ENTROPY OF QUANTUM LIMITS

JEAN BOURGAIN AND ELON LINDENSTRAUSS

1. Introduction

In this paper we report some progress towards a conjecture of Rudnick and Sarnak regarding eigenfunctions of the Laplacian Δ on a compact manifold M for certain special arithmetic surfaces M of constant curvature (see below for definitions):

Conjecture 1.1 (QUE [5]). *If M has negative curvature, then for any sequence of eigenfunctions ϕ_i of the Laplacian, normalized to have L^2-norm 1, such that the eigenvalues λ_i tend to $-\infty$, the probability measures $|\phi_i(x)|^2 d\,vol(x)$ converge in the weak* topology to the Riemannian volume $vol(M)^{-1} d\,vol$.*

(Recall that μ_i converge weak* to μ if for every continuous function with compact support,

$$\int f\,d\,\mu_i \longrightarrow \int f\,d\,\mu$$

as $i \to \infty$.) A similar conjecture can be stated also in the finite volume case [6].

Of particular number theoretic interest are manifolds of the form $\Gamma\backslash\mathbb{H}$ with Γ a congruence arithmetic lattice, in which case it is natural to assume that the eigenfunctions are Hecke-Maas forms, i.e. also eigenfunctions of all Hecke operators. We shall refer to this special case of Conjecture 1.1 as the Arithmetic Quantum Unique Ergodicity Conjecture. While most of our methods are quite general, the number theoretic argument used to prove Theorem 3.4 is specific to lattices coming from quaternion algebras over the rationals or to congruence sublattices of $\mathrm{SL}_2(\mathbb{Z})$. We plan to address the general case using a different technique in a future paper.

It is well known (see [2], [7], [11]) that any weak* limit as in the above conjecture of $|\phi_i(x)|^2 d\,vol(x)$ is a projection of a measure on $\Gamma\backslash\,\mathrm{SL}(2,\mathbb{R})$ invariant under the geodesic flow; our main result is that if we assume that ϕ_i are all Hecke-Maas forms, then all ergodic components of this

Date: August 7, 2002.

measure on $\Gamma\backslash \mathrm{SL}(2,\mathbb{R})$ have strictly positive entropy with an explicit lower bound, namely $\kappa' = 2/9$ (where the speed of the geodesic flow is normalized so that the entropy of the Haar-Lesbegue measure is 2). This in particular implies that the support of such a measure on X has Hausdorff dimension at least $1+\kappa'$.

The first result of this type was proved by Rudnick and Sarnak [5]. They proved that this limiting measure (or even its singular part if any) cannot be supported on a finite union of closed geodesics. Wolpert [10] gave explicit bounds (though substantially weaker than ours) on the modulus of continuity of the limiting measure for $\Gamma = \mathrm{SL}(2,\mathbb{Z})$; however he used the substantial additional assumption that the support of the singular part (if any) of the measure is compact. In [4], the second named author extended Rudnick and Sarnak's result to more general groups and lattices, as well as strengthening it by showing that the measure of any closed geodesic is zero.

While in general dimension is not preserved under projections, it can be shown that for the projection

$$\pi : \Gamma\backslash \mathrm{SL}_2(\mathbb{R}) \to \Gamma\backslash\mathbb{H}$$

dimension *is* preserved in the following sense: if μ is invariant under the geodesic flow on $\Gamma\backslash \mathrm{SL}_2(\mathbb{R})$ with the entropy of all ergodic components $\geq \eta$ then the dimension of $\pi\mu$ is at least $1+\eta$ if $\eta \leq 1$; if $\eta > 1$ then $\pi\mu$ is regular with respect to the natural measure on $\Gamma\backslash\mathbb{H}$ (see bellow for a more precise statement). This result is proved in Lindenstrauss and Ledrappier [3]. Thus our results on the dimension of the limiting measure on $\Gamma\backslash \mathrm{SL}(2,\mathbb{R})$ immediately give bounds on the dimension of any weak* limit of $|\phi_i(x)|^2 d\,vol(x)$.

Finally, we remark that it follows from an identity of T. Watson [9] that the Grand Riemann Hypothesis implies the Arithmetic Quantum Unique Ergodicity Conjecture, that is that any weak* limit as above is indeed the natural volume measure. In fact, the GRH gives a best possible rate of convergence of these measures.

2. Statement of main results

In this paper we deal with uniform lattices that arise from quaternion algebras over $\mathbb{Q}$. Thus, the following notations will be used throughout this paper:

- H a quaternion division algebra over $\mathbb{Q}$, split over $\mathbb{R}$.
- R an order in H
- Γ a lattice in $\mathrm{SL}_2(\mathbb{R})$ corresponding to the norm one elements of R (see below).

We recall that an order R is a subring of H that spans H over $\mathbb{Q}$ satisfying that for every $a \in R$ both the norm $n(a)$ and the trace $tr(a)$ are integral. Our techniques are also equally applicable to congruence sublattices of $\mathrm{SL}(2,\mathbb{Z})$, though the nonuniformity of the lattice requires some minor modifications which we present in §4..

We fix once and for all an isomorphism $\Psi\colon H(\mathbb{R}) \cong M_2(\mathbb{R})$. For $\alpha \in R$ of positive norm $n(\alpha)$, we let $\underline{\alpha} \in \mathrm{SL}(2,\mathbb{R})$ denote the matrix

$$\underline{\alpha} = n(\alpha)^{-1/2}\Psi(\alpha).$$

We let Γ be the image under Ψ of the norm one elements in R; as is well known this Γ is a uniform lattice in $\mathrm{SL}(2,\mathbb{R})$. While we do not require R to be a maximal order, we will require that $\pm 1 \in R$. Set $M = \Gamma\backslash \mathrm{SL}(2,\mathbb{R})/\mathrm{SO}(2,\mathbb{R})$ and $X = \Gamma\backslash \mathrm{SL}(2,\mathbb{R})$ which is a 2-to-1 cover of the unit tangent bundle of M.

We shall say an element $\alpha \in R$ is primitive if it cannot be written as $m\alpha'$ with $m \in \mathbb{N}\backslash\{1\}$. Let $R(m)$ be the set of all primitive $\alpha \in R$ with $n(\alpha) = m$, and define the Hecke operator $T_m\colon C^\infty(X) \to C^\infty(X)$ by

$$T_m : f(x) \mapsto \sum_{\alpha\in R(1)\backslash R(m)} f(\underline{\alpha}x).$$

Similarly, we define the Hecke points $T_m(x)$ of a $x \in X$ by

$$T_m(x) = \{\underline{\alpha}x\colon \alpha \in R(1)\backslash R(m)\}.$$

For all but finitely many primes, $T_{p^k}(x)$ (for all $k \geq 1$) consists of $(p+1)p^{k-1}$ distinct points. We will assume implicitly throughout this paper that all primes considered are outside this finite set. Similarly one can define Hecke operators for $\mathrm{SL}_2(\mathbb{Z})$ (and after dropping finitely many primes also for congruence sublattices). In this case we take $R' = M_2(\mathbb{Z}) \cap \mathrm{GL}(2,\mathbb{R})$, and taking $R'(m)$ to be all primitive integral matrices of determinant m, primitive being defined exactly as in the previous case. This again can be used to define Hecke operators as above with precisely the same properties.

