \eta < 3/5$. Then the number of primes $p \le x$ for which the order of the cat map modulo p satisfies $\operatorname{ord}(A,p) > x^\eta$ is at least $c(\eta)\pi(x) + o(\pi(x))$, where*

$$c(\eta) = \frac{3-5\eta}{2(1-\eta)}, \quad 1/2 < \eta < 3/5\,. \tag{6.1}$$

We first observe (following Hooley [12]):

Lemma 15. *The number of primes for which $\operatorname{ord}(A,p) \le y$ is $\ll y^2$.*

Proof. If $\operatorname{ord}(A,p) = k \le y$ then $A^k = I \mod p$ and so $p \mid \det(A^k - I)$. Thus the number of such primes is bounded by the total number of prime divisors of the integers $\det(A^k - I)$, $k \le y$, that is by

$$\sum_{k \le y} \omega(\det(A^k - I))$$

where $\omega(n)$ is the number of prime factors of n. Now trivially $\omega(n) \le \log|n|$, and $|\det(A^k - I)| \sim \epsilon^k$ where $\epsilon > 1$ is the largest eigenvalue of A. Thus we get a bound for the number of primes as above of

$$\sum_{k \le y} \omega(\det(A^k - I)) \ll \sum_{k \le y} k \ll y^2$$

as required. □

For $\eta \ge 1/2$, let $P_\eta(x)$ be the set of primes $p \le x$ for which there is a prime $q > x^\eta$, with $q \mid p - \chi(p)$. The main tool for proving Theorem 14 is:

Proposition 16. *For $1/2 < \eta < 3/5$ we have*

$$\# P_\eta(x) \ge c(\eta)\pi(x)\,(1 + o(1))$$

with $c(\eta) > 0$ given by (6.1).

Theorem 14 follows from Proposition 16 and the following observation: For all but $o(\pi(x))$ of the primes of $P_\eta(x)$ we have $\operatorname{ord}(A,p) > x^\eta$. Indeed, for $p \nmid D_A$, $\operatorname{ord}(A,p)$ divides $p - \chi(p)$. For $p \in P_\eta(x)$, if $\operatorname{ord}(A,p)$ is not divisible by the large factor $q > x^\eta$ of $p - \chi(p)$ then it divides $\frac{p-\chi(p)}{q} < x^{1-\eta}$ and so $\operatorname{ord}(A,p)$ is smaller than $y = x^{1-\eta}$; the number of such primes is by Lemma 15 at most $O(x^{2(1-\eta)}) = o(\pi(x))$ since $\eta > 1/2$. Thus for all but $o(\pi(x))$ of the primes in $P_\eta(x)$, we have $q \mid \operatorname{ord}(A,p)$ and so for these primes $\operatorname{ord}(A,p) \ge q > x^\eta$.

6.1. **Proof of Proposition 16.** The proof of Proposition 16 is a modification of a theorem due to Goldfeld [8] from the case of primes p for which $p+a$ has a large prime factor for fixed a, to the case when a is allowed to vary with p in a bounded fashion, depending on a fixed set congruence conditions.

The idea is as follows: By quadratic reciprocity, $\chi(p)$ only depends on the residue of p modulo $D_A = 4(\mathrm{tr}(A)^2-4)$. Thus the number of primes in $P_\eta(x)$ is the sum over all invertible residues $a \mod D_A$ of the number of primes in

$$P_\eta(x;D_A,a) = \{p \in P_\eta(x) : p = a \mod D_A\}$$

We will show

$$\#P_\eta(x;D_A,a) \gtrsim \frac{c(\eta)}{\phi(D_A)}\pi(x) \tag{6.2}$$

where $c(\eta)$ is given by (6.1). Summing (6.2) over all invertible residues $a \mod D_A$ will give Proposition 16.

6.1.1. As in [8], we consider the sum

$$S_a(x) = \sum_{\substack{m\le x\\(m,D_A)=1}} \sum_{\substack{p\le x\\ p=a \bmod D_A\\ m\mid p-\chi(a)}} \Lambda(m)$$

and more generally for $y_1 < y_2 \le x$, we set

$$S_a(y_1,y_2;x) = \sum_{\substack{y_1<m\le y_2\\(m,D_A)=1}} \sum_{\substack{p\le x\\ p=a \bmod D_A\\ m\mid p-\chi(a)}} \Lambda(m)$$

This is the weighted sum over prime powers $m \in (y_1,y_2]$, coprime to D_A, of the number of primes $p\le x$, $p = a \mod m$ with $m \mid p-\chi(p)$.

If $(m,D_A)=1$ then by the Chinese Remainder Theorem, there is a unique $a_m \mod mD_A$ so that

$$\begin{aligned} a_m &= \chi(a) \mod m\\ a_m &= a \mod D_A\,. \end{aligned}$$

Then we have

$$S_a(y_1,y_2;x) = \sum_{\substack{y_1<m\le y_2\\(m,D_A)=1}} \Lambda(m)\pi(x;mD_A,a_m)\,.$$

6.1.2. *Prime powers.* Let us first see that the contribution of proper prime powers $m = q^k$, $k > 1$, to $S_a(y_1, y_2; x)$ is at most $O(x/\log x)$, which will allow us to ignore their contribution: Indeed, this contribution is bounded by

$$\sum_{\substack{q^k<x \\ k>1}} \log q \cdot \pi(x; q^k D_A, a_{q^k}) \leq \left(\sum_{\substack{q^k<x^{3/4} \\ k>1}} + \sum_{\substack{x^{3/4}\leq q^k<x \\ k>1}} \right) \log q \cdot \pi(x; q^k D_A, a_{q^k}) .$$

By Brun-Titchmarsh (A.1), if $q^k < x^{3/4}$ then $\pi(x; q^k D_A, a_{q^k}) \ll x/(q^k \log x)$, so that the sum over $q^k < x^{3/4}$ is bounded by

$$\sum_{q^k<x^{3/4}} \log q \frac{x}{q^k \log x} \ll \frac{x}{\log x}$$

since

$$\sum_{q \text{ prime}} \sum_{k>1} \frac{\log q}{q^k} < \infty .$$

As for the sum over $x^{3/4} < q^k < x$, we use the trivial bound

$$\pi(x; q^k D_A, a_{q^k}) \ll \frac{x}{q^k D_A} < x^{1/4}$$

(which comes from counting *integers* in an arithmetic progression) plus the fact that the number of prime powers $q^k < x$ is $O(\log x/\log q)$. Since the primes contributing are no larger than $x^{1/2}$, we bound this sum by

$$\sum_{q<x^{1/2}} \log q \frac{\log x}{\log q} x^{1/4} \ll x^{3/4}$$

which is negligible.

6.1.3. *A reduction.* We reduce the study of $P_\eta(x; D_A, a)$ to that of $S_a(x^\eta, x; x)$:

$$\begin{aligned} P_\eta(x; D_A, a) &= \sum_{\substack{x^\eta<q\leq x \\ q\nmid D_A \text{ prime}}} \pi(x; D_A, a_q) \\ &\geq \frac{1}{\log x} \sum_{\substack{x^\eta<q\leq x \\ q\nmid D_A \text{ prime}}} \log q \cdot \pi(x; D_A, a_q) \\ &= \frac{1}{\log x} S_a(x^\eta, x; x) + O(\frac{x}{\log^2 x}) \end{aligned}$$

since the prime powers are negligible. (Also note that $q > x^{1/2}$ so that each p is counted exactly once in the first sum.) Thus in order to prove (6.2), we need to show that for $\eta < 3/5$,

$$S_a(x^\eta, x; x) \gtrsim \frac{3-5\eta}{2(1-\eta)} \frac{x}{\phi(D_A)}\,. \tag{6.3}$$

6.1.4. *A division.* We write

$$S_a(x) = S_a(1, \frac{x^{1/2}}{\log^c x}; x) + S_a(\frac{x^{1/2}}{\log^c x}, x^\eta; x) + S_a(x^\eta, x; x)$$

with $c > 1$ to be determined later. We will show

$$S_a(x) \sim \frac{x}{\phi(D_A)} \tag{6.4}$$

$$S_a(1, \frac{x^{1/2}}{\log^c x}; x) \sim \frac{1}{2}\frac{x}{\phi(D_A)} \tag{6.5}$$

$$S_a(\frac{x^{1/2}}{\log^c x}, x^\eta; x) \lesssim \frac{2\eta-1}{1-\eta}\frac{x}{\phi(D_A)} \tag{6.6}$$

which will give (6.3) and hence our proposition.