Let $\Lambda < \mathrm{SL}(2,\mathbb{R})$ be a lattice. We will denote by $\mathcal{QL}(\Lambda)$ the collection of all measures on $\Lambda\backslash \mathrm{SL}(2,\mathbb{R})$ that can be obtained as limiting measures of micro local lifts of L^2-normalized eigenfunctions of both the Laplacian and all Hecke operators on $\Lambda\backslash\mathbb{H}$. All measures in $\mathcal{QL}(\Lambda)$ are invariant under the geodesic flow; if Λ is uniform, then they are also clearly probability measures. It is a delicate and probably difficult issue to show that in the nonuniform case all measures in $\mathcal{QL}(\Lambda)$ are probability measures (this is however a consequence of the GRH).

We will need to use the following one parameter subgroups of $\mathrm{SL}(2,\mathbb{R})$:

$$u^+(x) = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}$$

$$u^-(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

$$a(t) = \begin{pmatrix} e^t & 0 \\ 0 & e^{-t} \end{pmatrix}$$

Set, for any $\varepsilon, \tau > 0$

$$B(\varepsilon, \tau) = a((-\tau, \tau))u^-((-\varepsilon, \varepsilon))u^+((-\varepsilon, \varepsilon))$$

and

$$B(\varepsilon) = B(\varepsilon, \varepsilon)$$

all of these sets are open neighborhoods of the identity in $\mathrm{SL}(2,\mathbb{R})$. Throughout this note, we let τ_0 be a small fixed number, satisfying

$$e^{10\tau_0} + e^{-10\tau_0} < 2.5 \tag{2.1}$$

say $\tau_0 = 1/50$.

Theorem 2.1. *Let $\Lambda = \Gamma$ or a congruence sublattice of $\mathrm{SL}(2,\mathbb{Z})$. For any $\mu \in \mathcal{QL}(\Lambda)$ and any compact subset of $\Lambda\backslash \mathrm{SL}(2,\mathbb{R})$, we have that for any x in this compact subset*

$$\mu(xB(\varepsilon, \tau_0)) \ll \varepsilon^{\kappa'}$$

for $\kappa' = 2/9$.

Corollary 2.2.
1. *Almost every ergodic component of a measure $\mu \in \mathcal{QL}(\Lambda)$ has entropy $\geq \kappa'$.*
2. *The Hausdorff dimension of the support of μ is at least $1 + \kappa'$ (unless Λ is nonuniform and $\mu = 0$).*

We derive this theorem from the following estimate regarding eigenfunctions of Hecke operators on X:

Theorem 2.3. *Let Λ be as above, and $\Phi \in L^2(\Lambda\backslash \mathrm{SL}(2,\mathbb{R}))$ be an eigenfunction of all Hecke operators with L^2-norm 1. Then for any compact subset Ω of $\Lambda\backslash \mathrm{SL}(2,\mathbb{R})$, for any $x \in \Omega$ and $r > 0$,*

$$\int_{xB(\varepsilon,\tau_0)} |\Phi(y)|^2 \, dvol(y) \ll r^{\kappa'}.$$

Proof of Theorem 2.1 assuming Theorem 2.3. Let ϕ_i be a sequence of eigenfunctions of the Laplacian and all Hecke operators on $M = \Lambda\backslash\mathbb{H}$, and let μ be a limiting measure of the micro local lift of the ϕ_i to the unit tangent bundle SM of M which can be identified with $X = \Lambda\backslash\operatorname{SL}(2,\mathbb{R})$. We recall the following important properties of the micro local lift (see [4] for details):

(1) $|\phi_i|^2 dvol$ converge weak* to the projection of μ to M.
(2) Let ω be the Casimir operator. Considering $L^2(M)$ as a subset of $L^2(X)$ one can find a sequence of Casimir eigenfunctions Φ_i which are also eigenfunctions of all Hecke operators on $L^2(X)$ with $\|\Phi_i\|_2 = 1$ such that:
   (a) ϕ_i and Φ_i have the same ω-eigenvalue.
   (b) μ is the weak* limit of $|\Phi_i|^2 dvol_X$.
   (c) μ is invariant under the geodesic flow (under the identification $SM \cong X$ this is the flow that arises from the action $\Lambda g \mapsto \Lambda g a(t)$).

By Theorem 2.3 for all $x \in \Omega$ and i,

$$\int_{xB(\varepsilon,\tau_0)} |\Phi_i(y)|^2 dvol_X(y) \ll \varepsilon^{\kappa'}.$$

Since μ is the weak* limit of $|\Phi_i|^2 dvol_X$,

$$\mu\left(xB(\varepsilon,\tau_0)\right) \leqslant \underline{\lim} \int_{xB(\varepsilon,\tau_0)} |\Phi_i(y)|^2 \, dvol_X(y),$$

so

$$\mu\left(xB(\varepsilon,\tau_0)\right) \ll \varepsilon^{\kappa'}.$$

□

Finally, we mention the following corollary of Theorem 2.1 and the results in [3]:

Corollary 2.4. *Let d_M denote the image of the standard hyperbolic metric on $\mathbb{H}$ to M, and $\tilde{\mu}$ a weak* limit of $|\phi_i|^2 dvol_M$ with ϕ_i a sequence of Hecke-Maas forms as above. Then for any $\kappa'' < \kappa'$*

$$\iint_M \frac{d\tilde{\mu}(x) d\tilde{\mu}(y)}{d_M(x,y)^{\kappa''+1}} < \infty$$

We note that if one could improve the constant κ' in Theorem 2.1 to be > 1 then one would have by [3] that $\tilde{\mu}$ is regular with respect to the Riemannian volume with an L^2 Radon Nikodyn derivative. The full Quantum Unique Ergodicity Conjecture in this case is equivalent to $\kappa' = 2$.