6.1.5. To show $S_a(x) \sim x/\phi(D_A)$, we first write $S_a(x)$ as

$$\sum_{\substack{m\le x\\(m,D_A)=1}} \Lambda(m) \sum_{\substack{p\le x\\ p=a \bmod D_A\\ m|p-\chi(a)}} 1 = \left(\sum_{m\le x} - \sum_{\substack{m\le x\\(m,D_A)\ne 1}}\right) \Lambda(m) \sum_{\substack{p\le x\\ p=a \bmod D_A\\ m|p-\chi(a)}} 1$$

To evaluate the sum over all $m \le x$, we switch the order of summation and use the identity $\sum_{d|n}\Lambda(d) = \log n$ to get

$$\begin{aligned}\sum_{m\le x}\Lambda(m) \sum_{\substack{p\le x\\ p=a \bmod D_A\\ m|p-\chi(a)}} 1 &= \sum_{\substack{p\le x\\ p=a \bmod D_A}} \sum_{m|p-\chi(a)} \Lambda(m)\\ &= \sum_{\substack{p\le x\\ p=a \bmod D_A}} \log(p-\chi(a)) \sim \frac{x}{\phi(D_A)}\,.\end{aligned}$$

To estimate the sum over prime powers $m \le x$, with $\gcd(m, D_A) \ne 1$, note that since the sum is only over the powers of the primes q dividing D_A, it suffices to treat each such prime separately. We will show that each contributes at most $O_q(x/\log x)$ and thus prove (6.4).

Indeed, the contribution of such a prime is

$$\log q \sum_{\substack{k\geq 1\\ q^k\leq x}} \sum_{\substack{p\leq x\\ p=a \bmod D_A\\ q^k|p-\chi(a)}} 1 \leq \log q \sum_{q^k\leq x} \sum_{\substack{p\leq x\\ q^k|p-\chi(a)}} 1$$
$$\leq \log q \sum_{q^k\leq x} \pi(x;q^k,\pm 1)\ .$$

The contributing exponents k consist of those ("small" k's) with $q^k \leq x/e$ and at most two "large" values of k for which $x/e < q^k \leq x$. The contribution of the "large" exponents can be shown to be at most $O(1)$ by noting that $\pi(x;q^k,\pm 1)$ is at most the number of *integers* $n \leq x$ congruent to ± 1 modulo q^k, which is at most $x/q^k + 1 = O(1)$.

For the "small" exponents ($k \geq 1$ such that $q^k \leq x/e$), we use the Brun-Titchmarsh theorem (A.1) to bound

$$\pi(x;q^k,\pm 1) < \frac{2}{1-q^{-1}}\frac{x/q^k}{\log x/q^k}$$

and so the sum over all $k \geq 1$ with $q^k \leq x/e$ is at most

$$\log q\frac{2}{1-q^{-1}}\sum_{q^k\leq x/e}\frac{x/q^k}{\log x/q^k}\ .$$

In the range $q \leq q^k \leq x/e$, the function $k \mapsto \frac{x/q^k}{\log x/q^k}$ is decreasing and so the sum over $1 \leq k \leq \log(x/e)/\log q$ is bounded by the integral

$$\int_0^{\log(x/e)/\log q}\frac{x/q^k}{\log(x/q^k)}dk = \frac{1}{\log q}\int_e^x \frac{dt}{\log t} \ll \frac{1}{\log q}\frac{x}{\log x}$$

Thus the total contribution of these "small" k's is at most $c_q x/\log x$. Summing over all prime divisors q of D_A gives (6.4).

6.1.6. To evaluate $S_a(1, \frac{x^{1/2}}{\log^c x}; x)$, we replace $\pi(x; mD_A, a_m)$ by $\mathrm{Li}(x)/\phi(mD_A)$ and use the Bombieri-Vinogradov theorem to bound the error by

$$\sum_{m<x^{1/2}/\log^c x}\log m \max_{(b,m)=1}\left|\pi(x;mD_A,b)-\frac{\mathrm{Li}(x)}{\phi(mD_A)}\right| \ll \log x\frac{x}{\log^2 x} \ll \frac{x}{\log x}$$

(c was chosen to give the exponent 2 on the RHS of (A.2)). The main term is evaluated by (note that $\phi(mD_A) = \phi(m)\phi(D_A)$ if m and D_A

are coprime)

$$
\begin{aligned}
\sum_{\substack{m<x^{1/2}/\log^c x\\(m,D_A)=1}} \frac{\Lambda(m)}{\phi(mD_A)}\operatorname{Li}(x) &= \frac{\operatorname{Li}(x)}{\phi(D_A)} \sum_{\substack{m<x^{1/2}/\log^c x\\(m,D_A)=1}} \frac{\Lambda(m)}{\phi(m)}\\
&= \frac{\operatorname{Li}(x)}{\phi(D_A)}\left(\sum_{m<x^{1/2}/\log^c x}\frac{\Lambda(m)}{\phi(m)}+O(1)\right)\\
&\sim \frac{\operatorname{Li}(x)}{\phi(D_A)}\log\frac{x^{1/2}}{\log^c x}\\
&\sim \frac{1}{2}\frac{x}{\phi(D_A)}
\end{aligned}
$$

as required to prove (6.5).

6.1.7. Finally we estimate $S_a(x^{1/2}/\log^c x, x^\eta; x)$, We will use the Brun-Titchmarsh inequality (A.1) which for $m < x^\eta$, $\eta < 3/5$ gives

$$
\pi(x; mD_A, a_m) < \frac{2}{1-\eta}\frac{x}{\phi(D_A m)\log x}\,. \tag{6.7}
$$

We now find using (6.7) that

$$
\begin{aligned}
S_a(\frac{x^{1/2}}{\log^c x}, x^\eta; x) &< \frac{2}{1-\eta}\frac{x}{\log x}\sum_{\substack{x^{1/2}/\log^c x<m\le x^\eta\\(m,D_A)=1}}\frac{\Lambda(m)}{\phi(mD_A)}\\
&= \frac{1}{\phi(D_A)}\frac{2}{1-\eta}\frac{x}{\log x}\left(\log x^\eta-\log\frac{x^{1/2}}{\log^c x}+O(1)\right)\\
&\sim \frac{2(\eta-1/2)}{1-\eta}\frac{x}{\phi(D_A)}
\end{aligned}
$$

which gives the required estimate (6.6).

7. Large order for almost all integers

In this section we will show that for a density one subsequence of the positive integers, the order of A is large enough to give give uniform distribution of all eigenfunctions of $U_N(A)$. We will show:

Theorem 17. *There exist $\delta > 0$ and a density one subset S of the integers such that for all $N \in S$ we have*

$$\operatorname{ord}(A, N) \gg N^{1/2} \exp((\log N)^{\delta}).$$

Fix $1/2 < \eta < 3/5$. We say that a prime p is *good* if $p \nmid D_A$ and $\operatorname{ord}(A,p) \geq p^{\eta}$. Let P_G be the set of good primes, and let $P_G(x)$ be the set of primes in P_G that does not exceed x. As shown in Theorem 14, there exists $\gamma = \gamma(\eta) > 0$ such that

$$P_G(x) \gtrsim \gamma \pi(x).$$

If $p \mid D_A$ or $\operatorname{ord}(A,p) < p^{\eta}$ we call p *bad*, and if $p \mid D_A$ or $\operatorname{ord}(A,p) < p^{1/2}/\log p$ we call p *terrible*. As for good primes we let P_B and P_T denote the set of bad, respectively terrible, primes (note that $P_T \subset P_B$), and by $P_B(x)$ resp. $P_T(x)$ the number of primes less than x in these sets. Since P_B is the complement of P_G which has lower density γ, we have

$$P_B(x) \lesssim (1-\gamma)\pi(x) \tag{7.1}$$

As for the size of P_T, it is immediate from Lemma 15 that

$$P_T(x) = O(\frac{x}{\log^2 x}). \tag{7.2}$$

Given an integer N we write $N = N_G N_B$ where

$$N_G = \prod_{\substack{p_i^{a_i} || N \\ p_i \in P_G}} p_i^{a_i}, \quad N_B = \prod_{\substack{p_i^{a_i} || N \\ p_i \in P_B}} p_i^{a_i}.$$

We also let $N_T \mid N_B$ be given by $N_T = \prod_{\substack{p_i^{a_i} || N \\ p_i \in P_T}} p_i^{a_i}$.

Define a set of integers $\mathbf{N}_G$ by $n \in \mathbf{N}_G$ if and only if all prime divisors of n are good, and similarly for $\mathbf{N}_B$ and $\mathbf{N}_T$. As for primes we let $\mathbf{N}_G(x)$ (respectively $\mathbf{N}_B(x)$ and $\mathbf{N}_T(x)$) be the elements of $\mathbf{N}_G$ (respectively $\mathbf{N}_B$ and $\mathbf{N}_T$) not exceeding x.