3. On the distribution of Hecke points and a proof of Theorem 2.3 for quaternion lattices

Lemma 3.1. *If α, β are two primitive commuting elements of $H(\mathbb{Q})\backslash\mathbb{Q}$ then*

$$\mathbb{Q}(\alpha)=\mathbb{Q}(\beta).$$

Proof. Since α,β commute, $K=\mathbb{Q}(\alpha,\beta)$ is a field embedded in $H(\mathbb{Q})$, and unless $\mathbb{Q}(\alpha)=\mathbb{Q}(\beta)$ we have that $[K:\mathbb{Q}]=4$. Let θ be a generator for K, i.e. $K=\mathbb{Q}(\theta)$. Then since $\theta\in H(\mathbb{Q})$ it has to satisfy the degree two polynomial with rational coefficients $\theta^2-tr(\theta)\theta+n(\theta)=0$ — a contradiction. $\square$

Lemma 3.2. *For any $\tau>0$ and $\varepsilon\in(0,0.1)$ we have that*

$$B(\varepsilon,\tau)B(\varepsilon,\tau)\subset B\left(O_\tau(\varepsilon),2\tau+O_\tau(\varepsilon^2)\right) \tag{3.1}$$

$$B(\varepsilon,\tau)^{-1}\subset B(O_\tau(\varepsilon),\tau+O_\tau(\varepsilon^2))$$

Proof. We prove only (3.1), the proof of the second equation being very similar. Let

$$g_1=a(t_1)u^-(a_1)u^+(b_1)$$
$$g_2=a(t_2)u^-(a_2)u^+(b_2)$$

then

$$\begin{aligned}g_1g_2&=a(t_1)u^-(a_1)u^+(b_1)a(t_2)u^-(a_2)u^+(b_2)\\&=a(t_1+t_2)u^-(e^{-2t_2}a_1)u^+(e^{2t_2}b_1)u^-(a_2)u^+(b_2).\end{aligned}$$

Set $\tilde b_1=e^{2t_2}b_1$, and rewrite $u^+(\tilde b_1)u^-(a_2)$ as

$$u^+(\tilde b_1)u^-(a_2)=\begin{pmatrix}1 & a_2\\ \tilde b_1 & 1+a_2\tilde b_1\end{pmatrix}$$

$$=u^-\left(a_2\left[1+a_2\tilde b_1\right]^{-1}\right)a\left(-\ln\left[1+\tilde b_1a_2\right]\right)u^+\left(\tilde b_1\left[1+a_2\tilde b_1\right]^{-1}\right);$$

thus

$$g_1g_2=a(t_1+t_2+O_\tau(\varepsilon^2))u^-(O_\tau(\varepsilon))u^+(O_\tau(\varepsilon))$$

$\square$

Lemma 3.3. *If $\alpha,\beta\in R$ satisfy, for some $x\in\mathrm{SL}(2,\mathbb{R})$, that*

$$\underline{\beta}x,\underline{\alpha}x\in xB(\varepsilon,\tau_0) \tag{3.2}$$

with $\varepsilon<0.1$,

$$C\varepsilon^2\le[n(\alpha)n(\beta)]^{-1}$$

(C some constant depending only on τ_0) then α and β commute.

Proof. Take t_α, t_β so that

$$\underline{\alpha} x \in xa(t_\alpha)B(\varepsilon, 0)$$

and similarly for β. Consider now

$$\rho = \left[\underline{\alpha}^{-1}, \underline{\beta}\right]_* = \underline{\alpha}\underline{\beta}^{-1}\underline{\alpha}^{-1}\underline{\beta} = \frac{1}{n(\alpha)n(\beta)}\alpha\bar{\beta}\bar{\alpha}\beta.$$

a straightforward calculation using (3.2) and Lemma 3.2 shows that

$$\begin{aligned}
\rho x &= \underline{\alpha}\underline{\beta}^{-1}\underline{\alpha}^{-1}\underline{\beta} x \\
&\in \underline{\alpha}\underline{\beta}^{-1}\underline{\alpha}^{-1} xa(t_\beta)B(\varepsilon, 0) \\
&\subset \underline{\alpha}\underline{\beta}^{-1} xa(t_\beta - t_\alpha)B(C_1\varepsilon, C_1\varepsilon^2) \\
&\subset \cdots \\
&\subset xa(0)B(C_2\varepsilon, C_2\varepsilon^2)
\end{aligned}$$

for some C_2 that can be calculated explicitly using Lemma 3.2. However,

$$tr(\rho) \in \mathbb{Z}[1/n(\alpha)n(\beta)],$$

and for any $z \in xB(C_2\varepsilon, C_2\varepsilon^2)x^{-1}$,

$$|tr(z) - 2| \leq C_3\varepsilon^2$$

as long as

$$C_3\varepsilon^2 \leq [n(\alpha)n(\beta)]^{-1}$$

this implies that

$$tr(\rho) = 2$$

hence, since R contains no unipotent elements, $\rho = 1$. This shows that α and β do indeed commute. □

We defer the proof of the following theorem to the next section

Theorem 3.4. *For any $\varepsilon > 0$, and any sufficiently large D and $N \geq D^{1/4+\varepsilon}$, there exists a set $W \subset \{1, \ldots, N\}$ of size $|W| \geq N^\kappa$ ($\kappa = 4/5$) of square free integers divisible by a bounded number of primes p, all with $\left(\frac{D}{p}\right) = -1$.*

Remark: It is possible to improve on the value of κ (see the remark following Lemma 5.6); the natural limit of the argument given here seems to be $\sqrt{e}/2 - \varepsilon \approx 0.824$.

Theorem 3.5. *For any set of primes $\mathcal{P}$, $x \in \Gamma\backslash \mathrm{SL}(2, \mathbb{R})$ and $\varepsilon > 0$, there is a set W of cube free integers with the following properties:*

1. *Any $n \in W$ has a bounded number of prime factors (uniformly in ε, x, δ).*

(2) *For any* $n \in W$, $p^2|n$ *iff* $p|n$ *and* $p \in \mathcal{P}$.
(3) *The sets in* $\{yB(\varepsilon, \tau_0) : y \in T_n(x), n \in W\}$ *are pairwise disjoint.*
(4) $|W| \gg \varepsilon^{-\kappa'/4}$, *with*

$$\kappa' = \frac{\kappa}{2(1+\kappa)} = 2/9.$$

Remark: Improving κ of Theorem 3.4 to $\kappa = 0.824$ will give $\kappa' \approx 0.225$.

Proof. Let $n_1 \le n_2$ be a pair of integers with smallest n_2 such that there are some $y_1 \neq y_2 \in X$ with

$$y_b \in T_{n_b}(x) \qquad \text{for } b = 1, 2$$

satisfying

$$y_1 B(\varepsilon, \tau_0) \cap y_2 B(\varepsilon, \tau_0) \neq \emptyset.$$

Choose a representative $\alpha_1 \in R(n_1)$ of the coset of $R(1)\backslash R(n_1)$ sending x to y_1. By definition of τ_0 (see (2.1)), there will be a unique $\alpha_2 \in R(n_2)$ such that

$$\underline{\alpha_1} x B(\varepsilon, \tau_0) \cap \underline{\alpha_2} x B(\varepsilon, \tau_0) \neq \emptyset.$$

Now set α to be a primitive element of R so that

$$\bar{\alpha}_1 \alpha_2 \in \mathbb{Z}\alpha.$$

Since $y_1 \neq y_2$ we have that $\alpha \in R(M)$ for some $M > 1$ dividing $n_1 n_2$. By definition of α, we have that

$$x \in \underline{\alpha} x B(4\varepsilon, 3\tau_0).$$

Consider the subring $\mathbb{Q}(\alpha) < H$. Since H is a division ring, $\mathbb{Q}(\alpha)$ is isomorphic to some number field L; let

$$i : L \to \mathbb{Q}(\alpha) < H$$

be this isomorphism. Since α is primitive, $\alpha \notin \mathbb{Q}$; since α satisfies the degree 2 polynomial over $\mathbb{Z}$

$$t^2 - tr(\alpha)t + n(\alpha) = 0$$

L is a quadratic extension of $\mathbb{Q}$, namely

$$L \cong \mathbb{Q}\left(\sqrt{D}\right) \qquad \text{for } D = tr(\alpha)^2 - 4n(\alpha).$$

Notice that since H splits over $\mathbb{R}$, $\alpha \in R$ hence $D \ge 0$. We give the following upper bound for D. By definition,

$$\frac{|tr(\alpha)|}{n(\alpha)^{1/2}} = |tr(\underline{\alpha})| \in \left|tr\left(xB(4\varepsilon, 3\tau_0)x^{-1}\right)\right| \ll 1$$

hence $|tr(\alpha)| \ll n(\alpha)^{1/2}$ and $D \ll n(\alpha) \le n_1 n_2$.

We define a multiplicative function $\zeta_{\mathcal{P}}$ by

$$\zeta_{\mathcal{P}}(1) = 1$$
$$\zeta_{\mathcal{P}}(p) = \begin{cases} p \text{ if } p \text{ prime } \notin \mathcal{P} \\ p^2 \text{ if } p \in \mathcal{P} \end{cases}$$
$$\zeta_{\mathcal{P}}(p^2) = 0$$

If $n_2 \geq \varepsilon^{-2\kappa'}$ we can take

$$W = \{\zeta_{\mathcal{P}}(p) : p \text{ prime } \leqslant n_2\},$$

and we are done. Thus we may assume that $D \ll \varepsilon^{-4\kappa'}$, $n_2 \leq \varepsilon^{-2\kappa'}$. Take

$$N \sim \left(\varepsilon^2 n_1 n_2\right)^{-1/4} \gg \varepsilon^{1/2-\kappa'} \gg D^{\frac{1/2-\kappa'}{4\kappa'}},$$

so in particular $N \gg D^{1/4+}$ (i.e. $N \gg D^{1/4+\varepsilon_0}$ for any ε_0). Apply Theorem 3.4 to find a set $\tilde{W} \subset \{2, \ldots, N\}$ with

$$\left|\tilde{W}\right| \geqslant N^{\kappa} \geq \varepsilon^{\kappa(1/2-\kappa')} = \varepsilon^{\kappa'} \tag{3.3}$$

satisfying the conditions of that theorem. We now take W to be

$$W = \left\{\zeta_{\mathcal{P}}(n) : n \in \tilde{W}\right\}.$$

By Theorem 3.4, any $n \in W$ has a bounded number of prime factors, and by definition of W and $\zeta_{\mathcal{P}}$ we have that $p^2|n$ iff $p|n$ and $p \in \mathcal{P}$. In view of (3.3) we know that the W has the prescribed number of elements. Thus it remains to be verified that the sets of the collection

$$\{yB(\varepsilon, \tau_0) : y \in T_l(x), l \in W\}$$

are all pairwise disjoint.

Assume to the contrary that there are distinct

$$z_b \in T_{l_b}(x) \qquad l_b \in W$$

such that

$$z_1 B(\varepsilon, \tau_0) \cap z_2 B(\varepsilon, \tau_0) \neq \emptyset$$

We find that there is some primitive β with

$$\begin{aligned} 1 \neq n(\beta) &| l_1 l_2 \\ x \in \underline{\beta} x &B(4\varepsilon, 3\tau_0). \end{aligned} \tag{3.4}$$

so in particular, $|n(\beta)| \leq l_1 l_2 \leq N^4$. By Lemma 3.3, since

$$|n(\alpha) n(\beta)|^{-1} \geq [N^4 n_1 n_2]^{-1} \gg \varepsilon^2 \tag{3.5}$$

α and β commute, hence $\beta \in \mathbb{Q}(\alpha) \cong_i L = \mathbb{Q}(\sqrt{D})$.

Since the conjugate $\bar{\beta}$ of β is mapped to the Galois conjugate of the image of β in L, the norm $n(\beta)$ is the same as the norm of the image

$i(\beta)$ of β in L. But by Theorem 3.4 any prime factor p of $n(\beta)$ satisfies $\left(\frac{D}{p}\right) = -1$. Thus any such prime p remains inert in the extension $L : \mathbb{Q}$, and so must divide $n(\beta)$ (indeed must divide the norm of any integral element of L) an even number of times. We conclude that $n(\beta) =: A^2$ is a square and moreover the two ideals (in the ring of integers of L)

$$\langle i(\beta)\rangle_L, \qquad \langle A\rangle_L$$

are equal. Equivalently, we have that $i(\beta)/A$ is a unit of the ring of integers of L. This in turn implies that

$$tr(\underline{\beta}) = tr_L(i(\beta)/A) \in \mathbb{Z}$$

combining (3.4) with (2.1), and assuming, as we may, that ε is sufficiently small, we have that

$$|tr(\underline{\beta})| \in \mathbb{Z} \cap [2, 5/2 + O_{\tau_0}(\varepsilon)] = \{2\},$$

or (since $H(\mathbb{Q})$ is a division domain) that $\underline{\beta} = \pm 1$, and β is not primitive — a contradiction. $\square$

Lemma 3.6. *Let $\mathcal{T}$ be a $r+1$ regular tree (or even any $r+1$ regular graph with girth ≥ 2). Let $T_{\mathcal{T}} : \mathbb{C}^{\mathcal{T}} \to \mathbb{C}^{\mathcal{T}}$ be the operator*

$$[T_{\mathcal{T}} f](x) = \sum_{d_{\mathcal{T}}(y,x)=1} f(y)$$

(with $d_{\mathcal{T}}$ denoting the usual metric on the tree).

Assume ϕ is an eigenfunction of $T_{\mathcal{T}}$, with eigenvalue λ. Then

$$|\phi(x)|^2 \ll \begin{cases} \sum_{d(y,x)=1} |\phi(y)|^2 & \text{if } |\lambda| > \frac{\sqrt{r}}{10} \\ \sum_{d(y,x)=2} |\phi(y)|^2 & \text{otherwise.} \end{cases}$$

Proof. Assume $|\lambda| > \frac{\sqrt{r}}{10}$. Then by Cauchy-Schwartz

$$|\phi(x)|^2 = \frac{1}{|\lambda|^2}\left|\sum_{d_{\mathcal{T}}(x,y)=1} \phi(y)\right|^2 \leq \frac{1}{|\lambda|^2}(r+1) \sum_{d_{\mathcal{T}}(x,y)=1} |\phi(y)|^2$$
$$\ll \sum_{d_{\mathcal{T}}(x,y)=1} |\phi(y)|^2.$$