Proposition 18. *The number $N_B(x)$ of integers $N \leq x$ having all their prime factors in P_B satisfies*

$$\mathbf{N}_B(x) \ll \frac{x}{(\log x)^{\gamma}}.$$

Proof. Let $b_p = 1$ if $p \in P_B$ and let $b_p = 0$ if $p \in P_G$, and for composite integers d put $b_d = \prod_{p|d} b_p$. Then $\mathbf{N}_B(x) = \sum_{n\le x} b_n$. Since $P_B(x) \le (1-\gamma)\pi(x)$ the sieve of Eratosthenes gives that $\mathbf{N}_B(x) = o(x)$. Indeed,

$$N_B(x) = \#\{n \le x : p \in P_G \Rightarrow p \nmid n\} = x \prod_{p \in P_G(z)} (1 - 1/p) + O(\exp(z)) .$$

Putting $z = \log\log x$ and noting that $\lim_{z\to\infty} \prod_{p\in P_G(z)}(1 - 1/p) = 0$ since $\sum_{p\in P_G} 1/p = \infty$ we obtain $N_B(x) = o(x)$.

Now following Wirsing [19], we consider the smoothed sum $\int_1^x \mathbf{N}_B(t)\frac{dt}{t}$. By partial summation we have

$$\int_1^x \mathbf{N}_B(t)\frac{dt}{t} = \mathbf{N}_B(x)\log x - \sum_{n\le x} b_n \log n . \tag{7.3}$$

Using the identity $\log n = \sum_{d|n} \Lambda(d)$ we obtain:

$$\begin{aligned} \sum_{n\le x} b_n \log n &= \sum_{n\le x} b_n \left(\sum_{d|n} \Lambda(d)\right) = \sum_{d\le x} b_d\Lambda(d) \sum_{n\le x/d} b_n \\ &= \sum_{n\le x} b_n \sum_{d\le x/n} b_d\Lambda(d) . \end{aligned} \tag{7.4}$$

Now,

$$\sum_{d\le x/n} b_d\Lambda(d) = \sum_{p\in P_B(x/n)} \log p + O((\frac{x}{n})^{1/2}\log(x/n)) \ll \frac{x}{n}$$

by Chebyshev's bound on $\pi(x)$. Moreover, $\mathbf{N}_B(t) = o(t)$ implies that $\int_1^x \frac{\mathbf{N}_B(t)}{t}dt = o(x)$. Hence

$$\mathbf{N}_B(x)\log x + o(x) \ll \sum_{n\le x} b_n\frac{x}{n}. \tag{7.5}$$

However,

$$\begin{aligned} \sum_{n\le x} \frac{b_n}{n} &\le \prod_{p\in P_B(x)} (1 + 1/p + 1/p^2 + \dots) = \exp(\sum_{p\in P_B(x)} (1/p + O(1/p^2))) \\ &\ll \exp\left((1-\gamma)\log\log x\right) = (\log x)^{1-\gamma} \end{aligned}$$

and thus

$$\mathbf{N}_B(x) \ll \frac{x}{\log x}(\log x)^{1-\gamma} + o(\frac{x}{\log x}) \ll \frac{x}{(\log x)^{\gamma}} . \tag{7.6}$$

□

Corollary 19. *We have*

$$\#\{N \le x : N_G \le \exp((\log x)^{\gamma/2})\} \ll \frac{x}{(\log x)^{\gamma/2}} \tag{7.7}$$

Proof. We may write $\#\{N \le x : N_G \le z\}$ as

$$\sum_{N_G \le z} N_B(\frac{x}{N_G}),$$

and by Proposition 18 we may bound this sum by

$$\sum_{N_G \le z} \frac{x}{N_G(\log \frac{x}{N_G})^\gamma} \ll \frac{x}{(\log \frac{x}{z})^\gamma} \sum_{N_G \le z} \frac{1}{N_G} \ll \frac{x}{(\log \frac{x}{z})^\gamma} \log z\,.$$

Putting $z = \exp((\log x)^{\gamma/2})$ we obtain the desired conclusion. □

We will also need to estimate the number of integers N with N_T large:

Lemma 20. *Let* $\beta(z) = \sum_{\substack{N \in \mathbf{N}_T \\ N \ge z}} 1/N$. *Then:*

i) The number of integers $N \le x$ *for which* $N_T \ge z$ *is at most* $x\beta(z)$.
ii) $\lim_{z\to\infty} \beta(z) = 0$.