Now assume $|\lambda| < \frac{\sqrt{r}}{10}$. Then for any y with $d_{\mathcal{T}}(x,y) = 1$,

$$\lambda\phi(y) = \sum_{\substack{d(z,y)=1 \\ d(z,x)=2}} \phi(z) + \phi(x)$$

$$\phi(x) = \frac{1}{r+1}\Bigg(\sum_{d(y,x)=1} \lambda\phi(y) - \sum_{d(z,x)=2} \phi(z)\Bigg)$$

$$= \frac{1}{r+1}(\lambda^2\phi(x) - \sum_{d(z,x)=2} \phi(z)).$$

So

$$|\phi(x)|^2 = [(r+1) - \lambda^2]^{-2} \left| \sum_{d(z,x)=2} \phi(z) \right| \leq$$

$$\leq \frac{r(r+1)}{[(r+1)-\lambda^2]^2} \sum_{d(z,x)=2} |\phi(z)|^2 \ll$$

$$\sum_{d(z,x)=2} |\phi(z)|^2.$$

Note that throughout the proof, the implicit constants are absolute and do not depend on λ, r. $\square$

Corollary 3.7. *Let Φ be an eigenfunction of all Hecke operators on X. Let n be a square free integer*

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$$

with $k = O(1)$. Take

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$$

where

$$\alpha_i = \begin{cases} 1 \text{ if } T_{p_i}\Phi = \lambda_{p_i}\Phi \text{ with } |\lambda_{p_i}| > \frac{\sqrt{p_i}}{10} \\ 2 \text{ otherwise.} \end{cases}$$

Then for all $x \in X$

$$|\Phi(x)|^2 \ll \sum_{y \in T_m(x)} |\Phi(y)|^2$$

Proof. We prove the corrolary by induction on k. The case $k = 0$, i.e. $m = n = 1$, states that $|\Phi(x)|^2 \ll |\Phi(x)|^2$, which is of course true. Now if

$$n' = p_1 \ldots p_{k-1}$$

$$m' = p_1^{\alpha_1} \cdots p_{k-1}^{\alpha_{k-1}}$$

then $T_m(x) = T_{p_k^{\alpha_k}} \circ T_{m'}(x)$. Furthermore, since Φ restricted on the Hecke tree associated with p_k is an eigenfunction of the tree Laplacian we may apply Lemma 3.6 to show $\forall y \in X$

$$|\Phi(y)|^2 \ll \sum_{z \in T_{p_k^{\alpha_k}}(y)} |\Phi(z)|^2$$

so

$$\begin{aligned} |\Phi(x)|^2 &\ll \sum_{y \in T_{m'}(x)} |\Phi(y)|^2 \\ &\ll \sum_{z \in T_{p_k^{\alpha_k}}(y)} \sum_{y \in T_{m'}(x)} |\Phi(z)|^2 \\ &\ll \sum_{z \in T_m(x)} |\Phi(z)|^2. \end{aligned}$$

Note that the implicit constant depends only on the bound on k. □

Proof of Theorem 2.3. Let λ_p denote the eigenvalue of Φ with respect to the Hecke operator T_p. Let $\mathcal{P}$ be the sets of all primes for which $|\lambda_p| \le \sqrt{p}/10$. By Theorem 3.5, there is a set W of cube free integers of size $\ge \varepsilon^{-\kappa'}$ such that for any $n \in W$, we have that $p^2|n$ iff $p|n$ and $p \in \mathcal{P}$, and such that

$$yB(\varepsilon, \tau_0) \qquad y \in T_n(x),\ n \in W \tag{3.6}$$

are all pairwise disjoint. Since Φ is a Hecke eigenfunction, by Corollary 3.7, for all $n \in W$ and any $y \in X$,

$$|\Phi(y)|^2 \ll \sum_{z \in T_n(y)} |\Phi(z)|^2$$

(note that the implicit constant in the above equation is universal and does not depend on any parameter) hence for any $n \in W$

$$\begin{aligned} \int_{xB(\varepsilon,\tau_0)} |\Phi(y)|^2 \, dvol_X(y) &\ll \int_{xB(\varepsilon,\tau_0)} \sum_{z \in T_n(y)} |\Phi(z)|^2 \, dvol_X(y) \\ &= \sum_{z \in T_n(x)} \int_{zB(\varepsilon,\tau_0)} |\Phi(y)|^2 dvol_X(y) \end{aligned}$$

Summing over $n \in W$, and using the disjointness property (3.6), we get that

$$\int_{xB(\varepsilon,\tau_0)} |\Phi(y)|^2 \, dvol_X(y) \ll \frac{1}{|W|} \sum_{n\in W} \sum_{z\in T_n(x)} \int_{zB(\varepsilon,\tau_0)} |\Phi(y)|^2 dvol_X(y)$$

$$\leqslant \varepsilon^{\eta} \int_X |\Phi(y)|^2$$

□

4. The case of Λ a congruence sublattice of $\mathrm{SL}(2,\mathbb{Z})$

In this section we present the modifications needed to carry out the proof of Theorem 2.3 to the nonuniform case. For simplicity we will discuss only the case of $\Lambda = \mathrm{SL}(2,\mathbb{Z})$, leaving the straightforward verification for congruence sublattices to the reader. Recall the notations $R' = M_2(\mathbb{Z}) \cap \mathrm{GL}(2,\mathbb{R})$, and $R'(m)$ = all primitive integral matrices of determinant m. As before we set $M = \mathrm{SL}(2,\mathbb{Z})\backslash\mathbb{H}$ and $X = \mathrm{SL}(2,\mathbb{Z})\backslash \mathrm{SL}(2,\mathbb{R})$. In order to conform more closely to the notations of the previous section, we set for $\alpha \in R'$ $\;n(\alpha) = \det(\alpha)$, and $\bar\alpha = n(\alpha)\alpha^{-1} \in R'$.

The starting point of the proof is Lemma 3.3. While the proof of this lemma essentially carries over to $\mathrm{SL}(2,\mathbb{Z})$, the final step, gives only that $tr(\rho) = 2$, which in view of the existence of unipotents in R' does not imply $\rho = 1$. As an alternative we use the following:

Lemma 4.1. *If $\alpha, \beta \in R$ satisfy, for some $x \in \mathrm{SL}(2,\mathbb{R})$, that*

$$\underline{\beta} x, \underline{\alpha} x \in xB(\varepsilon,\tau_0) \tag{4.1}$$

$$C\varepsilon^2 \leq [n(\alpha)n(\beta)]^{-1}$$

(with ε sufficiently small and C some constant depending on τ_0 and on x, uniformly on x in compact subsets of X) then α and β commute.

Proof. Let Ω be a compact subset of $\mathrm{SL}(2,\mathbb{R})$ with $x \in \Omega$. Define as before t_α and t_β so

$$\underline{\alpha} x \in xa(t_\alpha)B(\varepsilon, 0)$$

and similarly for β. Let $B_0(\epsilon_1,\epsilon_2) = \log B(\epsilon_1,\epsilon_2)$, so that $B_0(\epsilon_1,\epsilon_2)$ is a small neighborhood of the zero matrix in $M_2(\mathbb{R})$.

Then

$$\begin{aligned} \underline{\alpha}\underline{\beta} x &\in \quad xa(t_\alpha + t_\beta)B(C\varepsilon, C\varepsilon^2) \\ \underline{\beta}\underline{\alpha} x &\in \quad xa(t_\alpha + t_\beta)B(C\varepsilon, C\varepsilon^2). \end{aligned}$$

So

$$\begin{aligned}[\underline{\alpha}, \underline{\beta}]_+ = \underline{\beta}\underline{\alpha} - \underline{\beta}\underline{\alpha} &\in x^{-1} B_0(C'\varepsilon, C'\varepsilon^2) x \\ &\subset B_0(C''\varepsilon, C''\varepsilon)\end{aligned}$$

C'' some constant depending on Ω, τ_0.

But $[\alpha, \beta]_+ \in M_2(\mathbb{Z})$, so

$$[\underline{\alpha}, \underline{\beta}]_+ \in B_0(C''\varepsilon, C''\varepsilon) \cap \frac{1}{\det(\alpha\beta)^{1/2}} M_2(\mathbb{Z}).$$

Assuming

$$(\det \alpha \det \beta)^{-1} \gg \varepsilon^2$$

for sufficiently large implicit constant depending on Ω we have that indeed

$$[\alpha, \beta]_+ = 0.$$

□

Having proved a suitable substitute to Lemma 3.3, we discuss the modifications needed to prove Theorem 3.5. As usual our result will no longer be uniform in $x \in X$ but only uniform for x in an arbitrary compact subset of X. For the convenience of the reader we restate this theorem, from which Theorem 2.3 is easily derived in the same way as in the previous section.

Theorem 4.2. *For any compact subset $\Omega \subset \mathrm{SL}(2, \mathbb{Z}) \backslash \mathrm{SL}(2, \mathbb{R})$, for any set of primes $\mathcal{P}$, $x \in \Omega$ and $\varepsilon > 0$, there is a set W of cube free integers with the following properties:*

1. *Any $n \in W$ has a bounded number of prime factors (uniformly in ε, Ω, x).*
2. *For any $n \in W$, $p^2 | n$ iff $p | n$ and $p \in \mathcal{P}$.*
3. *The sets in $\{yB(\varepsilon, \tau_0) : y \in T_n(x), n \in W\}$ are pairwise disjoint.*
4. *$|W| \gg \varepsilon^{-\kappa'/4}$, uniformly on Ω, with $\kappa' = 2/9$ as in Theorem 3.5.*

Proof. We proceed exactly as in Theorem 3.5. Let $n_1 \leq n_2$ be a pair of integers with smallest n_2 such that there are some $y_1 \neq y_2 \in X$ with

$$y_b \in T_{n_b}(x) \qquad \text{for } b = 1, 2$$

satisfying

$$y_1 B(\varepsilon, \tau_0) \cap y_2 B(\varepsilon, \tau_0) \neq \emptyset.$$

Choose a representative $\alpha_1 \in R'(n_1)$ sending x to y_1. Take any $\alpha_2 \in R'(n_2)$ such that

$$\underline{\alpha_1} x B(\varepsilon, \tau_0) \cap \underline{\alpha_2} x B(\varepsilon, \tau_0) \neq \emptyset.$$

Now set α to be a primitive element of R' so that

$$\bar{\alpha}_1\alpha_2 \in \mathbb{Z}\alpha.$$

Since $y_1 \neq y_2$ we have that $\alpha \in R'(M)$ for some $M > 1$ dividing n_1n_2. By definition of α, we have that

$$x \in \underline{\alpha} x B(4\varepsilon, 3\tau_0).$$

Without loss of generality, as before, we can assume $n_2 \ll \varepsilon^{-2\kappa'}$, $M \ll \varepsilon^{-4\kappa'} \ll \varepsilon^{-1}$ (with a large implicit constant). In this case $\underline{\alpha}$ is $\mathbb{R}$-semisimple (i.e. α has two distinct real eigenvalues), since any element of $B(4\varepsilon, 3\tau_0)$ which is not $\mathbb{R}$-semisimple must lie in $B(4\varepsilon, C\varepsilon)$ for a suitably large absolute constant C. Since x is in some fixed compact set Ω, we conclude that unless α is $\mathbb{R}$-semisimple

$$\underline{\alpha} \in B(C_\Omega\varepsilon, C_\Omega\varepsilon) \cap M^{-1/2}M_2(\mathbb{Z}) = \{1\}$$

a contradiction. Thus again $\mathbb{Q}(\alpha)$ is isomorphic to some real quadratic number field $L = \mathbb{Q}(\sqrt{D})$, and the rest of the proof carries out without any additional difficulties. □

5. On primes which are quadratic nonresidues mod D

Theorem 5.1. *For any $\varepsilon > 0$ there is a $\alpha > 0$ so that for every large enough integer D which is not a perfect square, and $N \geq D^{1/4+\varepsilon}$ one has that the set P of primes $N^\alpha \leq p \leq N$ with $\left(\frac{D}{p}\right) = -1$ satisfy*

$$\sum_{p\in P} \frac{1}{p} > \frac{1}{2} - \varepsilon$$

We cite the following standard version of Brun's combinatorial sieve:

Theorem 5.2 ([8, Theorem 3, p. 60])**.** *Let A be a finite set of integers and let P be a set of prime numbers. Write*

$$A_d := \#\{a \in A : a \equiv 0 \pmod{d}\},$$

$$P(y) := \prod_{p\in P, p\leq y} p,$$

$$S(A, P, y) := card\{a \in A : (a, P(y)) = 1\}.$$

Assume there exist a non-negative multiplicative function w, some real number X, and positive constants κ, A such that

$$A_d =: Xw(d)/d + R_d \qquad (d|P(y)) \tag{5.1}$$

$$\prod_{\eta\leq p\leq\xi} \left(1 - \frac{w(p)}{p}\right)^{-1} < \left(\frac{\log\xi}{\log\eta}\right)^{\kappa} \left(1 + \frac{A}{\log\eta}\right) \qquad (2 \leq \eta \leq \xi). \tag{5.2}$$

Then we have, uniformly for A, X , y and $u \geq 1$,

$$S(A,P,y) = X \prod_{p\leq y, p\in P} \left(1 - \frac{w(p)}{p}\right) \{1+O(u^{-u/2})\} + O\left(\sum_{d\leq y^u, d|P(y)} |R_d|\right). \tag{5.3}$$

We will also use the following estimate of D. Burgess:

Theorem 5.3 ([1, Theorem 2])**.** *Let k be a cube free positive integer and let χ be a non-principal Dirichlet character belonging to the modulus k. Let*

$$S_H(N) = \sum_{n=N+1}^{N+H} \chi(n).$$

Then for any $\varepsilon > 0$ and $r \in \mathbb{Z}^+$ we have that

$$|S_H(N)| \ll H^{1-1/r} k^{\{(r+1)/4r^2\}+\varepsilon}, \tag{5.4}$$

with the implicit constant depending on ε and r.