Proof. i) We have

$$\#\{N \le x : N_T \ge z\} \le \sum_{N_T \ge z} \frac{x}{N_T} = x\beta(z).$$

ii) By (7.2),

$$\sum_{p \in P_T} 1/p < \infty$$

and hence

$$\sum_{N \in \mathbf{N}_T} 1/N = \prod_{p \in P_T} (1 + 1/p + 1/p^2 + \dots) < \infty.$$

□

Proof of Theorem 17. As in section 5, write $N = ds^2$ where d is square free, $d = d_0 \gcd(d, D_A)$, $D_A = 4(\mathrm{tr}(A)^2 - 4)$. By Proposition 11, for almost all $N \le x$ we have

$$\mathrm{ord}(A, N) \ge \frac{\prod_{p|d_0} \mathrm{ord}(A, p)}{\exp(3(\log\log x)^4)}\,.$$

Fix $1/2 < \eta < 3/5$. Write $d_0 = d_G d_B$ where d_G is "good" and d_B is "bad". By definition, if p is good then $\mathrm{ord}(A, p) > p^\eta$, hence

$$\prod_{p|d_G} \mathrm{ord}(A, p) \ge d_G^\eta.$$

Furthermore,

$$\prod_{p\mid \frac{d_B}{d_T}} \operatorname{ord}(A,p) \geq \prod_{p\mid \frac{d_B}{d_T}} \frac{p^{1/2}}{\log p} \geq \left(\frac{d_B}{d_T}\right)^{1/2} \frac{1}{(\log d_B)^{\omega(d_B)}}.$$

But trivially $\operatorname{ord}(A,p) \geq 1$ for $p \in P_T$, hence

$$\begin{aligned}\prod_{p\mid d_0} \operatorname{ord}(A,p) &\geq d_G^{\eta} \left(\frac{d_B}{d_T}\right)^{1/2} \times \frac{1}{(\log d_B)^{\omega(d_B)}} \\ &= \frac{d_G^{\eta-1/2} d^{1/2}}{d_T^{1/2} (\log d_B)^{\omega(d_B)}} \\ &= \frac{d_G^{\eta-1/2} N^{1/2}}{(d_T s^2)^{1/2} (\log d_B)^{\omega(d_B)}}\,.\end{aligned}$$

Now consider $N \leq x$. By the previous results we may, without affecting the density (i.e. for all but $o(x)$), assume that the following holds:

(7.8) $\qquad d_T \leq \log x \qquad$ (Lemma 20)

(7.9) $\qquad s \leq \log x \qquad$ (Lemma 21)

(7.10) $\qquad \omega(d_B) \leq \omega(N) \leq 2 \log\log x \qquad$ (Lemma 22)

(7.11) $\qquad d_G \geq \exp((\log x)^{\gamma/2}) \qquad$ (Corollary 19)

We also use $\log d_B \leq \log N \leq \log x$. Hence

$$\prod_{p\mid d_0} \operatorname{ord}(A,p) \geq \frac{N^{1/2} \exp\left((\eta - 1/2)(\log x)^{\gamma/2}\right)}{(\log x)^{3/2 + 3/2 \log\log x}}\,.$$

Hence by Proposition 11,

$$\begin{aligned}\operatorname{ord}(A,N) \geq& \frac{\prod_{p\mid d_0} \operatorname{ord}(A,p)}{\exp(3(\log\log x)^4)} \\ \geq& \frac{N^{1/2} \exp\left((\eta - 1/2)(\log x)^{\gamma/2}\right)}{\exp\left(3(\log\log x)^4 + (3/2 + 3/2 \log\log x)\log\log x\right)} \\ \gg& N^{1/2} \exp((\log N)^{\gamma/3})\,.\end{aligned}$$

This concludes the proof of Theorem 17. $\square$

Appendix A. Background from prime number theory

A.1. In this Appendix, we collect some facts which we will need in the rest of the paper. The first asserts that most integers have only small square factors:

Lemma 21. *The number of integers $N \leq x$ which have a square factor $s^2 \mid N$ with $s > \log N$ is $o(x)$.*