Since we may have to apply Theorem 5.3 with a character modulo $8k$, k odd, we note the following immediate corollary:

Corollary 5.4. *Suppose $k = dk'$ with k' cube free and $(d,k') = 1$, and χ a non-principal Dirichlet character modulo k then*

$$|S_H(N)| \ll_{\varepsilon,r,d} H^{1-1/r} k'^{\{(r+1)/4r^2\}+\varepsilon}. \tag{5.5}$$

Proof. Write

$$S_H(N) = \sum_{l=0}^{d-1} S_{H,l}(N) \tag{5.6}$$

with

$$S_{H,l}(N) = \sum_{\substack{N<n\leq N+H \\ n-N\equiv l (\bmod d)}} \chi(n) \tag{5.7}$$

We show that for all l,

$$|S_{H,l}(N)| \ll_{\varepsilon,r,d} H^{1-1/r} k'^{\left\{((r+1)/4r^2\right\}+\varepsilon} \tag{5.8}$$

We now note that

$$\chi'(m) = \chi(md)$$

is a non principal Dirichlet character modulo k', and we may apply Theorem 5.3 on

$$S_{H,l}(N) = \sum_{M+1\leq m\leq M+H/d} \chi(md) = \sum_{M+1\leq m\leq M+H/d} \chi'(m)$$

where M is defined by

$$dM \equiv N + l \pmod{k'}$$

$\square$

Proof of Theorem 5.1. We will prove the theorem in two steps. First we show that there are many integers $n \leq N$ satisfying $\left(\frac{D}{n}\right) = -1$ which have no prime factor less than N^α for a suitably chosen α using Brun's combinatorial sieve. Then we show how this implies that

$$\sum_{p \in P} \frac{1}{p} \text{ is large}$$

for which we again use the combinatorial sieve in a somewhat degenerate case.

Let P be the set of all primes, and

$$A = \left\{ n : \left(\frac{D}{n}\right) = -1 \right\}$$

We now set as in Theorem 5.2

$$S(B, P, y) = card\,\{a \in (a,p) = 1 \;\forall \text{ prime } p \leqslant y\}$$

We now set

$$w(n) = 1 \qquad \text{for all square free } n$$

and $X = N/2$. This choice satisfies (5.2). By quadratic reciprocity, $\left(\frac{D}{n}\right)$ is a non principal character modulo (at most) $8D$, and we may clearly assume D is square free. Burgess' estimate (Corollary 5.4) allows us to bound R_d of (5.1) by

$$|R_d| = \left| \frac{1}{2} \sum_{1 \leq n \leq N/d} \left\{ 1 + \left(\frac{D}{dn}\right) \right\} - \frac{N}{2d} \right| \ll_{\bar{\varepsilon}, r} (N/d)^{1-1/r}\, D^{\left\{(r+1)/4r^2\right\} + \bar{\varepsilon}} \tag{5.9}$$

By Theorem 5.2 we know that

$$S(A, P, y) \geqslant \frac{N}{2} \prod_{p \leqslant y} \left(1 - \frac{1}{p}\right) \left(1 - Cu^{-u/2}\right) + O\left(\sum_{d \leqslant y^u} |R_d| \right) \tag{5.10}$$

with C independent of A, u, y, X. We fix $r, \bar{\varepsilon}$ by requiring that

$$N^{-1/r} D^{\left\{(r+1)/4r^2\right\} + \bar{\varepsilon}} \ll N^{-\varepsilon/10r}$$

and take u so that

$$Cu^{-u} < \frac{\varepsilon}{100}$$

and α

$$\alpha \leqslant \bar{\varepsilon} u^{-1}/10$$

We now estimate the $O(\cdot)$ term in (5.10) for $y = N^\alpha$. By (5.9)

$$\sum_{\substack{d \leqslant y^u \\ d|P(y)}} |R_d| \ll \sum_{d \leqslant y^u} D^{\{(r+1)/4r^2\}+\varepsilon}$$

$$\ll N^{1-\varepsilon/10r} \sum_{d \leqslant y^u} d^{-(1-1/r)}$$

$$\ll N^{1-\varepsilon/10r} y^{u/r}$$

so we see that for D, N large enough

$$S(A, P, N^\alpha) \geq \frac{(1-\varepsilon/10)N}{2} \prod_{p \leq N^\alpha} \left(1 - \frac{1}{p}\right) \tag{5.11}$$

The second part of the proof will use the bound on $S(A, P, y)$ to show that there are many primes $\leq N$ with $\left(\frac{D}{p}\right) = -1$. We remark that any $n \leq N$ contributing to $S(A, P, N^\alpha)$, that is such that $\left(\frac{D}{n}\right) = -1$ and n is not divisible by a prime smaller than N^α, is divisible by some prime p in

$$P_0 = \left\{ \text{primes } N^\alpha \leq p \leq N, \left(\frac{D}{p}\right) = -1 \right\}.$$

A trivial application of the combinatorial sieve for the prime set

$$P_{p',N^\alpha} = \{\text{primes} \leqslant N^\alpha, p'\}$$

with p' some prime in P_0 shows that

$$|\{n \leqslant N \, \text{s.t.}\, p'|n \text{ but } (n,p) = 1 \text{ for all } p \leq N^\alpha\}| \leqslant N \prod_{p<N^\alpha} \left(1 - \frac{1}{p}\right) \frac{1+\varepsilon/10}{p'}$$

summing over all $p' \in P_0$, we have that

$$S(A, P, N^\alpha) \leqslant (1+\varepsilon/10)\, N \prod_{p<N^\alpha} \left(1 - \frac{1}{p}\right) \sum_{p' \in P_0} \frac{1}{p'}$$

Combining this with (5.11) gives

$$\sum_{p' \in P_0} \frac{1}{p'} \geqslant \frac{1-\varepsilon/10}{2\,(1+\varepsilon/10)} \geqslant \tfrac{1}{2} - \varepsilon$$

□

Corollary 5.5 (of Theorem 5.1)**.** *Let D and $N \geq D^{1/4+\varepsilon}$ as in Theorem 5.1. Then there is a subset $W \subset \{1, \ldots, N\}$ of size $\gg N^\kappa$ ($\kappa = 0.8$) so that for any $w \in W$ and $p|w$, we have that $\left(\frac{D}{p}\right) = -1$.*

The argument deducing Corollary 5.5 from Theorem 5.1 can be translated to the following purely combinatorial question:

Lemma 5.6. *For any $S \subset \mathbb{R}^+$ let*

$$m(S) = \int_S \frac{dx}{x}$$

$$\Sigma S = \{s_1 + s_2 + \cdots + s_r : r \geq 1\ \forall i, s_i \in S\}$$

Then if $\varepsilon > 0$ is small enough, for every $S \subset (0,1]$ with $m(S) > 1/2 - \varepsilon$

$$\Sigma S \cap [\kappa, 1] \neq \emptyset$$

for $\kappa = 0.5$.

Remark: a more refined analysis should probably enable improving κ from the above lemma to $\frac{\sqrt{e}}{2}-$, which is easily seen to be optimal by taking S to be the interval $[1/2, \kappa]$

Proof. Assume that

$$\Sigma S \cap [0.8, 1] = \emptyset. \tag{5.12}$$

Since for any $n \in \mathbb{N}$

$$nS \subset \Sigma S$$

we have that

$$S \subset [0,1] - \bigcup_{n \in \mathbb{N}} \left[\frac{4}{5n}, \frac{1}{n}\right] = \left[\frac{1}{2}, \frac{4}{5}\right] \cup \left[\frac{1}{3}, \frac{4}{10}\right] \cup \left[\frac{1}{4}, \frac{4}{15}\right].$$

Suppose first that

$$S \cap \left[\frac{1}{4}, \frac{4}{15}\right] \neq \emptyset \tag{5.13}$$

and let s be any element from this set. Then by (5.12),

$$S \cap [0.8 - s, 1 - s] = \emptyset;$$

notice that for any $s \in [1/4, 4/15]$

$$[4/5 - s, 1 - s] \subset [1/2, 4/5]$$

and

$$m[4/5 - s, 1 - s] = \ln \frac{1 - s}{4/5 - s} \geq 0.31.$$

Thus, if (5.13) holds,

$$m(S) \leq m\left[\frac{1}{2}, \frac{4}{5}\right] + m\left[\frac{1}{3}, \frac{2}{5}\right] + m\left[\frac{1}{4}, \frac{4}{15}\right] - m\left[\frac{4}{5} - s, 1 - s\right] \leq 0.401$$

a contradiction to $m(S) > 1/2-$.

Since $m(S) > 1/2-$, and since (5.13) does not hold, we have that

$$m\left(S \cap \left[\frac{1}{2}, \frac{4}{5}\right]\right) \geqslant m(S) - m\left(\left[\frac{1}{3}, \frac{2}{5}\right]\right) \geqslant 0.5 - \ln\frac{6}{5} - \geqslant 0.317,$$

hence if we define α by

$$m\left(\left[\alpha, \frac{4}{5}\right]\right) = 0.317,$$

i.e. $\alpha = 0.8e^{-0.317} \leq 0.583$ we would have that

$$S \cap \left[\frac{1}{2}, \alpha\right] \neq \emptyset.$$

Take s to be some element in $S \cap \left[\frac{1}{2}, \alpha\right]$. Then on the one hand

$$(s + S) \cap \left[\frac{4}{5}, 1\right] = \emptyset,$$

and on the other hand

$$s + \left[\frac{1}{3}, \frac{2}{5}\right] \subset \left[\frac{4}{5}, 1\right]$$

so $S \subset \left[\frac{1}{2}, \frac{4}{5}\right]$, hence

$$m(S) \leqslant m\left(\left[\frac{1}{2}, \frac{4}{5}\right]\right) = \ln\frac{8}{5} < 0.47 < 0.5-$$

a contradiction. $\square$

Proof of Corollary 5.5. Let P denote the set of primes $\in [N^\alpha, N]$ with $\left(\frac{D}{p}\right) = -1$. We recall that

$$\sum_{p \in P} \frac{1}{p} \geq 1/2 - \varepsilon.$$

Fix $\delta > 0$, $r = 1 + \delta$ very small depending only on ε. Let $\tilde{S}$ denote the integers

$$\tilde{S} = \left\{n : N^\alpha \leq r^n \leq rN,\ \left|P \cap [r^{n-1}, r^n]\right| \geqslant r^{n(1-\delta)}\right\}$$

And divide P into two sets:

$$P_1 = \bigcup_{n \in \tilde{S}} \left(P \cap \left[r^{n-1}, r^n\right]\right)$$

$$P_2 = \bigcup_{n \notin \tilde{S}} \left(P \cap \left[r^{n-1}, r^n\right]\right)$$

clearly,

$$\sum_{p\in P_2}\frac{1}{p}\leqslant\sum_{N^\alpha<r^n<rN}\frac{r^{n(1-\delta)}}{r^n}\ll_r N^{-\delta}$$

so for N large enough

$$\sum_{p\in P_1}\frac{1}{p}\geq 1/2-2\varepsilon.$$

Applying the previous lemma to

$$S=\bigcup_{s\in\tilde{S}}\left(\frac{(s-1)\log r}{\log N},\frac{s\log r}{\log N}\right]$$

we find that there are $s_1,\dots,s_k\in\tilde{S}$ with

$$\kappa\leq\frac{\log r(s_1+\cdots+s_k)}{\log N}\leq 1$$

and we can take

$$W=\big(P\cap[r^{s_1-1},r^{s_1}]\big)\times\cdots\times\big(P\cap[r^{s_k-1},r^{s_k}]\big)$$

$\square$

Acknowledgments: Both authors are very grateful to Peter Sarnak, who has introduced us independently to this question, with whom we had numerous discussions on this problem that have strongly influenced our work. The second named author would also like to thank him for his consistent helpful support and encouragement throughout his two year stay at the Institute for Advanced Study in Princeton.

We are indebt to Enrico Bombieri, Henryk Iwaniec and Kannan Soundararajan for their help regarding the sieve method.

References

[1] D. A. Burgess. On character sums and L-series. II. *Proc. London Math. Soc. (3)*, 13:524–536, 1963.

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

[3] F. Ledrappier and E. Lindenstrauss, On the Projection of Measures Invariant under the Geodesic Flow. preprint.

[4] E. Lindenstrauss. On quantum unique ergodicity for $\Gamma\backslash H\times H$. to appear in IMRN, 2001.

[5] Zeév Rudnick and Peter Sarnak. The behaviour of eigenstates of arithmetic hyperbolic manifolds. *Comm. Math. Phys.*, 161(1):195–213, 1994.

[6] Peter Sarnak. Some problems in number theory, analysis and mathematical physics. In *Mathematics: frontiers and perspectives*, pages 261–269. Amer. Math. Soc., Providence, RI, 200

[7] A. I. Schnirelman, *Ergodic properties of eigenfunctions*, Usp. Math. Nauk. 29 (1974), 181–182.
[8] Gérald Tenenbaum. *Introduction to analytic and probabilistic number theory.* Cambridge University Press, Cambridge, 1995. Translated from the second French edition (1995) by C. B. Thomas.
[9] T. C. Watson. PhD thesis, Princeton, 2001.
[10] Scott A. Wolpert. The modulus of continuity for $\gamma_0(m)\backslash\approx$ semi-classical limits. *Comm. Math. Phys.*, 216(2):313–323, 2001.
[11] S. Zelditch, *Uniform distribution of eigenfunctions on compact hyperbolic surfaces*, Duke Math. J. 55(4) (1987), 919–941.

School of Mathematics, Institute for Advanced Study, Olden Lane, Princeton NJ 08540
E-mail address: bourgain@ias.edu

Department of Mathematics, Stanford University, Stanford, CA 94305
E-mail address: elonl@math.stanford.edu