Proof. If $N \in [x^{1/2}, x]$ then $\log N \geq 1/2 \log x$, and the number of $N \in [x^{1/2}, x]$ such that $s^2 \mid N$ for some $s > \log N$ is bounded by

$$\sum_{s \geq 1/2 \log x} \frac{x}{s^2} \ll \frac{x}{\log x}.$$

Hence the number of $N \leq x$ for which $s^2 \mid N$ for some $s > \log N$ is $\ll \frac{x}{\log x} + x^{1/2} = o(x)$. □

A.2. We will need to know that most integers have few prime factors: Let $\omega(N)$ be the number of prime factors of N. As a consequence of the Hardy-Ramanujan theorem [10] (see [11], Theorem 431), we have:

Lemma 22. *The set of N such that $\omega(N) \geq 3/2 \log \log N$ has zero density.*

A.3. We recall two important theorems: The first is the Brun-Titchmarsh inequality, which we will use in the following convenient form [16]: For all $1 \leq k < x$, $(a, k) = 1$

$$\pi(x; k, a) < \frac{2x}{\phi(k) \log \frac{x}{k}}. \tag{A.1}$$

One consequence we will need is:

Lemma 23. *Let $q \leq x^{1/2}$. Then*

$$\sum_{\substack{p \leq x \\ p \equiv \pm 1 \mod q}} \frac{1}{p} \ll \frac{\log \log x}{\phi(q)}.$$

The second is the Bombieri-Vinogradov theorem [1] in the form: For every $A > 0$ there is some $B > 0$ so that

$$\sum_{k \leq \frac{x^{1/2}}{(\log x)^B}} \max_{(a,k)=1} \left| \pi(x; k, a) - \frac{\mathrm{Li}(x)}{\phi(k)} \right| \ll \frac{x}{(\log x)^A}. \tag{A.2}$$

REFERENCES

[1] E. Bombieri *On the large sieve*, Mathematatika **12** (1965), 201–225.

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

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

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

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

[6] P. Erdös and R. Murty, *On the order of* $a \pmod p$, Number theory (Ottawa, ON, 1996), 87–97, CRM Proc. Lecture Notes, **19**, Amer. Math. Soc., Providence, RI, 1999.

[7] G. Folland *Harmonic analysis in phase space*, Annals of Mathematics Studies **122**, Princeton University Press, Princeton, NJ, 1989.

[8] M. Goldfeld *On the number of primes p for which $p + a$ has a large prime factor*, Mathematika **16** (1969), 23–27.

[9] J.H. Hannay and M.V. Berry *Quantization of linear maps on a torus - Fresnel diffraction by a periodic grating*, Physica D **1** (1980), 267–291.

[10] G.H. Hardy and Ramanujan, Quarterly Jour. of Math. **48** (1917), 76–92.

[11] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers* (The Clarendon Press, Oxford University Press, New York, 1979).

[12] C. Hooley *on Artin's conjecture*, J. reine angewe. Math. **225** (1967), 209–220.

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

[14] P. Kurlberg and Z. Rudnick *Hecke theory and equidistribution for the quantization of linear maps of the torus*, preprint chao-dyn/9901031, to appear in the Duke Jour. of Math.

[15] J. Marklof and Z. Rudnick *Quantum unique ergodicity for parabolic maps*, preprint math-ph/9901001, to appear in Geom. and Func. Anal.

[16] H.L. Montgomery and R.C. Vaughan *the large sieve*, Mathematika **20** (1973), 119–134.

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

[18] O. Taussky *Introduction into connections between algebraic number theory and integral matrices*, appendix to H. Cohn *A classical invitation to algebraic numbers and class fields*, Springer, New York 1978.

[19] E. Wirsing *Das asymptotische Verhalten von Summen über multiplikative Funktionen*, Math. Ann. **143** (1961), 75–102.

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

[21] S. Zelditch *Quantum ergodicity of C^*-dynamical systems*, Comm. Math.Phys. **177** (1996), 507–528.

[22] S. Zelditch *Index and dynamics of quantized contact transformations*, Ann. Inst. Fourier (Grenoble) **47** (1997), 305-363.

Raymond and Beverly Sackler School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel. Current address: Department of Mathematics, University of Georgia, Athens, GA 30602, U.S.A. (kurlberg@math.uga.edu)

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